

SZ/78-10/2018. jkv.

J E G Y Z Ő K Ö N Y V

Készült: 2018. június hó 20. napján
Szirmabesenyő Nagyközség Önkormányzata Képviselő-testületének
ülésén

Jelen vannak: Huszti Gábor polgármester

Béres László alpolgármester

Asztalos Erika, Bodnár Krisztián, dr. Budai István,
Juhászné Molnár Mária, Szakos István képviselők

dr. Szakos Judit jegyző

dr. Rónai István aljegyző

Leskó Mária Gazdálkodási Csoport vezető
Gulyás Edit Judit óvodavezető
Győrfi Lászlóné iskolaigazgató
Fedorné Karmanóczy Zita Segítő Szolgálat és Konyha vezető
Ojtozi Attila műszaki vezető

Hadobás Istvánné bizottsági tag

Huszti Gábor polgármester köszöntötte a megjelenteket. Az aláírt jelenléti ív alapján megállapította, hogy a megválasztott 7 fő képviselő-testületi tagból megjelent 6 fő, így az ülés határozatképes, azt megnyitotta.

Távolmaradását bejelentette dr. Gerges Gábor alpolgármester.

Huszti Gábor polgármester köszöntötte az ülésen megjelent óvodás szülőket és tájékoztatta őket, hogy rendkívüli szülői értekezletre is sor kerül majd a héten a hiteles tájékoztatás érdekében.

A polgármester javaslatára a Képviselő-testület egyhangúlag, 6 fő támogató szavazatával, ellenszavazat és tartózkodás nélkül dr. Szakos Judit jegyzőt bízta meg az ülés jegyzőkönyvének vezetésével.

A polgármester javaslatára a Képviselő-testület egyhangúlag, 6 fő támogató szavazatával, ellenszavazat és tartózkodás nélkül a képviselő-testületi ülés jegyzőkönyvének hitelesítésére Asztalos Erika és Juhászné Molnár Mária képviselőket bízta meg.

dr. Szakos Judit jegyző:

Kérésem a megválasztott hitelesítőkhöz, hogy a következő 15 napban legyenek elérhetők, illetve jelezzék, ha nem.

Ezt követően Huszti Gábor polgármester javaslatot tett az ülés napirendjére módosítva és kiegészítve a meghívó szerinti napirendi pontokat.

A napirendre vonatkozó javaslattal a Képviselő-testület egyhangúlag, 6 fő támogató szavazatával, ellenszavazat és tartózkodás nélkül egyetértett, a napirendre vonatkozóan más javaslat nem volt.

A képviselő-testületi ülés napirendi pontjai:

- 1.) Jelentés a lejárt határidejű határozatok végrehajtásáról és a két ülés közötti időszak eseményeiről
Előadó: Huszti Gábor polgármester
- 2.) Javaslat a Szirmabesenyői Napsugár Óvoda és Bölcsőde alapító okiratának módosítására
Előadó: Huszti Gábor polgármester
Az előterjesztéshez a Humánterületi Bizottság állásfoglalása szükséges.
- 3.) Tájékoztató az iskola oktató-nevelő munkájáról
Előadó: Győrfi Lászlóné iskolaigazgató
Az előterjesztéshez a Humánterületi Bizottság állásfoglalása szükséges.
- 4.) Beszámoló az óvoda-bölcsőde nevelő munkájáról
Előadó: Gulyás Edit Judit intézményvezető
Az előterjesztéshez a Humánterületi Bizottság állásfoglalása szükséges.
- 5.) Tervezet Szirmabesenyő Nagyközség Önkormányzata Képviselő-testületének .../2018. (...) önkormányzati rendelete a közszolgálati tisztviselők napjáról
Előadó: Huszti Gábor polgármester
- 6.) Javaslat a hulladékgazdálkodással kapcsolatos határozatok elfogadására
Előadó: Huszti Gábor polgármester
- 7.) Javaslat Önkormányzati étkeztetési fejlesztések támogatására szóló pályázat benyújtására
Előadó: Huszti Gábor polgármester
Az előterjesztéshez a Pénzügyi Bizottság állásfoglalása szükséges.
- 8.) Javaslat a Szirmabesenyői Polgármesteri Hivatal Informatikai Biztonsági Szabályzatának elfogadására
Előadó: Huszti Gábor polgármester
Az előterjesztéshez a Pénzügyi Bizottság állásfoglalása szükséges.
- 9.) Javaslat a képviselői alap felhasználására
Előadó: Huszti Gábor polgármester
Az előterjesztéshez a Pénzügyi Bizottság állásfoglalása szükséges.

10.) Tervezet az intézményi térítési díj megállapításáról szóló 5/2012.(III.29.) önkormányzati rendelet módosítására

Az előterjesztéshez a Pénzügyi és a Humánterületi Bizottság állásfoglalása szükséges.

11.) Bejelentések, indítványok, javaslatok

Első napirendi pont:

A napirendi pont előadója az előterjesztéshez kiegészítést, módosítás nem fűzött.

A napirendi ponttal kapcsolatban a képviselők részéről kérdés, hozzászólás nem volt, annak megtárgyalását a polgármester lezárta.

A lejárt határidejű határozatok végrehajtásáról és a két ülés közötti időszak eseményeiről szóló jelentést a Képviselő-testület egyhangúlag, 6 fő egyetértésével, ellenvélemény és tartózkodás nélkül elfogadta.

Második napirendi pont:

Huszi Gábor polgármester:

Az előterjesztést a Humánterületi Bizottság előzetesen tárgyalta. Mielőtt rátérnénk a napirendi pont tárgyalására, szóbeli kiegészítést szeretnék tenni ezzel, illetve a kialakult helyzettel kapcsolatban.

Időben május 11-ig kell visszamennünk, akkor lettem szembesítve azzal, hogy az óvodai gyermeklétszám szeptembertől 132 fő körül fog alakulni, ami már azóta is változott. Ehhez néhány nap múlva kapcsolódott az, hogy a bölcsődei létszám pedig 34 fő körül fog alakulni. Még azon a napon leültünk az intézményvezetőkkel – óvodavezetővel, iskolaigazgatóval - jegyző asszonnyal. Próbáltunk megfejtetni a kialakult helyzet okát és próbáltunk a lehetséges megoldásokon gondolkodni. Amiben rögtön léptünk, hogy hétfőn egy rendkívüli szülői értekezletet tartottunk annak a 15 fő szülői társaságnak, akinek a gyermeke úgynevezett évvésztés, visszatartott gyermek lenne. Ezen a szülői értekezleten azt próbáltam kérni a szülőktől, hogy próbáljunk meg közösen valamilyen kooperatív megoldást találni. Egy olyan megoldás kezdett körvonalazódni, hogy indítanánk egy úgynevezett iskola előkészítő csoportot. Ez nem egy iskolás csoport, hanem ugyanúgy egy óvodás csoport lenne. Ezzel a csoporttal bővítenünk kell az óvoda alapító okiratban az óvodai csoport létszámát. Ehhez szükséges az okirat módosítása.

Előzetesen mindenféle konkrétum nélkül ez lett a szülőnek elmondva. A kezdeti sokk után elkezdtek a szülők ötletelni, hol lehetne új csoportot indítani. Extrémebbenél extrémebb helyek hangzottak el, a volt plébánia épülete, a volt rendőrség épülete, melyek vizesek, dohosak, a rendőrség épülete salétromos, raktárként vannak használva. Szóba került a napközi otthon épülete, mellyel kapcsolatban elmondtam, hogy egy olyan kényszer alatt vagyunk, hogy egyszerre több beruházás indul el a településen és még az is elképzelhető volt, hogy az Egészségügyi Központ egy része fog oda költözni a felújítás idejére. Azonban 8 vagy 10 nyári tábort hirdettünk, mindig ez az épület volt a táborozások helyszíne, amely az ÁNTSZ-nek be is lett jelentve. Jött az a lehetőség, hogy vizsgáljuk meg, hogy hol lehet összevonni, szétverni, konténerezni. Az a 15 gyerek, akinek a szülője ott volt összerakták és eljutottak odáig, hogy indítsunk egy iskola előkészítő csoportot, a gyerekek akkor kapnak tényleges fejlesztést, az iskola és az óvoda között sokak szerint lévő szakadék egy kicsit

összebb húzódik, közelebb kerülnek egymáshoz és rendszeren fel tudnak készülni az iskolára. Ezt követően az egyik szülő azt mondta, hogy kérdezzük meg a nagycsoportos szülőket is, mert hátha őket is érdekelné az, hogy a 3 éves gyerekek közül kiemelnék a nagycsoportosokat és ne az legyen, hogy nagyon sok a kicsi, 20 fő feletti, kevés a nagycsoportos gyerek és ilyenkor megoszlik a figyelem és nagyon nehéz 3 féle évfáratú gyerekekre figyelni, a sok kicsi leköti mind a dajka, mind pedig az óvónők figyelmét, erejét. Az óvoda részéről ezzel kapcsolatban elindult egy kérdőíves felmérés. Volt olyan szülő, aki nem olvasta el figyelmesen és úgy döntött és volt olyan aki nem tudott dönteni, mert nem volt kellő információ birtokában. Talán ők döntöttek felelősségteljesebben. Ami még menet közben történt ezt követő héten volt a Kocsis Fogadóban egy szülők által szervezett megbeszélés, amin nem volt ott sem a fenntartó, sem pedig az intézmény képviselője. Így kérdés az, hogy mennyire sikerült első kézből tájékozódni. A hirtelen, meglepetésszerű létszámadat után felvettem azzal az építéssel kapcsolatot, aki az óvoda átalakítást készítette, azzal foglalkoztunk, hogy mit hogyan lehetne összevonni. Az óvoda kapcsán azt kell tudni mind a szülőknek, mind pedig a képviselőknek, hogy a rendezési terv szerint az egy oldalhatáron álló épület, a bővíthetősége ilyen szempontból korlátozott. Nem egyszerű dolog, hogy hozzá toldok x db konténert. Logikusan oldal irányban kellene hozzátoldani, amihez nem fogunk építési engedélyt kapni. Ez történt rögtön azon a héten, amikor szembesültünk a helyzettel. A szülők természetesen rögtön eredményt vártak volna tőlünk. Az óvodával kapcsolatban még tudni kell, hogy van egy jogszabály, ami előírja, hogy milyen helyiségeknek kell rendelkezésre állni, például elkülönítő, személyzeti WC, óvónői öltöző, stb.

A csoportszoba kapcsán 2 m²-t kell biztosítani egy gyermek számára. Ez azt jelenti, hogy egy 25 fő csoportlétszám esetében 50 m², plusz hozzá kell tenni a vizesblokkot, öltöző részt, ez így durván 80 m², ennyi kellene tudnunk bővíteni. Elmondtam a szülőknek akkor, abban a fázisban, hogy jelen pillanatban -mivel ez egy derült égből villámcsapás - nincs a fiókban tervünk arra, hogy mondjuk egy tetőtérbeépítés meg lenne tervezve, le lenne engedélyezve és nem áll rendelkezésünkre az a forrás, ami ennek a kialakításához szükséges lenne.

Ezt követően abba az irányba léptünk, hogy elmentek levelek az ÁNTSZ-nek, óvoda, konyha és az egészségügy ügyében. Az ÁNTSZ rá egy hétre helyszíni szemlét tartott. Az óvodával kapcsolatban azzal a javaslattal álltunk elő, amit a szülők kértek, hogy nyissunk egybe mindent. A szakhatóság ezt a variációt nem tartotta kivitelezhetőnek, ehhez ők nem járulnak hozzá. Az iskolát is végig járták, megnézték, ott is megtették a megállapításait, majd átvittük őket a napközi otthonba, amit a legrosszabb helynek, legrosszabb megoldásnak tartottak. Az iskola kapcsán elmondták, hogy milyen beavatkozásokat szükséges megcsinálni ahhoz, hogy arra engedélyt tudjunk kapni. Elsődlegesen a radiátorokat le kell burkolni, nem lenne feltétel, de mi mondtuk, hogy a folyosót szeretnénk lerekeszteni. Elmondták azt, hogy a vizesblokkba a csapot lentebb kell rakni a gyerekek méretének megfelelően. A lépcsőhöz egy rámpát kellene, hogy építsünk, a nyílászárónál kell a kiesés elleni védelmet megteremtteni, illetve az üvegezett ajtóknál kell biztosítani azt, hogy az üveg ne gyerekmagasságba kezdődjön. Az ÁNTSZ-nek volt olyan javaslata, hogy ne a hátsó udvaron akarjunk elkerített játszóudvar részt kialakítani, hanem inkább az előkertben, mert hogy az védettebb, jobban körül határolható.

A legutolsó információim szerint azt a tájékoztatást kaptam az óvodától, hogy 28 szülő írta alá azt, hogy elképzelhetőnek tart egy összevont nagycsoportos, visszatartott gyerekes csoportot, egyfajta iskolaelőkészítő csoportként. Közben még a Tankerülettel is egyeztetettünk erről, akik közölték, hogy az épület az önkormányzaté, feljűk bejelentési kötelezettségünk van, amennyiben ezt az iskola meg tudja szervezni, akkor a hozzájárulásukat adják.

Puhatolóztunk a konténeres megoldás irányában is, illetve menet közben jöttek olyan újabb információk és cselekmények, hogy most készülünk beadni az óvodára egy pályázatot, melyből egy hatalmas óvodai étkezőt szeretnénk kialakítani és ott tudnánk kialakítani erre alkalmas teret. Amit a T.O.P-ra benyújtottunk pályázatot az nem kapott támogatást, most elkezdjük szeletenként csinálni a dolgot. Olyan információ birtokába is kerültünk, hogy a nyár folyamán lesz pályázat bölcsődei férőhely kapacitás bővítésére, amit szintén szeretnénk beadni. Amennyiben tényleges igény mutatkozik, és úgy tűnik, hogy igen, akkor adatokkal is alá tudjuk támasztani azt, hogy itt van igény bölcsődei kapacitás bővítésére. Ami nálunk folyamatosan lecsapódott és a szülőkkel is volt egyeztetve az az, hogy a szülők amiatt nem tartják jónak az iskolában történő elhelyezést, hogy a

gyerekekben ez törést fog okozni. A gyerekek több mint a fele mehetett is volna iskolába. Ez most a Humánterületi Bizottság ülésén derült ki, hogy 3 gyereknek van szakvéleménye, a többi intézményvezetői hatáskörben dőlt el pusztán az életkor alapján, amivel én nem tudok mit kezdeni. Bennem a másik oldalról az vetődik fel, ha most a bölcsődében fejlesztünk akár konténeres megoldással ideiglenes dolgot, akkor abban a szülőben és abban a gyerekben mi csapódik le, mert a 3 éves bölcsődés gyerek már arra lett felkészítve, hogy óvodába fog menni. Esetleg már voltak az óvodában szétnézni, arra kerékpároztak. A gyerek a jogot nem tudja kezelni, azt, hogy ő fizikailag óvodába van beírva, de maradt a bölcsiben. Ez egy 3 éves gyerek fejébe nem fog összeállni. Jelen pillanatban itt tartunk.

Konténer ügyében az egyik szülőtől kaptam javaslatot cégre, ugyanazt a céget javasolta, akit mi is megtaláltunk egy korábbi ügyben. Tőlük egy fél éves bérlésre kaptunk 5 konténerre 3,88 millió forintos összeget, amit duplázni kell, mert hogy egész évre szükségünk lenne rá. Elmozdultunk a vétel irányába, ahonnan kaptunk egy 14 milliós bruttó összeget, amiből 6.750 e/Ft a konténer, 2,9 millió a szaniter, 450-600 ezer a klíma, a kiszállítás, telepítés költsége plusz áfa. Ebben nincs benne az alap, valamint a közművek rákötése, hatósági engedélyezések. Ezek kész dolgok, mégis kell hozzá építési engedély. Erre kell egy építész tervet készítenünk, melynek átfutási ideje 2-3 hét. Hivatalosan 21 nap az építési engedélynek a megszerzése. Kb. még egy 4 millió forintot rá kell számolni. Az ÉMÁSZ ügyintézésnek is van átfutási ideje.

Az ÁNTSZ leírta azt és értelmes megoldásnak tartja az iskolában történő csoportszoba kialakítását, ezért a szakapparátus ebbe az irányba mozdult el. Jegyző asszony készített egy olyan előterjesztést, amely az alapító okiratnak az ez irányba történő módosítása lenne, ezt egyeztetette a Kincstárral. Amit pedig a napi szintű működésről gondolok az az, hogy úgy lehetne szervezni az óvoda életét, hogy az meg tudjon férni az iskolával. Tudjuk azt, hogy az iskolás szülők nem mehetnek fel a terembe. Az óvodás szülők igen. Igazgató asszony azt a részt jelölte ki az iskolában, ahol most jelenleg az első osztályos gyerekek vannak, ami a legelszeparáltabb terem. Bármilyen történik, vásárolnunk kell annyi fektetőt, amennyi a gyerek, bútort kell venni, kis széket, kis asztalt stb. Ezekbe így is úgy is be kell ruházni, ez fix költség. Számolgattuk, hogy a terem átalakítása mennyibe kerülhet, ez a költség egy 2-3 millió forint körül állna meg. Ez a pénz része, de szeretném hangsúlyozni, hogy ez most nem a pénzről szól. Jelen pillanatban még nem tudjuk megmondani, hogy bármilyen megoldás is születik, hogy honnan fogunk erre pénzt keríteni, hiszen februárban elfogadtunk egy éves költségvetést, ami lekötött tételeket tartalmaz. Jól hangzik a költségvetés összege, de ezek mind feladattal terheltek, ami pedig szabad forrás volt, azt célokhoz rendeltük hozzá, ahol már szerződések vannak kötve.

Visszatérve a napi működéshez azt gondolom, hogy járható út lehetne az, hogy az óvodás szülők ugyanúgy felmenjenek és ott adják át a gyerekeket. A folyosót lekerítenénk, van egy iskolai terem, ami átalakítódna óvodai csoportszobává és mellette van még egy kis terem is, amit döntés függvényében lehet használni fejlesztő teremnek, étkezőnek, fektető, altató helynek. Amit iskolaigazgató asszony felajánlott az az, hogy úgy fogja tervezni az órarendet, hogy legyen lehetősége ezeknek a gyerekeknek olyan plusz szolgáltatásokhoz hozzájutni, mint az informatika teremnek a használata, égető kemence, agyagozó műhely, tükrös terem használata mozgásfejlesztési céllal. Önkormányzatként pedig abban gondolkodok, hogy egy fejlesztő pedagógust fogunk felvenni, akinek csak az lenne a feladata, hogy az óvodai fejlesztéseket végezze. Ezen kívül találtam két olyan szakembert, logopédust és fejlesztő szakembert, akivel megbízásos jogviszony formájában támogatnánk azt, hogy ebben a közegben egy minél magasabb színvonalú ellátást tudjunk nyújtani. Ami még a humán erőforráshoz tartozik, hogy a dajka létszámot megkettőzve gondolnánk, két dajka tartozna a csoporthoz. A napi szintű működést nézve a reggeli órákban van egyfajta egyidejűség, akkor viszi a szülő a gyereket iskolába és az óvodás szülő is a gyereket óvodába. Meg lehet azt szervezni, hogy amikor óra van az iskolásoknak az ovisok akkor mennek le egy délelőtti játszó udvarozásra. Az étkezéssel kapcsolatban is egyeztetettünk az ÁNTSZ-el, ahol az hangzott el, hogy a tízórait, uzsonnát el lehet a csoportszobában fogyasztani, magát az ebédet pedig hamarabb kapják az óvodások, mint az iskolások, így akár le is mehetnek az iskolai étkezőbe. A szülő és gyerek így semmit nem érzékel. Ez nekünk most egy nagyon fontos megoldandó feladatunk, de nem kizárólag az egyetlen feladatunk. Nagyon sokszor egy külső, harmadik félre kell várnunk. Egyelőre nincs összehasonlító árajánlatunk, hiszen az még nem

érkezett meg, egy ajánlatunk van, ekkora tételnél három árajánlatot be szoktunk kérni. Most a gyorsaság kedvéért kettőt kértünk. Azzal mindenkinek tisztában kell lennie, hogy az önkormányzat nem dúskál az ingatlanokban, nincs 2-3 kockaházunk, ami erre megoldás lehetne. De tovább gondolva a dolgot az sem lenne megoldás, hiszen ami a rendezési terven nem intézményi terület, lakóterületbe van sorolva - egy rendezési terv módosítás legalább 6 hónap - lakóövezetbe nem lehet elhelyezni intézményt. Ezért szeretnénk az iskolába bekéredzkedni és ott minden feltételt, ami a komfortossághoz és ahhoz szükséges, hogy a gyerekek jól érezzék magukat, tényleges fejlesztést kapjanak megteremteni. Amennyiben a képviselő-testület úgy dönt, hogy adjuk ki 20 millió forintot azért, hogy egy ideiglenes megoldásba belemenjünk, akkor én is fel fogom tartani a kezem és meg fogom szavazni. Változatlanul nem tartom jó megoldásnak, mert azt gondolom, hogy nem ez szolgálja a közösség érdekeit. Nem lehet egyoldalúan nézni, hogy csak a nagy csoportos gyerekekről szól, mert ez ugyanúgy szól a kis csoportos gyerekekről is, aki lelkiileg arra van felkészítve, hogy mennek az oviba. Ez egy sokkal összetettebb kérdés. Kérdés, amennyiben utána adunk be pályázatot fix épületre, akkor mit kezdünk a konténerekkel, olyanokkal, amik össze vannak rendezve és hiányoznak oldalfalai. Ez a probléma számos kérdést felvet. Itt szeretném felhívni a képviselő társaim figyelmét is, hogy felelős döntést kell hozni ez ügyben. Amennyiben a konténer mellett döntünk, meg kell keresni és meg kell találni azt a 20 millió forintot, amit erre szeretnénk ráfordítani az egyébként kötött költségvetésünkből.

A tárgyalási sorrend szerint a Humánterületi Bizottság elmondja állásfoglalását, majd a képviselőknek van jogosultsága hozzászólni, ezt követően tudok szót adni a megjelent szülőknek. Számolgatnunk kell az idővel is, a rendelkezésre álló árajánlat szerint a konténeres cég 8-10 hetet írt szállításra, ezzel párhuzamosan tud készülni egy építési engedélyes terv és egyéb szükséges engedélyek. Van előttünk a július és egy augusztus hónap. Én a magam részéről azt tartanám racionális és kézenfekvő megoldásnak, hogy a szülőkkel partnerségben az iskolába kerüljenek elhelyezésre. Soha nem volt számunkra közömbös az óvoda, hiszen ingyenessé tettük az étkezést, nem kell tisztasági csomagot vinni az óvodába és minden gyerek ingyen tud járni úszni.

A humán erőforrást is próbáljuk összerakni, ami szintén nem egyszerű.

Átadnám a szót Juhászné Molnár Mária elnök asszonynak, hogy ismertesse a Humánterületi Bizottság állásfoglalását.

Kérdezem jegyző asszonyt, van e ezzel kapcsolatban még valami hozzáfűzni valója?

dr. Szakos Judit jegyző:

Finanszírozás részéről elfogadott a gyermeklétszám megemlése, telephelyként az iskola kijelölése. Az egyeztetés során a Kincstár és a Kormányhivatal részéről az volt meglepő, hogy azt kimondani, hogy Szirmabesenyőbe a tanköteles korú gyerekek - ami nem számít, hogy nyári gyerek - 42 %-a visszarad az óvodába. Ezt nem értette meg senki sem, hogy ez tulajdonképpen mi. Megkérdezték, hogy milyen gyerekek vannak itt. Amennyiben ezt száraz adatként nézzük úgy, hogy gyereket nem képzelünk mögé, a 42 % kimondása az nagyon sok. Biztos, hogy mindenkinek van magyarázata, egyedi oka. Én csak adatot, számot mondok, de ezen azért a reakció erős meghökkenés volt. Ez egy ilyen típusú, ilyen lakossági összetételű településen nem gyakorlott és nem jellemző.

Huszi Gábor polgármester:

Annyival egészíteném ki, amire pont jegyző asszony hívta fel a figyelmemet, hogy ez egy lavinát indít el, mert a következő évben a szülő azért akarja majd visszatartani a gyereket, mert nehogy más 7,5 éves gyerekekkel járjon az ő 6 éves gyereke iskolába. Innentől kezdve ez elszabadul. Most van egy olyan lehetőség a kezünkben, hogy a vegyes csoportos megoldásról vissza tudnánk állni a tiszta csoportra. El kell, hogy mondjam, hogy vita van ebben óvodavezető asszonnyal köztünk, ő már egy újhullámos intézményvezető, aki azt mondja, hogy ennek vannak előnyei, én pedig a szülők részéről hallom, hogy a nagy csoportos gyerekek nincsenek úgy felvértezve tudásban, mint amikor tiszta csoportok voltak. A tiszta csoportnak vitathatatlanul meg van az az előnye, hogy sokkal könnyebb egy nagy csoportos gyerekekkel elmenni kirándulni, uszodába, verseket, mondókákat tanulni, szerepléseket begyakorolni és egyáltalán készülni az iskola életre.

Győrfi Lászlóné iskolaigazgató:

Nem vagyok képviselő-testületi tag, de három fontos mondanivalóm lenne. Az iskola felújítása is szóba került, ott állunk ez előtt. Én magam is bizonytalan vagyok az iskolakezdés körülményeivel, azonban mindenkit nyugtatok, hogy minden rendben lesz, de ezt nem szabad figyelmen kívül hagyni.

A másik fontos dolog, hogy ha úgy dönt a képviselő-testület, hogy módosítja a szabályzatot, akkor azt egy évre tegye meg, mert egy évre le tudunk mondani egy tanteremről, de a továbbiakban szeretnénk mi is a fejlődésben gondolkodni.

A tisztánlátás érdekében szeretném még elmondani, hogy nem ragaszkodunk az óvodához, hanem felvetődött egy feladat, amiben azt mondtuk, hogy mivel az önkormányzatnak nagyon sokat köszönhetünk, illetve a Tankerületi igazgató úr áldását adta, bár a pedagógusok nem örülnek neki, elfogadják a tényt, hogy meg kell oldanunk.

Husztai Gábor polgármester:

Én abban gondolkodom, hogy megrendelünk építészeti tervet, megvizsgáljuk statikussal azt, hogy az óvoda fődémszerkezete mit bír és a tetőtérben kialakítani egy csoportszobát megfelelő szigeteléssel, légtechnikával. A hosszú távú tervem az óvodával ez, a bölcsődével kapcsolatban pedig az, hogy arra is adni be pályázatot és fix épületet építeni úgy, hogy az leválasztható, szakaszolható legyen. A demográfiai trendek egyáltalán nem támasztják alá azt, hogy itt robbanás szerűen egy vagy akár két csoportra is szükség van. Eddig mindig bevettek a szülők annyi gyereket Miskolcra praktikus okokból kifolyólag, hogy nem volt ilyen problémánk. A probléma két dologból állt össze, hogy túl sok gyereket tartanak vissza és nagyon sok, 18 fő külsős gyereket valamilyen oknál fogva felvett az óvoda, ami a 16 visszamaradó gyerekkel együtt 34 fő.

Kérem a Humánterületi Bizottság állásfoglalását.

Juhásznő Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

Köszönöm a szót. A bizottsági ülés után, még a döntésünk után is próbáltunk ötletelni, az elmúlt két napomat ennek a dolognak szenteltem. A Szirmabesenyői Napsugár Óvoda és Bölcsőde alapító okiratának módosítását a Bizottság nem támogatta. A létszámnöveléssel kapcsolatban senkinek nem volt kifogása, viszont az iskolai telephellyel igen. Én úgy gondolom, hogy az előzetesen elmondottakhoz képest külön kell választanunk az óvoda szervezetében esetleg a csoportban a korosztályok szétválasztását, az egy probléma, az az intézményvezető hatásköre, illetve a fenntartói az egy külön dolog. Most helyzet van, ennyi gyerek van beírva, ezeknek a gyerekeknek helyet kell biztosítani és ezt most itt nekünk meg kell oldani. Akkor is, ha ez 20 millió forintba fog kerülni az önkormányzatnak. Első körben a bölcsődéhez gondoltam egy csoportot konténer formában. Nagyon sok önkormányzat élt ezzel a lehetőséggel. Ezt most konténeres helyzettel kell megoldanunk. Én javasolnám, hogy az óvoda épületéhez hozzá tenni. Most ott annyi átalakulás lesz.

Husztai Gábor polgármester:

Oda nem fér el. Ott semmilyen átalakulás nem lesz, a konyhát verjük szét.

Juhásznő Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

Három-négy hónap alatt ezt komplex meg tudják oldani, 100-110 e/Ft m² áron. Én nem árajánlatot kértem, egy másik önkormányzattól kaptam adatokat, hogy ez milyen szinten valósul meg. Ebben kellene gondolkodjunk. Nagyon sok a megkeresés azóta is. Ismerem a kollégákat, amennyiben az iskolában lesz telephelye az óvodának, nagyon sok pedagógus ezt el fogja fogadni, nem leszünk ellene, segíteni fogjuk az óvodapedagógus munkáját. Az, hogy milyen pedagógiai szempontjai vannak, hogy a gyerekeket kiemeljük, átvisszük, van pozitív és van negatív szempontja is. Az, hogy a konténerekben milyen gyerekeket helyezünk el, a leendő beiratkozókat, vagy ugyanúgy kiemeljük a csoportból és ők kerülnek oda egy iskolaelőkészítő jelleggel ez megint a jövő kérdése. A tárgyi feltételeket kell biztosítani ahhoz, hogy ezeket a gyerekeket el tudjuk helyezni, a kötelező feladatát az önkormányzat biztosítani tudja. Próbáltam pénzügyileg is áttekinteni ezt a dolgot. Két dologban kell döntenünk, hogy az alapító okiratot támogatjuk-e ebben a kiküldött

formában, ahol meg van jelölve az iskola telephelynek vagy sem, a másik pedig, ha nem támogatjuk, akkor hogyan fogjuk folytatni, a konténert hová tegyük. Tervet kell készíteni. Azt, hogy utána milyen pályázatok jelennek meg nem tudjuk. Én csak annyit jegyeznek meg, hogy 3-4 éve ülünk itt és folyamatosan pályázatokra várunk. Most nem tudunk várni 3 évet, mert ezeknek a gyerekeknek most kell a feladatot megoldani. A költségvetést kinyomtatva azon gondolkodom, hogy mi az, amit tudunk változtatni. A februárban elfogadott költségvetésünkhöz képest is már voltak elmozdulások, lekötött dolgok. Nagyon szép költségvetése van a településünknek, de tudjuk, hogy ez egy úgynevezett pántlikás pénz, fel van címkézve, de azon kívül van egy kis tartalékunk is, a 6-os mellékletben a beruházási kiadások előirányzata. Ezen a táblán 476 millió forint körüli összeg van. Ebben van az adósságkonszolidáció, a sportudvar, az ÖKO tanterem, a sportkomplexum, tervezési költségek, a református parkoló, rendezési terv, bútorok és van egy 116 milliós összeg, amit arra gondoltunk, hogy menet közben különböző célokat jelölünk meg. Így került szóba az iskola 42 millióval, a közlekedésfejlesztés, különböző önrészek.

Husztai Gábor polgármester:

Az volt a cél, hogy beruházásokba saját dolgozóinkkal bedolgozunk és onnan próbálunk pályázati önrészeket csökkenteni. Ami felsorolásra került az mind címkézett, az ÖKO tanterem már épül. Pályázatra várunk 3 évet!

Az első évünk úgy kezdődött, hogy felkészültünk, gyártottunk terveket.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

Szeretném befejezni, mert még nem fejeztem be. Próbáltam ötletelni, mert, ha javaslatot mondok, mindig az van, hogy honnan. Számítunk adóbevétel emelkedésre is. Úgy gondolom, hogy időleges átcsoportosítással ezt a 20 millió forintot a konténerek megvásárlására meg tudjuk finanszírozni, ez nem okozhat gondot. A kivitelezésre is azt a 3-4 hónapot ki tudjuk várni, hiszen nagyon sok gyerek év közben fog bejönni, igazán januárban kezdődik feltöltésre a létszám, addig ez az idő elég kell, hogy legyen, hogy a kivitelezést meg tudjuk valósítani.

Husztai Gábor polgármester:

Köszönöm szépen. Kiegészítésként csak annyit, hogy a szülők részéről is volt olyan felvetés, hogy toljunk el EU-s nyertes projektet, hogy az önrészt később kelljen felhasználni. Ez nem lehetséges, mert kötött menetrend szerint haladunk. Amikor pályáztunk sokkal alacsonyabb árak voltak, most minden elszállt, mindezt hozzá kell tegyük. A korrektség kedvéért annyit elmondanék, hogy az első 2 évét a testület tervezéssel, előkészítéssel töltötte, nagyon sok mindent megtervezettünk, be is adtunk rengeteg pályázatot. Ült rajta a központi adminisztráció és most pedig minden egyszerre hullik ránk. Nyertünk egy kerékpárutat, egy ÖKO tantermet, egy iskola felújítást, egy orvosi rendelő felújítást, a postával szembeni épület felújítását, úgy tűnik, hogy nyertünk az Ongropack mellett egy utat, tehát nem unatkozott a képviselő-testület és személy szerint én sem. Bolond ember az, aki nem használ ki egy állami támogatást, és nem ad be aktívan pályázatokat. Most is ezen dolgozunk.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

Én ezt a pályázatokra várást arra mondtam, hogy most nincs arra időnk, hogy várjunk.

Husztai Gábor polgármester:

A bizottsági vélemény elhangzott, a bizottság ezt az előterjesztést nem támogatta. Átadom a szót a képviselőknek, utána pedig Járvásné Mátó Melindának. Jegyző asszony?

dr. Szakos Judit jegyző:

Amikor a szavazásra kerül a sor, érdekében az alapító okirat módosítására készített előterjesztés nem változik, de a Kincstárral a mai napon volt az utolsó egyeztetés, ennek a technikájáról még egy pár mondatot szeretnék mondani.

Asztalos Erika képviselő:

Az én gyermekem is az óvodába jár és nagy csoportos, érintve van. Sokat gondolkodtam rajta, tudom, hogy mi az, amikor a szülő a legjobbat akarja a gyerekének. Első megközelítésből egyértelműen úgy gondoltam, hogy semmi képen nem szabad a gyerekeket kiszakítani a megszokott környezetükből. Ott vannak a barátok, a biztonság, a szülő nyugodtan adja át az óvónőnek a gyereket. Ha abban a közegben marad, az a legjobb neki. Az iskolai elhelyezésben is meg lehet látni a jó dolgot, olyan lehetőség lenne a kezünkben, ami úgy fejleszti a gyereket, amire az óvodában nincs lehetőség. Megvan az előnye annak is, hogy együtt van egy korosztály, mennek kirándulni, több dolgot meg lehet velük csinálni, mint ahol kis csoportos is van. Ez a része jó lenne. Az, hogy kiszakítani a megszokott környezetéből, ez amellest szól, hogy ott kell maradni. Ez egy nehéz ügy, de amit iskolaigazgató asszony mondott, hogy egy évre szól ez a lehetőségünk, az elgondolkoztató, ez elveti azt a gondolatot, hogy iskola. Nem tudom, hogy mennyire egy év lesz ez a probléma, hiszen azon dolgozunk, hogy Szirmabesenyő vonzó legyen a betelepülők számára és egyre többen fogják választani lakóhelyükként. Az iskolai megoldásnál is nagyon sok plusz költség fog jelentkezni. Én arra gondoltam, hogy a bölcsőde udvarára kellene tenni a konténert, de jobban örülnék, ha az óvoda udvarán lenne, mert ugyanúgy együtt lennének. Mindenképpen meg kell vizsgálni azt, hogy az óvoda udvarán hogy fér el.

Husztai Gábor polgármester:

Ha a játszótérből veszünk el, el kell bontani azt az épületet, ahol a kinti eszközöket tárolják. Az infrastruktúra részt ki kell találni, néhány fát ki kell vágni. Csak hátrafelé lehet menni, mert az épület oldalhatáron helyezkedik el, arra nem fogunk engedélyt kapni. Ez egy műemléki környezet. Azt is látni kell, hogy ezáltal a játszóudvar mérete csökken. Oda eszközöket kellene tennünk, hiszen egy csoporttal több gyerek van, aki ugyanúgy szeretne játszani. Kialakult sajnos egy olyan rendszer, hogy sövényekkel fakkok vannak elválasztva és mindenki maradjon a saját fakkjában és mindenki azt figyeli, ami az övé. Az egyikben nincs hinta, a másikban nincs csúszda. Ezeket a problémákat görgetjük magunkkal. Ilyen szempontból több racionalitás szorul abba, hogy a bölcsőde udvaron történjen fejlesztés, ami egy sokkal nagyobb.

dr. Szakos Judit jegyző:

A bölcsődéhez egy adalék, hogy a bölcsőde nem oktatási intézmény, hanem egészségügyi intézmény. A bölcsőde nem az oktatási törvény hatálya alá tartozik, hanem az egy egészségügyi, szociális intézmény. Ha a bölcsődében akarunk bármit is csinálni, ott az engedélyeztetés a gyámhivatalhoz tartozik, ami egy teljesen új vonal, annak nekimenni? Én innen merem azt állítani, hogy én, aki engedélyeztettem az egészet, átmeneti megoldásként 1,5 hónapos átfutással lehetetlennek tartom, nem is érdemes nekifutni.

Asztalos Erika képviselő:

A rendkívüli állapotra való tekintettel nem lehet megsürgetni?

dr. Szakos Judit jegyző:

Nem. Ezek objektív előírások, itt nincs olyan indok, ami alapján ezen változtatni kell.

Asztalos Erika képviselő:

A bölcsőde udvarán tulajdonképpen nem tudjuk megvalósítani időben?

dr. Szakos Judit jegyző:

Én úgy gondolom most, hogy nem. Ez egy teljesen külön eljárás.

Asztalos Erika képviselő:

Az óvodával az a gond, hogy a gyerekek száma nő, a játszóterület pedig csökken.

Husztai Gábor polgármester:
Így van.

Asztalos Erika képviselő:
Hosszú távon ez megint nem jó a gyerekeknek.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:
Véleményem szerint szervezési kérdés, nem biztos, hogy egyszerre kell a gyerekek az udvaron hintázní. Nem messze készül az ÖKO tanterem, annak is biztos lesz valami környezete. Külső foglalkozások stb.

Husztai Gábor polgármester:
Ez az iskola esetében is fennáll, fent vannak a tetőtérben, de oda mennek, ahová akarnak. Szó sincs arról, hogy a szünetben vegyülne az óvodás gyerek az iskolással.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:
Én arra akartam felhívni a figyelmet, hogy a tárgyi feltételeket biztosítjuk, első sorban a gyerekek elhelyezését, mellette a szakmai részét hogyan fogjuk megoldani, az egy másik kérdés. Én javaslom, hogy a konténerre az óvoda területén tegyünk meg a lépéseket.

Bodnár Krisztián képviselő:
Szó esett arról, hogy műemlékvédelmi terület. A futballpálya felé ideiglenesen bővíteni nem lehet?

Husztai Gábor polgármester:
Az óvodai területtel borzasztó nehéz helyzetbe kerülünk. Nem fogunk építési engedélyt kapni.

Bodnár Krisztián képviselő:
Nem épületre gondoltam, hanem mint játszóteret bővíteni a pálya felé.

Husztai Gábor polgármester:
Benne van a gondolataimban, csak most nem tartunk ott. Ha a sportpályára teszek játszóteret, akkor azt hogy szeparálom el.

Bodnár Krisztián képviselő:
Úgy gondolom, hogy ez egy mobil kerítéssel megoldható lenne.

Husztai Gábor polgármester:
Ez egy annyira bonyolult és összetett kérdés. Az épületnek a traktusmélysége 5,6 méter, plusz falvastagság, kb. összesen 6,5 méter. Az épületnek valahogy ki kellene néznie még ha ideiglenes is. Egyébként ha már 20 milliót erre szánunk, kérdés, hogy annak ideiglenesnek kellene-e lennie. Azon kívül én már most látom, hogy nem fog kijönni 20 millióból. Ha megnézzük a bővítési tervet, akkor láthatjuk, hogy egyfajta folyósót is kell képezni a konténereknél, valahol be is kell jutni, nem lehet rögtön a csoportszobába toppanni. Nem biztos, hogy bele tudunk férti az 5 db konténerbe. Amit árajánlatba kaptunk az úgy néz ki, hogy négy konténer egybenyitva és egy szaniter konténer. Hol van az öltöző, átadó rész? Ez az öt inkább hat.

dr. Rónai István aljegyző:
Mellé van még egy másik dolog, amit ma beszéltünk jegyző asszonnyal, hogy ha nincs az óvodával összekötve, akkor kell egy tálaló konyha rész is.

Husztai Gábor polgármester:

Ezt csak úgy tudom összekötni az épülettel, ha bele nyúlok a személyzeti mosdóba, öltözőbe, raktárba. Jött az ötlet, hogy vágjunk ajtót, de az egy panel épület.

Győrfi Lászlóné iskolaigazgató:

Külső zárt folyósóval.

Husztai Gábor polgármester:

Ezt nyaktagnak mondják. Továbbra is egy műemléki környezetben vagyunk, ahol egy normális homlokzatot kellene kialakítani.

Amennyiben a képviselők részéről nincs további kérdés, hozzászólás, akkor átadnám a szót Járvásné Mátó Melindának, aki meg tudja világítani arról az oldalról, hogy mi az az ellenézés a szülők részéről, egy korrekten és jól szervezett napi szintű működés mellett mi a baj azzal, hogy az iskolában legyen egy ilyen dolog és a maximális fejlesztést kapja meg minden gyerek. Úgy, hogy a szülők közül nincs itt mindenki és nem beszéltünk kis csoportos szülőkkel.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

Hagyjuk már az óvoda szervezeti részét az óvodai munkának.

Husztai Gábor polgármester:

De az fontos, mert az összefügg.

Járvásné Mátó Melinda szülő, az SZMK képviselője:

Köszönöm szépen a lehetőséget, hogy szóhoz juthatok, Járvásné Mátó Melinda vagyok az SZMK képviselőjében. Köszönjük szépen, hogy előre hozták ezt a napirendi pontot, nem kell itt ülnünk estig, ami minket a legjobban érdekel, azt minél hamarabb hallhatjuk. Reflektálnék pár dolgot a polgármester úr mondanivalójára. Tényleg megvolt ez a megkeresés a szülők részéről, akik visszatartottak, azok a szülők voltak ezen a megbeszélésen. Viszont azt tudjuk, hogy ez a 15 fő amúgy sem tudná megoldani ezt a problémát, az információnak kellett volna direktbe jönnie. Találkoztunk azzal a kérdéssel, amit tényleg nem tudtunk, hogy aláírjunk-e vagy sem, ezért kerestük meg az óvodavezetőt, aki felvilágosított bennünket ezekről az információkról és pont abban az időpontban hívtuk fel polgármester urat az ötleteinkkel, hogy milyen lehetőségeket látnánk mi, mint szülők, ne szakadjanak ki a gyerekek a jelenlegi környezetükből, a jelenlegi óvónőktől, a jelenlegi társaktól. Ez után történt a szervezés, hogy azt az információt, amit az önkormányzattól kaptunk, megosszuk a szülőkkel, hogy minden érintett tisztában legyen azzal, hogy itt mik várhatóak. Ez a Kocsis Fogadóban volt egy csütörtöki napon és pénteken rögtön hoztuk a nyílt levelet, melyben megfogalmaztuk, hogy a szülőknél milyen aggodalmaik vannak és ugyanezzel a levéllel kerestük meg a Tisztelt Képviselő-testületet is. Ami nagy aggály, hogy a gyerekek kiszakadnak a környezetükből, kiszakadnak abból a környezetből, ahol már két, esetleg három éve járnak, átkerülnek az iskolába, ahová vagy majd járnak vagy egy másik iskolába kerülnek. Kiszakadnak a napi életből, kiszakadnak a napi programokból, az óvónőtől, a társaktól. Ez egy kardinális kérdés egy gyereknél, az utolsó évét tényleg nem tudja nyugodtan tölteni. Nagyon sok változás volt az óvoda életében már így is, mind óvónő terén, mind pedig a napközis átköltözés esetén is. Azt is nagyon sok gyerek rosszul élte meg. Sajnos sokan újra bepisiltek, körmöt rágtak, és ez nem tetszett a szülőknél. Úgy gondoltuk, hogy jogunk van dönteni arról, hogy milyen lehetőség van. Ezért volt az, hogy ötleteltünk, nagyon sok ötletet elhoztunk, még az ÖKO tanterem is felvetésre került, mert pontosan nem tudtuk, hogy ki néz ki. Az volt az általános vélemény, hogy szükséges egy felkészítés, de a felkészítésnek ne az iskola adja a helyet. Ezért jött az, hogy hol lehetne megvalósítani, így jöttek a konténer ötletek. Itt felvetődik az, hogy konténer, területet ad, de ki kerüljön bele. Szintén a másik dolog, hogy tényleg a nagy csoportosokat vesszük ki és tesszük át egy külön helyre, vagy azt mondjuk ami valahol az óvoda célja, hogy a tiszta csoportokat kialakítsa, már megfogjuk a kicsiket, őket egy helyre tesszük és utána az óvónénijükkel, a társaikkal együtt tudnak majd bemozogni az óvodába. Úgy véljük, bár ebben igazán a kis csoportos szülők tudnak állást foglalni, hogy ez kevésbé

nagy törés, mint az, hogy most 2-3 év után kivesszük a gyerekeket a csoportból, összerakjuk őket barátok nélkül, mert nem tudjuk, hogy a barátaik mennek-e, illetve a megszokott óvónő nélkül. E miatt van az a szülő támogatás, hogy inkább konténerben helyezzük el a kis csoportos gyerekeket. A másik érv, ami még mellette is szól, hogy ha a kis csoportosokat megfognánk, a 30 fő esetleg helyet kap a konténerben, akkor egy normális óvodai csoportlétszámmal tudunk működni. Egy normális óvodai létszámba, ami kb. 22 fő, nem a mostani 30-32 fő, ott valószínűleg már lehet iskolai felkészítést csinálni. Ezért van az, hogy egyre aktívabban részt veszünk itt az üléseken. Valóban elküldtem a konténeres kontaktot, úgy gondoltuk, hogy ez egy jó lehetőség megkérni. Mi sem ültünk tétlenül, mi is kerestünk olyan céget, aki konténereket bérbe ad, sőt megkerestük olyan céget is, aki már ilyen mobil óvodát alakított ki. Tőlük kértünk ajánlatot, amit most el is hoztunk. A bizottság tagjai már ismerik. Ami a lényeg, hogy több konténerre is kértünk ajánlatot, mi első körben nyolc konténerben gondolkodtunk. Kértünk bérlésre és vásárlásra is ajánlatot. Tudjuk, hogy ez nem hivatalos, csupán információként szolgál Önöknek egy későbbi döntéshez. Ami itt még fontos, hogy vannak a személyi szempontok, szakmai szempontok, nekünk a gyerekeinkről van szó, anyák, apák vagyunk, nekünk ők a legfontosabbak. Tudjuk, hogy minden átalakítás költséggel jár. Itt kézzel fogható ajánlat van. Tudjuk, hogy valamilyen átalakításra szükség van, rizikót mi is érzünk az iskolával kapcsolatban, pont a felújítás kapcsán, ami egyáltalán nem biztos, hogy befejeződik szeptemberre. Egyáltalán nem biztos, hogy az iskolában elhelyezhetőek lennének. Itt is vannak átfutási idők, mérlegelni kell és dönteni. E miatt kérnénk azt, és fordulunk a képviselő-testület felé, hogy amennyiben lehet vegyék figyelembe a szülői kérést, hogy inkább egy konténerben, inkább egy tiszta csoport felmenő rendszerben való kialakításában gondolkodni és ezt a lehetőséget megteremteni, mint most kiragadni az összes gyereket és megbolygatni az egész óvodát. Köszönöm szépen.

Husztai Gábor polgármester:

Köszönjük szépen. Annyit tennék hozzá, hogy egyrészt mi is attól a cégtől kértünk ajánlatot. Azzal én nem értek egyet, hogy 5 cm vastag murva kell neki. Leírja, hogy vásárlásnál 2,5 hónappal kell számolnunk, kérdés az, hogy szeptemberre ez hogy lesz kivitelezhető. Szeptemberben 16 gyerek jön fel a bölcsődéből és még vannak olyanok, akik nem voltak bölcsisiek, de beiratkoztak. A teljes létszámot január, februárra fogja elérni. A humán erőforrást hagyjuk meg az óvodavezetőnek. A szülők is a bölcsőde melletti elhelyezést favorizálták, nagyobb terület állna rendelkezésre. Még mindig nagyobb logikát látnék abban, hogy a bölcsődében oldjuk meg az elhelyezést akár egy telekmegosztással, mint az óvoda játszóudvarából vegyünk el 100 m²-t. Egyébként műemlékvédelmi környezetben az engedélyezés plusz idő.

Asztalos Erika képviselő:

Az iskolát muszáj elvetnünk. Azért muszáj, mert nem kockáztathatjuk a felújítás miatt.

Husztai Gábor polgármester:

A felújítás azért nem kockáztatja, mert gépészettel kell, hogy kezdjen a kivitelező. Az, hogy a külső homlokzatra mikor kerül fel egy szigetelés az már egy sokadik dolog.

Asztalos Erika képviselő:

Nekem az a gondom, hogy ezek a gyerekek egy évig járnak oda előkészítőbe. Úgy gondolom, hogy hasonló szituáció lesz, mint az óvoda felújításnál, hogy ki kell még bírni egy kis időt a napközibe. Építésről van szó, mindenki tudja, hogy csúszhat. Esetleg 2-3 hónapig rendezetlen lesz a terület. Még ha jól is megcsinálnánk ez annyira visszavetődne.

Husztai Gábor polgármester:

Kétségtelen, hogy ebben van kockázat, amit nagyobb dolognak tartok, mint a Melinda által többször is említett kiszakadást. A játszóudvaron együtt vannak, mindenki ismer mindenkit. Nyáron, illetve influenzás időszakban összevont csoport van. Ne úgy állítsuk be, hogy egy ilyen szituáció kapcsán majd pszichológushoz kell hordani a gyereket.

dr. Szakos Judit jegyző:

A konténerhez még csak annyit szeretnék mondani, ezt a képviselőknek, hogy amennyiben a konténer az óvoda vagy a bölcsőde területére van tervezve, azt az alapító okiratban nem kell szerepeltetni.

Husztai Gábor polgármester:

A szülőktől kérném, hogy tegye már fel a kezét az, aki visszatartott gyerekeknek a szülője. Döntési helyzetben van-e a képviselő-testület úgy, hogy nem tudjuk, hogy egy kis csoportos szülő hogy áll ehhez a kérdéshez és nem tudjuk azt, hogy egyébként az a 28 szülő, aki aláírta ezt a nagy csoportos megoldást, hogy ők hogyan állnak hozzá ha nincsenek itt. Senki nem tette fel a kezét.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

Ez szervezeti kérdés.

Husztai Gábor polgármester:

Nem mindegy, hogy kit hová pakolsz.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

Nekünk arról kell döntenünk, hogy a 20 millió forintot tudjuk-e biztosítani, valamint az alapító okirat módosításáról.

Husztai Gábor polgármester:

Nem tudom, hogy döntési helyzetben vagyunk-e, nem kellene egy szülői értekezletet tartani.

Bodnár Krisztián képviselő:

Az idő telik.

Husztai Gábor polgármester:

Az idő valóban telik, csak most olyan szülők feje felett döntünk, akik esetleg nem tudták elmondani a véleményüket. Én beszéltem olyan szülővel, aki teljesen jónak tartja ezt a 0. évfolyam megoldást.

Járvásné Mátó Melinda SZMK képviselője:

Polgármester Úr, ilyen nincs, hogy 0. évfolyam.

Husztai Gábor polgármester:

Jogilag az egy önálló óvodai csoport.

Járvásné Mátó Melinda az óvodai szülői szervezet képviselője:

A gyerekeknek a legfontosabb dolog a biztonság. Betegségek előfordulnak, például lebetegszik az óvónő, változik a személy, utána költözött a csoport, tehát olyan sok minden mentek keresztül a gyerekek. Ezért van a bizonytalanság, mit mondjunk a gyerekeknek, hol lesznek óvodások. Ahol kezdték, vagy máshonnét fognak ballagni. Egy év múlva jöjjenek vissza a gyerekek ballagni? Amikor a munkahelyéről elköszön valaki, nem egy év múlva megy vissza elbúcsúzni.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

Azt mondta polgármester úr, hogy kidobott pénz, amit a konténerre költünk az a 20 millió forint. A gyerekeink testi-lelki biztonsága érdekében áldozzuk be, máshová is tettünk nagyobb összegeket. Döntünk az alapító okirat módosításáról, a telephely módosítása nélkül. Hogy a konténerek hová kerülnek és melyik csoportos gyerekek kerülnek oda, döntse el az intézményvezető. Az udvar esetleges átalakítását szintén. Indítsuk el ezt a folyamatot.

Husztai Gábor polgármester:

A bölcsőde bővítésének mik a lehetőségei? Különösen, hogy ott 3 m² kell egy gyerekre. Ott óvodai, vagy bölcsődei csoport lenne? Nincs mire várni, mert az idő nagyon kevés. Nincs időnk vizsgálgatni. A bölcsődében nagyobb a terület, kevesebbet vennénk el az udvarból. Kell-e ott telekmegosztás, de az akkor már önálló intézményi terület lenne.

dr. Szakos Judit jegyző:

A konténer csak az alapító okirat szerinti telephelyekre kerülhet. A bölcsődei elhelyezéshez nem tudom, hogy az engedélyező hatóság mit szólna.

Husztai Gábor polgármester:

Ha egy nyaktaggal nincs a konténer az épülethez kötve, kell a tálalókonyha is és a személyzeti kiszolgáló helyiségek is. Ezek egyébként az épületben rendelkezésre állnának.

Bodnár Krisztián képviselő:

Nézzük meg az óvoda bővítésének lehetőségét. Még úgy is, hogy kisebb lesz az udvar.

Asztalos Erika képviselő, a Pénzügyi Bizottság elnöke:

Az előkertet kellene beépíteni és az udvar egy részét, és lehetne úgy egy csoportot elhelyezni.

Szakos István képviselő, a Területfejlesztési Bizottság elnöke:

Az öt konténernek mennyi a területe?

Husztai Gábor polgármester:

12-13 méter x 6,20 méter. Erre kellene még szigetelés.

Kertészné dr. Kocsis Krisztina az óvodai szülői szervezet képviselője:

Az általunk bemutatott árajánlat klímával felszerelt konténerre vonatkozik.

Asztalos Erika képviselő, a Pénzügyi Bizottság elnöke:

A konténer fenntartása is nagyon drága, főleg a villamos energia költsége.

Ojtozi Attila műszaki vezető:

Maga a kiépítés sem egyszerű, már végig csináltam a sportöltözővel, az ÉMÁSZ-nál két hónap alatt sem fut át.

Husztai Gábor polgármester:

Októberre ebből nem lesz semmi.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

Szerintem döntsünk.

Husztai Gábor polgármester:

Négy határozatot kellene hoznunk az előterjesztés szerint.

Firtkó Sándor szülő:

A régi napközi miért van elvetve? Olyan sokat kellene ráköltetni? A községi rendezvények pedig erre az egy évre elkerülhetnének innét.

Husztai Gábor polgármester:

Nem lehet minden puffert felhasználni. Meg van hirdetve 8-10 tábor, azt már meg kell tartani.

A konténer tekintve a vétel irányába mozdultunk el, mert nincs szignifikáns különbség a vétel és a bérlet között, de 10 millió forint lenne az éves bérlet és 25 millió körül a vétel, mert az ajánlathoz képest kell még két konténer. Kérdés, hogy a fix épület mennyiből jönne ki.

Asztalos Erika képviselő, a Pénzügyi Bizottság elnöke:

Ezért mondtam a könnyű szerkezetet, hogy ne szakadjon szét az óvoda.

Husztai Gábor polgármester:

Ezért egyeztettem az építésszel, hogy szabjuk át a tervet. 10 nap múlva látjuk a féléves költségvetési adatokat. Legyen meg mondjuk egy tornaszoba, amit csoportszobának használhatnánk egy évig.

Tíz nap múlva látjuk a költségvetésünk tartalékait és szabadabban tudnánk gondolkodni a fix építésről. Van engedélyes tervünk és építenénk egy sportszobát, nem tudom, mennyibe kerülne. Tendereztetni kellene, három ajánlatot kérni, nem közbeszerzéseköteles.

Járvásné Mátó Melinda az óvodai szülői szervezet képviselője:

A szülők először is ezt akarták és azóta már egy csomó idő eltelt, egy hónap is.

Husztai Gábor polgármester:

Mindent megvizsgáltunk, építésszel beszéltünk, az ÁNTSZ-szel egyeztetünk, rendezési tervet néztünk, hiába kérik a szülők tőlem pénteken, hogy szerdára mondjak határozott választ, az lehetetlen.

A konténeres cég se adott ajánlatot, mert nincs ideje, az építész nem tudott jönni, mert nem ért rá.

Csak a jövő héten, ahhoz képest, amikor hívtam. Mit csináljunk?

Ha elmegyünk a konténer irányába, akkor sem jutunk előbbre, mert nincs itt egy építész, aki megmondaná, hogy azt hová lehet letenni. Sematizált ábráink vannak. Hol lesz folyosó, öltöző, átadó, hogy toldjuk hozzá az épület végéhez, azt nem tudjuk.

Ha a hátsó részhez kötjük, belső átalakítás, tehát a belső helyiségekhez nem kell engedély, a nevelői mosdó, a mosókonyha, zuhanyzó és raktár elveszlik, ezeket tehát pótolni kell.,

A konténer-részt le kell engedélyeztetni.

Itt van a felmérési alaprajz és a sematizált ábra.

Győrfi Lászlóné iskolaigazgató:

Az lenne a legegyszerűbb, ha valaki létrehozna egy családi napközit.

Fedorné Karmanóczy Zita a Segítő szolgálat és Konyha vezetője:

Gyermekvédelmi intézmény a családi napközi.

Husztai Gábor polgármester:

Kérdés, hogy hol, mert nincs megfelelő ingatlanunk.

dr. Szakos Judit jegyző:

Az a gond, hogy a beiratkozás lezárult, minden gyerek fel van véve, ki van értesítve.

Elhelyezésüket biztosítani kell. Május 11. volt az utolsó nap a beiratkozásra.

Husztai Gábor polgármester:

Igen, akkor jött vezető asszony.

Gulyás Edit Judit óvodavezető:

Azóta már 41 gyerek van.

Husztai Gábor polgármester:

Akkor ezt most nem értem. Újra kell tervezni az egészet.

Gulyás Edit Judit óvodavezető:

Ha a teljes létszámot elosztom az 5 csoportra, 22,2 fő jön ki egyre.

Husztai Gábor polgármester:

És maradnak a vegyes csoportok.

Gulyás Edit Judit óvodavezető:

Nem feltétlenül.

Surányi Zsuzsanna szülő:

A vegyes csoport 25 fős lehet és most 32 fővel is működnek. Ez nem jó dolog.

Husztai Gábor polgármester:

24 fő az átlagos statisztikai létszám, ez a bizottsági ülésen hangzott el, a Humánterületi Bizottság ülésén. Beköltözők még év közben is jöhetnek, beiskolázási körzet vagyunk, kötelesek vagyunk felvenni. Hol a pufferolás vége?

A konténert fixen kellene telepíteni, szigetelni, válaszfalakkal ellátni. Utána mire fogjuk használni, ha nem lesz rá szükség? A villamos hálózat kiépítése és működtetés nagy probléma, ezt már tudjuk.

Éves szinten plusz 12 millió forinttal támogatjuk az óvodát a normatíván felül.

Nézzük a határozati javaslatokat.

dr. Szakos Judit jegyző:

Az első határozat az óvodai gyermeklétszám megemelésére vonatkozik.

A következő határozati javaslat az iskola telephelyként történő feltűntetésére vonatkozik.

dr. Rónai István aljegyző:

Módosíthatjuk az előterjesztést és akkor nem is kell erről dönteni.

A határozati javaslat az iskola telephelyként történő felvételének elhagyásával módosítható.

dr. Szakos Judit jegyző:

A konténer az óvoda telephelyein elhelyezhető, azt az alapító okiratban feltűntetni külön nem kell. Most az elsődleges az alapító okirat módosítása a normatíva igénylés miatt.

Husztai Gábor polgármester:

2 millió forintig csoportosíthatók át és a féléves költségvetés-módosításkor átvezetjük. Kell állásfoglalás a felhatalmazásra, hogy a konténert meg tudjuk rendelni.

dr. Budai István képviselő:

Az anyagi részt sokat emlegeti polgármester úr, bár tavaly úgy nyilatkozott, hogy egy 100 millió forintos hitel nem terhelne meg a település költségvetését, ami az iskola felújítására került volna felvételre. 5-10 millió forint hitel felvétele nem gond, ha ez a szülőket megnyugtatja.

Jövőre jelentős adóbevételt várunk, az anyagi részlet nem lehet vita tárgya.

Husztai Gábor polgármester:

10 millió forint hitelt nem éri meg felvenni. A stabilitási törvény értelmében a kormány jóváhagyása kell az önkormányzatok hitelfelvételéhez.

Igen, én szerettem volna a 100 millió forint hitelt felvenni az iskola felújításához, akkor a Testület leszavazott, most lehet, hogy nem szavazna le, két év alatt vissza tudnánk fizetni.

Ha veszünk fel hitelt, csináljuk meg az óvodát teljesen. egy csoportszobát csináljunk és oldjuk meg a vizesblokkot. Ez már az időbe nem fér bele.

Meg fogjuk találni azt a 20-25 millió forintot, de jobban megérné a fix épületet megépíteni.

dr. Szakos Judit jegyző:

Az előterjesztésből kikerül az iskola telephelyenkénti megjelölése.

Az intézményi besorolás változik szeptember 1-től, tehát aki módosítja az alapító okiratát, ezt is átvezeti, a közoktatási törvény 20.§ b.) pont alá soroljuk mi az intézményünket.

Az utolsó határozat az alapító okirat és a módosító okirat elfogadására vonatkozik.

A napirendi pont keretében egyéb hozzászólás, kérdés nem volt, annak megtárgyalását a polgármester lezárta, indítványára a Képviselő-testület egyhangúlag, 6 fő igen szavazatával, ellenszavazat és tartózkodás nélkül meghozta a következő határozatokat:

Szirmabesenyő Nagyközség Önkormányzata Képviselő-testületének

62/2018. (VI. 20.) Kt. határozata a Szirmabesenyői Napsugár Óvoda és Bölcsőde maximális óvodai gyermeklétszámáról

1. Szirmabesenyő Nagyközség Önkormányzata Képviselő-testülete egyhangúlag, 6 fő támogató szavazatával, ellenszavazat és tartózkodás nélkül úgy dönt, hogy a Szirmabesenyői Napsugár Óvoda és Bölcsőde maximális óvodai gyermeklétszámát 2018. szeptember 1. napjával 150 főben állapítja meg a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény 13.§ (1) bekezdés 6. pontja alapján és a nemzeti köznevelésről szóló 2011. évi CXC. törvény 8.§ (1)-(2) bekezdéseiben foglaltak alapján.
2. A határozat utasítja a Jegyzőt, hogy a határozatot és az 1. pontban foglaltak szerint elfogadott okiratokat a Magyar Államkincstár felé küldje meg a Törzskönyvi nyilvántartáson való átvezetés céljából

Határidő: azonnal

Felelős: polgármester, jegyző

Husztai Gábor s.k.

polgármester

dr. Szakos Judit s.k.

jegyző

Szirmabesenyő Nagyközség Önkormányzata Képviselő-testületének

63/2018. (VI. 20.) Kt. határozata a Szirmabesenyői Napsugár Óvoda és Bölcsőde típusának módosításáról

1. Szirmabesenyő Nagyközség Önkormányzata Képviselő-testülete egyhangúlag, 6 fő támogató szavazatával, ellenszavazat és tartózkodás nélkül úgy dönt, hogy a Szirmabesenyői Napsugár Óvoda és Bölcsőde típusát a nemzeti köznevelésről szóló 2011. évi CXC. törvény 20.§ (1) bekezdés b.) pontja alapján 2018. szeptember 1-től „többcélú intézmény óvoda-bölcsőde” megnevezésben állapítja meg.

2. A határozat utasítja a Jegyzőt, hogy a határozatot és az 1. pontban foglaltak szerint elfogadott okiratokat a Magyar Államkincstár felé küldje meg a Törzskönyvi nyilvántartáson való átvezetés céljából

Határidő: azonnal

Felelős: polgármester, jegyző

Husztai Gábor s.k.
polgármester

dr. Szakos Judit s.k.
jegyző

Szirmabesenyő Nagyközség Önkormányzat Képviselő-testületének

64/2018. (VI. 20.) Kt. határozata a Szirmabesenyői Napsugár Óvoda és Bölcsőde alapító okiratának módosításáról

1. Szirmabesenyő Nagyközség Önkormányzat Képviselő-testülete egyhangúlag, 6 fő támogató szavazatával, ellenszavazat és tartózkodás nélkül úgy dönt, hogy a Szirmabesenyői Napsugár Óvoda és Bölcsőde 1. melléklet szerinti Alapító okiratának Módosító okiratát és a 2. melléklet szerinti módosításokkal egységes szerkezetbe foglalt Alapító okiratát elfogadja.
2. A határozat utasítja a Jegyzőt, hogy az 1. pontban foglaltak szerint elfogadott okiratokat a Magyar Államkincstár felé küldje meg a Törzskönyvi nyilvántartáson való átvezetés céljából

Határidő: azonnal

Felelős: polgármester, jegyző

Husztai Gábor s.k.
polgármester

dr. Szakos Judit s.k.
jegyző

Béres László alpolgármester:

Eddig nem akartam beleszólni, mert én nem szavazok. El kell gondolkodni, hogy a konténeres megoldás egy évre 30-32 millió forintos költséget jelent. Nézzük meg az eredeti koncepciót, az óvoda teljes felújítását és bővítését, vegyünk fel hitelt.

Ezek a gyerekek nem mind szeptember 1-jén kerülnek be, de addigra konténer sem lesz.

Esetleg csak januárban működne a konténer. Érdemes lenne beszélni a tervezővel, és legalább részben az épület bővítését megkezdeni.

Husztai Gábor polgármester:

16 gyerek jön fel a bölcsődéből. Hányan jönnek szeptembertől és mennyi az összlétszám?

Gulyás Edit Judit óvodavezető:

Januártól jön 14 gyerek a 41-ből, a többi jön.

Husztai Gábor polgármester:

Akkor ez két csoport gyerek?

Gulyás Edit Judit óvodavezető:

25 gyerek ballagott el és 41 jön be.

Béres László alpolgármester:

Akkor szeptembertől nem lesz növekmény?

Husztai Gábor polgármester:

Ez teljesen értelmetlen. Át kell tekintenünk.

dr. Szakos Judit jegyző:

A létszámadatokat pontosan tisztázni szükséges.

Husztai Gábor polgármester:

Döntöttünk, és megyünk tovább. Lesz konténer, hívjuk az építészt. Jövő januárban lesz óvoda és fejlesztés nem lesz.

Asztalos Erika képviselő, a Pénzügyi Bizottság elnöke:

Lehet másik tervezőt javasolni?

Husztai Gábor polgármester:

A terv a tervező szellemi terméke. A konténer belső elosztását ki kell találni. A külső megjelenés beleillik a koncepcióba. A megnövekedett pedagóguslétszámot is el kell helyezni. göngyölődik a probléma.

Harmadik Napirendi pont:

**Asztalos Erika képviselő, a Pénzügyi Bizottság elnöke elhagyta a tanácskozótermet.
A határozatképességet tekintve az ülésen a továbbiakban jelenlévő képviselők száma: 5 fő.**

Husztai Gábor polgármester:

A Humánterületi Bizottság tárgyalta az előterjesztést, elnök asszony kérem az állásfoglalás ismertetésére.

Hozzászólások:

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

A Bizottság az előterjesztést megtárgyalta, nem volt megválaszolatlan kérdés.
Köszönjük az iskola tevékenységét a község életében. A tájékoztatást elfogadásra javasoltuk.

Husztai Gábor polgármester:

Igazgató asszonynak van-e kiegészítése? Ezzel kellett volna kezdeni.

Győrfi Lászlóné iskolaigazgató:

4,3 lett a tanév végi átlag. Sok kitűnő tanuló volt és közte sok felsős kitűnő. Nem volt gondunk hiányzásokkal sem. A kollégák között sok volt a helyettesítés, ennek betegség miatti távollét volt az oka.

A sok munka miatt az óvodával való együttműködés mértéke csökkent. A tornatermet viszont rendszeresen használják.

A Szülői Munkaközösség ősszel az iskolai szekrények felújítására szervezett bált, az alapítvány is segít. A Képviselő-testület-mint tulajdonos hozzájárulása kell ezeknek a több, mint 35 éves beépített szekrényeknek a felújításához.

Husztai Gábor polgármester:

Az iskolával az önkormányzat kapcsolata jó, partneri a viszonyunk. Megmutatták, hogy partnerek akkor, amikor annak kell lenni, ezt mutatja az előző napirendi pont is.

Méltányolják azt, amit az önkormányzat tesz az iskoláért és tenni fog a jövőben. Az óvoda-iskola kapcsolatban új elem a Hétpróba, ezen sokan részt vettek.

Fejlesztjük az iskola környékét, készen van a kosárlabdapálya felújítása, öltöző van a műfüves pálya mellett. Az óvodások tornaterem-használatának biztosítása is jó dolog, ismerkedhetnek a nagyobb óvodások az iskolával és helyiségeivel.

A tanulmányi versenyeken való szereplés kiemelendő, főleg a diákolimpiai helyezések.

A 4,3 átlag is komoly munkát és fejlesztést igazol.

Győrfi Lászlóné iskolaigazgató:

Fontos mutató, hogy minden 8. osztályos tanuló érettségit adó intézménybe nyert felvételt és 17 tanuló a 21-ből az általa megjelölt első helyre jutott be, sokan a Földes, a Fráter, a Lévy gimnázium tanulói lesznek.

Probléma újabban az iskola udvarán a randalírozás, sörösüvegeket találunk, egyéb szemetet minden reggel, kisebb rongálások is vannak.

Féltjük a kosárlabdapályát is. Úgy gondolom, a mostani eset kapcsán feljelentést tesztek.

dr. Szakos Judit jegyző:

A nagykapu általában nyitva van, késő este is.

Husztai Gábor polgármester:

Nagyon sok helyen lehet bemenni az iskolaudvarra és a kerítés is könnyen átmászható.

Vannak kamerák, majd meg fogjuk nézni, de aljegyző úr már úgy tájékoztatott, hogy elég jól látható. Együtt meg fogjuk majd nézni.

Lehet még további kamerákat is kitenni.

Az iskola pályázatokon való szereplését is szeretném kiemelni.

Asztalos Erika képviselő, a Pénzügyi Bizottság elnöke visszatért a tanácskozóterembe.

A határozatképességet tekintve az ülése a továbbiakban jelen lévő képviselők száma 6 fő.

A napirendi pont keretében egyéb hozzászólás, kérdés nem volt, annak megtárgyalását a polgármester lezárta, indítványára a Képviselő-testület egyhangúlag, 6 fő igen szavazatával, ellenszavazat és tartózkodás nélkül meghozta a következő határozatot:

**Szirmabesenyő Nagyközség Önkormányzata Képviselő-testületének
65/2018. (VI.20.) Kt. határozata az iskola oktató-nevelő munkájáról szóló tájékoztatóról**

Szirmabesenyő Nagyközség Önkormányzata Képviselő-testülete megtárgyalta a Szirmabesenyői Szinyei Merse Pál Általános Iskola és Alapfokú Művészeti Iskola oktató-nevelő munkájáról szóló tájékoztatóját és azt egyhangúlag, 6 fő igen szavazatával, ellenszavazat és tartózkodás nélkül elfogadta.

Husztai Gábor s. k.
polgármester

dr. Szakos Judit s. k.
jegyző

Husztai Gábor polgármester:

Nem volt benn képviselő asszony, mikor arról beszéltünk, hogy egy fél csoportnyi gyerek miatt jó döntést hoztunk-e. Az is kiderült, hogy a megjelent szülők között egy sem volt, akinek a gyermeke iskolaköteles lett volna és marad az óvodában.

Asztalos Erika képviselő, a Pénzügyi Bizottság elnöke:

Ezt egyeztettem a szülőkkel. Az lesz a megoldás, hogy a nagycsoportosokat kell kiemelni de az óvoda területén elhelyezni.

Husztai Gábor polgármester:

Aztán majd az lesz a szülők problémája, hogy nem lesz fejlesztés. Ebből a döntésből is tanulunk. Sokba fog kerülni.

Negyedik napirendi pont:

Husztai Gábor polgármester:

Kérdezem az intézményvezető, hogy van-e kiegészítése?

Gulyás Edit Judit óvodavezető:

Az úszásoktatás tapasztalata, hogy a gyerekek fele lemorzsolódott a nevelési év során. Ennek oka a szülői és a gyermeki magatartás. Természetesen köszönjük a lehetőséget az önkormányzatnak. Szeptembertől másképpen kellene megszervezni, intenzív formában. Nem minden pénteken mennék, hanem intenzív formában.

Nagyon jó oktatók vannak, jók a körülmények, ki kell használni. Vannak eredmények is, akik rendszeresen járnak, van, aki egyesületben úszik és érmekeket hoz.

Husztai Gábor polgármester:

Úgy kell szeptemberben meghirdetni, hogy hasznos legyen.

Ami program van, az legyen kötelező. Eddig nem így hirdettük.

A szülő legyen következetes és arra nevelje a gyermekét is, legyen felszerelés, és ne engedjen annak teret, ha éppen a gyerekeknek nincs kedve menni.

Szeptembertől úgy szerepeljen az intézmény, hogy ez egy olyan óvoda, ahol kötelező program az úszásoktatáson való részvétel.

Hozzászólások:

Asztalos Erika képviselő, a Pénzügyi Bizottság elnöke:

Az úszásoktatás szervezésével voltak gondok, nagyon sok idő elment rá, az egész délelőtt, két csoport járt, egymást megvárták, nem volt játék, nem volt csak egy kevés úszás és sokat kellett várni.

Husztai Gábor polgármester:

Ezek szerint 4 oktató kellett volna, hogy egyszerre legyen mindenkinek az oktatás és megfelelő vízfelület.

Szakos István képviselő, a Területfejlesztési Bizottság elnöke:

Ez nem a Képviselő-testület kompetenciája, nem a mi feladatunk, az intézmény szervezze meg.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

A Bizottság a beszámolót megtárgyalta és sok kérdés is felvetődött.

A testületre tartozik, hogy hatékony munka volt az óvodában, jó volt a kihasználtság a bölcsődében is, a személyi feltételek biztosítása nehézségekbe ütközött a betegségek miatti tartós távollétek kapcsán, de sikerült megoldani.

A tárgyi feltételek biztosítottak voltak.

Kiemelt problémának tartom, hogy a tanköteles korú gyermekek jó 40 %-a nem ment iskolába, ezt a kérdést pedagógiai szempontból meg kell vizsgálni, hogy mi az oka.

A pedagógusok szabadságának kiadása is gond, ezt meg kell oldani.

Az egészségügy vonatkozásában a gyermekorvossal és a védőnőkkel szorosabb kapcsolatot kell kialakítani.

Az iskola sokat tett azért, hogy az óvodásokkal megismertesse a programját, ehhez jó lenne, ha az óvoda is csatlakozna, elsősorban azzal, hogy az óvónők nézzék meg első osztályosként a volt óvodásaikat. Így könnyebben feltérképezhető közösen az a terület, ahol pedagógiai korrekció szükséges.

Az úszásoktatás megszervezése korosztályonként történjen, hogy hatékonyabb legyen.

Köszönjük az éves munkájukat és részvételüket a község életében.

A beszámolót a Bizottság elfogadásra javasolta.

Husztai Gábor polgármester:

Én most találkoztam először az egységes óvoda-bölcsőde megjelöléssel, nem láttam leírva.

dr. Rónai István aljegyző:

Pedig így van az alapító okiratban.

dr. Szakos Judit jegyző:

Az előterjesztésben az eredeti alapító okirat szerepel és abban pirossal a tervezett módosítás.

Husztai Gábor polgármester:

Jegyző asszonnyal egyeztetve az óvodától szeretnék kérni adatokat.

A bejáró gyerekek beiskolázása például mikor történik? Hogyan lett ezeknek a gyerekeknek a beíratása? Nyilván 94 fő létszámnál mondtam az intézményvezetőnek, hogy lehet felvenni körzeten kívüli gyereket, de mértékkel. A kihasználtság fontos, a rezsiköltség ugyanannyi, de a normatíva más a nagyobb gyereklétszámnál.

Évente 12 millió forintot teszünk az óvodához, idősebbek az óvoda pedagógusok, nagyobb a bérköltség.

A jövőre nézve ki kell vizsgálni, hogyan alakult így ez, hogy 18 körzeten kívüli gyerek van az óvodában és 16 tanköteles korú gyermek maradt vissza.

Hogyan alakulhat ez?

A Difer mérés központi, vagy az intézmény állítja össze?

Gulyás Edit Judit óvodavezető:

Ezt a mérést elvileg nem alkalmazzuk. Minden intézmény csinál viszont valamiféle szűrést.

A mai pedagógia álláspontja, hogy nem szabad szűrni a gyerekeket, főleg nem az óvodásokat.

Viszont a szülők felé meg kell mutatni a fejlődésüket.

Ez a mérés érzékszervi, szociális, tapasztalati következtetés, számolási készség, beszédképesség írásképesség vonatkozásában térképezi fel az alanyt.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

Ez egy sztemerd mérés. Kötelező első osztályosoknak.

Győrfi Lászlóné iskolaigazgató:

Az első osztályban október végéig kell választania a tanítónak, hogy melyik gyereket szeretné szűrni, mert szeretné alátámasztani, hogy milyen fejlesztésre van szüksége.

A szűrés alapján készül a fejlesztési terv, amit a tanév során alkalmaznak és áprilusra kiderül az eredménye.

Husztai Gábor polgármester:

Ha ez elsősökre vonatkozik, hogyan alkalmazza az óvoda és hogyan dönti el, hogy melyik gyerek iskolaérett?

Asztalos Erika mondta a Humánterületi Bizottság ülésén, hogy olyan kérdések voltak a felmérésben, amit szerinte csak iskolás gyerekeknek kell tudniuk. Az óvodások nem tudhatják, mert nem kaptak ilyen jellegű fejlesztést.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

Ez a mérés nagyon bonyolult munka, több órát vesz igénybe egy-egy gyerekre.

Akkor kell végezni, hogyha valamelyik gyerek vonatkozásában felmerül a gyanú, hogy fejlesztésre van szüksége. Például le van maradva a szókéncse. Melyik a gyerekeknek az a rész képessége, amelyik gyenge és melyik amelyik kiemelten erős.

Én ezt elkülöníteném az iskolaérettség vizsgálatától. Nem ugyanaz a kettő.

Gulyás Edit Judit óvodavezető:

Készségeket fejlesztünk. Viszont a szülők felé mutatnunk kell a gyermek fejlődését. Sokkal több gyerek maradt volna vissza, ha nem erősítjük a szülők felé a gyermekek képességeit. Ugyanezért beszéltem is több szülővel.

Husztai Gábor polgármester:

Ezt nem is értem. Egy önkormányzat nem lehet arra felkészülve, hogy évente egy-két csoportszobával bővítsen egy óvodát. Utána meg öt évig nem. Óriási gondok, alapvető pedagógiai problémák vannak egy óvodában, ha még ennél is több gyerek maradt volna vissza.

Gulyás Edit Judit óvodavezető:

Ezt kikérem magamnak és az óvónők nevében. Foglalkozunk a gyerekekkel. Ezt már többször mondtad, nem fogadom el.

Husztai Gábor polgármester:

16 gyereket tartottatok vissza, ebből trend lesz.

Gulyás Edit Judit óvodavezető:

A többi gyerek, aki iskolába megy, elmúlt 7 éves, ezért nem viszik a szülők a gyerekeket, hanem ők is visszatartják.

dr. Rónai István aljegyző:

Ez tehát nem mostani probléma, a visszamaradás?

Husztai Gábor polgármester:

Ez a probléma, hogy ebből trend lesz.

Ezt esetleg a 9 osztályos általános iskola tudja kezelni, amikor lesz egy nulladik évfolyam. 4-5 mindig visszamaradt, de 16 sosem.

Asztalos Erika képviselő, a Pénzügyi Bizottság elnöke:

A tankötelezettségre a május 31-i határidő volt a jó.

Ez a visszamaradás biztos, hogy máshol is megvan és gondot okoz.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

A mostani végzett 5. osztály volt az az évfolyam, ahol a törvény határozottan meghúzta a tankötelezettség határát, de 5 év alatt sokat lágyult a rendszer és a szülők találhattak nyomós okot arra, hogy szerintük a gyerek nem iskolaérett.

Egy szülő pedig talál okot.

Gulyás Edit Judit óvodavezető:

A szülő joga erős és az óvoda nem tud vele szembe szállni.

Husztai Gábor polgármester:

Te, mint intézményvezető kérheted a gyerek vizsgálatát.

Gulyás Edit Judit óvodavezető:

Három gyereknek van szakvéleménye a tizenhatból: egynek lelki problémái vannak, egy külföldre megy, a nyáriak szülei természetesnek vették, hogy marad a gyerek, ők nem is adtak be kérelmet.

De minden szülő azt mondta, hogyha nem engedélyezem, jönnek a polgármesterhez.

Husztai Gábor polgármester:

Én pedig visszaküldtem volna őket az intézményvezetőhöz.

Annyi probléma van az óvodával, mint azelőtt soha.

Gulyás Edit Judit óvodavezető:

A szülők, ha jöttek, polgármester úr nem küldte vissza őket, hanem engem rótt meg.

Husztai Gábor polgármester:

A 15 fős szülői értekezleten meg sem szólaltál Edit, én vezettem le az egészet.

Hagyjuk, mert sokat foglalkoztunk már az óvodával a mai ülésen is és évek óta. Az önkormányzat intézményfenntartó, a szakmai munka az intézményvezető felelőssége.

Gulyás Edit Judit óvodavezető:

Igen, a szakmai munka megfelelő, ezt bizonyítja két dolgozó szereplése a minősítésen, 96 és 98 % teljesítménnyel.

Husztai Gábor polgármester:

Ez nagyon jó, csak menjen is át a gyerekekkel való foglalkozás területére is. Képviselő asszony sem ezt tapasztalja a saját gyerekével.

dr. Szakos Judit jegyző:

Dönteni szükséges az óvodával kapcsolatos fenntartói intézkedésekről szóló határozat módosításáról is, az előterjesztés szerint.

A napirendi pont keretében egyéb hozzászólás, kérdés nem volt, annak megtárgyalását a polgármester lezárta, indítványára a Képviselő-testület egyhangúlag, 6 fő igen szavazatával, ellenszavazat és tartózkodás nélkül meghozta a következő határozatokat:

**Szirmabesenyő Nagyközség Önkormányzata Képviselő-testületének
66/2018. (VI.20.) Kt. határozata az óvoda-bölcsőde nevelő munkájáról szóló beszámolóról**

Szirmabesenyő Nagyközség Önkormányzata Képviselő-testülete megtárgyalta a Szirmabesenyői Napsugár Óvoda és Bölcsőde nevelő munkájáról szóló beszámolóját és azt egyhangúlag, 6 fő igen szavazatával, ellenszavazat és tartózkodás nélkül elfogadta.

Husztai Gábor s. k.
polgármester

dr. Szakos Judit s. k.
jegyző

Szirmabesenyő Nagyközség Önkormányzat Képviselő-testületének

**67/2018. (VI. 20.) Kt. határozata az óvodával kapcsolatos fenntartói döntésekről szóló
27/2018. (IV.9.) Kt. határozat módosításáról**

Szirmabesenyő Nagyközség Önkormányzata Képviselő-testülete egyhangúlag, 6 fő támogató szavazatával, ellenszavazat és tartózkodás nélkül úgy dönt, hogy az óvodával kapcsolatos fenntartói döntésekről szóló 27/2018. (IV.9.) Kt. határozatot a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény 13.§ (1) bekezdés 6. pontja alapján és a nemzeti köznevelésről szóló 2011. évi CXC. törvény 8.§ (1)-(2) bekezdéseiben foglaltak alapján az alábbiak szerint módosítja:

1. **A határozat 2. pontja helyébe a következő rendelkezés lép:**
Engedélyezett felvételi keretszám az óvodában (az Alapító okirat 6.2. pontjában foglaltak szerint): 150 fő
Engedélyezett felvételi keretszám a bölcsődében (az Alapító okirat 6.2. pontjában foglaltak szerint): 26 fő
2. **A határozat 6. pontja helyébe a következő rendelkezés lép:**
Az indítható óvodai csoportok száma: 5 csoport.

Az indítható bölcsődei csoportok száma: 2 csoport.

A határozat utasítja a jegyzőt a 27/2018. (IV.9.) Kt. határozatnak a módosítással egységes szerkezetbe foglalására és továbbítására az Oktatási Hivatal felé.

Határidő: azonnal

Felelős: polgármester, jegyző

Husztai Gábor s.k.
polgármester

dr. Szakos Judit s.k.
jegyző

Ötödik napirendi pont:

Husztai Gábor polgármester:

A jogszabály szerint megszűnt a köztisztviselők napjának munkaszüneti nap jellege.
Helyi szabályozás lehetséges, élni szeretnénk ezzel a lehetőséggel. Gondolom, a Humánterületi Bizottság foglalkozott vele.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

Nem foglalkoztunk vele bizottsági szinten, ez később készült előterjesztés, de elfogadásra javasolt mindenképpen.

A napirendi pont keretében egyéb hozzászólás, kérdés nem volt, annak megtárgyalását a polgármester lezárta, indítványára a Képviselő-testület egyhangúlag, 6 fő igen szavazatával, ellenszavazat és tartózkodás nélkül megalkotta a következő rendeletet:

Szirmabesenyő Nagyközség Önkormányzata Képviselő-testületének

13/2018. (VI.20.) önkormányzati rendelete

a közszolgálati tisztviselők napjáról

Szirmabesenyő Nagyközség Önkormányzata Képviselő-testülete a közszolgálati tisztviselőkről szóló 2011. évi CXCV. törvény 232/A. § (1) bekezdésében kapott felhatalmazás alapján az Alaptörvény 32. cikk (1) bekezdés a.) pontjában meghatározott feladatkörében eljárva a következőket rendeli el:

1.§

A Szirmabesenyői Polgármesteri Hivatal közszolgálati tisztviselői számára a Közszolgálati Tisztviselők Napja, július 1-je munkaszüneti nap.

2.§

A rendelet a kihirdetését követő napon lép hatályba.

Husztai Gábor s.k.
polgármester

dr. Szakos Judit s.k.
jegyző

Hatodik napirendi pont:

Husztai Gábor polgármester:

Döntések születtek a konzorciumban és a társulásban is, ezekhez szükséges a képviselő-testületek előterjesztés szerinti 2 határozata.

Az üléseken a polgármesterek a felmerült kérdéseikre választ kaptak.

A napirendi pont keretében egyéb hozzászólás, kérdés nem volt, annak megtárgyalását a polgármester lezárta, indítványára a Képviselő-testület egyhangúlag, 6 fő igen szavazatával, ellenszavazat és tartózkodás nélkül meghozta a következő határozatokat:

**Szirmabesenyő Nagyközség Önkormányzat Képviselő-testületének
68/2018. (VI.20.) Kt. határozata bérleti szerződés módosításának jóváhagyásáról**

†

Szirmabesenyő Nagyközség Önkormányzatának Képviselő-testülete megtárgyalta a „**Javaslat a Miskolc Térségi Konzorciumot képező tagönkormányzatok és a Miskolci Regionális Hulladékgazdálkodási Önkormányzati Társulás közötti bérleti szerződéssel kapcsolatos döntések meghozatalára**” című előterjesztést és egyhangúlag, 6 fő igen szavazatával, ellenszavazat és tartózkodás nélkül a következő határozatot hozza:

Tárgy: A Miskolc Térségi Konzorcium és a Miskolci Regionális Hulladékgazdálkodási Önkormányzati Társulás közötti bérleti szerződés 1. számú módosításnak elfogadása

Szirmabesenyő Nagyközség Önkormányzatának Képviselő-testülete a Miskolc Térségi Konzorcium és a Miskolci Regionális Hulladékgazdálkodási Önkormányzati Társulás között 2017. december 12. napján a 442.043/2017. iktatószámom létrejött bérleti szerződés 1 számú módosítását a határozat melléklete szerinti tartalommal elfogadja.

A bérleti szerződés módosítás érvényességének feltétele, hogy a bérbeadásra kerülő osztatlan közös vagyonnal kapcsolatos valamennyi döntést a konzorciumot alkotó települések önkormányzatának képviselő-testületei is meghozzák, és a határozati kivonatokat Miskolc Megyei Jogú Város Önkormányzata részére megküldésre kerüljenek, valamint további feltétele a Közreműködő Szervezet hozzájárulása.

Felelős: Polgármester

Határidő: azonnal

Husztí Gábor s.k.
polgármester

dr. Szakos Judit s.k.
jegyző

Ügyiratszám:

Bérleti szerződés 1.számú módosítása

amely létrejött egyrészről **Miskolc Térségi Konzorciumot képező tagönkormányzatok (a továbbiakban: Konzorcium) képviselőjében eljáró, az alábbiak szerint azonosított Gesztor önkormányzat**
megnevezése: Miskolc Megyei Jogú Város Önkormányzata
székhelye: 3525 Miskolc, Városház tér 8.
képviselőjében: Tarnóczy József Polgármester

adószám: 15735605-2-05
KSH azonosító: 15735605-8411-321-05
egyéb szervezeti azonosító: 735605

továbbiakban mint *Konzorcium, Bérbeadó*

másrészről

Miskolci Regionális Hulladékgazdálkodási

Önkormányzati Társulás

székhely: 3525 Miskolc, Városház tér 8.

törzskönyvi azonosító szám: 837523

KSH statisztikai számjel: 15837525-3811-327-05

képviselőjében: Dr. Kriza Ákos elnök

Miskolci Tibor alelnök

továbbiakban mint, *Bérlő*

között alulírott napon az alábbi feltételekkel:

1. A Miskolc Térségi Konzorciumot képező tagönkormányzatok (a továbbiakban: Konzorcium) és a Miskolci Regionális Hulladékgazdálkodási Önkormányzati Társulás között 2017. december 12. napján a 442.043/2017. iktatószámon bérleti szerződés jött létre. A bérleti jog biztosításának célja a Konzorcium osztatlan közös tulajdonában álló, a hulladékgazdálkodási közfeladat ellátását szolgáló vagyon egységes és hatékony a Társulás, mint közszolgáltatóval szerződő fél általi működtetésének, hasznosításának és nyilvántartásának biztosítása, a hulladékgazdálkodási közszolgáltatás hatékony ellátása és a közfeladat-ellátás feltételeinek biztosítása érdekében.

2. Az előzőekben meghatározott bérleti szerződés mellékleteinek felülvizsgálata okán a szerződés 1. és 4. számú mellékleteinek módosítása vált szükségessé.
3. Felek az 1. pontban megjelölt bérleti szerződés 1. számú mellékletét közös megegyezéssel az alábbiak szerint módosítják:
 - 3.1. az ISPA/KA 2000/HU/16/PE/004.,811 EGGEP beszerzés keretében a 45574 eszköz azonosító számon nyilvántartott hulladéklerakó-aprítógép és a 122070 eszköz azonosító számon nyilvántartott Miskolc, József Attila hulladékudvar/átrakó állomás a társasági és osztalékadóról szóló 1996. LXXXI. törvény szerinti értékcsökkenés kulcsa 10% -ról, 2% -ra módosul.
 - 3.2. ISPA/KA 2000HU/16/PE 004., 811 jármű beszerzés keretében a 48227 eszköz azonosító számon nyilvántartott Renault autó-tömörítőlapos h. a társasági és osztalékadóról szóló 1996. LXXXI. törvény szerinti értékcsökkenés kulcsa 10% -ról, 2% -ra módosul.
 - 3.3. az ISPA/KA 2000/HU/16/PE/004.,811 EGGEP beszerzés keretében a 45574 eszköz azonosító számon nyilvántartott hulladéklerakó-aprítógép használatba vételében dátuma 2010.06.01. napjáról 2007. 12.31. napjára módosul.
 - 3.4. az ISPA/KA 2000/HU/16/P/PE/004. egyéb gép berendezés 45230 eszközazonosító számon nyilvántartott Hulladéklerakó Törő-osztályozógép MFL törlésre kerül.
4. A Felek a bérleti szerződésnek a hulladékgazdálkodási közfeladat ellátását szolgáló vagyon használatáért fizetendő 2018. évi bérleti díjat tartalmazó 4. számú mellékletében megállapított nettó 579.759.058,-Ft bérleti díjat a bérleti szerződés 1. számú mellékletben rögzített TAO szerinti értékcsökkenési kulcsok változására tekintettel nettó 560.932.066,- Ft összegre módosítják.
5. Felek kijelentik, hogy jelen szerződésmódosítást 2018. január 1. napjára visszamenőleges hatállyal kötik meg.
6. Felek rögzítik, hogy a bérleti szerződés jelen módosítással nem érintett pontjai változatlan tartalommal érvényben maradnak, azokat magukra nézve továbbra is kötelezőnek ismerik el.
7. Jelen szerződésmódosítást a Felek elolvasták és kölcsönös értelmezés után, mint akaratuknak mindenben megfelelő helybenhagyólag aláírták.

Mellékletek:

- 1 számú melléklet: az ISPA/KA 2000/HU/16/P/PE/004. azonosítószámú „Miskolci Regionális Hulladékgazdálkodási Projekt” elnevezésű projekt során megvalósult Bérbeadó tulajdonában álló a bérlemény tárgyát képező egyes vagyonelemek
4. számú melléklet: induló bérleti díj

Kelt: Miskolc, 2018. évhónapnapján

.....
Miskolc Térségi Konzorcium

Bérbeadó képviselőjében

Tarnóczy József
polgármester

.....
**Miskolci Regionális Hulladékgazdálkodási
Önkormányzati Társulás**

Bérbeadó képviselőjében

Dr. Kriza Ákos
elnök

Miskolci Tibor
alelnök

Pénzügyi ellenjegyző: Miskolcon, 2018. évhónapnapján

.....
Polgári Mátyás
főosztályvezető
Gazdálkodási Főosztály

**Szirmabesenyő Nagyközség Önkormányzat Képviselő-testületének
69/2018. (VI.20.) Kt. határozata bérleti szerződés jóváhagyásáról**

Szirmabesenyő Nagyközség Önkormányzatának Képviselő-testülete megtárgyalta a „Javaslat a Miskolc Térségi Konzorciumot képező tagönkormányzatok és a Miskolci Regionális Hulladékgazdálkodási Önkormányzati Társulás közötti bérleti szerződéssel kapcsolatos döntések meghozatalára” című előterjesztést és (szavazati arány) a következő határozatot hozza:

Tárgy: A Miskolc Térségi Konzorcium és a REGIHU-HEJŐPAPI Kft. közötti bérleti szerződés elfogadása

Szirmabesenyő Nagyközség Önkormányzatának Képviselő-testülete a határozat melléklete szerinti tartalommal a Miskolc Térségi Konzorcium és a REGIHU-HEJŐPAPI Kft. közötti bérleti szerződést elfogadja.

A szerződés érvényességének feltétele, hogy a bérbeadásra kerülő osztatlan közös vagyonnal kapcsolatos valamennyi döntést a konzorciumot alkotó települések önkormányzatának képviselő-testületei is meghozzák, és a határozati kivonatok Miskolc Megyei Jogú Város Önkormányzata részére megküldésre kerüljenek, valamint további feltétele a Közreműködő Szervezet hozzájárulása.

Felelős: Polgármester

Határidő: azonnal

Husztai Gábor s.k.
polgármester

dr. Szakos Judit s.k.
jegyző

1.melléklet a 69/2018. (VI.20.) Kt. határozathoz

Ügyiratszám:

Bérleti szerződés

amely létrejött egyrészről **Miskolc Térségi Konzorciumot képező tagönkormányzatok (a továbbiakban: Konzorcium) képviselőtestületében eljáró, az alábbiak szerint azonosított Gesztor önkormányzat**
megnevezése: Miskolc Megyei Jogú Város Önkormányzata
székhelye: 3525 Miskolc, Városház tér 8.
képviseletében: Dr. Kriza Ákos elnök

adószám: 15735605-2-05
KSH azonosító: 15735605-8411-321-05
egyéb szervezeti azonosító: 735605

továbbiakban mint *Konzorcium, Bérbeadó*

másrészről

REGIHU-HEJŐPAPI Regionális Hulladéklerakó Korlátolt Felelősségű Társaság

székhelye: 3594 Hejőpapi, külterület 073/6 hrsz.
képviseli: Ladányi Roland ügyvezető
adószám: 26214973-2-05
cégjegyzékszám: 05-09-030469

továbbiakban mint *Bérlő*

között alulírott napon az alábbi feltételekkel:

I. Bevezető rendelkezések

1. A Miskolc Térségi Konzorciumot képező tagönkormányzatok (a továbbiakban: Konzorcium) és a Miskolci Regionális Hulladékgazdálkodási Önkormányzati Társulás között 2017. december 12. napján a 442. 043/2017. iktatószámom bérleti szerződés jött létre. A bérleti jog biztosításának célja a Konzorcium osztatlan közös tulajdonában álló, a hulladékgazdálkodási közfeladat ellátását szolgáló vagyon egységes és hatékony a Társulás, mint közszolgáltatóval szerződő fél általi működtetésének, hasznosításának és nyilvántartásának biztosítása, a hulladékgazdálkodási közszolgáltatás hatékony ellátása és a közfeladat-ellátás feltételeinek biztosítása érdekében.

A Konzorcium és a Társulás közötti bérleti szerződés mellékletében szerepel az ISPA/KA 2000/HU/16/P/PE/004. egyéb gép berendezés 45230 eszközazonosító számon nyilvántartott Hulladéklerakó Törő-osztályozógép MFL, amely nem a hulladékgazdálkodási közszolgáltatási feladat ellátását szolgálja, tekintettel arra, hogy az említett vagyontárgy a hulladékok hulladéklerakón való technológiai céllal történő - elsősorban inert hulladék - hasznosításhoz igénybe vett eszköz.

Jelenleg a Hejőpapi I. hulladéklerakót a REGIHU-HEJŐPAPI Kft. üzemelteti BO-08/KT/12660-3/2017, valamint BO-08/KT/9264-10/2017 és BO/16/15011-3/2016 számon módosított BO/16/367-3/2016 számon kiadott egységes környezethasználati engedély alapján.

Az alaphatározat I.1.C1 pontja alapján a REGIHU-HEJŐPAPI Kft. jogosult az inert hulladék hasznosításra, egyúttal a beszállított hulladékok megfelelő szemcseméretűre törésére és osztályozására.

II. A szerződés tárgya és a felek jogai és kötelezettségei

1. Felek rögzítik, hogy jelen szerződés alapján Bérbeadó Bérlőnek bérbe adja, Bérlő pedig a jelen szerződésben foglalt feltételek szerint bérbe veszi az *ISPA/KA 2000/HU/16/P/PE/004. azonosítószámú projekt* során megvalósult, beszerzett, Bérbeadó használatában álló jelen szerződés 1. számú mellékletében megjelölt törő és osztályozógépet (a továbbiakban: bérlemény)
2. A Bérlő rögzíti, hogy a fentebb hivatkozott számú ISPA/KA projekt támogatási szerződését, annak valamennyi mellékletére kiterjedően megismerte, és a jelen szerződés teljesítése során jogait és kötelezettségeit a támogatási szerződés előírásaira is tekintettel úgy gyakorolja, hogy a támogatott projekt rendeltetését betöltse.
3. Szerződő felek a bérleményi vagyonelemet tartalmazó mellékletre utalva rögzítik, hogy az adott melléklet tartalmazza a vagyonelem vonatkozásában az alábbiakat:
 - megnevezését,
 - a közhiteles nyilvántartásba vétel esetén a közhiteles nyilvántartásba feltüntetett azonosító számot vagy jelet,
 - az eszköz bruttó értékét
4. Bérbeadó a bérleményt Bérlő részére bérbe adja, aki azt bérbe veszi és vállalja annak jelen szerződés alapján történő működtetését és igénybevételét, továbbá a jelen bérleti szerződésben megállapított bérleti díj megfizetését.
5. A Bérlő feladata a bérlemény jogszabályoknak és előírásoknak, valamint Bérbeadó illetve tagönkormányzatai érdekeivel összhangban álló teljes körű, szakszerű, biztonságos és jó

gazda gondosságának megfelelő működtetése, rendeltetésszerű használata, hasznosítása, a vagyonvédelem biztosítása, továbbá a rendeltetésszerű használat mértékét meghaladó állagromlás és értékvesztés megakadályozása és megelőzése, valamint a bérlemény elemeiben bekövetkező változások folyamatos nyomon követése.

6. Bérbeadó kötelezettséget vállal arra, hogy kizárólagos bérleti és hasznosítási jogot biztosít Bérló számára a bérleményre, szavatolja, hogy más harmadik személynek olyan joga nem áll fenn a bérlemény tárgyán, amely annak Bérló általi használatát gátolná vagy akadályozná.
7. A Bérló a bérleményt a hulladékgazdálkodáshoz kapcsolódó feladatai ellátásához köteles bérbe venni és működtetni, továbbá Bérló tudomásul veszi, hogy a bérlemény tárgyát képező vagyonelem jelen pontban foglaltaktól eltérő célú felhasználása Bérló számára nem engedélyezett. Bérló az Nvtv. 11 § (11) bekezdés b) pontja alapján kifejezetten akként nyilatkozik, hogy a bérleményt a szerződési előírásoknak és a tulajdonosi rendelkezéseknek, valamint a jelen szerződésben meghatározott hasznosítási célnak megfelelően használja.
8. A bérlemény bármely jelen szerződésben foglalt céltól eltérő felhasználása kizárólag a Bérbeadó előzetes írásbeli jóváhagyása mellett történhet a vagyon működtetésére vonatkozó előírások betartás mellett. A jelen pont szerint engedélyezett egyéb bevételszerző tevékenység bevételeit Bérló köteles jogcímenként, elkülönítetten nyilvántartani. Az így realizált bevételeket, és a kapcsolódó költségeket, ráfordításokat elkülönítetten kell nyilvántartani és a jelen szerződés szerinti időszakos adatszolgáltatással együtt Bérbeadóval közölni.
9. A Bérló kijelenti, hogy a jelen szerződés szerinti tevékenysége ellátásához szükséges környezetvédelmi, hatósági engedélyekkel a szerződés fennállása alatt rendelkezik.
10. A Bérló kijelenti, hogy a jelen szerződésben vállalt kötelezettségei teljesítéséhez szükséges feladatok tartós, rendszeres, a jogszabályoknak és a vonatkozó előírásoknak, valamint a környezetvédelmi szempontoknak maradéktalanul megfelelő ellátásához szükséges személyi szakmai, tárgyi és technikai feltételekkel rendelkezik.
11. A Bérló az irat átvételétől számított 3 napon belül, köteles a Bérbeadót értesíteni minden olyan hatósági eljárásról, amely rendelkezést, kötelezést vagy ajánlást tartalmaz és a bérleményre, vagy annak valamely részére, elemére vonatkozik.
12. A Bérló köteles tőrni, hogy a Bérbeadó – vagy az általa felkért harmadik személy megbízásának igazolásával – a bérleményt (rendszeresen vagy belátása szerinti időpontban) legalább 1 munkanappal történő előzetes tájékoztatást követően ellenőrizze.
13. Az ellenőrzési jogosultság kiterjed a bérleményre, valamint az azokkal kapcsolatos iratok (szerződések, feljegyzések, hatósági iratok) megtekintésére, illetve azok másolatának igénylésére. Amennyiben a Bérbeadó az ellenőrzési tevékenységek során harmadik személy alvállalkozót vagy teljesítési segédet vesz igénybe, úgy a megbízott köteles meghatalmazó levéllel igazolni magát. A meghatalmazó levélnek tartalmaznia kell a harmadik személy azonosítását lehetővé tevő adatokat, a megbízás tárgyát, és az ellenőrzési tevékenység időtartamát.
14. A Bérló köteles minden olyan iratot –az irat elküldésével párhuzamosan- a Bérbeadó részére másolatban megküldeni, amellyel a bérleménnyel kapcsolatban bármely személy hatósághoz fordul (különösen építészeti hatóság, környezetvédelmi hatóság) vagy ezen hatóságoknál eljárást kezdeményez, illetve peres vagy nem peres eljárás keretében a bérleményre vonatkozó tulajdoni, használati, vagy birtokigény, vagy az ingatlan nyilvántartásba bejegyzett jogot, tényt vagy adatot tanúsít vagy befolyásol.

15. A Bérló a bérlemény átadásának időpontjától viseli a kárveszélyt.
16. A Bérló köteles a vagyont fenyegető veszélyről és a beállott kárról haladéktalanul értesíteni a Bérbeadót – ideértve azt az esetet is, ha őt harmadik személy a jogainak gyakorlásában akadályozza –, köteles továbbá tűrni, hogy a Bérbeadó a veszély elhárítására, illetőleg a kár következményeinek a megszüntetésére a szükséges intézkedéseket megtegye.
17. A Bérló vállalja a bérleti jog gyakorlásával kapcsolatos adminisztratív feladatok ellátást, így különösen a jelen szerződésben előírt beszámolási, nyilvántartási, adatszolgáltatási kötelezettségek teljesítését.
18. Bérló köteles a bérlemény megóvásáról gondoskodni, az ennek érdekében tett, halaszthatatlan intézkedéseiről Bérbeadót írásban tájékoztatni.
19. A bérlemény használatának teljesítésével összefüggő adatszolgáltatás rendszeres teljesítése és a jogszabályokban, valamint a vonatkozó engedélyekben meghatározott nyilvántartási rendszer működtetése a Bérló kötelezettsége.
20. A Bérló a bérlemény használatából működtetéséből, hasznosításából származó bevételeit valamint közvetlen költségeit és ráfordításait elkülönítetten köteles nyilvántartani olyan módon, hogy az a saját vagyonával folytatott egyéb bevételeitől, illetve költségeitől és ráfordításaitól egyértelműen elhatárolható legyen.
21. Bérló köteles a bérlemény karbantartásáról, őrzéséről, üzemképességének biztosításáról, tisztántartásáról és ápolásáról gondoskodni. A Bérló e kötelezettségeinek szakvállalattól elvárható gondossággal köteles eleget tenni. A jelen pontban foglalt kötelezettségek teljesítésének költségei Bérlőt terhelik.
22. A bérlemény felújításáról, pótlólagos beruházásáról vagyontárgy mindenkor tulajdonosa köteles gondoskodni. Az eszközpótlás mértékéről és rendezési módjáról a Bérló és a Bérbeadó az esedékesség időpontjában a hatályos jogszabályoknak megfelelően állapodik meg azzal, hogy ennek fedezetét a mindenkor tulajdonosa biztosítja.
23. A Bérló köteles minden év szeptember 30 napjáig a bérlemény tárgyát képező vagyontárgyaknak a következő év tételes illetve a második és harmadik év koncepcionális rekonstrukciós felújítási eszközpótlási és fejlesztési ütemtervére és ehhez kapcsolódóan az általa javasolt beruházások finanszírozásai igényére, figyelemmel az eszköz gazdaságilag hasznos élettartamára – Gördülő Beruházási terv – vonatkozó javaslatát elkészíteni és arról a mindenkor tulajdonost írásban tájékoztatni.
24. Felek megállapodnak abban, hogy a Gördülő Beruházási terv elfogadása érdekében együttműködnek, és egyeztetések útján rendezik vitás kérdéseiket. Tulajdonos írásbeli elfogadó nyilatkozata alapján a Gördülő Beruházási terv elfogadottnak tekintendő.
25. Felek megállapodnak abban, hogy a Gördülő Beruházási tervben elfogadott, de a Tulajdonos érdekkörében felmerülő okból elmaradó beruházások következményeiért Tulajdonos mentesíti, Bérlőt a harmadik személlyel szemben fennálló minden felelősség alól.
26. Felek megállapodnak abban, hogy a Gördülő Beruházási terv alapján megvalósuló pótlás, fejlesztés eredménye a Tulajdonos tulajdonába kerül.

27. A Bérelőnek a bérlemény tárgyát képező vagyona vonatkozóan adatszolgáltatási kötelezettsége van. A Bérelő évente egyszer, a tárgyévét követő év január 15.-éig köteles a bérlemény tárgyát képező vagyonelem állapotának tárgyévi változásairól leltárt készíteni és adatot szolgáltatni.
28. A Bérelő a mindenkor hatályos jogszabályi előírások és a jelen szerződésben foglalt feltételek szerint beszámolási, adatszolgáltatási kötelezettségei teljesítése érdekében is a bérlemény tárgyát képező vagyontárgyról külön egységes nyilvántartást vezet. A nyilvántartásban szerepel legalább:
 - a) a vagyontárgy megnevezése, műszaki jellemzői, tulajdonosa (i), a használat jogcíme
 - b) a vagyontárgyon elvégzett nagyobb hibaelhárítás és karbantartás, minden felújítás és rekonstrukció a műszaki tartalom és a ráfordítási érték megjelölésével,
 - c) a nagyobb hibaelhárítások és karbantartások vagyontárgyankénti nyilvántartása, mely tartalmazza legalább a hibaelhárítás helyét, idejét, műszaki jellemzőit,
29. A bérleményt képező vagyontárgyakra a Bérelő köteles a bérlet teljes időtartamára általános vagyonbiztosítási és felelősségbiztosítási szerződést kötni.

III. A bérleti díj

1. A szerződő felek megállapodnak, hogy a Bérelő a bérleti jogának ellentételezéseként évi két alkalommal bérleti díjat fizet. Az bérleti díj összegét a szerződés az 1. számú melléklete tartalmazza.
2. Bérleti díjfizetés módja, esedékessége: a Bérbeadó a szerződés szerint alkalmazandó bérleti díjra nézve minden év július 15. és december 31. napjáig köteles a Bérelővel a számviteli szabályoknak megfelelően kiállított – az alább meghatározott fizetési határidőt előíró – számlát közölni. A Bérelő a számlában előírt 90 napos fizetési határidőben köteles a bérleti díjat megfizetni a Bérbeadó által a jelen szerződésben foglalt előírások szerint meghatározott pénzforgalmi számlaszámra.
3. A bérleti díj a mindenkor érvényes általános forgalmi adóról szóló törvény szerint tartozik az általános forgalmi adó hatálya alá.

IV. A szerződés módosítása

A jelen szerződés módosítása csak írásban lehetséges a Ht. és a végrehajtására vonatkozó jogszabályok, valamint a Ptk. rendelkezéseinek megfelelően.

V. A szerződés megszűnése

1. Jelen szerződést a felek 2018. január 1. napjára visszamenőleges hatállyal határozatlan időtartamra kötik.
2. Jelen szerződés megszűnik továbbá:
 - a) A felek közös írásos megegyezésével
 - b) Bármely fél jogutód nélküli megszűnésével,

- c) A jelen szerződésben foglaltak szerinti rendkívüli felmondással, a felmondási idő lejártával
 - d) a teljesítés megkezdése előtti elállás folytán
 - e) jogszabályban meghatározott egyéb esetekben, így különösen az Nvtv. 11. § (12) bekezdésében meghatározott felmondás gyakorlása esetén
3. Bármely fél jogosult a jelen szerződést a másik félhez címzett írásbeli nyilatkozattal rendkívüli felmondás útján megszüntetni a másik fél súlyos szerződésszegése esetén.
 4. A felmondási idő 30 nap.
 5. A Bérelő részéről a szerződéses kötelezettségek súlyos megsértésének minősül különösen:
 - a. Bérelő ellen jogerős bírósági határozattal csőd-, felszámolási eljárás indul, vagy végelszámolás alá kerül;
 - b. Bérelő a tevékenység végzésére vonatkozó jogszabályi és szerződéses feltételeknek nem felel meg (engedélyét / engedélyeit visszavonják, nem hosszabbítják meg, nyilvántartásból törlik, tevékenységtől eltiltják, munkavédelmi, tűzvédelmi, környezetvédelmi és egyéb hatósági előírásoknak nem felel meg, vagy azokat nem tartja be) vagy hatósági ellenőrzés során vele szemben súlyos szabálysértést állapítanak meg;
 - c. A beszámolási vagy nyilvántartási, vagy adatszolgáltatási kötelezettségét Bérbeadó írásbeli felhívását követően sem teljesíti, vagy ennek során súlyos gondatlanságából eredően, vagy szándékosan valótlan adatokat tüntet fel, szolgáltat
 - d. Bérelő a bérleti díj megfizetésével 90 napon túl késedelembe esik és kötelezettségének írásbeli felszólítás ellenére, annak kézhez vételétől számított 15 napon belül nem tesz eleget;
 - e. A hatósági ellenőrzéseket, és/vagy a jelen szerződés alapján a Megrendelőt megillető ellenőrzési jogok gyakorlását akadályozza és azokat felszólítás ellenére sem teszi lehetővé
 - f. Ha a Bérelő a vagyonban különösen nagy kárt okoz és annak helyreállításáról nem gondoskodik
 - g. A jelen szerződésben meghatározott egyéb esetekben.
 6. A Bérbeadó részéről a szerződéses kötelezettségek súlyos megsértésének minősül különösen:
 - a) Bérelő szerződésszerű teljesítését, más módon, bizonyítottan és indokolatlanul akadályozza vagy a jelen szerződésben meghatározott kötelezettségét súlyosan megszegi és ezzel a Bérelőnek kárt okoz.
 8. Amennyiben Felek bármelyike, a jelen szerződésben foglalt kötelezettségét súlyosan megszegi, a másik fél írásban és részletesen köteles tájékoztatni a szerződésszegő felet a kötelezettségzegés tartalmáról és az elvárt, szerződésszerű intézkedés módjáról. A szerződésszegő fél köteles a szerződéses kötelezettségének ésszerű határidőn, de legkésőbb 60 napon belül eleget tenni, vagy a szerződésszegést más, a másik fél által elfogadható módon orvosolni.
 9. Amennyiben a szerződésszegő fél kötelezettségét a felszólítás ellenére sem teljesíti, a másik fél jogosult a jelen szerződést a határidő eredménytelen lejárta követő 6 hónapon belül írásban felmondani.
 10. Felek megállapodnak abban, hogy a jelen szerződés Bérelő hibájából történő megszűnése esetén a Bérelő köteles viselni a Bérbeadónak a bérlemény tulajdonosával szemben esetlegesen keletkező kötelezettségeinek elmulasztásából eredő kárát.

11. Felek megállapodnak abban, hogy a Szerződés bármely oknál fogva történő megszűnéséig, (megszűntetésig) kötelesek egymással teljes körűen elszámolni.
12. Az elszámolás keretén belül Bérelő köteles a folyamatos közszolgáltatás biztosításához szükséges, valamint jogszabályban előírt információkat, adatokat, illetőleg dokumentumokat átadni a Bérbeadónak.

VI. Vegyes és záró rendelkezések

1. Egyik fél sem követ el szerződésszegést, ha kötelezettségei teljesítését vis maior akadályozza meg, amely a Szerződés aláírásának időpontja után következett be.
2. Vis maior alatt értendők különösen elemi csapások, sztrájkok vagy egyéb munkahelyi zavargások, hadüzenettel indított vagy anélküli háborúk, blokádok, zendülés, lázadás, járványok, földcsuszamlások, földrengések, viharok, villámcsapások, áradások, zavargások, robbantások, valamint egyéb hasonló, előre nem látható események, amelyek mindkét fél érdekkörén kívül merülnek fel, és amelyeket a felek kellő gondoskodással sem tudnak kiküszöbölni.
3. A jelen szerződésre, alkalmazására és értelmezésére a magyar jogszabályokat kell alkalmazni.
4. Amennyiben a szerződő felek között a szerződés értelmezésével, teljesítésével, az állított szerződésszegéssel kapcsolatban bármilyen jogvita felmerülne, a szerződő felek a hatásköri szabályoktól függően, a Miskolci Járásbíróság vagy a Miskolci Törvényszék illetékességét kötik ki.
5. A szerződő felek kötelezik magukat arra, hogy a jelen szerződés teljesítése során tudomásukra jutott valamennyi információt, adatot, a szerződéssel összefüggésben keletkezett dokumentumok tartalmát üzleti titokként kezelik, azokat kizárólag a jelen szerződés céljaira használják fel, és csak azon munkatársaik számára teszik azokat megismerhetővé, akiknek a feladatai ellátásához azok megismerése szükséges, és írásban kötelezettséget vállaltak az üzleti titok megtartására. Az üzleti titok fogalma értelemszerűen nem foglalja magában azokat az információkat, adatokat stb., amelyek jogszabály alapján közérdekű vagy közérdekből nyilvános adat, felek bármelyike vagy a közvélemény előtt már ismertek voltak vagy később, a titoktartási kötelezettség megsértése nélkül váltak széles körben ismertté vagy megismerhetővé.
6. A jelen szerződés egyes rendelkezéseinek érvénytelensége esetén a szerződés egyéb részei érvényben maradnak. Az érvénytelen rendelkezést a felek érvényes, gazdasági szempontból a lehető legnagyobb mértékben egyenértékű rendelkezéssel váltják fel.
7. A felek képviselői kijelentik, hogy a jelen szerződés aláírására teljes körű felhatalmazással rendelkeznek.
8. A szerződés teljesítése során keletkező bármilyen szellemi alkotáshoz fűződő (szerzői jogi, iparjogvédelmi, stb.) jog a személyhez fűződő jogok kivételével a Bérbeadó kizárólagos tulajdonát képezi, a vagyoni jogok a Bérbeadót illetik meg, aki ezeket (fel)használhatja, módosíthatja, közzéteheti, továbbadhatja, vagy belátása szerint átengedheti, átruházhatja földrajzi vagy bármely más korlát nélkül.

Mellékletek:

- 2 számú melléklet: az ISPA/KA 2000/HU/16/P/PE/004. azonosítószámú „Miskolci Regionális Hulladékgazdálkodási Projekt” elnevezésű a Bérbeadó tulajdonában álló a bérlemény tárgyát képező vagyonelem

Kelt: Miskolc, 2018. évhónapnapján

.....
Miskolc Térségi Konzorcium
Bérbeadó képviselőjében

Dr. Kriza Ákos
elnök

.....
REGIHU-HEJŐPAPI Kft.
Bérlő képviselőjében

Ladányi Roland
ügyvezető

Pénzügyi ellenjegyző: Miskolcon, 2018. évhónapnapján

.....
Polgári Mátyás
főosztályvezető
Gazdálkodási Főosztály

Hetedik napirendi pont:

Husztai Gábor polgármester:

Magyar állami forrás terhére van kiírva, így részegységként tudjuk fejleszteni az óvodát, mivel a TOP-ba egységként benyújtott pályázatunk nem kapott támogatást.

A második napirendi pont keretében hozott döntés erre a projektre is hatással van, építészeti áttervezésre van szükség, a vezető óvónő, a pedagógiai asszisztens irodája és még mellette néhány

helyiség összevonódik, kijövünk az épületből a kerítés felé, de úgy, hogy ne legyen oldalhatáron álló az épület és lesz egy közel 100 m²-es összevont étkező, amit pufferként másra is tudnánk használni. Ezért érzem elhamarkodottnak a második napirendi ponti döntést. Nyilván az elvett helyiségeket máshol vissza kell adni, ez a játszóudvar felé lehetséges, ahová most konténereket készülünk tenni. A sportszobát a földszintre kell tenni, majd az irodák mennek a tetőtérbe., lehet, hogy ez lesz a következő döntés.

Minden összefügg mindennel. De nyilván pályázni kell és részletekben megvalósítani, ami egységként nem ment.

A Pénzügyi Bizottság állásfoglalását kérem.

Asztalos Erika képviselő, a Pénzügyi Bizottság elnöke:

A Bizottság tárgyalta az előterjesztést és elfogadásra javasolta, azzal a módosítással, hogy 2 millió forint az önerő maximuma és 95 % a pályázat támogatottsága.

Husztai Gábor polgármester:

5% önerőt kell biztosítani, az adóerő-képesség változása miatt ez valóban maximum 2 millió forint. Egyébként a projekt nem lesz 40 millió, 22-23 millió forint az építési költség, plusz a beszerzendő bútorzat költsége.

A napirendi pont keretében egyéb hozzászólás, kérdés nem volt, annak megtárgyalását a polgármester lezárta, indítványára a Képviselő-testület egyhangúlag, 6 fő igen szavazatával, ellenszavazat és tartózkodás nélkül meghozta a következő határozatot:

Szirmabesenyő Nagyközség Önkormányzata Képviselő-testületének

70/2018. (VI.20.) Kt. határozata az „Önkormányzati étkeztetési fejlesztések támogatására” szóló pályázat benyújtására

Szirmabesenyő Nagyközség Önkormányzata Képviselő-testülete az „Önkormányzati étkeztetési fejlesztések támogatására” szóló pályázat benyújtására vonatkozó előterjesztést megtárgyalta és egyhangúlag, 6 fő igen szavazatával, ellenszavazat és tartózkodás nélkül az alábbi határozatot hozza:

1. Szirmabesenyő Nagyközség Önkormányzata Képviselő-testülete támogatja az „Önkormányzati étkeztetési fejlesztések támogatására” szóló pályázat benyújtását.
2. A felújítással érintett cél: A Szirmabesenyői Napsugár Óvoda és Bölcsőde étkezőjének kialakítása (helyrajzi szám: 206/6)
3. A Képviselő-testület úgy dönt, hogy a pályázat benyújtásához szükséges 5 %-os saját erőt, maximum 2.000.000 Ft-ot biztosítja, amelynek fedezete a Szirmabesenyő Nagyközség Önkormányzata Képviselő-testületének a 2018. évi költségvetésről szóló 4/2018. (II.14.) önkormányzati rendeletében rendelkezésre áll.

4. A Képviselő-testület felhatalmazza a polgármestert, hogy a pályázat benyújtásához szükséges nyilatkozatokat tegye meg, a pályázati dokumentációt állítsa össze és nyújtsa be.

Felelős: polgármester

Határidő: azonnal

Husztai Gábor s. k.

polgármester

dr. Szakos Judit s. k.

jegyző

Nyolcadik napirendi pont:

Husztai Gábor polgármester:

Pénzügyi Bizottság tárgyalta. A szabályzatot egy szakértő cég csinálta, mintegy 100 oldalas anyag, az ASP pályázat lefinanszírozza. Ugyanakkor egy korábban elindított dolog. Pénzügyi Bizottság tárgyalta.

Hozzászólások:

Asztalos Erika képviselő, a Pénzügyi Bizottság elnöke:

A Bizottság tárgyalta és elfogadásra javasolta a határozat-tervezetet.

A napirendi pont keretében egyéb hozzászólás, kérdés nem volt, annak megtárgyalását a polgármester lezárta, indítványára a Képviselő-testület egyhangúlag, 6 fő igen szavazatával, ellenszavazat és tartózkodás nélkül meghozta a következő határozatot:

Szirmabesenyő Nagyközség Önkormányzata Képviselő-testületének

71/2018. (VI.20.) Kt. határozata a Szirmabesenyői Polgármesteri Hivatal Informatikai Biztonsági Szabályzatának elfogadása

Szirmabesenyő Nagyközség Önkormányzata Képviselő-testülete a Szirmabesenyői Polgármesteri Hivatal Informatikai Biztonsági Szabályzatának elfogadására vonatkozó előterjesztést

megtárgyalta és egyhangúlag, 6 fő igen szavazatával, ellenszavazat és tartózkodás nélkül az alábbi határozatot hozza:

1. Szirmabesenyő Nagyközség Önkormányzata Képviselő-testülete a Szirmabesenyői Polgármesteri Hivatal Informatikai Biztonsági Szabályzatát az 1. melléklet szerinti tartalommal, 2018. június 25-i hatállyal jóváhagyja.
2. A Képviselő-testület felkéri a jegyzőt, hogy a Szirmabesenyői Polgármesteri Hivatal Informatikai Biztonsági Szabályzatát a helyben szokásos módon hirdesse ki.

Felelős: polgármester, jegyző

Határidő: 2018. június 25.

Husztai Gábor s. k.
polgármester

dr. Szakos Judit s. k.
jegyző

Szirmabesenyői Polgármesteri Hivatal jegyzője

...../2018.
JEGYZŐI UTASÍTÁS

Szirmabesenyői Polgármesteri Hivatal

3711 Szirmabesenyő, Kossuth u. 5.

INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

érvényes:

.....

jóváhagyta:

.....

Dr. Szakos Judit jegyző

Dokumentum története

Verzió	Készült	Változás oka
1.0	2014.08.08.	első kiadás
1.1	2018.04.03.	ASP működési rend szabályozása

Bizalmas, belső használatú dokumentum

A szabályzat szerzői jogvédelem alatt áll, bármely részének felhasználása - a Hivatal kivételével - csak a jogtulajdonos IP Monitoring Kft. írásbeli engedélyével lehetséges.

A szerzői jog nem korlátozza a Hivatalt a szabályzat módosításában, publikálásában a szerzői jogra való hivatkozás megtartása mellett.

Tartalom

Az Informatikai biztonsági szabályzat	7
Célok	7
Felülvizsgálat	8
Hatály	9
Hatásköri és illetékességi szabályok	10
Szerepkörök, tevékenységek, felelőségek	10
Elektronikus információs rendszerek biztonsági osztályba sorolása, a Hivatal biztonsági szintje.....	16
ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK	18
1.1. HIVATALI SZINTŰ ALAPFELADATOK.....	18
1.1.1. Informatikai biztonsági szabályzat.....	18
1.1.2. Az elektronikus információs rendszerek biztonságáért felelős személy	18
1.1.3. Az intézkedési terv és mérföldkövei	19
1.1.4. Az elektronikus információs rendszerek nyilvántartása	20
1.1.5. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás	20
1.2. KOCKÁZATELEMZÉS	22
1.2.1. Kockázatelemzési és kockázatkezelési eljárásrend	22
1.2.2. Biztonsági osztályba sorolás	22
1.2.3. Kockázatelemzés	23
1.3. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS	27
1.3.1. Beszerzési eljárásrend	27
1.3.2. Erőforrás igény felmérés	27
1.3.3. Beszerzések	28
1.3.3.2. A védelem szempontjainak érvényesítése a beszerzés során	29
1.3.6. Külső elektronikus információs rendszerek szolgáltatásai	29
1.4. ÜZLETMENET- (ÜGYMENET-) FOLYTONOSSÁG TERVEZÉSE.....	30
1.4.1. Ügymenet-folytonosságra vonatkozó eljárásrend	30
1.4.2. Ügymenet-folytonossági terv informatikai erőforrás kiesésekre.....	30
1.4.2.4. Kritikus rendszerelemek meghatározása	32
1.4.3. A folyamatos működésre felkészítő képzés	32
1.4.5.3. Üzletmenet folytonosság elérhetőség	32
1.4.7. Infokommunikációs szolgáltatások	32
1.4.7.2. Szolgáltatás prioritási rendelkezések	33
1.4.8. Az elektronikus információs rendszer mentései	33
1.4.9. Az elektronikus információs rendszer helyreállítása és újraindítása.....	34
1.5. A BIZTONSÁGI ESEMÉNYEK KEZELÉSE	34
1.5.1. Biztonsági eseménykezelési eljárásrend	34
1.5.4. A biztonsági események figyelése	35
1.5.6. A biztonsági események jelentése	35
1.5.7. Segítségnyújtás a biztonsági események kezeléséhez	36
1.5.8. Biztonsági eseménykezelési terv	36
1.5.9. Képzés a biztonsági események kezelésére	38
1.6. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY - BIZTONSÁG	38
1.6.1. Személybiztonsági eljárásrend.....	38
1.6.2. Munkakörök, feladatok biztonsági szempontú besorolása.....	38
1.6.3. A személyek ellenőrzése.....	39
1.6.4. Eljárás a jogviszony megszűnésekor	40
1.6.5. Az áthelyezések, átirányítások és kirendelések kezelése	41
1.6.6. A Hivatallal szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények .	42
1.6.7. Fegyelmi intézkedések	43
1.6.8. Belső egyeztetés	43

1.6.9.	Viselkedési szabályok az interneten	44
1.7.	TUDATOSSÁG ÉS KÉPZÉS	47
1.7.1.	Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és az e célt szolgáló ágazati szervezetekkel	47
1.7.2.	Képzési eljárásrend	48
1.7.3.	Biztonság tudatosság képzés.....	48
1.7.4.	Belső fenyegetés	49
1.7.5.	Szerepkör, vagy feladat alapú biztonsági képzés	49
1.7.6.	A biztonsági képzésre vonatkozó dokumentációk	50
	FIZIKAI VÉDELMI INTÉZKEDÉSEK	51
2.1.	FIZIKAI ÉS KÖRNYEZETI VÉDELEM	51
2.1.2.	Fizikai védelmi eljárásrend	51
2.1.3.	Fizikai belépési engedélyek.....	52
2.1.4.	A fizikai belépés ellenőrzése	53
2.1.5.	Hozzáférés az adatátviteli eszközökhöz és csatornákhöz	54
2.1.6.	A kimeneti eszközök hozzáférés ellenőrzése.....	55
2.1.7.	A fizikai hozzáférések felügyelete	55
2.1.7.2.	Behatolás riasztás, felügyeleti berendezések	56
2.1.8.	A látogatók ellenőrzése	56
2.1.9.	Áramellátó berendezések és kábelezés.....	56
2.1.12.	Tűzvédelem	57
2.1.14.	Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem	57
2.1.15.	Be- és kiszállítás.....	57
2.1.16.	Az elektronikus információs rendszer elemeinek elhelyezése	59
2.1.19.	Karbantartók	59
2.1.19.3.	Időben történő javítás	60
	LOGIKAI VÉDELMI INTÉZKEDÉSEK	61
3.1.	ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK	61
3.1.1.	Engedélyezés	61
3.1.3.	Az elektronikus információs rendszer kapcsolódásai.....	61
3.1.3.2.	Belső rendszerkapcsolatok	61
3.1.3.3.	Külső kapcsolódásokra vonatkozó korlátozások.....	61
3.1.4.	Személybiztonság	61
3.2.	TERVEZÉS	62
3.2.2.	Rendszerbiztonsági terv	62
3.2.3.	Cselekvési terv	62
3.2.4.	Személyi biztonság.....	63
3.3.	RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS	64
3.3.2.	A rendszer fejlesztési életciklusa	64
3.6.	KONFIGURÁCIÓKEZELÉS	65
3.6.1.	Konfigurációkezelési eljárásrend.....	65
3.6.2.	Alap konfiguráció	66
3.6.7.	Legszűkebb funkcionalitás	66
3.6.8.	Elektronikus információs rendszerem leltár	67
3.1.3.3.	Duplikálás elleni védelem	68
3.6.10.	A szoftver használat korlátozásai	68
3.6.11.	A felhasználó által telepített szoftverek	69
3.7.	KARBANTARTÁS	69
3.7.1.	Rendszer karbantartási eljárásrend	69
3.7.2.	Rendszeres karbantartás	69
3.7.3.2.	Adathordozó ellenőrzés.....	70
3.7.4.	Távoli karbantartás	71

3.8.	ADATHORDOZÓK VÉDELME.....	71
3.8.1.	Adathordozók védelmére vonatkozó eljárásrend	71
3.8.2.	Hozzáférés az adathordozókhoz.....	72
3.8.4.	Adathordozók tárolása.....	72
3.8.5.	Adathordozók szállítása	72
3.8.5.2.	Kriptográfiai védelem.....	73
3.8.6.	Adathordozók törlése.....	73
3.8.7.	Adathordozók használata.....	74
3.8.7.2.	Ismeretlen tulajdonos	74
3.9.	AZONOSÍTÁS ÉS HITELESÍTÉS	74
3.9.1.	Azonosítási és hitelesítési eljárásrend	74
3.9.2.	Azonosítás és hitelesítés (hivatalon belüli felhasználók)	75
3.9.4.	Azonosító kezelés	75
3.9.5.	A hitelesítésre szolgáló eszközök kezelése	75
3.9.5.2.	Jelszó (tudás) alapú hitelesítés	76
3.9.5.3.	Birtoklás alapú hitelesítés.....	78
3.9.5.5.	Személyes vagy megbízható harmadik fél általi regisztráció.....	78
3.9.6.	A hitelesítésre szolgáló eszköz visszacsatolása	78
3.9.8.	Azonosítás és hitelesítés (hivatalon kívüli felhasználók)	78
3.9.8.	Hitelesítésszolgáltatók tanúsítványának elfogadása.....	78
3.10.	HOZZÁFÉRÉS ELLENŐRZÉSE	79
3.10.1.	Hozzáférés ellenőrzési eljárásrend	79
3.10.2.	Felhasználói fiókok kezelése.....	79
3.10.3.	Hozzáférés ellenőrzés érvényesítése	80
3.10.5.	A felelőségek szétválasztása.....	81
3.10.6.	Legkisebb jogosultság elve	81
3.10.6.2.	Jogosult hozzáférés a biztonsági funkciókhoz	82
3.10.6.3.	Nem privilegizált hozzáférés a biztonsági funkciókhoz	82
3.10.6.4.	Privilegizált fiókok	82
3.10.10.	A munkaszakasz zárolása	82
3.10.10.2.	Képernyőtakarás	83
3.10.11.	A munkaszakasz lezárása.....	83
3.10.12.	Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek.....	83
3.10.14.	Vezeték nélküli hozzáférés.....	83
3.10.15.	Mobil eszközök hozzáférés ellenőrzése.....	83
3.10.15.2.	Titkosítás	83
3.10.16.	Külső elektronikus információs rendszerek használata	84
3.10.16.2.	Korlátozott használat	84
3.10.16.3.	Hordozható adattároló eszközök.....	84
3.10.17.	Információ megosztás	84
3.10.18.	Nyilvánosan elérhető tartalom	84
3.11.	RENDSZER- ÉS INFORMÁCIÓ SÉRTETLENSÉG.....	85
3.11.2.	Rendszer- és információsértetlenségre vonatkozó eljárásrend	85
3.11.3.	Hibajavítás	85
3.11.4.	Kártékony kódok elleni védelem.....	86
3.11.4.3.	Automatikus frissítés	87
3.11.5.	Az elektronikus információs rendszer felügyelete	87
3.11.6.	Biztonsági riasztások és tájékoztatások.....	88
3.11.10.	Bemeneti információ ellenőrzés	88
3.11.12.	A kimeneti információ kezelése és megőrzése	88

3.12.	NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG.....	89
3.12.1.	Naplózási eljárásrend.....	89
3.12.2.	Naplózható események.....	89
3.12.3.	Naplóbejegyzések tartalma.....	89
3.12.8.	Időbélyegek.....	89
3.12.9.	A naplóinformációk védelme.....	90
3.12.11.	A naplóbejegyzések megőrzése.....	90
3.12.12.	Naplógenerálás.....	90
3.13.	RENDSZER- ÉS KOMMUNIKÁCIÓ VÉDELEM.....	90
3.13.1.	Rendszer- és kommunikáció védelmi eljárásrend.....	90
3.13.6.	A határok védelme.....	91
3.13.10.	Kriptográfiai kulcs előállítás és kezelése.....	92
3.13.12.	Együttműködésen alapuló számítástechnikai eszközök.....	92
3.13.22.	A folyamatok elkülönítése.....	92
	Kapcsolódó mellékletek.....	93
	Alapfogalmak.....	94

Az Informatikai biztonsági szabályzat

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (a továbbiakban lbtv.) kapott felhatalmazás alapján A Szirmabesenyői Polgármesteri Hivatal (továbbiakban Hivatal) Informatikai biztonsági szabályzatát az alábbiakban határozza meg.

- meghatározza a célokat, a szabályzat tárgyi és személyi hatályát;
- az elektronikus információbiztonsággal kapcsolatos szerepköröket;
- a szerepkörhöz rendelt tevékenységet;
- a tevékenységhez kapcsolódó felelősséget;
- az információbiztonság hivatalrendszerének belső együttműködését
- az elektronikus rendszerbiztonsággal kapcsolatos főbb területeket.

A szabályzatnak összhangban kell lenni a hatályos jogszabályokkal, köztük az alábbiakkal:

- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvénnyel,
- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet
- az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelettel,
- Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvénnyel.

Az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet értelmében a Hivatalnak csatlakoznia kell az önkormányzati ASP rendszer szakrendszereihez. A csatlakozás egyik feltétele, hogy a Hivatal teljesíti az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (továbbiakban: lbtv.) meghatározott követelményeket.

Mivel az ASP nem tartozik a hivatal saját hatókörébe, így az azzal kapcsolatos biztonsági követelmények megoszlanak a Hivatal és a szolgáltató/üzemeltető között.

A Hivatallal szemben elvárt követelményekkel kapcsolatban figyelembe kell venni a Magyar Állam Kincstár tájékoztatóit (pl. Tájékoztatás az önkormányzati ASP rendszerekhez csatlakozáshoz megvalósítandó informatikai biztonsági követelményekről). A Tájékoztató tartalmazza azokat a követelményeket, amelyeket kötelező jelleggel kell megvalósítani az ASP-hez történő csatlakozással. Ennek megfelelően jelen Informatikai biztonsági szabályzat az ASP csatlakozási projekt kapcsán kapott információk birtokában került felülvizsgálatra/elkészítésre. A jogszabály elvárja az önkormányzati ASP-hez történő csatlakozás után a szabályzat és az eljárásrendek szükség szerinti felülvizsgálatát, ismételt kihirdetését.

Célok

Az Informatikai biztonsági szabályzat célja, hogy a Hivatal számára értéket képviselő információk védelméről történő gondoskodást szabályozza. Az információ védelmének a célja, hogy biztosítsa az információ

- rendelkezésre állását (ahol, és amikor kell, az információ elérhető legyen)
- sértetlenségét (az információ legyen hiteles és autentikus)
- bizalmasságát (csak az arra jogosultak jussanak hozzá az információhoz)

A szabályzat meghatározza az információk védelméhez szükséges felelősségeket, feladatokat, folyamatokat és eljárásokat, valamint az általánosan betartandó informatikai üzemeltetési, információkezelési és viselkedési szabályokat.

A szabályzatban szereplő követelményeket, rendelkezéseket és ajánlásokat a hatályos jogszabályok keretei között kell használni.

A szabályozás célja a következő:

- a jogkövető magatartás és a jó hírnév érdekében védeni a szervezet értékeit,
- a tudatosság, a szervezettség, a hatékonyság és a technikai megoldások használata segítségével növelni az információbiztonságot,
- a megelőzés, a tájékoztatás, az oktatás, a felderítés és a szankcionálás eszközeivel segíteni az intézkedések érvényesítését.

Jelen szabályzat a Hivatal szervezeti szintű információbiztonsági szabályozó rendszerének egyik alapvető eleme. A hatályos jogszabályokkal, a Hivatal működési és ügyrendi előírásaival összhangban megteremti az elektronikus információs rendszerek és az azokban kezelt adatok biztonságát. Tartalmazza a Hivatal elektronikus információs rendszereivel kapcsolatba kerülő személyek felé támasztott minimum információbiztonsági követelményeket, továbbá meghatározza azokat az elvárásokat, kötelezettségeket és a felelősséget, amelyekre a biztonságos információellátás érdekében szükség van. Megfogalmazza azokat a biztonsági követelményeket is, amelyeket az önkormányzati ASP-hez való csatlakozással teljesíteni szükséges.

A Hivatal informatikai szolgáltatóival kötött szerződéseknek és azok mellékleteinek összhangban kell lenniük jelen szabállyal.

A célok elérése érdekében, az elektronikus információs rendszerek legmagasabb osztályba sorolt értékének megfelelően további eljárásrendek, részletszabályozások elkészítését a Hivatal vezetője rendelheti el, az elektronikus információs rendszerek biztonságáért felelős szakmai javaslatára. A részletszabályozásokat az elektronikus információs rendszerek biztonságáért felelős vagy a Hivatal vezetője által kijelölt személy készíti el, a rendszergazdával együttműködve, a Hivatal vezetője lépteti hatályba.

A Hivatal informatikai szolgáltatóival kötött szolgáltatási szerződéseknek és azok mellékleteinek összhangban kell lenniük jelen szabállyal.

Felülvizsgálat

A Hivatal az Informatikai biztonsági szabályzatot és hivatkozott eljárásrendjét folyamatosan fejleszti és tökéletesíti. A szabályzatot évente legalább egy alkalommal felül kell vizsgálni. A megfelelőségi vizsgálat kiterjed a szabályzat végrehajtásának, valamint a felmerülő informatikai, információbiztonsági és adatvédelmi eseményeknek és az ezekkel összefüggő biztonsági tevékenységeknek az ellenőrzésére.

A szabályzatot módosítani kell, ha a benne szereplő adatok megváltoztak, ha a Hivatal elektronikus információs rendszereinek működésében vagy a Hivatal elektronikus információs rendszereinek működését meghatározó jogszabályi környezetben változások következnek be. Módosítani kell továbbá az elavult informatikai technológiai megoldások kivezetése, és az új technológiai újítások bevezetése során.

A szabályzat felülvizsgálatának, módosításának kezdeményezése és a felülvizsgálat, valamint a módosítás elvégzése az elektronikus információs rendszerek biztonságáért felelős személy vagy a Hivatal vezetője által kijelölt személy feladata. A módosítások engedélyezése és az újabb változat jóváhagyása a Hivatal vezetőjének hatásköre.

Hatály

Az Informatikai biztonsági szabályzat a Hivatal egészére vonatkozik, **tárgyi hatálya** kiterjed a Hivatal birtokában levő összes olyan eszközre (például: hardver, szoftver és hálózati elemek, dokumentációk), amelyek az alaprendeltetésből adódó, a Hivatal ügyviteli tevékenységével kapcsolatos feladatok ellátását biztosítják. A tárgyi hatály alá esnek mindazon eszközök is, amelyek harmadik személyek birtokában vannak ugyan, de a fenti tevékenységek ellátását biztosítják. E tárgyi hatályt a Hivatal szolgáltatói, vállalászási vagy megbízási szerződések keretében érvényesítik. A szabályzat rendelkezik a Hivatal tevékenysége során feldolgozott, vagy azzal kapcsolatban keletkezett információk védelméről is, azok sértetlenségének, hitelességének és rendelkezésre állásának biztosításával, a hatálya kiterjed a kezelt, keletkezett információkra. A tárgyi hatály kiterjed azokra a hardver és szoftver elemekre, amely felhasználja, feldolgozza, felügyeli, ellenőrzi, tárolja, továbbítja a Hivatalnál keletkező vagy felhasznált adatokat, azaz a szakrendszerek használatához szükséges felhasználói (önkormányzati) munkaállomásokra, szoftverekre, nyomatkészítő eszközökre, kártyaolvasóra, és minden olyan egyéb eszközre, amely a munkavégzéshez szükséges, továbbá a rendszerelemek dokumentációira.

A szabályzat **személyi hatálya** kiterjed a Hivatal valamennyi, a Hivatal informatikai rendszeréhez hozzáféréssel rendelkező munkatársára, szerződéses partnerére (a Hivatal munkavégzésre irányuló bármely jogviszonyban álló természetes és jogi személyre), akik részt vesznek a Hivatalnál keletkező, tárolt, illetve továbbított adatok kezelésében. Harmadik személyekkel szemben a Hivatal a személyi hatályt szolgáltatói, vállalászási vagy megbízási szerződések keretében érvényesíti.

A szabályzat **szervezeti hatálya** a Hivatal valamennyi olyan szervezeti egységére kiterjed, amely a Hivatal elektronikus információs rendszereit használja, üzemelteti, fejleszti, továbbá ilyen tevékenységeket irányít és ellenőrzi. A szabályzat **területi hatálya** kiterjed A Szirmabesenyői Polgármesteri Hivatalra, valamint a Szervezeti és Működési Szabályzat szerinti, a 2013. évi L. törvény hatálya alá tartozó szervezeti egységeire, települési és nemzetiségi önkormányzatra.

Időbeni hatály: jelen Informatikai biztonsági szabályzat a kiadás napján lép hatályba, mellyel a korábbi Informatikai biztonsági szabályzat hatályát veszti.

Jelen szabályzat egyes követelményeinek hatályba lépési időpontja megfelel az adott követelményre a Hivatal Cselekvési tervében meghatározott határidőnek, összhangban a 2013. évi L. törvénnyel, a törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelettel, a Hivatalra és az elektronikus információs rendszereire érvényes biztonsági osztályhoz és szinthez előírt határidővel.

Új elektronikus információs rendszer bevezetése vagy már működő elektronikus információs rendszer fejlesztése során megállapított biztonsági osztályhoz tartozó követelményeket a használatbavételig teljesíteni kell.

Hatásköri és illetékességi szabályok

Az Informatikai biztonsági szabályzat és a kapcsolódó eljárásrendek, módszertanok, nyilvántartások kizárólag a Hivatal belső használatú dokumentumai, amelyeket a Hivatal elektronikus információs rendszerének felhasználói (a szabályzat személyi hatálya alá tartozók) kizárólag a rájuk vonatkozó követelmény szerint megismerhetnek, de azokat illetékteleneknek nem adhatják tovább.

Szerepkörök, tevékenységek, felelőségek

A Szirmabesenyői Polgármesteri Hivatal szervezeti szintű felépítését a Szervezeti és Működési Szabályzatban (SzMSz) rögzíti. Az elektronikus információs rendszer biztonsága érdekében történő, a Hivatalon belüli együttműködés jelen szabályzat tételes előírásain túl az érintett személyek önkéntes, szabálykövető magatartásán és biztonságtudatos, proaktív viselkedésén is alapul.

Az egyes kontrollfolyamatokban kötelező együttműködési szabályokat az eljárásrendek vonatkozó előírásai részletezik.

Általában minden érintett személy köteles:

- jelen szabályzat és kapcsolódó dokumentumok előírásait megismerni és magára nézve, nyilatkozat keretében kötelezőnek elismerni,
- az információbiztonsági tárgyú belső képzéseken részt venni,
- személyét érintő biztonsági ellenőrzéseket, auditokat tűrni, azokban az ellenőrző személyek kérése szerint részt venni,
- az általa biztonsági eseményként vélelmezett történéseket a felettes vezetőnek és/vagy az Elektronikus információs rendszer biztonságáért felelős munkatárs felé jelenteni.

Az Információbiztonsági szabályzat (és kapcsolódó dokumentumai) előírásainak betartása, betartatása, illetve a napi szintű munkavégzés során annak alkalmazása a dokumentum személyi hatálya pontban megjelöltek számára kötelező. A szabályok be nem tartása jogi, munkaügyi, illetve szerződésben meghatározott következményeket vonhat maga után. A szabályzat el nem olvasása nem mentesít a felelősség alól.

A Hivatali munkavégzéshez szükséges elektronikus információs rendszereket csak a hozzáférési jogosultság tudomásulvételét és a kapcsolódó szabályok megismerését igazoló nyilatkozat (Felhasználói titoktartási nyilatkozat) aláírása után lehet használatba venni.

Az információbiztonság megvalósítása, fenntartása, fejlesztése és ellenőrzése érdekében a Hivatal a feladatok és felelőségek tekintetében az alábbi szerepköröket azonosítja:

Szerepkör	Főbb felelősségek, tevékenységek
<p>az elektronikus információs rendszerek védelméért felelős vezető (a Hivatal vezetője, a jegyző)</p>	<ol style="list-style-type: none"> 1. biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését, 2. biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését, 3. az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg, 4. meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot, 5. gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról, 6. rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak, 7. gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről, 8. biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről, 9. ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek, 10. ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek, 11. felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért, 12. megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket, 13. a feladatokért a szervezet vezetője a 9. és 10. pontjában meghatározott esetben is felelős, kivéve azokat az esetköröket, amikor jogszabály által kijelölt központi adatkezelőt és adatfeldolgozó szolgáltatót kell a szervezetnek igénybe venni, 14. a jogszabály által kijelölt központi adatkezelő és adatfeldolgozó szolgáltató igénybevétele esetén a feltételek teljesítését a jogszabály által kijelölt központi adatkezelő és adatfeldolgozó szolgáltató úgy biztosítja, hogy közreműködik a szervezet és az elektronikus információs rendszer biztonságáért felelős személy feladatai ellátásában a jogkörébe tartozó tevékenységek tekintetében, a két szervezet közötti feladatmegosztást kétoldalú szolgáltatási szerződések biztosítják, amelyek a központi szolgáltató felett felügyeletet gyakorló miniszter vagy megbízottja ellenjegyzésével lépnek hatályba, 15. együttműködik a hatósággal a hatóság feladatainak elvégzésében, ennek során az lbtv. 12. § alapján: <ol style="list-style-type: none"> a) az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt, b) a szervezet Informatikai biztonsági szabályzatát tájékoztatás céljából megküldi, c) az ellenőrzés lefolytatásához szükséges feltételeket biztosítja a hatóság részére.

Szerepkör	Főbb felelősségek, tevékenységek
<p>az elektronikus információs rendszerek biztonságáért felelős személy (vállalkozási szerződés alapján külső szakértő)</p>	<ol style="list-style-type: none"> 1. feladata ellátása során a Hivatal vezetőjének közvetlenül adhat tájékoztatást, jelentést, 2. felel a Hivatalnál előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért, 3. gondoskodik a Hivatal elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról, 4. elvégzi vagy irányítja a 3. pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését, 5. előkészíti a Hivatal elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot, eljárásrendeket, terveket 6. előkészíti a Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását, 7. véleményezi az elektronikus információs rendszerek biztonsága szempontjából a Hivatal e tárgykört érintő szabályzatait és szerződéseit, 8. kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal, 9. a törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervezet, 10. biztosítja a törvényben meghatározott követelmények teljesülését a Hivatal valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők, ha a Hivatal az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők a törvény hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén. 11. a törvény szerinti feladatai és felelőssége a 10. pont szerinti esetekben más személyre nem átruházható, 12. jogosult az 10. pont szerinti közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelés alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot. 13. nyilvántartja az elektronikus információs rendszereket 14. nyilvántartást vezet a biztonsági incidensekről 15. nyilvántartást vezet az információbiztonsági és biztonsági eseménykezelési oktatásokról
<p>Elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy (megbízott felelős és/vagy az elektronikus információs rendszer biztonságáért felelős személy)</p>	<ol style="list-style-type: none"> 1. Feladata az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt kielégítő informatikai biztonsági rendszerrel kapcsolatos, a jegyző és az elektronikus információs rendszer biztonságáért felelős szakmai utasításainak megfelelő feladatok elvégzése.

Szerepkör	Főbb felelősségek, tevékenységek
<p>Megbízott szervezeti egység vezető (osztály/irodavezetők, hiányukban a Hivatal vezetője)</p>	<ol style="list-style-type: none"> 1. együttműködik az elektronikus információs rendszerek biztonságáért felelőssel, az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárások, szabályok, felelősségek, kötelező vagy tiltott tevékenységek, viselkedési szabályok meghatározásában. 2. gondoskodik arról, hogy a felelőssége alá tartozó szervezeti egység munkatársai megismerjék és betartsák a rájuk vonatkozó információbiztonsági követelményeket, szabályokat 3. közreműködik az elektronikus információs rendszerek biztonságáért felelős által tartott előző pontban megjelölt követelmények teljesülésének ellenőrzése során, 4. saját és a felelőssége alá tartozó munkatársak információbiztonsági, informatikai fennakadásról tett észrevételeit jelenti a rendszergazdának
<p>Adatgazda (szervezeti egység vezető)</p>	<ol style="list-style-type: none"> 1. meghatározza a hatókörébe tartozó elektronikus információs rendszerekhez, adatokhoz, tevékenységekhez hozzáférők körét, 2. engedélyezi a szükséges jogosultságokat a hatáskörébe tartozó elektronikus információs rendszerek, adatok, tevékenységek tekintetében (nyilatkoztatást követően), 3. a jogosultságok kiosztásánál törekedni kell a „legkisebb jogosultság” elvének érvényesítésére, vagyis mindenki a munkája elvégzéséhez szükséges jogosultságot kapja meg, 4. közreműködik az információbiztonsági kockázatok elemzésében.
<p>Rendszergazda (megbízott köztisztviselő)</p>	<ol style="list-style-type: none"> 1. felelős az elektronikus információs rendszerek felügyeletéért, az alkalmazások, a kiszolgálók és az alapszoftverek, az informatikai hálózat és a munkaállomások működésének folyamatos figyelemmel kíséréseért, az üzemeltetéshez szükséges dokumentációk kidolgozásáért, a törvényi előírásoknak megfelelő nyilvántartások vezetéséért és naprakészen tartásáért. 2. elvégzi és felügyeli az informatikai hálózat, számítógépek, eszközök biztonsági beállításait (pl. operációs rendszer, router beállítások), 3. telepíti és felügyeli a Hivatal munkájához szükséges szoftvereket, a Hivatal Szoftver Etikai Kódexében megfogalmazott elveknek megfelelően, 4. biztosítja a rendszerfelügyeletet, a felhasználói fiókok felügyeletét, 5. felügyeli a fizikai belépést ellenőrző eszközöket 6. az elektronikus információs rendszer biztonságáért felelős személlyel és az adatgazdákkal együttműködve kialakítja és működteti az adatokhoz, rendszerekhez való hozzáférési jogok rendszerét, 7. közreműködik az elektronikus információs rendszer biztonságáért felelőssel és az adatgazdákkal az információbiztonsági kockázatok elemzésében, 8. elvégzik a logok elemzését és jelentést készít róla az elektronikus információs rendszerek biztonságáért felelős felé 9. információbiztonsági incidens észlelése esetén haladéktalanul jelentést tesz az elektronikus információs rendszerek biztonságáért felelős felé, a biztonsági esemény elhárítását megkezdi, az eredményéről tájékoztatást nyújt az érintetteknek 10. saját hatókörében rendszeres fizikai és logikai karbantartásokat végez és dokumentál (karbantartásnapló), 11. az az elektronikus információs rendszer biztonságáért felelőssel közreműködve, meghatározza az információbiztonsági követelmények megvalósításához szükséges informatikai eszközöket, 12. elvégzi az időszakos mentéseket, szükség szerinti helyreállításokat, visszaállítási teszteket és jegyzőkönyvezi azokat, 13. hiba esetén elvégzi vagy felügyeli az eszközök javítását (a szerződésnek/a jegyző utasításának megfelelően vagy vele egyeztetve),

Szerepkör	Főbb felelőségek, tevékenységek
	<p>14. közreműködik az elektronikus információs rendszer biztonságáért felelőssel a BCP/DRP tervek kidolgozásában és megvalósításában,</p> <p>15. kidolgozza a hatáskörébe tartozó üzemeltetési eljárásokat,</p> <p>16. az elektronikus információs rendszer biztonságáért felelőssel egyeztetve vezeti az Informatikai biztonsági szabályzatban előírt nyilvántartásokat, vagy számára alap adatokat szolgáltat (a Hivatal vezetőjének utasítása szerint), pl.:</p> <ul style="list-style-type: none"> a) hardver/ szoftver nyilvántartás b) alapkonfiguráció nyilvántartása c) informatikai szolgáltatást nyújtó szerződött partnerek listája, d) jogosultságok nyilvántartása (eszközökhöz, rendszerekhez, felhasználói fiókok) e) jogosultságigények nyilvántartása f) hordozható eszközök listája, kiadott eszközök nyilvántartása g) karbantartások naplózása, karbantartást végzők listája h) szerverterembe történő belépés logolása i) minden egyéb olyan nyilvántartás, amelyet az elektronikus információs rendszer biztonságáért felelős vezető a hatáskörében előír, pl.: j) belépésre jogosultak listája (irodába, hivatali helyiségekbe) k) nyilvántartja a fizikai belépést ellenőrző eszközöket
<p>Felhasználók (a szabályzat személyi hatálya alá tartozók a közszolgálati jogviszony, a munkaviszony alapján foglalkoztatott munkatársak, a Hivatallal szerződéses kapcsolatban álló természetes és jogi személyek)</p>	<ol style="list-style-type: none"> 1. köteles az információbiztonsági szabályzatban rá vonatkozó szabályokat megismerni, elolvasni 2. betartja végrehajtja az elektronikus információbiztonsági szabályokat, utasításokat, magatartásával segíti a hatékony és biztonságos informatikai biztonság megteremtését, 3. együttműködik a Hivatalt érintő információbiztonsági kérdéskörökben felettesével és az elektronikus információs rendszerek biztonságáért felelőssel 4. haladéktalanul jelenti felettesének vagy a rendszergazdának, ha az informatikai rendszerben fennakadást, leállást, zavart, jogosulatlan hozzáférést észlel, ha információbiztonsági eseményt/incidenst észlel, 5. Információbiztonsági incidens esetén - ha az személyét érinti, vagy felettese erre felkéri - együttműködik a kivizsgálásban, 6. bizalmasan kezeli felhasználói azonosítóját, jelszavait, védett zónákba belépést biztosító kártyáit, kódjaikat, 7. köteles részt venni a Hivatalon belül szervezett információbiztonsági oktatásokon, illetve a jegyző utasítása szerint más külső oktatásokon, 8. a birtokában lévő, vagy tudomására jutott információkat bizalmasan kezeli, 9. felelőséggel tartozik a munkavégzése során az elektronikus információs rendszerben végzett feladatokért, a szakrendszerek szakszerű használatáért, 10. felelőséggel tartozik a munkavégzéséhez szükséges, számára kiadott eszközök megfelelő fizikai, logikai védelméért, 11. elszámoltatható minden olyan tevékenységért, amelyet bárki a számára kiadott azonosítói alapján végzett, 12. valamennyi üzemeltető, pl. az ASP központ működtetője által kiadott felhasználói biztonsági követelményeket köteles követni és betartani, 13. megtagadhatja az utasítást, ha annak végrehajtása jogszabályba, az informatikai biztonsággal kapcsolatos kiadott utasításba, szabályzatba ütközik, vagy megítélése szerint veszélyeztetné az informatikai biztonságot, 14. köteles az utasítást adó figyelmét felhívni és egyben kérheti az utasítás írásba foglalását, ha az, vagy annak végrehajtása jogszabályba vagy a kiadott informatikai biztonsággal kapcsolatos utasításba ütközne, vagy teljesítése kárt idézhet elő, és a felhasználó a következményekkel számolhat, vagy az utasítás

Szerepkör	Főbb felelősségek, tevékenységek
	<p>az érintettek jogos érdekeit sérti. Az utasítást adó felettes az utasítás írásba foglalását nem tagadhatja meg.</p> <p>15. Az utasítástól való eltérést felettesének azonnal jelezni kell.</p>
<p>Weblap fejlesztő, üzemeltető, tartalom felelős</p>	<p>Weblap fejlesztő:</p> <ol style="list-style-type: none"> a mindenkori OWASP top 10-es sérülékenységek ellenőrzése, a nyilvánosságra hozott hibák kijavítása, a weblap motor / telepített modulok folyamatos ellenőrzése, frissítése <p>Üzemeltető:</p> <ol style="list-style-type: none"> a védekezés külső (belső) támadás ellen, a használt szolgáltatások folyamatos frissítése karbantartása, lehetőség szerint a szolgáltatások verziószámainak elrejtése <p>A tartalom felelős (Hivatal által kijelölt munkatárs):</p> <ol style="list-style-type: none"> a jogszabályi követelményeknek megfelelően a tartalom ellenőrzéséért felelős által jóváhagyott tartalom feltöltési és karbantartási feladatok ellátása, a Hivatal weboldalán elsősorban hírközlő, információs, tájékoztató jellegű adatok közzlése (a település bemutatása, aktuális hírek, információk közzlése az állampolgárok számára), <p>A tartalom ellenőrzéséért felelős (Hivatal által kijelölt vezető vagy munkatárs):</p> <ol style="list-style-type: none"> a tartalom feltöltése előtt átvizsgálja és rendszeres időközönként ellenőrzi a nyilvánosan hozzáférhető elektronikus információs rendszertartalmat a nem nyilvános információk tekintetében és eltávolítja azokat.
<p>ASP Központ super adminisztrátor</p>	<ol style="list-style-type: none"> az önkormányzat által bérlő fiókonként, tenantonként kijelölt önkormányzati ASP adminisztrátor (tenant adminisztrátor) felvétele, annak adminisztrációja és karbantartása
<p>ASP adminisztrátor (tenant adminisztrátor)</p>	<ol style="list-style-type: none"> az önkormányzati ASP adminisztrátor feladata a bérlő fiók, tenant (önkormányzat, intézmény, nemzetiségi önkormányzat) szintű felhasználó kezelés, azaz. <ol style="list-style-type: none"> az adott tenant felhasználóinak felvétele és szakrendszeri szerepkör(ök)höz rendelése, annak adminisztrációja és karbantartása, intézményi kapcsolattartóként az adott tenant felhasználók tanúsítvány igénylésének adminisztrációja és karbantartása, illetve a tanúsítványokat hordozó tokenek csoportos átvétele és felhasználók közötti kiosztása, az önkormányzat szakrendszeri adminisztrátor(ok) feladata a szakrendszer szintű jogosultságkezelés, azaz a szolgáltatást igénybe vevő felhasználók számára a szakrendszeri jogosultságok beállítása, adminisztrációja és karbantartása.

Az információbiztonsággal kapcsolatos felelősségeket, tevékenységeket a munkaköri leírásokkal összhangba kell hozni.

Elektronikus információs rendszerek biztonsági osztályba sorolása, a Hivatal biztonsági szintje

A Hivatal az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 7. § (1) bekezdésében foglaltak alapján, valamint a törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet 1. és 2. sz. melléklete és a Kockázatkezelési eljárásrend alapján biztonsági osztályba kell, hogy sorolja saját elektronikus információs rendszereit, meg kell állapítania a Hivatal elvárt és aktuális biztonsági szintjét.

Az elektronikus információs rendszerek biztonságáért felelős személy feladata, hogy a rendszerek biztonsági osztályba sorolását elvégezze, a Hivatal biztonsági szintjét megállapítsa, *Biztonsági osztályba és szintbe sorolás mellékletben, Rendszerbiztonsági tervben vagy egyéb dokumentumban rögzítse*, szükség esetén jelen Informatikai biztonsági szabályzatot aktualizálja, a hatósági adatszolgáltatást előkészítse és a jegyző számára előterjessze. A biztonsági osztályba sorolást, a Hivatal vagy szervezeti egység biztonsági szintbe sorolását, az Informatikai biztonsági szabályzatot a Hivatal vezetője hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfeleléséért, a felhasznált adatok teljességéért és időszerűségéért, gondoskodik a módosított szabályzat életbe léptetéséről, az elektronikus információs rendszerek biztonságáért felelős személy közreműködésével az adatszolgáltatás teljesítéséről a Hatóság (Nemzeti Kibervédelmi Intézet Nemzeti Elektronikus Információbiztonsági Hatóság) által előírt módon.

A biztonsági osztályba sorolás eredményét a kizárólag az érintettek és a Hatóság számára hozzáférhető *dokumentum*, a [NEIH-OVI] *Osztályba sorolás és védelmi intézkedés*, a szintbe sorolás eredményét a [NEIH-SZVI] *Szintbe sorolás és védelmi intézkedés* űrlapok (illetve XML állományok) tartalmazzák.

Azokban az esetekben, amikor a Hivatal külső szolgáltatót, illetve jogszabály alapján kijelölt szolgáltatót vesz igénybe, a biztonsági osztályba sorolás a szolgáltató feladata, amelyről a Hivatal tájékoztatást kell, hogy kérjen. A Hivatalnak figyelembe kell vennie a külső szolgáltató, illetve jogszabály alapján kijelölt szolgáltató által meghatározott biztonsági osztály értékét, és a szolgáltatóval történő megállapodás (szerződés) vagy a tőle kapott tájékoztatás alapján a rá vonatkozó biztonsági követelményeket kell teljesítenie. A Hatóság részére a [NEIH-OVI] *Osztályba sorolás és védelmi intézkedés* űrlapot annak megfelelően kell kitöltenie a Hivatalnak, ami a szolgáltatóval kötött megállapodás vagy tájékoztatás alapján rá nézve teljesítendő

A 2013. évi L. törvény 9. § (4) bekezdésében foglaltak alapján a Hivatal biztonsági szintjének meghatározását az elektronikus információs rendszer felhasználásának módja határozza meg, jogszabályban meghatározott szempontok szerint (41/2015. (VII. 15.) BM rendelet 2. melléklet).

A biztonsági osztályba és szintbe sorolás eredményét új elektronikus információs rendszer be- és kivezetésekor, vagy az azzal összefüggő adatkezelési célok jelentős változása esetén, az elektronikus információs rendszer biztonságát érintő jogszabályban meghatározott változásakor, de legalább 3 évente felül kell vizsgálni.

A besorolás alapján a 41/2015. (VII. 15.) BM rendeletben a Hivatalra és az elektronikus információs rendszereire érvényes biztonsági osztályhoz és szinthez rendelt követelményeket és azok megvalósításának módját a következő fejezet tartalmazza (adminisztratív, fizikai és logikai védelmi intézkedések). Az intézkedések és sorszámaik a Hatósági elvárásoknak megfelelően megegyeznek a rendelet követelményeivel.

Ha a Hivatal az elektronikus információs rendszernek csak egyes elemeit vagy funkcióit üzemelteti vagy használja – részben vagy teljesen –, a rendeletben meghatározott követelményeket ezen elemek és funkciók tekintetében kell teljesíteni.

Külső szolgáltató, illetve jogszabály alapján kijelölt szolgáltató esetében az elektronikus információs rendszer nem tartozik a Hivatal saját hatókörébe, így az azzal kapcsolatos biztonsági követelmények megoszlanak a Hivatal és a szolgáltató/üzemeltető között. A Hivatal számára egységes biztonsági megfelelés van előírva, amely minimalizálja a kliens oldali kockázatokat.

Az ASP szakrendszerekre vonatkozó követelményekhez figyelembe vettük a jogszabály alapján kijelölt szolgáltatót biztonsági osztályba sorolását. Az új elektronikus információs rendszer bevezetése vagy már működő elektronikus információs rendszer fejlesztése során megállapított biztonsági osztályhoz tartozó követelményeket a használatbavételig teljesíteni kell.

Biztonsági osztályba sorolás eredménye:

Biztonsági osztályba és szintbe sorolás melléklet tartalmazza (1. sz. melléklet)

Elektronikus információs rendszerek biztonsági osztálya

Biztonsági szintbe sorolás eredménye:

Biztonsági osztályba és szintbe sorolás melléklet tartalmazza (1. sz. melléklet)

ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

Az ebben a fejezetben leírt adminisztratív védelmi intézkedéseket egységesen, valamennyi elektronikus információs rendszerre vonatkozóan kell megvalósítani.

1.1. HIVATALI SZINTŰ ALAPFELADATOK

1.1.1. Informatikai biztonsági szabályzat

A Hivatal vezetője megfogalmazza, dokumentálja és kihirdeti jelen Informatikai biztonsági szabályzatát. Jelen Informatikai biztonsági szabályzatot és eljárásrendet szükség szerint, de legalább évente egyszer az informatika biztonsági rendszer felülvizsgálata során felülvizsgálja, szükség szerint módosítja. Az informatikai biztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztével a szabályzatot újra vizsgálja, szükség szerinti módosítja. A módosítás az elektronikus információs rendszerek biztonságáért felelős személy szakmai irányításával történik. A Hivatal vezetőjének feladata biztosítani, hogy az Informatikai biztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható.

1.1.2. Az elektronikus információs rendszerek biztonságáért felelős személy

A Hivatal vezetője az elektronikus információs rendszerek biztonságáért felelős személyt nevez ki vagy bíz meg, aki: ellátja az állami és Hivatali szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott feladatokat (lbtv. 13. §).

A Hivatal vezetője gondoskodik a biztonságáért felelős személy képzettségéről, alvállalkozó esetén szerződésben elvárja azt. Adatszolgáltatási kötelezettsége kiterjed a vonatkozó munka-, megbízási vagy más szerződés hatóság felé megküldésére és a jogosultság igazolására.

Csak olyan személy végezheti az elektronikus információs rendszer biztonságáért felelős személy feladatait, aki:

- büntetlen előéletű (a büntetlen előélet követelményének való megfelelést az elektronikus információs rendszer biztonságáért felelős személy a szervezettel fennálló jogviszonya keletkezését megelőzően köteles igazolni, a Hivatal vezetője kötelezheti, hogy a fennálló jogviszonya alatt a büntetlen előélet követelményének való megfelelést igazolja).
- rendelkezik a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel, a Nemzeti Közszolgálati Egyetem továbbképzésén, éves továbbképzéseiben részt vesz, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet alapján.

A 2013. évi L. törvény alapján az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Az információbiztonság ellenőrzésével és irányításával kapcsolatos feladatait a Szerepkörök, tevékenységek, felelősségek pont tartalmazza.

Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet 11. § alapján az elektronikus információs rendszer biztonságáért felelős személy – ideértve az információbiztonsági szolgáltatást nyújtó vállalkozás tagjait és alkalmazottait is – az érintett szervezet igényeihez igazodva és annak rendelkezése szerint feladatát elláthatja:

- a) részmunkaidőben,
- b) a vonatkozó szerződésben meghatározott időtartamban, vagy
- c) több érintett szervezetnél.

Az elektronikus információs rendszerek védelméért felelős személy az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet alapján képzésre és éves továbbképzésre kötelezett.

A Hivatal vezetője a Nemzeti Kibervédelmi Intézet Nemzeti Elektronikus Információbiztonsági Hatóság számára, az lbtv. 11. § (1) bekezdés c) pontjában meghatározott, az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt.

1.1.3. Az intézkedési terv és mérföldkövei

A Hivatal vezetője az informatikai biztonsági követelmények megvalósításához az lbtv.-ben meghatározott határidőkkel Intézkedési tervet (*Cselekvési terv*) készít, amennyiben a meghatározott biztonsági osztálynál/szintnél hiányosságot állapít meg, ha valamely védelmi intézkedés nem valósul meg, vagy a bevezetett kontroll hibás, és ezekhez határidőket rendel.

A Cselekvési tervet szükség szerint, de legalább évente egyszer az informatikai biztonsági rendszer felülvizsgálata során (belső audit) felül kell vizsgálni, szükség szerint aktualizálni a kockázatkezelési stratégia és a kockázatokra adott válaszok, tevékenységek prioritása alapján (jellemzően a nagy kockázattal járó hiányosságokat kell előtérbe helyezni). Az informatikai biztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor a Cselekvési tervet újra felül kell vizsgálni, szükség szerinti módosítani. Ha az adott elektronikus információs rendszerre vonatkozó biztonsági osztály meghatározásánál (belső vagy külső vizsgálat során) hiányosság kerül megállapításra, vagy a meghatározott biztonsági szint alacsonyabb, mint az elvárt biztonsági szint akkor a Hivatal vezetője a vizsgálatot követő 90 napon belül felülvizsgálatot készít, a hiányosság megszüntetése érdekében.

A kitűzött feladatok megvalósulását a Cselekvési tervben a Hivatal vezetője az elektronikus információs rendszer biztonságáért felelős közreműködésével nyomon követi és dokumentálja.

A jegyző feladata biztosítani, hogy a Cselekvési tervben meghatározott intézkedéseket bevezesse, az azokhoz szükséges erőforrásokról gondoskodjon.

Mivel az intézkedési terv (Cselekvési terv) bizalmas információkat tartalmaz, ezért ezt csak a jegyző, a biztonságért felelős, és az általuk kijelölt személyek, valamint az ellenőrzésre jogosult hatóságok ismerhetik meg.

1.1.4. Az elektronikus információs rendszerek nyilvántartása

Az elektronikus információs rendszer biztonságáért felelősnek az elektronikus információs rendszerekről nyilvántartást kell vezetni, azt szükség szerint aktualizálni.

A nyilvántartásnak tartalmaznia kell:

- a. az információs rendszer alapfeladatait;
- b. a rendszerek által biztosítandó szolgáltatásokat;
- c. az érintett rendszerekhez tartozó licenc számot (amennyiben azok a Hivatal kezelésében vannak);
- d. a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;
- e. a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.

Az elektronikus rendszerek nyilvántartását egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban vagy elektronikus nyilvántartásban kell kezelni.

1.1.5. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás

Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, a Hivatal hatáskörébe tartozó:

- emberi, fizikai és logikai erőforrásra,
- eljárási és védelmi szintre és folyamatra

A fizikai és logikai jogosultságok engedélyezése az alábbiakat foglalja magába:

- a. melyek a jogosultsággal rendelkező személyek felelősségei, velük szembeni szabályok, követelmények
- b. hogyan történik az elektronikus információs rendszerhez való hozzáférés engedélyezése, jogosultság adás
- c. melyek a rendszer jogosultsági szintjei (biztonsági zónák védelme, minimum jogosultság, privilegizált, stb), mit tartalmaznak az egyes jogosultsági szintek
- d. melyek a legkisebb jogosultság elve alapján, a jogosultsági körök
- e. kik az elektronikus információs rendszerhez hozzáféréssel rendelkező személyek és milyen jogosultságaik vannak, kik rendelkeznek/rendelkezhetnek privilegizált jogosultsággal
- f. melyek azok a tevékenységek, amelyek az elektronikus információs rendszer használata során engedélyezettek, illetve tiltottak
- g. hogyan történik a jogosultsággal rendelkező személyek nyilatkoztatása (biztonsági szabályok és kötelezettségek megismerése)
- h. hogyan történik a jogosultság visszavonás

Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárást (a jogosultságok kiosztását és visszavonását) az *Informatikai biztonsági eljárásrend* vagy egyéb dokumentum tartalmazza, illetve az engedélyezések a további védelmi intézkedések alatt kerülnek részletezésre (pl. 1.6.4. Eljárás a jogviszony megszűnésekor).

Ha a kockázatkezelés keretében, vezetői feladatszabás következtében vagy egyéb igény nyomán az információbiztonsággal kapcsolatos folyamatok, eljárások és dokumentumok változtatása válik szükségessé, a módosítást kezdeményező személy a javaslatot az elektronikus információs rendszer biztonságáért felelős elé terjeszti, aki – a javaslatok mérlegelése és elfogadása után – átvezeti a módosításokat a dokumentumokon. Beszerzést, belső erőforrások átcsoportosítását igénylő, biztonsági osztályba és szintbe sorolás változását jelentő módosítások jóváhagyása a Jegyző jogköre, ilyen esetekben az elektronikus információs rendszer biztonságáért felelős az előterjesztő.

Az egyes dokumentumok változásának követése céljából valamennyi irat elején fel kell tüntetni a változásokat nyilvántartó táblázatot a következő adattartalommal, :

- Verzió
- Készült (dátum)
- Változás oka
- Jóváhagyta
- Hatálybalépés dátuma

Hatósági engedélyezés szükséges, ha a Hivatal az elektronikus információs rendszerre a jogszabályi alapértelmezettnél alacsonyabb biztonsági osztályt kíván megállapítani. A Hatóság felé írásbeli kérelmet kell benyújtania, a kérelemhez csatolni kell az eltérő biztonsági osztályba sorolás alapjául szolgáló kockázatelemzés dokumentációját.

Az Ibtv. 3. § (2) - (5) bekezdése lehetőséget ad arra, hogy a Hivatal egyes elektronikus információs rendszereit Magyarország területén kívül üzemeltesse, illetve azokban külföldön végezzenek adatkezelést. A Hivatal az adatkezelés kezdetét legalább 90 nappal megelőzően írásbeli kérelmet nyújthat be a Hatóságnak. A kérelemhez csatolni kell:

- a. az EGT tagállamaiban történő adatkezelés indokát,
- b. az EGT tagállamaiban kezelt adatok és adatbázisok leírását,
- c. azt, hogy az adatkezelő rendszer, valamint üzemeltetője nevesített-e, és az adatkezelés jogszabályi megfeleléséért felelős személy neve, beosztása, elérhetősége ismert-e,
- d. az adatkezelő rendszer technikai és technológiai leírását, ideértve a hardver- és szoftverkomponenseket is,
- e. az adatkezelő rendszer információbiztonságának ismertetését, a rendszerhez kapcsolódó, továbbá az üzemeltetőre vonatkozó belső szabályozásokat és utasításokat,
- f. a kötelezően lefolytatandó biztonsági rendszerfelülvizsgálat eredményét,
- g. a magyar információvédelmi szabályok megtartásáról szóló üzemeltetői nyilatkozatot,
- h. azt, hogy az üzemeltetés helyszínén illetékes hatóságok jogosultak-e a kezelt adatokba betekinteni.

Nem szükséges a hatóság engedélye, ha a külföldi adatkezelést vagy üzemeltetést nemzetközi szerződés írja elő.

1.2. KOCKÁZATELEMZÉS

1.2.1. Kockázatelemzési és kockázatkezelési eljárásrend

A Hivatal vezetője a helyes módszertan szerinti kockázatkezelést és az ehhez kapcsolódó ellenőrzések megvalósítását elősegítő eljárást Kockázatkezelési eljárásrendben határozza meg. A törvényi célok teljesítése, a munkatársak, a lakosság és a partnerek bizalmának megtartása érdekében biztosítja az információk kockázatarányos kezelését, ennek érdekében minden munkatárs számára tudatossá kell válnia az információbiztonság fontosságának és a Hivatalnak ezen egységes értelmezése alapján kell tevékenykednie az információbiztonság érdekében.

Ez vonatkozik különösképpen az új, innovatív informatikai technológiák hasznosítására. Valamennyi alapfeladatot ellátandó terület saját felelősséggel bír az általa hasznosított és feldolgozott információk biztonságáért és megfelelő védelméért azok értékének és kockázatának megfelelően, ez a felelősség magában foglalja az egyes személyeknek az információk használatával kapcsolatosan felmerülő elszámoltatási kötelezettségét is.

1.2.2. Biztonsági osztályba sorolás

A Hivatal annak érdekében, hogy az lbtv. hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen - az elektronikus információs rendszerek biztonságáért felelős személy irányításával - jogszabályban meghatározott szempontok, kockázatelemzés alapján megvizsgálja (alvállalkozó igénybevétele esetén megvizsgáltatja) elektronikus információs rendszereit és meghatározza, hogy azok melyik biztonsági osztályba sorolandók. melynek eredményét a kizárólag az érintettek számára hozzáférhető *Elektronikus információs rendszerek biztonsági osztálya, Rendszerbiztonsági terv* vagy egyéb dokumentum, és a rendszerenként a [NEIH-OVI] *Osztályba sorolás és védelmi intézkedés űrlap*-ok tartalmazzák.

Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást kockázatelemzés alapján kell elvégezni. A kezelt adatok és a funkciók figyelembe vételével a lehetséges kármértéket kell megállapítani, míg a kár bekövetkezésének valószínűsége a körülmények mérlegelésével becsülhető. A biztonsági osztályba soroláskor figyelembe veendő káreseményeket a 41/2015. (VII. 15.) BM rendelet 1 melléklet 2. pontja rendeli az egyes biztonsági osztályokhoz.

Azokban az esetekben, amikor a Hivatal külső szolgáltatót, illetve jogszabály alapján kijelölt szolgáltatót vesz igénybe, a biztonsági osztályba sorolás a szolgáltató feladata, amelyről a Hivatal tájékoztatást kell, hogy kérjen. A kockázatelemzés és kockázatkezelés során a Hivatalnak figyelembe kell vennie a külső szolgáltató által meghatározott biztonsági osztály értékét.

A biztonsági osztályba sorolás alkalmával – az érintett elektronikus információs rendszer vagy az általa kezelt adat bizalmosságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján – 1-től 5-ig számozott fokozatot kell alkalmazni, a számozás emelkedésével párhuzamosan szigorodó védelmi előírásokkal együtt (a 41/2015 [VII.15.] BM rendelet iránymutatása alapján). Az elektronikus információs rendszer biztonsági osztálya alapján kell megvalósítani az előírt védelmi intézkedéseket az adott elektronikus információs rendszerre vonatkozóan.

A jegyző a törvényben meghatározott feltételeknek megfelelő, az elektronikus információs rendszerre irányadó biztonsági osztálynál magasabb, kivételes esetben a hatóság előzetes engedélyével, kockázatokra kiterjedő indoklással ellátva alacsonyabb biztonsági osztályt is megállapíthat az elektronikus információs rendszerre vonatkozóan.

Azokat a kontrollokat, amelyek nem valósulnak meg, kockázatelemzés útján prioritásukat tekintve intézkedési tervben (Cselekvési tervben) kell kezelni.

A biztonsági osztályba és biztonsági szintbe sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni. A soron kívüli biztonsági osztályba és szintbe sorolást az elektronikus információs rendszer biztonságát érintő jogszabályban meghatározott változás vagy új elektronikus információs rendszer bevezetése esetén, ill. a szervezet státuszában, szervezetében, ill. az általa kezelt vagy feldolgozott adatok vonatkozásában bekövetkezett változás esetén szükséges elvégezni.

Az elektronikus információs rendszerek biztonságáért felelős személy vagy a Hivatal vezetője által megbízott személy feladata, hogy a rendszerek biztonsági osztályba sorolását elvégezze, a Hivatal és szervezeti egységeinek biztonsági szintjét megállapítsa, *Biztonsági osztályba és szintbe sorolás* mellékletben vagy egyéb dokumentumban rögzítse, szükség esetén jelen Informatikai biztonsági szabályzatot aktualizálja, a hatósági adatszolgáltatást előkészítse és a jegyző számára előterjessze.

A Hivatal és szervezeti egységei által használt informatikai rendszerek biztonsági osztályba sorolásait, a Hivatal vagy szervezeti egység biztonsági szintbe sorolását, az Informatikai biztonsági szabályzatot a Hivatal vezetője hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfeleléséért, a felhasznált adatok teljességéért és időszerűségéért, gondoskodik a módosított szabályzat hatályba léptetéséről, az érintettekkel való megismertetéséről, az elektronikus információs rendszerek biztonságáért felelős személy közreműködésével az adatszolgáltatás teljesítéséről a Hatóság (Nemzeti Kibervédelmi Intézet Nemzeti Elektronikus Információbiztonsági Hatóság) által előírt módon (feltöltés a NEIH hivatali kapujára vagy tömörített, titkosított/jelszóval védett állomány elküldése).

1.2.3. Kockázatelemzés

Az információbiztonság területén fellépő kockázatokat az elektronikus információs rendszer biztonságáért felelős az adatgazdák és a rendszergazda bevonásával értékeli és teszi meg az intézkedési javaslatait a kockázatok kezelésére a jegyző felé. A Hivatalnak évente legalább egyszer dokumentált módon végre kell hajtania a biztonsági kockázatelemzéseket jelen szabályzat vagy a Kockázatelemzési és kockázatkezelési eljárásrend alapján (ha készül). Ezenkívül, bármilyen változás (fejlesztés, fenyegetések, sebezhetőségek) esetében ismételt kockázatelemzési tevékenységet kell végeznie. Az elektronikus információs rendszer biztonságáért felelős a kockázatelemzés során megismert eredményeket, az intézkedéshez szükséges feladatokat, felelősöket, határidőket valamint maradék kockázatokat rögzíti és megismerteti a jegyzővel.

A kockázatelemzés eredményei és a kockázatkezelésre hozott intézkedések bizalmas információnak minősülnek ezért megfelelő jogosultsági szintekkel szükséges tárolni.

A kockázatelemzés eredményeit, illetve az abból származó szükséges intézkedéseket az érintettek felé kommunikálni szükséges, amelyet az elektronikus információs rendszer biztonságáért felelős tesz meg.

A Kockázatkezelési és kockázatelemzési eljárásrend tartalmazza azokat a közvetett, vagy közvetlen kárt okozó hatásokat, veszélyeket és károkat, amelyeket – a Hivatal jellemzőire tekintettel – a kockázatelemzés és kockázatkezelés során figyelembe kell venni.

A kockázat-felmérési módszertan és a kockázatmenedzsment rendszer kialakítása során figyelembe vettük az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM. rendelet, informatikai biztonsági szabványok és a kapcsolódó útmutatók előírásait.

A módszertan, menedzsment meghatározásáról a Hivatal vezetője - a kockázatfelmérésért felelős szakmai javaslata alapján – dönt, figyelembe véve a Nemzeti Elektronikus Információbiztonsági Hatóság és egyéb hatóság elvárásait, szakmai ajánlásait.

A Hivatal hatáskörébe tartozó informatikai rendszerekre vonatkozóan a biztonsági osztályba sorolást az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást, amelyet az érintett szervezet vezetője hagy jóvá, kockázatelemzés alapján kell elvégezni. A kockázatelemzés elvégezhető a hatóság által ajánlásként kiadott kockázatelemzési módszertana (segédlete) vagy egyéb, a követelményeket figyelembe vevő saját kockázatelemzési módszertan alapján, melyet eljárásrendben rögzíteni kell. Az elektronikus információs rendszerek besorolását a Rendszerbiztonsági terv vagy egyéb dokumentum tartalmazza. A besorolás és nyilvántartás az elektronikus információs rendszer biztonságáért felelős feladata.

A kockázatok azonosítása és felmérése információs rendszerenként, a kockázatok értékelése a vonatkozó jogszabályok alapján, a valószínűsíthető káresemény (közvetett és közvetlen) nagysága és annak a szervezetre gyakorolt, becsült hatása alapján történik.

Az éves felülvizsgálat, illetve felmérés során számba kell venni a belső eredetű kockázatokat (sérülékenységek), a külső okokat (fenyegetések), a bekövetkezés valószínűségét (gyakororiságát), ill. azt, hogy milyen adatok és milyen mennyiségbe sérülhetnek.

Meg kell határozni az okok (sérülékenységek, fenyegetések) nyomán előforduló helyzet, esemény (kockázati esemény) hatásait, következményeit, és ennek nagyságát.

Az alábbi közvetett, vagy közvetlen kárt okozó hatásokat, veszélyeket és károkat kell – a Hivatal jellemzőire tekintettel – figyelembe venni:

1. társadalmi-politikai káros hatásokat, károkat vagy a jogsértésből, kötelezettség elmulasztásából fakadó káros hatásokat, károkat (így pl. alaptervékenységek akadályozása, különösen a létfontosságú információs rendszeresemények működési zavarai, a nemzeti adatvagyon sérülései, jogszabályok és egyéb szabályozások megsértése, jogszabály által védett adatokkal történő visszaélés vagy azok sérülése, a közérdekűség követelményének sérülése, személyiséghez fűződő jogok megsértése, bizalomvesztés hatóságokkal, felügyeleti szervekkel szemben, az ország jogrendjének sérülése, vagy ennek lehetővé tétele);
2. személyeket, csoportokat érintő károk, káros hatások (pl. különleges személyes adatok, banktitkok, üzleti titkok megsértése, szervezet, személyek vagy csoportok jó hírének károsodása, személyi sérülések, vagy haláleset bekövetkeztének – ideértve az elektronikus információs rendszer működésének zavara, vagy információhiány miatt kialakult veszélyhelyzetet – veszélye);
3. közvetlen anyagi károk (az infrastruktúrát, az elektronikus információs rendszert ért károk, és ezek rendelkezésre állásának elvesztése miatti pénzügyi veszteség, adatok sértetlenségének, rendelkezésre állásának elvesztése miatti költségek, dologi kár);
4. közvetett anyagi károk (pl. helyreállítási költségek, elmaradt haszonnal arányos költségek, a környezet biztonságának veszélyeztetése, perköltségek).

5. A veszélyeztetettségnek a bekövetkezés valószínűségének megfelelő kárérték szinteknek megfelelő biztonsági osztályba sorolásakor a bizalmasság, sértetlenség és rendelkezésre állás követelménye külön-külön értékelendő.

A kockázatok kezelése

A Hivatal a feltárt kockázatokra a vonatkozó jogszabályban meghatározott biztonsági intézkedések mielőbbi megvalósításával reagál. A megvalósítandó biztonsági intézkedéseket, és azok megvalósításának sorrendjét a kívánt biztonsági osztály és biztonsági szint elérésére készített Cselekvési tervben kell meghatározni. Amennyiben a kockázat kezelésére javasolt válasz reakció beruházással jár, a jegyző az egyéb szabályzatokban meghatározott engedélyezési szabályok szerint jár el.

A kockázatokra adott válaszingtézkedéseket a következők kockázatkezelési stratégiák alapján lehet kiválasztani:

1. A kockázat elviselése

A Kockázat elviselés a következő esetekben alkalmazható:

- a. ha a kialakult működési rend olyan, hogy napi működése során minden beavatkozás nélkül automatikusan kezeli a kockázatot, ezért a kockázat gazdának nincs szüksége külön beavatkozásra,
- b. tudatos vezetői döntés esetén, amennyiben a kockázat elhárításának költsége magasabb az elhárításból eredő haszonnál, vagy kezelése technikai, időbeli, vagy anyagi korlátba ütközik. Amennyiben a vezetői döntés ilyen kockázat elviseléséről dönt, a válaszreakció helyett, köteles a kockázati tényező bekövetkezése után jelentkező hatások kezeléséről gondoskodni.

2. A kockázat kezelése

A kockázat kezelése akkor alkalmazható, ha a kockázatos tevékenység nem szüntethető meg és nem hárítható át. A kockázat kezelés az alábbi típusú kontroll tevékenységeken keresztül valósítható meg.

- c. Megelőző kontrollok: Korlátozzák egy negatív következménnyel járó kockázat bekövetkezésének lehetőségét, vagyis a megelőző kontrollok a szervezeten belüli belső kontrollok (pl. feladatok szétválasztása, „4 szem elve”, tartalék erőforrások, helyettesítési rendszer, képzések).
- d. Korrekciós kontrollok. A realizálódott, nem kívánt kockázat következményeit korrigálják, úgy, hogy kiegészítő megoldást nyújtanak a kár vagy veszteség csökkentésére. Fontos eleme a folytonossági és katasztrófatervek kidolgozása, illetve az eljárásrendekbe beépítve, váratlan helyzetek kezelésének szabályozása, amellyel a szervezet működésének folytonosságát tudja biztosítani a negatív hatásokkal, veszteséggel járó esemény bekövetkezése esetén.
- e. Iránymutató kontrollok: Egy bizonyos, kívánt eredmény elérését biztosítják. Általában egy tevékenység vagy tevékenységcsoport konkrét lépéseit, időbeni ütemezésüket tartalmazzák. Hasznos lehet a szervezet korábbi, hasonló tevékenységekből nyert tapasztalatainak beépítése az ilyen jellegű kontrollokba, amely ugyancsak biztosítékként szolgálhat a kívánt cél eléréséhez és így a kockázatok elkerüléséhez, csökkentéséhez (pl. eljárásrendek, utasítások, egyéb szabályozások, útmutatók).
- f. Felderítő kontrollok: Azt a célt szolgálják, hogy fényt derítsenek olyan esetekre, amikor nem kívánt események következtek be. Mivel csak az esemény bekövetkezése után fejtik ki hatásukat, ezért csak abban az esetben használhatók, amennyiben lehetőség van a kár vagy veszteség elfogadására (pl. rendszeres ellenőrzések, naplók áttekintése, a monitoring jelentések, folyamatok, projektek áttekintései, a célvizsgálatok, az auditok, stb.).

3. A kockázat átadása

A kockázat átadását esetén a kockázat (sem a valószínűsége, sem hatása) nem csökken, de megváltozik a kockázatviselő (szervezeten kívülre kerül). Tipikus példa a biztosításkötés, illetve a kockázatos művelet átadása olyan (külső vagy belső) partnernek, aki felkészült a kockázat kezelésére. Ilyen megállapodás esetén vizsgálendő, hogy a kockázati esemény bekövetkezése esetén milyen maradványkockázat marad az átadó szervezetnél, illetve a Hivatalnál (pl. reputáció-vesztés).

4. A kockázatos tevékenység befejezése;

A kockázatos tevékenység befejezése akkor alkalmazható, ha a kockázatok nem csökkenthetők elfogadható szintre a tevékenység megszüntethető, és megszüntetése nem akadályozza az Hivattal szembeni követelmények teljesítését, csak megszüntethetők az adott tevékenység befejezésével.

Felelőségek

A Hivatal vezetője (jegyző)

- felelős a kockázatkezelési rendszer(ek) kialakításáért, működtetéséért
- felelős a kockázatkezelési kritériumok azonosításáért
- kinevezi a kockázatelemzésért felelősöket, tevékenységüket felügyeli
- gondoskodik a kockázatkezelési irányelvek betartásáról
- biztosítja a kockázatelemzéshez és -kezeléshez a szükséges erőforrásokat
- dönt a kockázatelemzés elfogadásáról, kockázatok elfogadásáról, az elfogadható kockázati szintről, a szükséges intézkedésekről, figyelemmel kíséresi feladatokról
- gondoskodik a kockázatkezelés fontosságának tudatosításáról a teljes szervezetben

A kockázatelemzésért felelős (elektronikus információs rendszerek biztonságáért felelős vagy a jegyző által kijelölt személy)

- felelős a kockázat-felmérési módszertan(ok) kialakításáért, jóváhagyásáért
- kezdeményezi az éves rendszeres felmérés indítását
- koordinálja a kockázat-felmérési tevékenységeket
- javaslatokat tesz kockázatkezelési, javítási intézkedésekre
- gondoskodik a kockázatkezelési intézkedések, kontrollok szabályozásokba, dokumentációs rendszerbe illesztéséről
- rendszeresen tájékoztatja a Hivatal vezetőjét a kockázati szint alakulásáról, bekövetkezett kockázati eseményekről
- nyilvántartja a Hivatal információs rendszereit a 41/2015. (VII. 15.) BM. rendelet követelményeinek megfelelően

A szakterület kijelölt képviselője / jegyző vagy az általa kijelölt személy

- a kockázatelemzésért felelős segítségével azonosítja, felméri, értékeli a területére vonatkozó kockázatokat
- javaslatot tesz a magas kockázatok kezelésére a saját területére vonatkozóan
- intézkedik a saját hatáskörükben kezelhető kockázatok csökkentésére, kezelésére
- felelős a területére eső kockázatok figyelemmel kíséréséért, kezeléséért
- a kockázatok változása, újak felmerülése esetén aktualizálja a felmérést, tájékoztatja a kockázatelemzésért felelőst

A munkatársak

- felelősek a közzétett, kiadott kockázatkezelési előírások betartásáért
- feladatuk a nem kezelt, illetve az új vagy változó kockázatok jelzése közvetlen vezetőjüknek és/vagy a kockázatfelmérésért felelősnek.

1.3. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS

1.3.1. Beszerzési eljárásrend

Az informatikai, üzemeltetési eszközök, információbiztonsági követelmények megvalósításához szükséges informatikai eszközök és szoftverek beszerzésénél mindig a Hivatali beszerzésekre vonatkozó elvek szerint kell eljárni, figyelembe kell venni a Hivatal hatályos szabályzatait (összeghatárok, érvényes ajánlatkérések, a kiválasztás menete, garancia stb.). A Hivatal IT fejlesztés és üzemeltetés – az információbiztonság rendelkezésre állás céljait támogató – beszerzéssel kapcsolatos szabályait – ha szükséges - külön szabályzat vagy eljárásrend tartalmazza.

A beszerzési eljárásrendet abban az esetben kötelező bevezetni, ha a Hivatal saját hatókörében informatikai szolgáltatást, vagy eszközöket szerez be, rendszerfejlesztési tevékenységet (ide nem értve a jellemzően kis értékű, kereskedelmi forgalomban kapható általában irodai alkalmazásokat, szoftvereket, vagy azokat a hardver beszerzéseket, amelyek jellemzően a tönkrement eszközök pótlása, vagy az eszközpark addigiakkal azonos, vagy hasonló eszközökkel való bővítése céljából történnek, valamint a javítás, karbantartás céljára történő beszerzéseket) végez, vagy végeztet (nem minősül fejlesztésnek a kereskedelmi forgalomban kapható szoftverek beszerzése és frissítése).

A beszerzett számítástechnikai eszközöket, szoftvereket a rendszergazdának vagy a nyilvántartásra kijelölt felelősnek haladéktalanul nyilvántartásba kell venni

Az irodai munkavégzéshez szükséges irodatechnikai eszközök, alkalmazások megfelelő minőségben és mennyiségben történő készletezése (készletezés tervezése) a megbízott szervezeti egység vezető vagy rendszergazda feladata. Ezekből a kellékekből mindig akkora készlettel kell rendelkezni, mely biztosítja a folyamatos üzemvitelt. Azokban az esetekben, amikor a Hivatal olyan elektronikus információs rendszert vesz igénybe, amelynek használatához jogszabályi előírásban kerül meghatározásra a szükséges eszközök beszerzése, értelemszerűen a követelményeknek megfelelő eszközök beszerzése az elvárt.

1.3.2. Erőforrás igény felmérés

Ha a Hivatal saját hatókörében informatikai szolgáltatást vagy eszközöket szerez be, rendszerfejlesztési tevékenységet végez, vagy végeztet, vagy az erőforrás igény felmérés jogszabály alapján, a külső szolgáltató/jogszabály alapján kijelölt szolgáltató által előírt, akkor az elektronikus információs rendszerre és annak szolgáltatásaira vonatkozó biztonsági követelmények teljesítése érdekében a beruházás tervezés részeként meghatározza, és dokumentálja, valamint biztosítja az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges erőforrásokat (eszközöket, szolgáltatásokat, humán erőforrásokat), elkülönítetten kezeli az elektronikus információs rendszerek biztonságát beruházás tervezési dokumentumaiban.

A beruházással járó fejlesztések, módosítások, felújítások során figyelembe kell venni a már meglévő technikai és humán kapacitásokat is az egyes erőforrások beszerzése előtt, ugyanakkor a további feladatterhelés nem eredményezheti a már meglévő erőforrások túlzott kimerítését és ezzel összességében a biztonság gyengítését.

1.3.3. Beszerzések

Az elektronikus információs rendszer biztonságáért felelős a rendszergazdával egyeztetve meghatározza a Hivatal elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben szerződéses követelményként:

- a. a funkcionális biztonsági követelményeket;
- b. a garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint);
- c. a biztonsággal kapcsolatos dokumentációs követelményeket;
- d. a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket;
- e. az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.

A szolgáltatók/szállítók felé a releváns információbiztonsági szabályokat kommunikálni szükséges.

A külső féllel történő megállapodás megkötését megelőzően az elektronikus információs rendszer biztonságáért felelős megvizsgálja, hogy a külső fél által nyújtott szolgáltatásnak milyen információbiztonsági kockázatai vannak. Az így megállapított kockázatokkal arányosan kell meghatározni a megállapodásban a külső fél által teljesítendő információbiztonsági kötelezettségeket.

A szerződések átvizsgálása, véleményezése és releváns információbiztonsági szabályok meghatározása az elektronikus információs rendszer biztonságáért felelős, a szolgáltatók/szállítók felé történő kommunikálásról a jegyző gondoskodik.

Szolgáltató/szállító, harmadik személy részére logikai vagy fizikai hozzáférés megadása csak a szállítóval kötött szerződéses megállapodás alapján történhet. A szerződésnek tartalmaznia kell a kockázatokat elfogadható mértékre csökkentő intézkedéseket, szabályokat.

A Hivatal részéről az elektronikus információs rendszer biztonságáért felelős (egyeztetve a rendszergazdával) feladata;

- a. a harmadik féllel kapcsolatos kockázatok felmérése,
- b. a vonatkozó biztonsági követelmények azonosítása,
- c. az esetleg szükséges egyedi óvintézkedések meghatározása,
- d. a biztonsági követelmények dokumentálása, jegyző felé történő kommunikálása.

A partnereknek a megfelelő titoktartási megállapodás aláírása után, a szükséges hozzáférés kiadható. A hozzáféréseket nyilván kell tartani és rendszeresen felülvizsgálni.

A hosting szolgáltatást nyújtó külső szolgáltatók kiválasztásánál azok szolgáltatási képességeit, kapacitásait, referenciáit és szolgáltatásuk megbízhatóságát értékelni és ellenőrizni kell. A szolgáltatók kiválasztásánál preferálni kell a tanúsított információbiztonsági rendszerrel rendelkező szolgáltatókat.

A külső szolgáltatókkal kötött szolgáltatási szerződésekben a Hivatal információbiztonságot érintő elvárásait meg kell határozni. A szerződésben meg kell határozni, hogy a szolgáltató miként biztosítja a szolgáltatás rendelkezésre állását, a szolgáltatásban érintett és Hivatal tulajdonát képező információ és informatikai eszközök sértetlenségének és bizalmasságnak megőrzését. Ha egy szolgáltatás esetén a sértetlenség és a bizalmasság nem biztosítható maradéktalanul, az adatbiztonság megőrzésére egyéb eljárásokat kell alkalmazni (pl. titkosítás).

A szerződésben meg kell határozni, hogy a szolgáltató miként képes egy esetleges katasztrófa helyzetben szolgáltatását folytatni. Amennyiben ilyen kitétel a szerződésben nem szerepel, a Hivatal feladata a szolgáltatás kiesése esetén alkalmazott eljárás kialakítása, szükség esetén további szolgáltatók és üzemelési helyszínek bevonása a szolgáltatásba.

A Hivatal működése szempontjából kiemelten fontos szolgáltatások vonatkozásában lehetőség szerint több egyenértékű szolgáltatást kell igénybe venni (kivéve azoknál a szolgáltatóknál, amelyek jogszabályi előírás alapján kerültek igénybevételre), vagy legalább tervet kell készíteni a szolgáltatás elvesztése esetén a szolgáltatás aktiválására, az átállásra.

A megrendeléseket írásban kell megtenni, és a beszerzéshez kapcsolódó feljegyzéseket meg kell őrizni. A beszerzett termékeket, eszközöket a lehetséges mértékig az átvétel során ellenőrizni szükséges.

1.3.3.2. A védelem szempontjainak érvényesítése a beszerzés során

Ahhoz, hogy a Hivatal védeni tudja az elektronikus információs rendszert, rendszerelemet vagy rendszerszolgáltatást a beszerzés, vagy a beszerzett eszköz beillesztéséből adódó kockázatok ellen, szerződéses követelményként meg kell határozni a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak a leírását.

Az elektronikus információs rendszer biztonságáért felelős feladatai teljesítéséhez szükséges mértékben az elektronikus információs rendszerek valamennyi elemének tervezésével, fejlesztésével, beszerzésével és üzemeltetésével kapcsolatban megilleti a tanácskozási, véleményezési, javaslattevői kezdeményezési, ellenőrzési, betekintési és hozzáférési jogosultság.

1.3.6. Külső elektronikus információs rendszerek szolgáltatásai

A külső elektronikus információs rendszer szolgáltatók értékelése és a szolgáltatási szerződések átvizsgálása (ahol az lehetséges) az elektronikus információs rendszer biztonságáért felelős (egyeztetve a rendszergazdával) feladata. Az ügymenethez kritikus szállítók felé a releváns információbiztonsági szabályokat kommunikálni szükséges, amelyről a jegyző gondoskodik. A szerződésben meg kell határozni, hogy a szolgáltató miként biztosítja a szolgáltatás rendelkezésre állását, funkcionális és garanciális biztonsági követelményeket (pl. biztonságkritikus termékek elvárt garanciaszintje), illetve, hogy mik a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelmények.

A Hivatal eljárásában rögzíti a külső elektronikus információs rendszer felhasználóinak feladatait és kötelezettségeit.

A szolgáltatási szerződésben lehetőség szerint meg kell határozni, hogy a szolgáltató tevékenységét milyen formában lehet ellenőrizni. Amennyiben erre nincs lehetőség, úgy a szolgáltató munkáját ettől függetlenül ellenőrizni és értékelni kell (például a szolgáltatás során tapasztaltak alapján, amelyet a szolgáltató felé kommunikálni szükséges). A szolgáltatók tevékenységének folyamatos információbiztonsági ellenőrzése az elektronikus információs rendszer biztonságáért felelős kötelessége. A külső szállítókat/szolgáltatókat/harmadik feleket a rendszergazda vagy a nyilvántartásra kijelölt felelős nyilvántartja.

A külső szállító/szolgáltató/harmadik fél szolgáltatásában bekövetkező változások információbiztonságot érintő várható hatásait értékelni kell, és az ebből eredő kockázatok csökkentése érdekében intézkedni kell.

A megrendeléseket írásban kell megtenni, és a beszerzéshez kapcsolódó feljegyzéseket meg kell őrizni. A beszerzett termékeket, eszközöket a lehetséges mértékig az átvétel során ellenőrizni szükséges.

1.4. ÜZLETMENET- (ÜGYMENET-) FOLYTONOSSÁG TERVEZÉSE

1.4.1. Ügymenet-folytonosságra vonatkozó eljárásrend

A Hivatal tevékenységére vonatkozó jogszabályok, a szolgáltatások jellege egyértelműen előírják, hogy a Hivatalnak rendelkeznie kell olyan tervekkel, melyek lehetővé teszik a rendeltetésszerű működéstől eltérő, rendkívüli helyzetek kezelését. Ezen tervekben az alapvető információbiztonsági követelményeket be kell építeni. (A terv nem ronthatja le az eredetileg tervezett és megvalósított biztonsági elemeket).

Az ügymenet-folytonossági folyamat kiterjed a következőkre:

- a. kritikus erőforrások, funkciók, szolgáltatások azonosítása,
- b. elvárások és prioritások azonosítása,
- c. tervezés – folyamat létrehozása, szerepkörök rögzítése, megszemélyesítése,
- d. kommunikáció,
- e. tesztelés,
- f. rendkívüli események bekövetkezése esetén a tervek aktiválása,
- g. tapasztalatok alapján a tervek felülvizsgálata, fejlesztése.

Az ügymenet-folytonosság tervezés (BCP) célja a legfontosabb (kritikus) folyamatok kiesési idejének minimalizálása, a rendszer normál állapotának lehető legrövidebb időn belül történő visszaállításán túl az, hogy ezt kockázatokkal arányosan lehessen megvalósítani.

A katasztrófa-elhárítási terv (DRP) célja pedig első sorban a támogató információs / informatikai rendszerek teljes működésének (minden funkcionalitásának) a visszaállítása, vagy újra felépítése.

A folyamat, valamint az ügymenet-folytonosság tervezés és a katasztrófa-visszaállítási terv gazdája az elektronikus információs rendszer biztonságáért felelős, aki a terv kidolgozásába bevonja a rendszergazdát.

A külső elektronikus információs rendszerek szolgáltatói által a Hivatal felé nyújtott szolgáltatások ügymenet-folytonosságának a biztosítása és tervezése, a szolgáltatás üzemeltetését végző feladata (amelyet a szolgáltatási szerződés keretében szükséges meghatározni). A Hivatalnak a saját felhasználói környezetében ügyfelei számára szintén biztosítani kell a szolgáltatás folytonosságát egy esetleges kompromittálódást követően is.

1.4.2. Ügymenet-folytonossági terv informatikai erőforrás kiesésekre

Az ügymenet-folytonossági terv eljárások, vagy tevékenységlépések sorozata annak biztosítására, hogy a Hivatal információfeldolgozó képességeit – a szükséges aktuális adatokkal – a bekövetkezett katasztrófa után elfogadhatóan rövid időn belül helyre lehessen állítani.

A Hivatalon belül kizárólag a folyamatos működés szempontjából kulcsfontosságú személyek számára szükséges kihirdetni az elektronikus információs rendszerekre vonatkozó ügymenet-folytonossági tervet.

A terveknek ki kell térniük minimum az alábbiakra:

- a. alapeladatok, alapfunkciók, alapfunkciót támogató kritikus rendszerelemek,
- b. definiált alapszolgáltatások fenntartása, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is,
- c. tervezhető rendkívüli helyzetek / katasztrófahelyzetek,

- d. ügymenet-folytonossági célértékek (alapfunkciók, alapszolgáltatás és összes funkció újakezdésének időpontja, az ügymenet-folytonossági terv életbelépését követően, tervezett szolgáltatási szint),
- e. a folytonosság biztosításába bevont szerepkörök meghatározása és megszemélyesítése,
- f. a tervek aktiválási (életbe léptetési) körülményei,
- g. az aktiválásról értesítendő személyek,
- h. a végrehajtásba bevonandó személyek, azok elérhetősége, valamint kapcsolódó feladatok,
- i. incidens (biztonsági események is) kezelési folyamatának integrálása a tervekben,
- j. rendkívüli helyzetek / katasztrófa helyzet kezelési folyamatainak részletei, szabályai, prioritások,
- k. a normál üzletmenetre történő visszaállási eljárásokat (úgy, hogy az nem ronthatja az eredeti ügymenet minőségét),
- l. rendkívüli helyzetekben szükséges kritikus erőforrások egyes rendkívüli helyzetekhez kapcsolódó információbiztonsági elvárt szinteket.

Az alapfeladatok és alapfunkciók folyamatosságát úgy kell megtervezni, hogy azok üzemeseli folyamatosságában semmilyen, vagy csak csekély veszteség álljon elő, fenntartható legyen a folyamatosság az elektronikus információs rendszer elsődleges feldolgozó vagy tárolási helyszínén történő teljes helyreállításáig.

A változó környezet, változó érdekelt felek változásai a tervek folyamatos naprakésztségének a megőrzését követelik meg. A Hivatal szervezetében, működésében, az informatikai rendszerekben bekövetkező minden lényegi változással párhuzamosan, azzal összehangoltan meg kell történnjen az érintett terv elemeinek naprakészre tétele. Ennek érdekében a terveket folyamatosan és rendszeresen felül kell vizsgálni azok alkalmazhatósága, naprakésztsége vonatkozásában.

A terveket éves rendszerességgel, illetve szervezeti változások, vagy tesztelés nem megfelelő eredménye esetén minden esetben felül kell vizsgálni. Változások esetén az érintettek felé történő kommunikáció az elektronikus információs rendszer biztonságáért felelős felelőssége.

Az ügymenet- folytonosság tesztelését évente legalább egyszer tervezetten el kell végezni, annak megállapítása céljából, hogy a tervek alkalmasak-e adott rendkívüli helyzetek megfelelő módon történő kezelésére az alábbi tesztelési típusok valamelyikével: szimulációs teszt, végig járás teszt, dokumentum ellenőrzés.

A tervek jogosulatlanok számára nem kommunikálhatók, védeni kell azt a jogosulatlan hozzáféréstől.

Példa ügymenet-folytonosság tervezéséhez:

- az elemi kár,
- az áramszünet,
- a rendszerleállítás, szolgáltatásszünetelés, hálózati hiba,
- az adatsérülés,
- az adatvesztés,
- információ-feldolgozó eszközök, adattárolók rongálódása,
- eszközök megszokottól eltérő működése (hardver hibás működése),
- futtatási hiba (program hibás működése),
- biztonsági események.

1.4.2.4. Kritikus rendszerelemek meghatározása

Meg kell határozni az elektronikus információs rendszer alapfunkcióit támogató kritikus rendszerelemeket, ezeket az ügymenet-folytonossági tervben kezelni szükséges.

1.4.3. A folyamatos működésre felkészítő képzés

A képzés célja az üzletmenet-folytonosság jelentőségének tudatosítása, az üzletmenetfolytonosság-tervezés alapismereteinek átadása, a tervben foglaltak megismerése és elsajátítása. A folyamatos működésre felkészítő képzésben szimulált eseményeket kell alkalmazni, hogy elősegítse a személyzet hatékony reagálását a kritikus helyzetekben.

Az elektronikus információs rendszer biztonságáért felelős feladata a munkatársak ügymenet- és szolgáltatásfolytonossággal, valamint az ehhez kapcsolódó információbiztonsági szempontokkal kapcsolatos képzések tervezése, valamint ezen képzések elvégzése.

Minden a tervek végrehajtásában, valamint a rendkívüli események észlelése és eszkalálási folyamatában érintett munkatársat oktatni szükséges évente legalább egyszer (releváns belépő munkatársat a munkakezdés előtt kell oktatni).

A képzések tervezésének bemenő elemei:

- a. tesztek és gyakorlatok eredményei,
- b. érintett felektől gyűjtött direkt visszajelzések,
- c. rendkívüli helyzetek tapasztalatai,
- d. információs rendszerben történő változások,
- e. munkatársi változások,
- f. kapcsolódó utasításokban történő változások.

A képzés, tudatosítás történhet a következő módokon:

- a. e-mail tájékoztatás,
- b. dokumentum elosztás,
- c. személyes képzés, szimulált esemény.

1.4.5.3. Üzletmenet folytonosság elérhetőség

A Hivatalnak ki kell jelölnie egy biztonsági tárolási helyszínt, ahol az elektronikus információs rendszer mentéseinek másolatát az elsődleges helyszínnel azonos módon, és biztonsági feltételek mellett tárolja. A biztonsági tárolási helyszínhez történő hozzáférés érdekében (egy esetleges vészhelyzet/katasztrófa esetén) vészhelyzeti eljárásokat kell kidolgozni (ha a mentett adatoknak az elsődleges tárolási helyszínen bajuk esne, hogyan férünk hozzá a másodlagos tárolási helyszínen tárolt adatokhoz).

1.4.7. Infokommunikációs szolgáltatások

A Hivatal - a Nemzeti Távközlési Gerinchálózatra csatlakozó elektronikus információs rendszerek kivételével - tartalék infokommunikációs szolgáltatásokat létesít (internet szolgáltatás), és erre vonatkozóan olyan megállapodásokat köt, amelyek lehetővé teszik az elektronikus információs rendszer alapfunkciói, vagy meghatározott műveletek számára azok meghatározott időtartamon belüli újrakezdését, ha az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a biztonsági tárolási helyszínen.

1.4.7.2. Szolgáltatás prioritási rendelkezések

Ha az elsődleges és a tartalék infokommunikációs szolgáltatások nyújtására szerződés keretében kerül sor, az tartalmazza a szolgáltatás-prioritási rendelkezéseket, a Hivatal rendelkezésre állási követelményeivel (köztük a helyreállítási idő célokkal) összhangban.

1.4.8. Az elektronikus információs rendszer mentései

A Hivatal olyan mentési megoldásokat alkalmaz, illetve működtet, amivel biztosítani tudja, hogy az informatikai eszközök sérülése, meghibásodása, adathordozókon tárolt adatok sérülése, használhatatlanná válása esetén, a kiesett informatikai szolgáltatás elfogadható időn belül visszaállítható, illetve az elvesztett adatmennyiség mértéke még kezelhető szinten marad. Azon adatok esetén, amelyek hosszú távú megőrzéséért a Hivatal felelős, a mentéseknek alkalmasnak kell lenni az adatok jogszabályban előírt megőrzési idejének végéig történő visszaállítására.

A mentések szakszerű elvégzését a rendszergazda, vagy a Hivatallal kötött megállapodásban rögzítettek szerint az adott elektronikus információs rendszer üzemeltetője (az ASP esetében a szolgáltató) végzi saját adatmentési és naplózási eljárása körében.

A 466/2017. (XII. 28.) Korm. rendelet az elektronikus ügyintézésrel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezzorról 8. pont 15. § (1) bekezdése alapján, a Hivatal az adattrezor-archiválási kötelezettségének az önkormányzati ASP rendszer útján tesz eleget.

A Hivatal a rendszerbiztonsági, ügymenet-folytonossági elvárásokkal összhangban mentést végez, amely:

- a. meghatározott gyakorisággal inkrementális (növekményes),
- b. meghatározott gyakorisággal teljes (full) mentést

A rendszergazda az elektronikus információs rendszer biztonságáért felelőssel való egyeztetés után felülbíráhatja, hogy mennyi adatvesztést képes a Hivatal áthidalni, és ennek megfelelően mi az elfogadható adatvesztési kockázat.

Mentés az alábbi adatállományokról kell, hogy történjen, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal:

- a. az elektronikus információs rendszerben tárolt felhasználószintű információkról,
- b. az elektronikus információs rendszerben tárolt rendszerszintű információkról,
- c. az elektronikus információs rendszer dokumentációiról, köztük a biztonságra vonatkozókat is.

Az elkészült mentéseket:

- a. védelmi intézkedésekkel kell ellátni (jelszóval védett tömörített állomány vagy titkosított partíció),
- b. offline mentés esetén – helyrajzilag máshol, de minimum másik irodában - védelmi intézkedésekkel ellátott helyiségben található páncélszekrényben szükséges elhelyezni,
- c. dokumentált visszaállíthatósági ellenőrzést kell végrehajtani (adatvisszaállítás teszt jegyzőkönyvek),
- d. biztonsági mentés - rotációban történő törlés esetén, az aktuális ellenőrzés korábban kell, hogy végrehajtásra kerüljön, minthogy az utolsó, még meglévő vissza ellenőrzött biztonsági mentés törlődjön.

A Hivatal a további, egyedi mentési szabályokat szükség esetén *Mentési eljárásrend* vagy egyéb dokumentumban részletezi, melynek elkészítése és naprakészen tartása az elektronikus információs rendszer biztonságáért felelős és a rendszergazda feladata. A mentéseknek biztosítaniuk kell bármely információbiztonsági eseményből következő adatvesztések, vagy adat sérülések esetén az adatok hiánytalan visszaállításának lehetőségét, oly módon, hogy azok bizalmassága mindvégig megmaradjon.

1.4.9. Az elektronikus információs rendszer helyreállítása és újraindítása

A rendszergazda gondoskodik az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően (saját hatókörén belül). A mentési és visszaállítási eljárásokat úgy kell kialakítani, hogy az elektronikus információs rendszerek üzemszerű működése és a bennük kezelt adatok előre nem látható esemény, különösen katasztrófa vagy hardver, illetve szoftver meghibásodása vagy emberi mulasztás bekövetkezésekor szükség esetén helyreállíthatók legyenek, biztosítva a folyamatos napi működést. Biztosítani kell továbbá, hogy az üzemidő-kiesés, adatsérülés és adatvesztés oly mértékű legyen, amely a Hivatal által meghatározott elfogadható kockázati értéken belül marad.

1.5. A BIZTONSÁGI ESEMÉNYEK KEZELÉSE

1.5.1. Biztonsági eseménykezelési eljárásrend

Biztonsági eseménynek kell tekinteni a nem kívánt vagy nem várt egyedi eseményt vagy eseménysorozatot, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amely hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, rendelkezésre állása, funkcionalitása elvész, megsérül.

A biztonsági esemény kezelése az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység

Ennek megfelelően az elektronikus információs rendszer biztonságáért felelős megfogalmazza, dokumentálja a biztonsági eseményekre vonatkozó eseménykezelési eljárást, amely szabályozza az előkészületet, az észlelést, a vizsgálatot, az elszigetelést, a megszüntetést és a helyreállítást.

Az elektronikus információs rendszer biztonságáért felelős:

- a. összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével,
- b. egyezteti az eseménykezelési eljárásokat az ügymenet-folytonossági tervéhez tartozó tevékenységekkel,
- c. az eseménykezelési tevékenységekből levont tanulságokat beépíti az eseménykezelési eljárásokba, továbbképzésekbe és tesztelésbe.

A Hivatal nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági események típusát, terjedelmét, az általuk okozott károkat, helyreállítás lehetőségeit és költségeit, a helyreállítás időtartamát.

Az eseménykezelési folyamat fejlesztéséhez kapcsolódó ötleteket bármelyik munkatárs jelezheti az elektronikus információs rendszer biztonságáért felelősnek.

A folyamat működtetése és fejlesztése, a kapcsolódó szabályrendszer naprakészen tartása (személyi változások, infrastruktúra változások, gyakorlati események tapasztalatai stb. miatt), valamint azok kommunikálása az elektronikus információs rendszer biztonságáért felelős feladata. A felülvizsgálatot évente minimum egyszer el kell végezni, illetve változások esetén azonnal.

A biztonsági eseményre adandó gyors és hatékony megoldások érdekében az elektronikus információs rendszer biztonságáért felelős személy ügymenet-folytonossági tervben határozza meg a váratlan eseményekkel kapcsolatos felelősségeket és eljárásokat (lásd 1.4.1. *Ügymenet-folytonosságra vonatkozó eljárásrend*)

1.5.4. A biztonsági események figyelése

A Hivatal nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági eseményeit. A biztonsági eseményekkel kapcsolatos tevékenységeket az elektronikus információs rendszerek biztonságáért felelős koordinálja.

Az elektronikus információs rendszerek működése során fellépő eseményeket megfelelő részletességgel naplózni kell. Az üzemeltetőknek ezeket a naplóállományokat rendszeresen ellenőrizniük kell, az ellenőrzés eredményéről rendszeresen és szükség esetén időszakosan jelentést kell tenniük az elektronikus információs rendszer biztonságáért felelős személy részére.

A biztonsági események folyamatos figyelése és észlelés esetén azok jelentése, valamennyi munkatárs, szerződött fél felelőssége.

1.5.6. A biztonsági események jelentése

Minden vélt vagy valós információbiztonsági incidenst a felhasználóknak azonnal jelenteniük kell a felelősüknek és/vagy a rendszergazdának, aki jelenti azt az elektronikus információs rendszer biztonságáért felelősnek. A felhasználó köteles a tapasztalt jelenséget, a jelenséget kísérő hibaüzenetet regisztrálni és haladéktalanul a rendszergazda rendelkezésére bocsátani (pl. feljegyzés, képernyőkép). A jelentési csatornákat biztonságáért felelős kommunikálja az érintettek felé.

Példák információbiztonsági eseményekre:

- a. betörés, lopás,
- b. bizalmas információk kiszivárgása, kiszivárgásának gyanúja,
- c. vírustámadás,
- d. jogosulatlan hozzáférés elektronikus információs rendszerhez és rendszerelemhez,
- e. emberi mulasztás (dokumentált eljárások megszegése),
- f. hálózatbiztonsági incidensek.

A biztonsági esemény észlelésekor, a biztonsági eseményt meg kell szüntetni, vagy az esemény jellegéből adódóan azt izolálni szükséges. Az izolálást azonnal meg kell kezdeni, amelyért a rendszergazda a felelős az érintett felek bevonásával.

Az információbiztonsági incidensről, valamint annak életútjáról jegyzőkönyvet kell készíteni, amelyet az elektronikus információs rendszer biztonságáért felelős készít el és jelenti azt a Hivatal vezetője felé.

Az információbiztonsági eseményről készült jegyzőkönyveket megfelelő jogosultsági szinttel kell ellátni.

Az elektronikus információs rendszer biztonságáért felelős a 41/2015 (VII.15.) BM rendelet értelmében jelenti azokat a biztonsági eseményekre vonatkozó információkat az elektronikus információs rendszerek biztonságának felügyeletét ellátó szervezetnek (GovCERT-Hungary), amelyek hálózatbiztonsági incidensekből adódnak.

Biztonsági incidensek esetén a Hivatal IBSZ-e szerint kell eljárni, azonban az önkormányzati ASP-t ért incidensek észlelését jelenteni kell az ASP Központ felé is a Kormányzati Eseménykezelő Központ mellett (utóbbi esetén az észlelés nem feltétlenül jelentkezik a Hivatalnál, de kizárni sem lehet). A jelentés nem tartalmazhat olyan szenzitív adatot (pl. személyes adatot), elemeket, amelyet harmadik fél nem ismerhet meg. Ennek bejelentési felülete a hibabejelentő rendszer. Az ASP Központ a bejelentéseket fogadja, továbbítja az illetékes terület felé és a jogszabály szerinti lépéseket megteszi.

Ha az önkormányzati ASP-t üzemeltető, működtetői oldalon éri biztonsági incidens, az üzemeltető szervezet veszi fel a kapcsolatot a jogszabályban megjelölt Hatósággal.

A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács (EU) 2016/679 rendelet (GDPR) előírásai alapján a természetes személyek adatait érintő adatvédelmi incidenseket haladéktalanul jelenteni kell az adatvédelmi tisztviselő felé, akinek legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, jelentési kötelezettsége van az illetékes felügyeleti hatóság felé (kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve).

Adatvédelmi incidens az a biztonsági esemény, amely megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

1.5.7. Segítségnyújtás a biztonsági események kezeléséhez

A felhasználók felé az információbiztonsági események kezeléséhez kapcsolódó információk és irányelvek megadása, tanácsadás és támogatás az elektronikus információs rendszer biztonságáért felelős feladata, a rendszergazda közreműködésével. A támogatást a felhasználók szükség szerint igényelhetik. A biztonsági események figyeléséről, észleléséről és jelentéséről a felhasználókat oktatni kell.

1.5.8. Biztonsági eseménykezelési terv

Az elektronikus információs rendszer biztonságáért felelős megfogalmazza és dokumentálja a biztonsági eseménykezelési tervet. Évente legalább egyszer tervezetten felülvizsgálja, illetve frissíti, figyelembe véve az elektronikus információs rendszer és a szervezet változásait vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat. Gondoskodik arról, hogy a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető, módosítható.

Az információbiztonsági események, incidensek kezelési folyamatához kapcsolódóan meg kell határozni és folyamatosan pontosítani kell a biztonsági események kiértékelésének, kategorizálásának (pl. súlyosság, stb.) kritériumrendszerét.

Tervezni kell azokat az erőforrásokat és vezetői támogatást, melyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására.

A tervben meg kell határozni azokat a hálózatbiztonsági incidenseket (pl. DDOS támadás), amelyeket be kell jelenteni az elektronikus információs rendszerek biztonságának felügyeletét ellátó szervezetnek (Nemzeti Kibervédelmi Intézet Kormányzati Eseménykezelő Központnak).

Ezekben az esetekben elsősorban:

- a. az elektronikus információs rendszer biztonságáért felelős,
- b. biztonságiesemény-kezelési megbízott, valamint,
- c. a hatáskörrel rendelkező Kormányzati Eseménykezelő Központ vehet részt.

A biztonsági eseménykezelés a következő folyamatokra terjed ki:

- 1) Észlelés, jelentés, felelős: észlelő
- 2) Vizsgálat, felelős: elektronikus információs rendszer biztonságáért felelős, rendszergazda, érdekelt munkatársak, kijelölt szakértők
 - a) incidensek okának azonosítani, és elemzése, kivizsgálása,
 - b) bizonyítékok gyűjtése,
 - c) incidens behatárolása.
 - d) A vizsgálat során meg kell állapítani, hogy:
 - milyen események történtek?
 - az események milyen és mekkora kárt okoztak, illetve okozhattak?
 - milyen intézkedések szükségesek a kárelhárításhoz, illetve mérsékléshez?
 - mik voltak az események kiváltó okai, előzményei?
- 3) Elszigetelés (az esemény jellegéből adódóan)
- 4) Megszüntetés, felelős: elektronikus információs rendszer biztonságáért felelős, rendszergazda, érdekelt munkatársak, kijelölt szakértők
 - a) a szükséges intézkedések meghatározása,
 - a) az incidensekre hozott döntéseket, intézkedéseket dokumentáltan szükséges megtenni,
 - b) intézkedések végrehajtása,
 - c) az incidenssel kapcsolatos jegyzőkönyvet, egyéb feljegyzéseket meg kell őrizni, annak érdekében, hogy ha egy incidens következtében bármilyen peres (polgári, vagy büntető) eljárásra kerül sor, megfelelő bizonyítékokat lehessen bemutatni.
- 5) Helyreállítás, felelős: elektronikus információs rendszer biztonságáért felelős, rendszergazda, érdekelt munkatársak, kijelölt szakértők

Helyreállítási felelősségek kijelölése:

- a) az ügymenet-folytonosságot érintő események esetén (az esemény jellegéből adódóan) az ügymenet-folytonossági terv, vagy a Katasztrófa-elhárítási tervben rögzített módon kell eljárni.
- b) a helyreállítási tevékenység ellenőrzése.

A biztonsági eseménykezelési folyamatok tesztelését az ügymenet-folytonossághoz kapcsolódó kidolgozott tervek tesztelési folyamatával együtt kell elvégezni.

1.5.9. Képzés a biztonsági események kezelésére

Az információbiztonsági incidensekkel kapcsolatos képzések, valamennyi munkatárs felé belépéskor az alap információbiztonsági oktatás részeként megtörténnek. Ezen felül évente legalább egyszer, vagy súlyos információbiztonsági események után ismétlődő képzés történik a tudatosság fenntartása, illetve fejlesztése érdekében. A képzéseket az elektronikus információs rendszer biztonságáért felelős tartja.

1.6. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY - BIZTONSÁG

1.6.1. Személybiztonsági eljárásrend

A személybiztonsággal kapcsolatos elvárás, eljárás kiterjed a Hivatal teljes személyi állományára, valamint minden olyan természetes személyre, aki az elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. A Hivatal szerződéses partnereivel, harmadik felekkel szembeni elvárásokat, kötelezettségeket a tevékenységet képező, jogviszonyt megalapozó szerződésekben, megállapodásokban kell érvényesíteni. Meg kell ismertetni a szerződéses partnerekkel, harmadik felekkel a Hivatal szabályzatait, eljárásrendjeit, titoktartási kötelezettségekre vonatkozó felételeket.

Az elektronikus információs rendszerek felhasználói, illetve a bevezetésben és felhasználásában közreműködő külső fél munkatársai és vezetői titoktartási nyilatkozat tételére kötelesek, vagy a Hivatal és a külső fél közötti jogviszony alapjául szolgáló megállapodásban kell rendelkezni a külső fél titoktartási kötelezettségéről. A titoktartási kötelezettségnek ki kell terjedni az elektronikus információs rendszerekkel kapcsolatos, illetve ezek bevezetése során tudomásukra jutó valamennyi információra. Figyelembe kell venni a központi szolgáltató előírásait.

Az elektronikus információs rendszerek felhasználói, illetve a bevezetésben és felhasználásában közreműködő külső fél munkatársai és vezetői titoktartási nyilatkozat tételére kötelesek, vagy a Hivatal és a külső fél közötti jogviszony alapjául szolgáló megállapodásban kell rendelkezni a külső fél titoktartási kötelezettségéről. A titoktartási kötelezettségnek ki kell terjedni az elektronikus információs rendszerekkel kapcsolatos, illetve ezek bevezetése során tudomásukra jutó valamennyi információra. Figyelembe kell venni a központi szolgáltató (a jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató) előírásait.

Az elektronikus információs rendszerek üzemeltetőinek, szolgáltatóknak az emberi erőforrás megbízhatóságának biztosítása érdekében a háttérszolgáltatást biztosító szolgáltatói állomány tekintetében gondoskodnia kell a vonatkozó jogszabályokban rögzített megfelelőségi követelmények teljesítéséről (például érzékeny adatok feldolgozását végző rendszerhez kik kaphatnak fizikai és logikai hozzáférést).

1.6.2. Munkakörök, feladatok biztonsági szempontú besorolása

A Hivatal minden érintett szervezeti munkakört, vagy a szervezethez kapcsolódó feladatot biztonsági szempontból besorol, felméri a nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat, rendszeresen felülvizsgálja és frissíti a munkakörök és feladatok biztonság szempontú besorolását. A besorolásnál figyelembe kell venni a vonatkozó jogszabályok előírásait.

Az egyes munkakörökbe, feladatokra csak az előre meghatározott képzettséggel és képességekkel rendelkező munkavállalót, szerződéses partnert, harmadik felet lehet alkalmazni.

A szükséges képzettségi szinteket, gyakorlati elvárásokat a munkaköri leírásokban, szerződéseknél szükséges meghatározni. Új munkakör esetén a kereséshez profil, majd az alapján a belépés napjáig munkaköri leírás készül.

A jelentkező, valamint az átlépő munkavállalóknál az átvilágítás mértéke arányos az egyes munkakörök, pozíciók információbiztonsági szempontok szerinti fontosságával, az ennek megfelelően történő besorolásával.

A munkaköröket a Hivatal:

- a. „normál”,
- b. „közepes”,
- c. „magas”,

biztonsági kategóriákba sorolja.

A biztonsági kategóriákat és az adott kategóriába tartozó munkaköröket a Hivatal a *Munkakörök biztonsági szempontú besorolása* vagy egyéb dokumentum tartalmazza (ha van intézkedést igénylő munkakör).

A nemzetbiztonsági ellenőrzés célja annak vizsgálata, hogy a fontos és bizalmas munkakörre jelölt, illetve az ilyen munkakört betöltő személyek megfelelnek-e az állami élet és nemzetgazdaság jogszerű működéséhez szükséges biztonsági feltételeknek. A biztonsági feltételek vizsgálata azt jelenti, hogy az ellenőrzés alá vont személlyel kapcsolatban felvetődnek-e olyan kockázati tényezők, körülmények, információk, amelyek miatt tevékenysége jogellenes céllal befolyásolhatóvá, illetve támadhatóvá válhat, és ez által a nemzetbiztonságot sértő vagy veszélyeztető helyzet állhat elő. A nemzetbiztonsági ellenőrzés kockázat-vizsgálat, nem annak bizonyítására vagy kizárása irányul, hogy az ellenőrzöttet jogellenesen befolyásolták és ez által a nemzetbiztonság veszélyeztetett, hanem hogy a feltárt tények, körülmények, információk alapján okkal feltételezhető-e, hogy ilyen helyzet kialakulhat. A nemzetbiztonsági ellenőrzésre az érintett tudtával kerülhet sor.

A Hivatalnál nincsen nemzetbiztonsági ellenőrzés alá eső munkakör és feladat.

1.6.3. A személyek ellenőrzése

A Hivatal a hozzáférési jogosultság megadása előtt ellenőrzi, hogy a hozzáférési jogosultságot igénylő személy (munkavállaló, szerződéses partner, harmadik fél) az adott szervezeti munkakörnek vagy a szervezethez kapcsolódó feladat biztonsági szempontból történő besorolásának megfelelő feltételekkel rendelkezik-e.

A munkafelvételi eljárás során – törvényes keretek között – olyan vizsgálatokat kell lefolytatni, melyek egyértelmű képet adnak a jelentkező;

- a szakmai, erkölcsi, informatikai, információbiztonság tudatosság oldaláról tett alkalmasságáról,
- b mérlegelni kell a foglalkoztatni kívánt személy egyéni tulajdonságait is (pl. megbízhatóság, felelősségtudat, elkötelezettség, terhelhetőség, koncentrációképesség stb.).

Az átvilágításon túl a Hivatalnál az alkalmazási kikötések és feltételek a következők:

- a minden munkavállaló, szerződéses partner, harmadik fél, aki hozzáfér az érzékeny információkhoz (az ASP szakrendszerein túl), alá kell írjon egy titoktartási megállapodást (Titoktartási nyilatkozat, 2. sz. melléklet, minta), mielőtt a hozzáférés biztosítása megtörténik. Ezen kívül minden munkavállaló az ASP szakrendszereinek használatba vétele előtt, Felhasználói titoktartási nyilatkozat ír alá, amelyet a szolgáltatási szerződés tartalmaz;

- b. a munkakörökhöz meghatározott, releváns szabályozó dokumentumokat minden munkavállalónak, szerződéses partnernek, harmadik félnek figyelembe kell venni, valamint a mindenkor érvényes Informatikai Biztonsági Szabályzatot meg kell ismernie, azt elfogadni és betartani köteles;
- c. a betartandó szabályozó dokumentumokkal kapcsolatban alá kell írjon, egy nyilatkozatot, hogy azokat szerepköréhez kapcsolódóan megismerte, betartja és a nem ismerete nem ad felmentést a be nem tartásuk következményei alól (Megismerési nyilatkozat, 2. sz. melléklet, minta)
- d. kötelező képzések elvégzését igazoló feljegyzések (Munka és tűzvédelem, informatikai biztonsági oktatás).

Az elektronikus információs rendszer biztonságáért felelős véleményezi az egyes munkakörökhöz, feladatokhoz tartozó leírásokat és javaslatot tesz annak információbiztonsági kikötéseire, amelyeket a jegyzői jóváhagyás után a jegyző által kijelölt munkatársnak a munkaköri leírásokban, szerződésekben rögzítenie kell.

A humán erőforrás fentebb leírt pontjai nem lehetnek ellentmondásban jelen szabállyal. Az átvilágítás módját és a szükséges átvilágítási elemeket a Hivatal *Munkakörök biztonsági szempontú besorolása* dokumentuma tartalmazza (ha szükséges készíteni). A besorolási eljárás előkészítése és dokumentálása az elektronikus információs rendszer biztonságáért felelős feladata.

1.6.4. Eljárás a jogviszony megszűnésekor

Az alkalmazás megszűnéséről a Hivatal munkáltatói jogait gyakorló vezető dönt. A jogosultságok megszüntetése során figyelembe kell venni, a felmondás jellegét (felmondás, közös megegyezés, azonnali hatályú felmondás), illetve a szerződésben rögzített felmondási és egyéb határidőket és a jogosultságok visszavonásának ütemezését ehhez kell igazítani.

A jogviszony megszűnésekor az alkalmazottnak, a szerződőknek, harmadik félnek az információkhoz és információ-feldolgozó eszközökhöz való hozzáférési jogosultságát meg kell szüntetni, amikor alkalmazásuk megszűnik, szerződésük, illetve megállapodásuk lejár. A jogosultságok visszavonása szakrendszerek esetén a szervezeti egység vezető, egyéb jogosultságok esetén (pl. felhasználói fiókok, levelezőrendszer) a rendszergazda feladata, az elektronikus információs rendszer biztonságáért felelős a jogosultságok visszavonásáról meggyőződik, hiba esetén intézkedést kezdeményez.

A jogosultság megszűnését a nyilvántartás vezetésével megbízott feladata dokumentálni a rendszeresített dokumentumban vagy elektronikus nyilvántartásban.

A rendszergazda vagy a kijelölt felelős megszünteti, vagy visszaveszi a Hivatal által az érintett személynek kibocsátott egyéni hitelesítő eszközeit, beleértve a hitelesítésre szolgáló eszközöket, felhasználói kártyákat (pl. anyakönyvi kártya), a Hivatal területére való belépésre jogosító kártyákat (pl. proximity kártya).

Az alkalmazás megszűnésekor a kilépő munkatársnak, szerződőknek, harmadik félnek kötelessége minden a Hivatal tulajdonát képező vagyontárgyat visszaszolgáltatni. A rendszergazda a kiadott eszközökről nyilvántartást vezet, és a nyilvántartásnak megfelelően ellenőrzi a munkavállalóra bízott vagyontárgyak hiánytalanságát. A hiányokat vagy károkat a munkatárs köteles megtéríteni.

Abban az esetben, ha a dolgozó saját eszközt használt, meg kell győződni arról, hogy az eszköz nem tartalmaz üzleti információt.

A távozó munkatárs jogosult távozását megelőzően a személyes adatait tartalmazó elektronikus üzeneteket és dokumentumokat törölni, de nem jogosult a munkavégzésével, feladatkörével kapcsolatos üzenetek és dokumentumok törlésére.

A távozó munkatárs levelezési fiókját, elektronikus információs rendszerhez való hozzáférést az elektronikus információs rendszer biztonságáért felelős hozzájárulásával, szorosan csak a munkavégzés folyamatosságának fenntartása érdekében ameddig szükséges a rendszergazda archiválja, megtartja (szükség esetén más munkatárshoz irányítja). Minden egyéb esetben a fiókot törölni kell.

Az ASP szakrendszerek esetében az önkormányzat szakrendszerei adminisztrátor(ok) feladata a szakrendszer szintű jogosultságkezelés, azaz a szolgáltatást igénybe vevő felhasználók számára a szakrendszerei jogosultságok beállítása, adminisztrációja és karbantartása.

A Hivatal vezetője az érintetteket értesíti a munkatárs, szerződő, harmadik fél jogviszonyának megszűnéséről, és gondoskodik még a jogviszony megszűnése előtt az elektronikus információs rendszerrel és annak biztonságával kapcsolatos feladatok ellátásáról. Megelőzi az elektronikus információs rendszert, illetve abban tárolt adatokat érintő, információbiztonsági szabályokat sértő magatartását.

Az alkalmazás megszűnését követő meghatározott időszakra történő titoktartást a munkatársaktól, szerződő partnertől, harmadik féltől az alkalmazás megkezdésekor kitöltött titoktartási nyilatkozatban kell rögzíteni. Emlékeztetni kell a titoktartásban vállalt felelősségekről, a távozó munkatársat, szerződő partnert, harmadik felet.

Gondoskodni kell a jogviszony megszűnését követően a megszűnt jogviszonyú felhasználó azonosítójával történő visszaélések elkerüléséről. A jelentést, vagy eszközök visszavételét elmulasztók, mulasztások arányában együttesen felelnek.

Az elektronikus információbiztonsággal kapcsolatos további engedélyezési eljárást (a jogosultságok kiosztását és visszavonását) az *Informatikai biztonsági eljárásrend* vagy egyéb dokumentum tartalmazza.

1.6.5. Az áthelyezések, átirányítások és kirendelések kezelése

Áthelyezések, átirányítások esetén, ha szükséges el kell végezni a munkakörnek megfelelően a személyek ellenőrzésére vonatkozó eljárást.

Biztosítani kell mind a logikai, mind pedig a fizikai hozzáférést az újonnan használni kívánt elektronikus információs rendszerhez.

Amennyiben szükséges, módosítani kell, vagy meg kell szüntetni az áthelyezés miatt megváltozott hozzáférési engedélyeket.

A Hivatal vezetője az érintetteket értesíti a munkatárs, szerződő, harmadik fél jogviszony változásáról.

A szerepkörök és jogosultságok változtatását, változáskezelés keretében kell végrehajtani, és a szükséges dokumentumokat módosítani kell (pl. szerződésben meghatározott szerepkör, feladatok, jogok és kötelezettségek, munkaköri leírás). A jogosultság változást jogosultság igénylő lapon vagy egyéb feljegyzésen, elektronikus nyilvántartásban kell dokumentálni, illetve központi szolgáltató esetén, az általa meghatározott dokumentált módon. Az adatgazdának kell funkciója keretében, valamennyi személyi változást és a jogosultságok ebből eredő változásait a rendszergazda és az információbiztonsági felelő felé, a jogosultságok aktualizálása érdekében dokumentáltan jelenteni.

1.6.6. A Hivatallal szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények

A Hivatal más, külső szervezettel történő szerződés létesítésekor megköveteli, hogy a partner szervezet rendelkezzen olyan, belső biztonsági szabályozással, amelyben meghatározza a biztonsági szerep- és feladatköröket, azonosítja az ilyen feladatkörbe kinevezett vagy azzal megbízott személyeket, rögzíti a velük szembe támasztott elvárásokat.

A partner szervezet által, a saját hatáskörbe tartozó biztonsági munkatársakkal szemben támasztott követelmények és kiválasztási elvek, legalább feleljenek meg a Hivatal által is megkövetelt biztonsági szintnek és eljárásnak, melyet követhető módon dokumentálnak is. A személybiztonsági követelményeknek való megfelelésre a Hivatal a partnernél ellenőrzési jogot köt ki magának, az ellenőrzéssel érintettek körét a szerződésben rögzíteni kell.

A partnernek a Hivatalt haladéktalanul tájékoztatnia kell arról, ha változik a saját elektronikus információs rendszer biztonságáért felelősének személye, a biztonsági eseményeket kommunikálni jogosult kapcsolattartó személye és/vagy az elérhetőségének módja, illetve, ha a Hivatal rendszeréhez bármilyen hitelesítési eszközzel vagy kiemelt jogosultsággal hozzáférő munkatársának jogviszonya megszűnik, vagy munkaköre módosul.

Hitelesítési eszközt vagy kiemelt jogosultságot a partner nem ruházhat át másik munkatársára. Alap felhasználói jogosultság kiadására és visszavonására azonban a partner egy munkatársát a Hivatal felhatalmazhatja, aki a végzett módosításokért ekkor teljes felelősséggel tartozik.

A Hivatal törekszik arra, hogy a meglévő szolgáltatási és egyéb, harmadik féllel kötött szerződéseiben, azok módosításai útján következetesen érvényesítse a fenti kötelezettségeket.

Az elektronikus információs rendszer biztonságáért felelős felelőssége, hogy az informatika külsős felek által, a szerződött feladatok végrehajtására kijelölt személyek a munkavégzés kockázataival arányos mértékben átvilágításra kerüljenek.

A jegyző gondoskodik arról, hogy a szerződő felek a szerződésben rögzítsék a kockázatokkal arányosan a titoktartás követelményeit és az együttműködés egyéb kikötéseit.

A külső féllel történő megállapodás megkötését megelőzően a jegyző – az elektronikus információs rendszer biztonságáért felelős személy bevonásával – megvizsgálja, hogy a külső fél által nyújtott szolgáltatásnak milyen információbiztonsági kockázatai vannak. Az így megállapított kockázatokkal arányosan kell meghatározni a megállapodásban a külső fél által teljesítendő információbiztonsági kötelezettségeket.

A Hivatal előírja és folyamatosan ellenőrzi a szerződő fél személybiztonsági követelményeknek való megfelelését. Elvárja, hogy a külső fél munkavégzése során:

- a. gondoskodjon arról, hogy az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége, rendelkezésre állása és az adatvédelem elvei nem sérülhetnek,
- b. gondoskodjon arról, hogy a hozzáférési jogot kapott munkatársai a jogosultságot nem adhatják át más személynek,
- c. gondoskodjon arról, hogy a hozzáférési azonosítókat és az ezekhez kapcsolódó fizikai eszközöket bizalmasan kezelje, és biztosítsa, hogy azokhoz illetéktelen személyek ne férhessenek hozzá,
- d. gondoskodjon arról, hogy ha olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik a Hivatal elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést a Hivatalnak;

- e. garantálja az elektronikus információs rendszerek és infokommunikációs eszközök megfelelő védelmét, a szükséges és elégséges hozzáférés elvének betartását, fizikai és logikai védelem kialakítását, rendszerszintű titkosítási eljárások alkalmazását, illetve a biztonsági naplózást, valamint
- f. ha távolról éri el a Hivatal hálózatát, illetve valamely elektronikus információs rendszerét, akkor a biztonságos elektronikus adatcsere-kapcsolat érdekében köteles a Hivatal által előírt információbiztonsági megoldásokat megvalósítani mindazon saját eszközein, amelyekről a távoli elérés lehetséges.
- g. Bizalmas adatforgalom a Hivatal és a külső fél között csak titkosított kommunikációs csatorna biztosításával történhet.
- h. Az elektronikus információs rendszerhez kapcsolódó rendszergazdai feladatok ellátásáért az üzemeltetést végző külső fél felel.
- i. A külső fél által megállapodás alapján nyújtott szolgáltatásainak megfelelőségét a Hivatal vezetője és a rendszergazda – szükség esetén az elektronikus információs rendszer biztonságáért felelőssel együttműködve – folyamatosan ellenőrzi.

1.6.7. Fegyelmi intézkedések

Minden alkalmazottnak és külső partnernek (az Informatikai biztonsági szabályzat személyi hatálya alá tartozóknak) be kell tartania a Hivatal információbiztonsági szabályait. Minden ennek megtagadásából származó információbiztonsági incidens fegyelmi eljárást vonhat maga után. A szervezeti egység vezetője – szükség esetén az elektronikus információs rendszer biztonságáért felelős és a rendszergazda bevonásával – a tudomására jutott incidenst mérlegeli annak súlyosságától függően, és jelenti azt a jegyző felé. A fegyelmi eljárás módját a jegyző szükség esetén az elektronikus információs rendszer biztonságáért felelőssel a rendszergazdával együttműködve határozza meg az eset súlyosságát figyelembe véve. A fegyelmi intézkedés a jogszabályok és a Hivatal belső szabályai szerint történik.

Szerződéses (külső) partner esetén az információbiztonsági szabályok megsértése során fellépő következményeket a szerződésben rögzíteni kell. A szerződésben foglaltak megszegése esetén érvényesíteni kell a szerződésben meghatározott következményeket, és szükség szerint meg kell vizsgálni és alkalmazni kell az egyéb jogi lépéseket.

A Hivatal vezetője belső eljárási rend szerint fegyelmi eljárást kezdeményez az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben. Amennyiben az elektronikus információbiztonsági szabályokat nem a Hivatal személyi állományába tartozó személy sérti meg, érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja és szükség szerint alkalmazza az egyéb jogi lépéseket.

1.6.8. Belső egyeztetés

A Hivatal tervezi és egyezteti az elektronikus információs rendszer biztonságát érintő tevékenységeit, hogy csökkentse annak a nem érintett szervezeti egységeire gyakorolt hatását.

1.6.9. Viselkedési szabályok az interneten

Az internethasználat legbiztonságosabb módjának kialakításáért a rendszergazda gondoskodik, az elektronikus információs rendszer biztonságáért felelőssel együttműködve.

A Hivatal az internethasználatról és az elektronikus levelezéssel, az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal, a szabályzat személyi hatálya alá tartozókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységeket *Informatikai biztonsági eljárásrendben* vagy egyéb dokumentumban (pl. Oktatási anyagban) részletezi.

A felhasználónak a Hivatal hálózatában tilos:

- a. a mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése (pl. rágalmozás), tiltott haszonszerzésre irányuló tevékenység (pl. piramisjáték), szerzői jogok megsértése (pl. szoftver nem jogszerű terjesztése);
- b. egyéni profitszerzést célzó, a szervezettől eltérő üzleti célú tevékenység és reklám;
- c. a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetészerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése;
- d. a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybevevő tevékenység;
- e. a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés kísérlete, a hozzáférés átruházása más személy részére;
- f. a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megromlására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység;
- g. a Hivatal weboldala ellen bármiféle betörési kísérletet végrehajtani, illetve a szervezet hálózatát felhasználni más oldalak ellen elkövetett szabálysértés támogatására (kivéve a tervezett információbiztonsági ellenőrzéseket);
- h. a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele;
- i. az Interneten elérhető nyilvános chat-és fórum oldalakon hivatali email címmel hozzászólni;
- j. fájlcsere-alkalmazásokat futtatni, illetve nem hivatali munkavégzéshez szükséges letöltéseket végezni;
- k. a Hivatal elektronikus levelezési rendszerét és a Hivatal tulajdonában lévő internet hálózatot feladatellátásain kívül másra használni;
- l. a Hivatal informatikai hálózatán, eszközein a képernyőmegosztás, külföldi felhőszolgáltatás, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták stb. használata.

Weboldalak tiltása:

- a. azokon az eszközökön, amelyeken a Hivatal szakfeladataihoz szükséges elektronikus információs rendszerek elérhetőek, vagy a szakfeladatokhoz szükséges adatok, dokumentumok tárolására kerül sor, csak a munkavégzéshez közvetlenül szükséges weboldalak használata engedélyezett;

- b. technikai intézkedésekkel tiltani kell a szakfeladatokhoz nem szükséges weboldalak elérését. A munkavégzéshez engedélyezett weboldalakat a felhasználókkal való egyeztetést követően a rendszergazda és az elektronikus információs rendszer biztonságáért felelős határozza meg, amelyet jegyzői/szervezeti egység vezetői jóváhagyás után a rendszergazda vagy az ezzel a feladattal megbízott felelős, szolgáltató tesz elérhetővé;
- c. a közösségi oldalak (pl. a Hivatal facebook oldala), egyéb a szakrendszerei hálózaton tiltott oldalak elérése, kizárólag a Hivatal szakrendszerei hálózatáról leválasztott számítógépeken engedélyezettek, a munkavégzéshez szükséges minimális időtartamban (pl. közösségi célból).

A Hivatal a felhasználók által böngészett oldalak listáját naplózza. A naplófájl készítésének és ellenőrzésének célja, hogy a felhasználók Internet használata megfeleljen a Hivatal biztonsági követelményeinek és jogos érdekeinek.

A Hivatal kizárólag a számára dedikált kommunikációs kapcsolaton keresztül vagy saját infrastruktúráján megvalósított felhő alapú szolgáltatást (magánfelhőt) használhat. Az informatikai kockázatok és az adatok feletti felügyelet hiánya miatt tilos nyilvános felhőalapú rendszerek használata.

A rendszergazda köteles rendszeresen ellenőrizni, hogy a felhasználók számára biztosított az Internet elérést lehetővé tevő szoftverek mentesek a komolyabb biztonsági hibáktól.

Levelezés a Hivatal saját tulajdonú domain névhez kapcsolódó tárhelyen történhet, a rendszergazda által meghatározott vagy a tárhely szolgáltató által biztosított levelező rendszer használatával (lehetőség szerint (SSL) POP3 hozzáféréssel vagy webmail igény esetén (SSL) IMAP hozzáféréssel).

A rendszergazda az elektronikus levelezést korlátozza, az Internetről letöltött, illetve a tárhelyeken tárolt állományokat ellenőrzi. A nem a feladatellátáshoz szükséges állományokat törölni kell.

E-mail biztonsági szabályok:

- a. a Hivatal tulajdonát képező levelező rendszer csak Hivatali célokra alkalmazható. Magáncélra, valamint etikailag kifogásolható célokra a hivatali postafiókok nem használhatók. A felhasználó felel valamennyi, a címéről elküldött levél rendeltetési helyéért és annak tartalmáért;
- b. ha a felhasználó hosszabb időn át nem tudja postaládáját ellenőrizni, állítson be „Házon kívül” szabályt, így a feladó tudatában lesz annak, hogy a közeljövőben nem fog üzenetére közvetlen választ kapni. Ezzel egyidejűleg adja meg a helyettesítő személy nevét és elérhetőségét, hogy sürgős esetben legyen kihez fordulniuk távolléte alatt;
- c. szükséges a felhasználóhoz kötött egyéni, teljes névvel ellátott, a Hivatal által használt domain nevű egyedi email címek létrehozása (vezetéknév.keresztnev@domain.hu);
- d. tilos a Hivatal saját tulajdonú domain névhez tartozó levelezőrendszerén kívüli levelezőrendszer-használat. Az ingyenes levelezőrendszerek (pl. freemail, gmail, stb.) használatát a szakrendszerek munkaállomásain technikai korlátozásokkal tiltani kell;
- e. ha a felhasználó nem ismeri a külső rendszerből érkező levél feladóját, akkor az üzenet megnyitása előtt igyekezzen azt beazonosítani, gyanús esetben törölje az üzenetet, illetve jelezze ezt felettetésének vagy a rendszergazdának. Amennyiben a megnyitás szükséges annak megállapítására, hogy mi az üzenet célja, úgy ezt megfelelő előrelátással (lehetőleg a hivatal belső hálózatától elszeparált, szakfeladathoz nem kapcsolódó dokumentumot nem tartalmazó, informatikai rendszer elérést lehetővé nem tevő számítógépen) tegye, és az esetleges csatolt melléklet megnyitását vírus veszély miatt feltétlenül kerülje, további címzettnek nem küldheti tovább;

- f. az alkalmazottaknak tilos más alkalmazottak postafiókjához felhatalmazás nélkül hozzáférniük;
- g. a kilépett alkalmazott, megszünt szerződésű partner levelezési hozzáférést azonnal meg kell szüntetni, az érintett levelezési fiókját a rendszergazda a kilépést követően legalább 30 napig figyeli (vagy ameddig indokoltan szükséges) vagy tartalmát más munkatárshoz irányítja, ezt követően a fiókot meg kell szüntetni;
- h. tilos a távozott munkatárs nevében elektronikus üzenetet küldeni;
- i. a levelezési rendszerben a hozzáférést biztosító jelszavak létrehozására, kezelésére és változtatására vonatkozóan az általános jelszó használati szabályok érvényesek (*Isd. 3.7.5. Jelszó (tudás) alapú hitelesítés*);
- j. a munkatársak kötelesek a levelezési fiókjuk hozzáférést biztosító jelszót titkosan kezelni, azt mások tudomására hozni még a munkafolyamat felgyorsítása érdekében is tilos;
- k. az munkatársak kötelesek azonnal jelenteni a jelszavuk nyilvánosságra kerülésére utaló minden gyanút és körülményt;
- l. tilos a Hivatal levelezési rendszerében használt e-mail címmel magánérdekből, publikus rendszerekben regisztrálni, fórumokon megjelenni, hírlevelekre feliratkozni;
- m. tilos a Hivatal nevében olyan e-mailt küldeni, melyek:
 - bizalmas, kritikus információt tartalmaznak vagy szerződési, illetve jogi következménnyel lehetnek a Hivatalra nézve,
 - a Hivatal hírnevét, vagy az ügyfelekkel való kapcsolatát ronthatja, illetve a Hivatal ügyfeleinek érdekét sértheti,
 - a Hivatal bizonyos területekre vonatkozó álláspontját képviselik, fejezik ki és a felhasználó erre nem lett felhatalmazva, vagy munkakörének nem része az adott területre vonatkozó vélemény nyilvánítása,
 - szerzői jogokat sérthetnek,
 - vírusokkal fertőzhetik meg a Hivatal infrastruktúráját,
 - vallási, etnikai, politikai vagy egyéb másokra nézve potenciálisan sértő, zaklató tevékenység.
- m. a felhasználó által küldött elektronikus leveleket a felhasználónak kell aláírnia. Nem használható önállóan csupán a Hivatal neve, vagy annak variációi önálló aláírásként – a felhasználóknak a saját nevüket, és opcionálisan beosztásukat kell használni aláírásként;
- n. a munkavégzéssel kapcsolatosan már nem használható leveleket rendszeresen el kell távolítani a felhasználók postafiókjából, archiválni szükséges;
- o. a csatolt állományok készítéséhez és a partnerekhez való küldéshez a dokumentumokat előzetesen PDF formátumra kell átalakítani, amennyiben nem szükséges azt szerkeszthető formátumban továbbítani.

Az Ibtv 3. § (2) -(3) bekezdése alapján a külföldi adatkezelést, az egyes elektronikus információs rendszerek Magyarország területén kívül üzemeltetését előzetesen engedélyeztetni kell. (honlap üzemeltetés, email szerver).

Tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, illetve a vírusellenőrző és Internet böngésző kontrollok kiiktatása.

Az elektronikus levelekben, vagy azok mellékleteként a csatolt állományokat az informatikai rendszer automatikusan ellenőrzi, és a biztonságos üzemeltetést veszélyeztető állományok esetében a használatot, illetve a küldés/fogadást megakadályozza. Az állományok küldésére és fogadására vonatkozó korlátozás kiterjed a rendeltetészerű- és az ésszerű használat kereteit meghaladó méretű állományokra is.

Ha a felhasználó saját Hivatali postafiókjára elektronikus levélben vagy annak mellékletében kapott olyan állományt, amely nem munkavégzéshez kapcsolódik, azt haladéktalanul törölnie kell, a Hivatal adathordozóra tilos a munkavégzéshez nem kapcsolódó, személyes adatot tartalmazó dokumentum (beleértve a fényképeket is) mentése. A felhasználónak rendszeresen ellenőriznie kell a hozzárendelt mappák, a rendszergazdának a Hivatal összes adathordozójának adattartalmát. Ha a munkavégzéshez nem kapcsolódó vagy személyes adatot tartalmazó dokumentum észlelésére kerül sor, az észlelőnek fel kell hívni a tulajdonos – ha ismert – figyelmét erre, fel kell szólítani az észszerű időn belüli végleges törlésre. Ennek elmulasztását jelenteni kell a szervezeti egység vezetője és szükség esetén az adatvédelmi tisztviselő felé. Ha nem azonosítható be egyértelműen a munkavégzéshez nem kapcsolódó vagy személyes adatot tartalmazó dokumentum tulajdonosa, a rendszergazda kötelessége az adott állomány végleges törlése helyreállíthatatlanságot biztosító törlési technika alkalmazásával (beleértve az archivált állományokat is).

A Hivatalnak figyelembe kell venni a vonatkozó jogszabályok előírásait, így a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács (EU) 2016/679 rendeletét (GDPR).

A felhasználó tudomásul veszi, hogy a Hivatal informatikai hálózatára, eszközeire vonatkozóan a Hivatal ellenőrzési és felelősségre vonási jogosultsága fennáll, a meghatározott viselkedési szabályok megsértése fegyelmi intézkedést vonhat maga után.

1.7. TUDATOSSÁG ÉS KÉPZÉS

1.7.1. Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és az e célt szolgáló ágazati szervezetekkel

A Hivatal, a 2013. évi L. törvény (Ibtv.) hatálya alá tartozik. A 41/2015. (VII. 15.) BM rendelet nevesíti a Hivatal információbiztonsági felügyeletét ellátó Hatóságot, mely e hatáskörében a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH).

Az Ibtv. alapján a szervezet vezetője köteles együttműködni a hatósággal. Ennek során az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt, az informatikai biztonsági szabályzatát tájékoztatás céljából megküldi, az ellenőrzés lefolytatásához szükséges feltételeket biztosítja a hatóság részére.

A biztonságáért felelős személy feladata, hogy kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal, a törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervezet. Az információcsere és a Központ kárenyhítő intézkedései során a Hivatal együttműködni köteles.

Az elektronikus információs rendszerek biztonságáért felelős a fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információk megosztása érdekében kapcsolatot alakít ki és tart fenn az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és e célt szolgáló ágazati szervezetekkel (Nemzeti Kibervédelmi Intézet Kormányzati Eseménykezelő Központ). Figyelemmel kíséri a kiadott tájékoztatókat, riasztásokat, a Hivatal informatikai rendszereit érintő események esetén értesíti az érintetteket, megteszi a szükséges teendőket.

1.7.2. Képzési eljárásrend

A Hivatal vezetőjének feladata az elektronikus információs rendszerek biztonságáért felelőssel együttműködve az elektronikus információs rendszerhez hozzáféréssel rendelkező személyek (beleértve az elektronikus információs rendszerekkel kapcsolatba kerülő külső személyeket, pl. üzemeltetőket is) folyamatos oktatásának, képzésének elősegítése, az ajánlott elektronikus információbiztonsági eljárások, technikák és technológiák naprakészen tartása. Cél, hogy a felhasználók tudatában legyenek az információbiztonsági elvárásoknak és fenyegetettségeknek, illetve felelőségeiknek (pl. jelentési kötelezettségüknek).

A biztonság tudatosítása a felhasználók esetében oktató anyagok terjesztésével és képzések útján történik, melyről a jegyző gondoskodik. Az oktatási tematikákat és anyagokat az elektronikus információs rendszer biztonságáért felelős személy készíti, a jegyző véleményezi, szükség szerint a rendszergazda bevonásával. A képzés része az Ügymenet-folytonossági tervvel kapcsolatos tudnivalók oktatása.

1.7.3. Biztonság tudatosság képzés

A Hivatal annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói, vagy ahhoz hozzáféréssel rendelkezők számára.

A képzés szükséges:

- a. az elektronikus információs rendszer újonnan belépő felhasználói számára, a kezdeti képzés részeként (a munkába állást megelőzően),
- b. eltérő munkakörbe kerülés esetén, ha indokolt,
- c. amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi,
- d. ismétlődően 3 évente,
- e. amikor a jegyző erre utasítást ad vagy erre vonatkozóan utasítás, elrendelés érkezik (pl. biztonsági fenyegetettségek, vagy biztonsági esemény bekövetkezését követően).

A jegyző biztosítja, hogy a Hivatal munkavállalói az informatikai biztonsági rendszer követelményeiről és az abban bekövetkezett esetleges változásokról megfelelő képzésben részesüljenek. Felelős a képzési kritériumok meghatározásáért, kinevezi a felelősöket, tevékenységüket felügyeli, gondoskodik a képzési szabályok betartásáról, biztosítja a képzéshez a szükséges erőforrásokat, dönt a képzési szabályok elfogadásáról, a szükséges intézkedésekről, figyelemmel kísérei feladatokról.

Az elektronikus információs rendszerek biztonságáért felelős feladata az érintettek, felhasználók számára az informatikai biztonsági tudatosság megszerzéséhez, szintentartásához szükséges oktatási anyag összeállítása, naprakészen tartása. Az oktatási anyag része az Ügymenet-folytonossági tervben meghatározott intézkedések tudatosítása (minden alkalmazott ismerje, milyen esetben, és kit kell értesíteni katasztrófa esetén – ezek az információk mindenki számára elérhetőek a belső hálózaton).

Az Ügymenet-folytonossági tervben speciális feladatokat ellátók (pl. döntések meghozataláért felelős vezetők, informatikai alkalmazásokért, hardver, szoftver eszközökért felelősök) külön képzésben részesülnek, melynek keretében egyeztetésre kerülnek az általuk elvégzendő feladatok.

Az oktatási anyagnak kellő mélységű gyakorlati ismereteket is kell tartalmaznia. Az oktatási anyag összeállítása során fel kell használni a rendszergazda rendszerüzemeltetési tapasztalatait (felmerült problémák, informatikai incidensek kezelése, megelőző intézkedések).

Az elektronikus információs rendszerek biztonságáért felelős gondoskodik a képzési intézkedések, kontrollok szabályozásokba, dokumentációs rendszerbe illesztéséről.

A biztonság tudatosság képzések elvégzése a kijelölt személy (biztonságért felelős, rendszergazda vagy egyéb szakértő) feladata, a képzés elvégezhető e-learning képzési formában).

A képzési felelős (képzési referens vagy a jegyző) kezdeményezi a képzéseket, követi a képzési intézkedések megvalósulását, megőrzi a képzési feljegyzéseket.

A munkatársak felelősek a közzétett, illetve számukra kiadott előírások betartásáért, az oktatásokon átadott ismeretek elsajátításáért, lehetőség szerinti fejlesztéséért önképzéssel. Feladatuk az informatikai biztonság tudatosítása, fejlesztése érdekében javaslatainak eljuttatása felettesei vagy az elektronikus információs rendszerek biztonságáért felelős felé. A belső oktatásokon, illetve a jogszabály vagy hatóság által elrendelt éves továbbképzéseken kötelező a részvétel, amelyről részvételi nyilvántartást kell vezetni.

1.7.4. Belső fenyegetés

A biztonságtudatossági képzés feladata, hogy az érintett személyeket készítse fel a belső fenyegetések felismerésére, és tudatosítsa jelentési kötelezettségüket.

1.7.5. Szerepkör, vagy feladat alapú biztonsági képzés

A Hivatal szerepkör vagy feladat alapú biztonsági képzést szervez, nyújt vagy biztosít az egyes szerepkörök szerinti, azért felelős személyeknek:

- a. az elektronikus információs rendszerhez való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően;
- b. amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;
- c. a Hivatal által meghatározott rendszerességgel

A Hivatal a *Szerepkörök, tevékenységek felelősségek* fejezetben határozta meg a Hivatal információbiztonságával kapcsolatos szerepköröket, így ezekre a szerepkörökre nézve kell biztonsági oktatást tervezni és tartania.

Az új munkavállalók a betanulási időszak alatt személyre szabott program alapján a szervezeti egység vezető vagy az általa kijelölt személy közreműködésével sajátítják el a szükséges ismereteket. Akkor lehet önálló munkával megbízni, ha a munkavállaló megfelelő gyakorlatot szerzett és a felelős meggyőződött a felkészültségéről. Az új munkavállaló képzése során gondoskodni kell az informatikai biztonsággal kapcsolatos képzéséről, tudatosításáról. Meg kell ismertetni a rá vonatkozó informatikai biztonsággal kapcsolatos előírásokkal, szabályzatokkal.

Az informatikai rendszerekhez felhasználói jogosultságot csak olyan személyek részére szabad kiadni, akik elfogadják a Hivatal információbiztonsági szabályait. Az új munkavállaló munkaköréhez szükséges felhasználói jogosultságait a vonatkozó eljárásrend kell kiadni.

A felhasználót az azonosító(k) átadását megelőzően oktatásban kell részesíteni a használat feltételeiről és szabályairól, meg kell ismertetni a rá vonatkozó informatikai biztonsággal kapcsolatos előírásokkal, szabályzatokkal. Az oktatás *Oktatási tematika* vagy egyéb dokumentum alapján vagy e-learning módszerrel történhet.

Szakrendszerhez kapcsolódó felhasználói azonosító átadását megelőzően a felhasználót oktatásban kell részesíteni az adott szakrendszer használatáról. Az oktatás, a betanulási időszakban az új munkavállaló szakrendszerben végzett munkájának fokozott ellenőrzése a megbízott szervezeti egység vezető vagy a jegyző által kijelölt felelős feladata. Az új bevezetésű szakrendszerek felhasználóinak (pl. ASP keretrendszer és szakrendszerek) részt kell venni az előírt oktatásokon, amely alapján a rendszert az elvárásoknak megfelelően, önállóan is használni tudják.

A Hivatal azoknak a munkatársaknak, akiknek az idevonatkozó törvény és jogszabályok előírják, külső képzést biztosít. A képzéseket az erre szolgáló központi alkalmazással tervezni szükséges, melynek felelőse a jegyző vagy az általa megbízott felelős.

Új szabályozás vagy a szabályozás jelentős változása esetén az érintetteket képzésben kell részesíteni, a szabályzatot, szabályozást, az abban foglaltak megismerését, tudomásulvételét, betartását Megismerési nyilatkozaton vagy egyéb feljegyzésen kell dokumentálni.

Az oktatásokat úgy kell szervezni, hogy minimálisan három évente egyszer ismétlő, frissítő ismereteket kapjanak a munkatársak. Az új belépő munkatárs oktatását a munkakörétől függően, a lehető legrövidebb időn belül kell elvégezni. Rendkívüli oktatást kell tartani, ha biztonsági vagy egyéb incidens történik, a rendkívüli oktatást a jegyző a rendszergazda vagy az elektronikus információs rendszerek biztonságáért felelős javaslata alapján rendeli el.

Az lbtv. által előírt, az elektronikus információs rendszerek biztonságáért felelős vezető, felelős személy(ek), valamint a feladatok ellátásában résztvevő személy(ek) számára a vonatkozó jogszabály kötelező képzést ír elő. A továbbképzéseket (belépő képzések) és az éves továbbképzéseket (ismétlődő képzések) a Nemzeti Közszolgálati Egyetem szervezi.

Az elektronikus információs rendszerek védelméért felelős vezető (a jegyző) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet alapján képzésre és éves továbbképzésre kötelezett.

Amennyiben nem megfelelő jogosultsággal rendelkező munkatárs vagy külső szakértő látja el az elektronikus információs rendszerek biztonságáért felelős feladatait, a kijelölt személy beiskolázásáról is gondoskodni kell. A szakirányú továbbképzés beiskolázási feltételeit a rendelet tartalmazza.

Amennyiben nem kizárólag az elektronikus információs rendszerek biztonságáért felelős látja el az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy feladatait, akkor a feladatok ellátásában részt vevő személy(ek) képzését, éves továbbképzését is tervezni kell, meg kell valósítani a jogszabály előírása szerint.

1.7.6. A biztonsági képzésre vonatkozó dokumentációk

A Hivatal dokumentálja a biztonságtudatosságra vonatkozó alap-, és szerepkör alapú biztonsági képzéseket, a képzésen résztvevőkkel a képzés megtörténtét elismerteti, és ezt a dokumentumot megőrzi. A belső képzésről dokumentum születik, mely tartalmazza a képzés helyét, tárgyát, idejét, stb. és a résztvevők illetve oktató aláírásait. Az oktatásokkal kapcsolatos dokumentumokat a kijelölt képzésért felelős kezeli, tárolja. A belső képzéseken túl a külső képzésekről a részvételi, ill. látogatási igazolást és egyéb dokumentumokat, a kapott bizonyítványokat is archiválja a személyi anyagban, melyet zárt tűzvédelem pánccsészekrényben tárol. A képzési dokumentációk megtekintését a Hatóságoknak biztosítani kell.

FIZIKAI VÉDELMI INTÉZKEDÉSEK

2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM

2.1.2. Fizikai védelmi eljárásrend

A Hivatalnak gondoskodnia kell a fizikai és környezeti védelmére vonatkozó folyamatainak működtetéséről és fejlesztéséről, a kapcsolódó szabályrendszer naprakészen tartásáról, valamint azok kommunikálásáról az érintettek felé. Az elektronikus információs rendszer biztonságáért felelős a jegyző és a rendszergazda közreműködésével kidolgozta a Hivatal fizikai védelmére vonatkozó eljárásrendet. Az informatika biztonsági rendszer rendkívüli módosításakor, vagy biztonsági esemény bekövetkeztekor, de legalább évente az eljárásrendet újra kell vizsgálni, szükség szerint módosítani.

A fizikai védelemmel kapcsolatos további eljárásokat (pl. egyedi kulcskezelési előírásokat) az *Informatikai biztonsági eljárásrend* vagy egyéb dokumentum tartalmazza.

A Hivatalnak figyelembe kell vennie a külső szolgáltató, ill. jogszabály alapján kijelölt szolgáltató által meghatározott biztonsági osztály értékét, és a szolgáltatóval történő megállapodás (szerződés) vagy a tőle kapott tájékoztatás alapján a rá vonatkozó biztonsági követelményeket teljesítenie kell.

Az eljárásrend kidolgozása és alkalmazása során figyelemmel kell lenni a más jogszabályban meghatározott tűz-, és személyvédelmi, valamint a személyes adatok kezelésére vonatkozó rendelkezésekre (a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács (EU) 2016/679 rendeletét (GDPR)).

A védelmi eljárásrendnek ki kell terjednie az elektronikus információs rendszerek szempontjából érintett létesítményekre, helyiségekre. Az informatikai infrastruktúra különböző funkcionális területeinek optimális megválasztásával lehetőség van a fizikai biztonságot veszélyeztető fenyegetések csökkentésére. A Hivatal szakfeladataihoz kapcsolódó elektronikus információs rendszereket fizikailag védett, biztonságos helyre kell telepíteni. Ezen elektronikus információs rendszereknek helyt adó helyiségekre vonatkozóan jogszabályi és hatósági elvárás, hogy legyen kialakítva az objektum védelme beléptető, behatolás védelmi, tűzjelző és lehetőség szerint video-megfigyelő rendszer. Az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (szerverhelyiség) szükség esetén biztosítani kell a megfelelő környezeti feltételeket. A bárki által szabadon látogatható, vagy igénybe vehető publikus területekre nem vonatkoznak a fizikai és környezeti biztonsági követelmények.

A fizikai biztonságra vonatkozó követelmények betartását a jegyző és az elektronikus információs rendszer biztonságáért felelős legalább évente ellenőrzi, az eredményt jegyzőkönyvben rögzíti. A jegyzőkönyvet egy esetleges vizsgálat során az ellenőrzésre jogosult hatóságoknak amennyiben kéri, át kell adni.

Ha a Hivatal az lbtv.-ben meghatározott határidőkkel nem tudja teljesíteni az informatikai biztonsági követelmények megvalósítását, akkor a hiányosságokról Intézkedési tervet készít és rendelkezik annak megvalósításáról (lásd. 1.1.3. Az intézkedési terv és mérföldkövei).

2.1.3. Fizikai belépési engedélyek

A Hivatalhoz tartozó épületek, helyiségek biztonsági zónákhoz történő hozzárendelése lehetővé teszi a belépésvédelemmel kapcsolatos intézkedések hatékony végrehajtását a mindenkori védelmi igény függvényében (összhangban a jogszabályi és a hatósági elvárásokkal).

Az elvárt fizikai védelem érdekében a Hivatal a különböző funkcionális területeit biztonsági zónákba sorolja, melyek elhelyezkedésére a hagymahéj-elv a jellemző. Kívül találhatóak a nyilvános területek, majd az alacsony biztonsági igényű területek. Védett területként ezen belül az informatikai infrastruktúra és más fokozottan védendő helyiségek, majd azon irodai helyiségek, amelyekben lehetőség nyílik bizalmas, nagymennyiségű személyes információkhoz való hozzáféréshez (a központi IT- és ellátó infrastruktúra helyisége(i), irattár(ak)). A zónák között lehetőség szerint biztonsági határvonalak (zárt, ellenőrzött áthaladási pontok, ajtók) helyezkednek el.

A szabályzat magában foglalja a biztonsági zónák definícióját, ami a belépésre jogosult személyek, a belépésvédelemmel szemben támasztott követelmények meghatározásának alapjául szolgál.

Ehhez az alábbi biztonsági zónák kerültek meghatározásra:

Zóna	Biztonsági követelmények	Helyszínek/belépésre jogosultak
0 biztonsági zóna	Alacsony biztonsági követelmény	A Hivatal épületein belül és kívül elhelyezkedő mindazon területek, amelyek bárki (pl. ügyfél, látogató) részére nyilvánosan elérhetőek (pl. váróterem, nyilvános folyosó, parkoló)
1. biztonsági zóna	Közepes biztonsági követelmények	A Hivatal azon helyiségei, irodái, amelyekben nincsenek elhelyezve szakfeladatait támogató elektronikus információs rendszerek (pl. tárgyalók). Belépési jogosultsággal a Hivatal minden munkatársa rendelkezik. Látogatók/ügyfelek csak kíséret és felügyelet mellett.
2. biztonsági zóna	Magas biztonsági követelmények	A Hivatal szakfeladatait támogató elektronikus információs rendszereinek (pl. ASP, anyakönyv, választási, egyéb szakrendszereknek) helyt adó helyiségek A belépés csak az arra jogosultaknak lehetséges, a látogatók/ügyfelek belépése és ott tartózkodása csak kíséret és felügyelet mellett engedélyezett.
3. biztonsági zóna	Kritikus biztonsági követelmények	IT- és ellátó infrastruktúra valamennyi helyisége, pl. elosztó- és szerverhelyiségek (ideértve a szerverfunkciójú számítógépeket, adatmentő szervereket, NTG hálózati eszközöket). A belépés kizárólag a rendszergazdának, üzemeltetésért felelősnek engedélyezett, egyéb személyek kizárólag indokolt esetben, felügyelettel léphetnek be és tartózkodhatnak ott.

A Hivatal szakfeladatait támogató elektronikus információs rendszereinek helyt adó helyiségek (2. biztonsági zóna), illetve az informatikai erőforrásokat koncentráltan tartalmazó helyiségek (3. biztonsági zóna) esetében biztosítani kell a jogszabály és a hatóság által elvárt fizikai védelmet.

A szakrendszerek munkaállomásainak helyiségei védelmére riasztórendszert kell kialakítani, melynek részeként kellő számú jelzést adó egységet kell felszerelni:

- mozgásérzékelőt,
- üvegtörés érzékelőt (ahol a kockázatelemzés alapján indokolt, pl. földszinti helyiségek esetén),
- füstérzékelőt (a tűzvédelemre vonatkozó 3.2.1.12. követelmény teljesítésére)

A helyiségekbe történő belépést úgy kell szabályozni és technikai eszközökkel (proximity kártyás beléptető rendszerrel vagy kódzárral) biztosítani, hogy csak a feljogosított személyek léphessenek be (a nyilvános és a magas biztonsági követelményű területeket fizikai akadályokkal kell egymástól elkülöníteni).

A jegyző a szervezeti egységek vezetőivel együttműködve meghatározza az egyes biztonsági zónákba (helyiségekbe) a belépésre jogosult személyek listáját. A jegyző a jogosultság kiosztását átruházhatja a szervezeti egység vezetőjére, polgármesterre.

Ahhoz, hogy az engedélyezett belépési jogosultságok ellenőrizhetőek legyenek, szükséges a Hivatalnak belépési jogosultságot igazoló dokumentumokat (pl. kítűzők, azonosító kártyák, intelligens kártyák) kell kibocsátania. A kulcsokhoz, kártyákhoz, intelligens kártyákhoz, vagy kódhoz való hozzájutás csak dokumentált módon történhet, a jogosultság kiosztását követően.

A jegyző, mint az elektronikus információs rendszerek védelméért felelős vezető a biztonságért felelőssel együttműködve meghatározza a kulcsok/kártyák, intelligens kártyák felvételére és leadására vonatkozó egyedi szabályokat, az illetékeséget, a kulcsok/kártyák, intelligens kártyák megőrzési rendjét (ha készül, az *Informatikai biztonsági eljárásrend* vagy egyéb dokumentum tartalmazza).

Állandó belépési jogosultságot alapesetben csak a Hivatal munkavégzésre irányuló bármely jogviszonyban álló természetes személyek (pl. közszolgálati jogviszony, munkaviszony alapján foglalkoztatott munkatársak) kaphatnak. Külső személyek (pl. alpolgármester, képviselők, intézményvezetők, az önállóan működő intézmények gazdasági ügyintézői, közcélú vagy projektmunkához foglalkoztatottak, stb.) számára indokolt esetben, meghatározott munkára és/vagy időtartamra szükséges belépési jogosultságot csak a feladat elvégzéséhez helyéhez kötötten (az adott irodai helyiségekre vonatkozóan) lehet kiadni.

A jóváhagyást és átvételt dokumentálni kell. A kulcsot, kártyát, intelligens kártyát vagy kódot a jegyző vagy az által kijelölt felelős (pl. rendszergazda) adja ki és tartja nyilván. A belépésre jogosultak listáját a jegyző folyamatosan felülvizsgálja. A nyilvántartás vezetésére kijelölnek az érvénytelen/megszűnt jogosultságokat dokumentálnia kell. Jogosultságvisszavonás esetében gondoskodni kell a Hivatal által kiadott kulcsok, kítűzők, kártyák, intelligens kártyák visszavonásáról, megsemmisítéséről, törléséről. Új jogosultság igénye esetén a jegyző döntésének megfelelően kell eljárni.

A kulcsokat, kártyákat, intelligens kártyákat olyan helyen kell tárolni, ami nem teszi lehetővé illetéktelenek számára a hozzáférést.

2.1.4. A fizikai belépés ellenőrzése

A Hivatalnak meg kell határoznia az ügyélforgalom számára a be-, és kilépési pontokat, melyet az ügyélfogadási időn kívül zárva kell tartania, ügyélfogadáson kívül a belépés csak felügyelet és kíséret mellett lehetséges. Ezekre a bejáratokra lehetőség szerint kerüljön felszerelésre proximity kártyás beléptető ajtó vagy kódzár. Ennek hiányában a nem az ügyélforgalom számára kijelölt bejáratokat kulccsal zárva kell tartani, a belépést csak a kiosztott kulccsal rendelkezők számára lehet biztosítani.

A nyilvános területeken kívül, minden belépő ügyfelet, látogatót felügyelet alatt kell tartani, az irodákba, tárgyaló termekbe kizárólag kísérettel mehetnek be és tartózkodhatnak ott (a fogadónak kell kísérni). A látogatót, ügyfelet fogadó munkatárs felelős a látogatóért, annak minden, az információbiztonságot veszélyeztető tetteért. Elvárás, hogy a szakrendszerek és központi infrastruktúra helyiségeibe történő látogatói, ügyfél belépésekről információkat kell gyűjteni és megőrizni (lásd 2.1.8. *A látogatók ellenőrzése*).

A nyilvános ügyfélterületeken kívüli védett területeken (a szakrendszerek helyiségeiben) felügyelet nélkül tartózkodó, ismeretlen személyeket meg kell szólítani, nem szabad egyedül hagyni, személyesen kell a meglátogatandó személyhez kísérni. Egyedi mérlegelést követően vizsgálatot kell indítani, indokolt esetben felelősségre vonás alkalmazható azzal szemben, aki belépést biztosított/felügyelet nélkül hagyta az ügyfelet, látogatót, vagy a helyiséget.

Azokban az esetekben, amikor az épületbe karbantartási (akár épület, akár eszköz), vagy ellenőrzési célból érkeznek, a szervezeti egység vezető vagy az általa kijelölt személynek (informatikai jellegű esetekben a rendszergazdának) kísérnie kell ezeket a személyeket is és figyelemmel kell követnie a tevékenységüket.

A karbantartó szervezetekről, személyekről folyamatosan aktualizált nyilvántartást kell vezetni *(lásd 2.1.19. Karbantartók)*, kizárólag az engedélyezett karbantartók rendelkezhetnek a munkavégzés idejére belépési jogosultsággal.

A Hivatal takarítását végző személy/személyzet nem takaríthat felügyelet nélkül az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. szerverszoba, NTG hálózati végpont).

Az 1. biztonsági zóna helyiségeinek legalább kulccsal (a kulcs ne legyen a zárban), a 2. és 3. biztonsági zóna helyiségeinek intelligens kártyával, vagy kóddal zárhatónak kell lennie, amely így lehetővé teszi a biztonsági ponton való átjutás ellenőrzését, felügyeletét. A rendszergazda a beléptető eszközöket úgy konfigurálja, hogy az a belépési ponton ellenőrizze az egyéni belépési engedélyt, jogosultságot.

Vészhelyzetek esetére a kulcs, kártya vagy kód másodpéldányát a titkárságon vagy portán (ha van) védett helyen, pl. páncélszekrényben vagy zárt kulcsszekrényben kell elhelyezni lezárt, hitelesítéssel ellátott borítékban vagy lepecsételhető kulcsdobozban. A kulcsdoboz vagy boríték rendkívüli felnyitásáról a felhasználónak telefonon és írásos feljegyzésben értesítenie kell a szervezeti egység vezetőjét. A hitelesítéssel ellátott boríték felnyitását, a kód használatát követően a kódot meg kell változtatni.

A rendszergazdának vagy a kijelölt felelősnek meghatározott rendszerességgel (minimum éves gyakorisággal) meg kell változtatni a hozzáférési kódokat és kulcsokat, vagy azonnal, ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az adott személy elveszti/megszünteti a belépési jogosultságát. Az információbiztonsági oktatások keretében a Hivatal minden tagjának fel kell hívni a figyelmét a rendellenességek jelentésére, amelyet a felettesük vagy a rendszergazda felé kell megtenniük (pl. elvesztett eszköz, jogosulatlan hozzáférés, belépési jogosultság ellenére belépés megtagadása, stb).

2.1.5. Hozzáférés az adatátviteli eszközökhöz és csatornákhöz

A Hivatal a fizikai védelmi eljárásrend szerint ellenőrzi az elektronikus információs rendszer adatátviteli eszközeinek és kapcsolódási pontjainak helyt adó helyiségekbe történő fizikai belépést.

A fizikai belépések naplózása szükséges az informatikai erőforrásokat koncentráltan tartalmazó helyiségek (pl. szerverszoba) esetében.

A központi IT rendszereket (beleértve az aktív eszközöket, routereket) is felügyelt biztonsági zónában, vagy ha a fizikai adottságok miatt nem lehetséges, akkor folyamatos felügyelettel és vagyonvédelmi rendszerrel (lehetőség szerint kameraképet rögzítő kamerarendszerrel is) védeni kell, valamint folyamatosan zárva tartott (rack-) szekrényben/védett magasságban kell elhelyezni. A (rack-) szekrény kulcs átvételét, leadását az eljárásrendben előírt módon dokumentálni kell (elvárás, hogy a kulcs felvételének, leadásának vagy a helyiségben tartózkodásnak a tényét - az időpont feltüntetésével - a felvételre jogosult/megőrzésre kijelölt/nyilvántartásra kötelezett az erre a célra szolgáló nyilvántartási naplóban aláírásával igazolja).

A helyiségekbe állandó belépéssel, kulcs felvételére jogosultsággal kizárólag a rendszergazda, illetve a karbantartásra jogosultak rendelkeznek (lásd 2.1.19. Karbantartók).

2.1.6. A kimeneti eszközök hozzáférés ellenőrzése

A fénymásoló és nyomtató berendezéseket/multifunkcionális nyomatkészítőket, a fax készülékeket és minden egyéb kimentí eszközt védett területen belül kell elhelyezni, ahol a felügyeletük biztosítható, illetve illetéktelen hozzáférés megakadályozható (harmadik fél, ügyfél és látogatók részére nem hozzáférhetőek).

Lehetőség szerint úgy kell beállítani a kimeneti eszközöket, hogy a munkafolyamat azonosítható legyen (pl. a nyomtatóknál kód használata). Nyilvános zónában védett nyomtatás beállítása (PIN kóddal védett dokumentum nyomtatása) szükséges.

A szkennelt dokumentumok bizalmosságának védelmére érdekében hitelesítést igénylő FTP kapcsolaton keresztül szükséges megoldani a szkennelést, hitelesítést igénylő megosztott mappa beállítása (jelszóval védett mappába mentés), vagy ha nem lehetséges, akkor a szkennelt mappa tartalmának rendszeres automatikus törlése szükséges.

Lehetőség szerint alkalmazni kell az „Üres íróasztal - tiszta képernyő” szabályt:

- a. a monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és semmiképpen se legyen látható az épületen kívülről (ha monitor elhelyezéssel nem biztosítható, akkor sötétítő függöny használatával);
- b. a felhasználó a számítógépet zárolni köteles, ha azt rövidebb időre őrizetlenül hagyja;
- c. hosszabb idejű távollét esetén a számítógépből ki kell jelentkezni, illetve ki kell azt kapcsolni;
- d. a munkafázis végeztével ki kell jelentkezni az alkalmazásokból, majd leállítani a számítógépet;
- e. munkavégzés után minden érzékeny információt tartalmazó anyagot (papír alapú anyagokat, valamint elektronikus adathordozókat) el kell tenni az asztalokról, és zárható irodabútorban kell tárolni;
- f. gondoskodni kell arról, hogy a nyomtatókból, faxokból, fénymásolókból kijövő dokumentumokhoz illetéktelenek ne férjenek hozzá;
- g. ügyelni kell arra, hogy érzékeny információt tartalmazó dokumentumot ne felejtünk a fénymásolóban, a kinyomtatott, faxolt vagy másolt dokumentumokat nem szabad őrizetlenül az eszközökben hagyni;
- h. a hibásan nyomtatott, nem használt dokumentumokat meg kell semmisíteni (pl. iratmegsemmisítő);
- i. be kell tartani a fizikai biztonságra vonatkozó követelményeket (pl. ügyfelet ne hagyjunk felügyelet nélkül az irodában).

2.1.7. A fizikai hozzáférések felügyelete

A rendszergazda vagy a jegyző által kijelölt felelős a 2. és 3. biztonsági zóna szerinti - magas és kritikus biztonsági követelményű - elektronikus információs rendszereknek helyt adó helyiségekre vonatkozóan meghatározott rendszerességgel ellenőrzi a fizikai hozzáférésekről készült naplókat, annak érdekében, hogy észlelje a fizikai biztonsági eseményeket és reagáljon arra.

Azonnal át kell vizsgálni a hozzáférésekről készült naplókat, ha a rendelkezésre álló információk jogosulatlan belépésre utalnak. Ezekben az esetekben össze kell hangolni a biztonsági események kezelését a napló átvizsgálásának eredményével.

2.1.7.2. Behatolás riasztás, felügyeleti berendezések

A fizikai behatolás riasztások és a felügyeleti berendezések felügyeletére hatósági engedéllyel rendelkező távfelügyeleti szolgáltatóval kell szerződést kötni. Biztosítani kell, hogy a vagyonvédelmi rendszer behatolás- és műszaki jelzései automatikusan átjelzésre kerüljenek (lehetőség szerint független kommunikációs csatornán, pl. GPRS vagy rádiós átjelzéssel), a távfelügyeleti szolgáltató biztosítsa az intézkedésre jogosultak és szükség esetén a hatóságok értesítését (rendőrség, tűzoltóság). A műszaki felügyelet része a rendszer működését biztosító feltételek (pl. kommunikáció) meglétének folyamatos ellenőrzése.

A vagyonvédelmi rendszereknek (riasztó- és beléptetőrendszereknek) olyan eseménynaplókat kell tárolnia, mely biztonsági esemény bekövetkezése esetén a vizsgálathoz adatot szolgáltat. A riasztórendszer telepítéskor vagy felülvizsgálata során be kell állítani a teljes eseménynaplózást (beleértve a nyitás-zárás naplózást, a beérkező nyitás-zárás jelzések rögzítését, tárolását). A biztonsági rendszerek adatait a jogszabályok által megengedett maximális megőrzési időig archiválni kell.

A vagyonvédelmi rendszerek eseménynaplóit a szervezeti egység vezetőjének utasítására indokolt esetben a kijelölt szakértőnek (rendszergazdának, a riasztórendszer karbantartásával megbízott szakértőnek vagy kiemelt jogosultsággal (mesterkóddal) rendelkező személynek) át kell vizsgálnia. Szükség esetén ki kell kérni a távfelügyeleti szolgáltató által rögzített eseményeket.

A fizikai hozzáférésekről készült naplók meglétét a rendszergazdának vagy a kijelölt személynek az előírt időközönként (minimálisan az éves ellenőrzések alkalmával) ellenőrizni szükséges.

2.1.8. A látogatók ellenőrzése

A Hivatalnak a 2. és 3. biztonsági zóna szerinti helyiségekbe (szakrendszerek és központi infrastruktúra helyiségeibe) történő látogatói, ügyfél belépésekről információkat kell gyűjteni és megőrizni.

A nyilvántartást a jegyző utasításának megfelelően az ügyfél- portaszolgálat munkatársa vagy a látogatót/ ügyfelet fogadó ügyintéző vezeti, a nyilvántartás legalább az alábbiakat tartalmazza:

- a. dátum,
- b. látogató/ügyfél neve,
- c. ügyfajta, vagy ügyintéző neve.

A megőrzési időt a kockázattal arányosan a jegyző határozza meg (eltérő rendelkezés hiányában 3 hónapban), a selejtezésekről jegyzőkönyvet kell készíteni és megőrizni.

2.1.9. Áramellátó berendezések és kábelezés

A Hivatalnak meg kell védenie az elektronikus információs rendszert árammal ellátó berendezéseket, valamint a kábelezést a sérüléssel és rongálással szemben. A Hivatal területén az elektronikus információs rendszert, áramellátó hálózatot, telefonhálózatot érintő bármilyen beavatkozást, építést, karbantartást, átalakítást csak a Hivatal vezetőjének vagy az erre a feladatra kijelölt felelősnek a tájékoztatása után, annak jóváhagyásával és felügyeletével lehet végezni.

Az elsődleges áramforrás kiesése esetére azokra a rendszerekhez, ahol az indokolt vagy elvárt (pl. szerverfunkciójú számítógépek, adatmentő szerverek, NTG hálózati eszközök), az eszközök szabályos leállításához a tevékenységhez méretezett, rövid ideig működőképes szünetmentes áramellátást kell biztosítani.

2.1.12. Tűzvédelem

A Hivatalnak az elektronikus információs rendszereknek helyt adó irodákban, helyiségekben, szerverszobában (2. és 3. biztonsági zóna szerinti helyiségekben) független áramellátással támogatott észlelő berendezést (füstérzékelőt) szükséges alkalmazni.

A füstérzékelők jelzéseit a vagyonvédelmi rendszer részeként hatósági engedéllyel rendelkező távfelügyeleti szolgáltató felügyeleti rendszerére kell csatlakoztatni (automatikus, lehetőség szerint független kommunikációs csatornán, pl. GPRS vagy URH rádiós átjelzéssel).

A távfelügyeleti szolgáltatónak biztosítani kell tűzjelzés esetén a hatóság (tűzoltóság) és az intézkedésre jogosultak értesítését.

Az informatikai eszközök központi helyiségeibe (elosztó-, szerverhelyiségekbe) és ahol az tűzvédelmi szempontból indokolt, minimális elvárás a tanúsított gázzal oltó (CO²) hordozható, kézi tűzoltó készülék biztosítása (az elektromos tüzek oltására nem megfelelő a porral oltó készülék).

2.1.14. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem

A Hivatalnak védenie kell a 2. és 3. biztonsági zónában lévő elektronikus információs rendszereket, rendszerelemeket a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzárószelepek hozzáférhetőek, és megfelelően működnek, valamint a kulcsszemélyek számára ismertek.

Lehetőség szerint az informatikai erőforrásokat koncentráltan tartalmazó helyiségek (pl. szerver szoba, NTG végpont) tervezése, elhelyezése során biztosítani kell, hogy az a víz-, és más hasonló kártól védett legyen.

2.1.15. Be- és kiszállítás

A jegyző utasításának megfelelően a szervezeti egység vezető, vagy megbízására a rendszergazda engedélyezi vagy tiltja a Hivatal területére bevitt, onnan kivitt információs rendszerelemeket. Az eszközök igénylését a megbízott szervezeti egység vezetőhöz vagy a rendszergazdához kell benyújtani.

A Hivatal tulajdonában lévő, a Hivatalból kiszállításra engedélyezett eszközökről nyilvántartást (jegyzőkönyvet, átvételi elismervényt) kell írni vagy elektronikus nyilvántartást vezetni, amely egyértelműen tartalmazza a kiadott eszköz jellemzőit és a kiadással járó felelősségeket. Az eszköz visszaszolgáltatásakor a visszavevőnek meg kell győződnie arról, hogy az megfelel a kiadáskori állapotának.

Behozott eszköz esetében az üzembehelyezést megelőzően a rendszergazdának meg kell vizsgálni az eszközt, hogy megfelel-e a munkavégzéshez szükséges követelményeknek, információbiztonsági elvárásoknak. Amennyiben az eszköz nem felel meg az elvárt követelményeknek, úgy nem engedélyezhető a Hivatal belső hálózatára való csatlakoztatása.

A behozott eszköz munkahelyi használatból való kivonását megelőzően a rendszergazdának át kell azt vizsgálnia, hogy nem tartalmaz-e a munkavégzés során keletkezett bizalmas, illetve egyéb adatokat.

A rendszergazda vagy a kijelölt felelős a kiadott/behozott eszközökről (mobil eszközökről) nyilvántartást kell, hogy vezessen.

A nyilvántartás legalább az alábbiakat tartalmazza:

- a. eszköz megnevezése, (pl. laptop, pendrive, telefon stb.),
- b. szériaszám, modellszám, ha szükséges az azonosításhoz),

- c. kinek adta ki/ki hozta be,
- d. mikor adta ki/ mikor hozta vissza, mikor hozta be/mikor viszi el,
- e. alapkonfiguráció (operációs rendszer, szoftverek, stb) ahol értelmezhető,
- f. ellenőrzés eredménye (pl. a visszahozott eszköz megfelel a kiadáskori állapotának, a korábban behozott eszköz nem tartalmaz munkavégzésből származó adatokat),
- g. szükséges intézkedések (pl. telepítés, frissítés, törlés, javítás),
- h. aláírás (rendszergazda, munkatárs/harmadik személy).

Az eszköz szervizbe történő szállítása esetén jegyzőkönyvet kell készíteni, és a rendszergazdának az adathordozókra vonatkozó adatvédelmi szabályoknak megfelelően kell eljárnia (Lásd.3.8 Adathordozók védelme). A szerviz által kiadott szállító levelet a hardver nyilvántartásokkal együtt meg kell őrizni.

Az infokommunikációs eszközök használata során tilos:

- a. az eszközt illetéktelen személynek átengedni,
- b. az eszköz közelében folyadékot, éghető anyagot, illetve felette, alatta vagy rajta az eszköz rendeltetésétől eltérő anyagot, tárgyat elhelyezni és tárolni és
- c. az eszközt – hordozható infokommunikációs eszközök kivételével – a telepítési helyéről elmozdítani és elvinni az üzemeltető engedélye és közreműködése nélkül.

A Hivatal más szervezettel adat- és programcserét kizárólag írásos nyilatkozat alapján bonyolíthat, amelyben utalni kell az érzékeny adatok kezelésére is.

A csere biztonsági feltételeire vonatkozó megállapodásokban meg kell határozni:

- a. az adatátvitel, -feladás, -fogadás és -átvétel ellenőrzésének és bejelentésének eljárási szabályait,
- b. az adatok biztonságos átvitele előkészítésének és tényleges átvételének műszaki szabványait,
- c. az adatvesztéssel kapcsolatos kötelezettséget és felelősséget,
- d. az adatátvitel során a biztonságos – szükség esetén titkosított – környezet előírásait minden érintett félnél,
- e. az érzékeny adatok védelméhez szükséges speciális eszközök igénybevételét.

Az adatcsere esetében:

- a. épületen kívüli szállítást csak az önálló szervezeti egység vezetője rendelhet el,
- b. az átadás-átvételtől jegyzőkönyvet kell felvenni,
- c. a szállításnál egyszerre több személynek kell jelen lennie,
- d. épületen kívüli szállítás esetén a legrövidebb és leggyorsabb útvonalat kell kiválasztani,
- e. tömegközlekedési eszközön adathordozó nem szállítható,
- f. épületen kívüli szállítás esetén megfelelő tárolóeszközt szükséges használni, és
- g. épületen kívüli szállítás esetén az adatokat titkosított formában kell az adathordozóra rögzíteni, és a titkosítás feloldásához szükséges kulcsot külön csatornán kell eljuttatni a címzetthez, elektronikusan rögzített adatokat tartalmazó mágneses adathordozó szállításakor el kell kerülni a nyilvánvalóan erős mágneses tereket,
- h. a szállítás során a vagyonbiztonság érdekében fokozott figyelemmel kell eljárni,
- i. az adathordozót nem lehet őrizetlenül hagyni,
- j. az adathordozókat óvni kell a fizikai sérülésektől,
- k. az adathordozókon a minősítési szintet megváltoztathatatlanul kell feltüntetni.

Rendkívüli esemény esetén a szállítást elrendelő szervezeti egység vezetőjét – szükség esetén a rendőrséget is – értesíteni kell. A vezetőnek haladéktalanul meg kell tennie a további károk elkerülése érdekében szükséges intézkedéseket, valamint ezzel egy időben tájékoztatnia kell az elektronikus információs rendszer biztonságáért felelős személyt az eseményről és a megtett intézkedésekről.

Megfelelő technikai eljárásokkal és ellenőrzőeszközökkel gondoskodni kell a távközlési és adatátviteli eszközökön keresztül kicserélt információk védelméről. Ennek során figyelembe kell venni, hogy a távközlési eszközökben bekövetkező üzemzavar, az eszközök túlterheltsége vagy a kapcsolat kimaradása esetén a folyamatos üzletmenet megszakadhat, valamint illetéktelen személyek is hozzáférhetnek a különböző információkhoz.

2.1.16. Az elektronikus információs rendszer elemeinek elhelyezése

A Hivatal a lehetőségeihez mérten törekszik az elektronikus információs rendszerek elemeinek elhelyezése során arra, hogy a legkisebb mértékre csökkentse a fizikai és környezeti veszélyekből adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét. Ide tartozik a helyiségek átszervezése, ez ügyfélforgalom optimalizálása, a fokozott védelmet igénylő informatikai rendszerek (pl. szerverhelyiségek, ASP, választási, anyakönyvi szakrendszerek) ügyfélforgalomtól elkülönített elhelyezése

Az irodahelyiségekben az íróasztalokon rendet kell tartani. Csak a munkához felhasznált iratok, adathordozók lehetnek az asztalokon. Munkavégzés után az íróasztalokról az adathordozókat, munkához felhasznált iratokat zárható szekrénybe szükséges elhelyezni. Lásd 2.1.6. *A kimeneti eszközök hozzáférés ellenőrzése.*

Ha a monitoron személyes, minősített információk jelennek meg, biztosítani kell, hogy illetéktelen személy ne lássa a képernyőt (gondolni kell azokra az esetekre is, amikor az épületen kívülről láthatnak be). A felhasználók kötelesek a munkájuk megszakítása vagy befejezése után a számítógépüket zárolni vagy kikapcsolni. Amennyiben a felhasználó elhagyja munkaállomását, úgy használja a képernyő zárolását.

A tárgyalókkal kapcsolatosan az alábbi szabályokat kell betartani:

- a. tilos a tárgyalókban felügyelet nélkül hagyni számítógépet,
- b. bizalmas információ kivetítése, vagy táblán (flipchart-on) történő bemutatása esetén az illetéktelenek betekintését meg kell akadályozni, a táblákon, flipchart-okon hagyott információkat a terem elhagyása előtt törölni kell,
- c. a tárgyalóteremben is alkalmazni kell a "Tiszta asztal" szabályt.

2.1.19. Karbantartók

A külső szolgáltatónak, illetve a karbantartást végző személynek meg kell ismernie a Hivatal információbiztonsági előírásait, és titoktartási nyilatkozatot kell aláírnia.

A karbantartást csak, az arra kijelölt személyek végezhetik el, akik névsora szerepel a létrejött szerződéses megállapodásban, illetve az eszközökhöz, rendszerekhez, **szükséges** karbantartási jogosultságuk megfogalmazására került. A szerződésben ki kell kötni, hogy **személyi változás** esetén, haladéktalanul tájékoztatást kell küldeni a Hivatalnak.

A Hivatalba történő belépéshez, a karbantartási feladatok ellátásához a személyazonosságot igazolni szükséges (külső karbantartók esetében). E nélkül a belépés nem lehetséges.

Az eszközök, rendszerek karbantartási munkálatait külső karbantartók esetében a rendszergazdának felügyelni szükséges, hogy kizárásra kerüljenek a jogosulatlan hozzáférések, illetve hibás karbantartási tevékenységek.

A hibákat, rendszerleállásokat, minden karbantartási tevékenységet (pl. karbantartási naplóban) dokumentálni kell.

A jegyző által kijelölt felelősnek (elektronikus információs rendszerek biztonságáért felelősnek vagy rendszergazdának) nyilvántartást kell vezetnie a karbantartó szervezetekről/személyekről, elérhetőségeikről, azok jogosultságairól (szükség szerint a karbantartandó eszközökről), melyet változások esetén aktualizálnia kell.

Amennyiben a harmadik fél logikai hozzáférést kap, további szerződéses követelményt a *Harmadik felekkel szembeni szerződéses követelmények dokumentum* tartalmaz.

2.1.19.3. Időben történő javítás

A biztonsági követelmények teljesítése érdekében az elektronikus információs rendszerelemek (eszközök) karbantartásáról gondoskodni kell. Gondoskodni kell arról, hogy az elektronikus információs rendszerelemek időben történő javítása megtörténjen.

Ehhez szükséges tudatosítani a felhasználókban a hiba/eltérés időben történő jelentését, illetve naprakészen kell tartani a karbantartást végzők nyilvántartását, azok elérhetőségeit és azonnal fel kell venni velük a kapcsolatot a mielőbbi elhárítás érdekében.

A karbantartást csak **az** arra kijelölt személyek végezhetik el.

LOGIKAI VÉDELMI INTÉZKEDÉSEK

3.1. ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK

3.1.1. Engedélyezés

A Hivatal jelen fejezetben fogalmazza meg az információbiztonsággal kapcsolatos logikai engedélyezéseket, amelyek kiterjednek a rendszer- és felhasználó, valamint külső és belső hozzáférési engedélyek folyamatára. A Hivatal a *Szerepkörök, tevékenységek, felelőségek* fejezetben határozta meg az információbiztonsággal összefüggő szerepköröket, tevékenységeket, felelőségeket. Az elektronikus információbiztonsági engedélyezési folyamatokat kockázatkezelési eljárásban rögzíteni kell, összhangban jelen szabállyal. Felügyelni kell az elektronikus információs rendszer és környezet biztonsági állapotát.

A jogszabály által kijelölt központi adatkezelő informatikai rendszerére vonatkozó engedélyezési szabályok: Központi rendszerekben, pl. az önkormányzati ASP rendszerben fejlesztői, tesztelési, üzemeltetői, működtetői tevékenységet csak a központi adatkezelők vagy a jogszabály által kijelölt szolgáltatók (pl. az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendeletben), említett szereplők végeznek, illetve végeztetnek.

3.1.3. Az elektronikus információs rendszer kapcsolódásai

Szabályozni kell és szükség esetén belső engedélyhez kell kötni az elektronikus információs rendszerek kapcsolódását más elektronikus információs rendszerekhez, dokumentálni kell az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.

3.1.3.2. Belső rendszerkapcsolatok

A Hivatal belső engedélyhez köti az elektronikus információs rendszereinek összekapcsolását.

3.1.3.3. Külső kapcsolódásokra vonatkozó korlátozások

Szabályrendszert kell felállítani és alkalmazni a külső elektronikus információs rendszerekhez való kapcsolódásokhoz, amelynek eredménye lehet az összes kapcsolat engedélyezése vagy tiltása, meghatározott kapcsolatok engedélyezése, meghatározott kapcsolatok tiltása.

3.1.4. Személybiztonság

Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed a Hivatal teljes személyi állományára, valamint minden olyan természetes személyre, aki a Hivatal elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet.

A Hivatal szerződéses partnereivel, harmadik felekkel szembeni elvárásokat, kötelezettségeket a tevékenységet képező, jogviszonyt megalapozó szerződésekben, megállapodásokban kell érvényesíteni. Meg kell ismertetni és el kell fogadtatni a szerződéses partnerekkel, harmadik felekkel a Hivatal szabályzatait, eljárásrendjeit, titoktartási kötelezettségekre vonatkozó feltételeket.

Az elektronikus információs rendszerek felhasználói, illetve a bevezetésben és felhasználásában közreműködő külső fél munkatársai és vezetői titoktartási nyilatkozat tételére kötelesek, vagy a Hivatal és a külső fél közötti jogviszony alapjául szolgáló megállapodásban kell rendelkezni a külső fél titoktartási kötelezettségéről.

A titoktartási kötelezettségnek ki kell terjedni az elektronikus információs rendszerekkel kapcsolatos, illetve ezek bevezetése során tudomásukra jutó valamennyi információra. Figyelembe kell venni a központi szolgáltató előírásait is.

A Hivatal minden érintett szervezeti munkakört, vagy a szervezethez kapcsolódó feladatot besorol az *1.6.2 Munkakörök, feladatok biztonsági szempontú besorolása* fejezetben leírtaknak megfelelően a hozzáférési jogosultság megadása előtt. Az *1.6.3 A személyek ellenőrzése* fejezetnek megfelelően ellenőrzi, hogy a hozzáférési jogosultságot igénylő személy az adott szervezeti munkakörnek vagy a szervezethez kapcsolódó feladat biztonsági szempontból történő besorolásának megfelelő feltételekkel rendelkezik-e.

Amennyiben a harmadik fél logikai hozzáférést kap, további szerződéses követelményt a *Harmadik felekkel szembeni szerződéses követelmények dokumentum* tartalmaz.

3.2. TERVEZÉS

3.2.2. Rendszerbiztonsági terv

A Hivatalnak saját hatókörébe tartozó elektronikus információs rendszer tervezésekor rendszerbiztonsági tervet kell készítenie, amely összhangban áll a szervezeti felépítésével, vagy szervezeti szintű architektúrájával.

A rendszerbiztonsági terv a következőket tartalmazza:

- a. az elektronikus információs rendszer hatókörét, alap feladatait (biztosítandó szolgáltatásait), biztonságkritikus elemeit és alap funkcióit,
- b. az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát,
- c. az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerrel való kapcsolatait.

Az elektronikus információs rendszer biztonsági követelményeit rendszerdokumentációba kell foglalni. Ezen követelmények tekintetében meg kell határozni az aktuális vagy tervezett védelmi intézkedéseket és intézkedés bővítéseket, végre kell hajtani a jogszabály szerinti biztonsági feladatokat.

A rendszerbiztonsági tervet és azok változásait csak az érintett személyi és szerepkörökben dolgozók ismerhetik meg. A terv és kapcsolódó rendszerdokumentációk elkészítése az elektronikus információs rendszer biztonságáért felelős feladata.

Az elektronikus információs rendszer rendszerbiztonsági tervet évente felül kell vizsgálni, illetve soron kívül, ha a rendszerbiztonsági tervben, vagy az elektronikus információs rendszerben vagy annak üzemeltetési környezetében változás történt, vagy ha a terv végrehajtása vagy a védelmi intézkedések értékelése során problémák kerültek feltárásra.

3.2.3. Cselekvési terv

A Hivatal az elektronikus információs rendszer biztonságáért felelőssel együttműködve Cselekvési tervet készít, amennyiben a meghatározott biztonsági osztálynál/szintnél hiányosságot állapít meg (tehát, ha valamely védelmi intézkedés nem valósul meg, vagy a bevezetett kontroll hibás/hiányos) és ezekhez mérföldkövet rendel.

A feltárt hiányosságokat kockázatelemzést követően a kockázatokra adott válasz tevékenységek prioritása alapján teszi sorrendbe (jellemzően a nagy kockázattal járó hiányosságokat helyezi előtérbe).

A Cselekvési tervet a hiányosságok megállapítását követően kell elkészíteni:

- a. a kockázatkezelési stratégia és a kockázatokra adott válasz tevékenységek prioritása alapján,
- b. az elektronikus információs rendszerre vonatkozó biztonsági osztály meghatározásánál megállapított hiányosságot, a vizsgálatot követő 90 napon belül kell felülvizsgálni, a hiányosság(ok) megszüntetése érdekében,
- c. ha a meghatározott biztonsági szint alacsonyabb, mint a Hivatalra érvényes szint, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni, az előírt biztonsági szint elérése érdekében.

A cselekvési tervnek minimálisan tartalmaznia kell:

- a. megvalósulatlan védelmi intézkedés (meghatározott biztonsági osztályhoz tartozó OVI-úrlapból a „nem valósult meg” sorok), bevezetett hibás/hiányos kontrollok, elektronikus információs rendszer ismert sérülékenységei, lehetőség szerint a kockázatelemzés eredményének sorrendjében,
- b. tervezett intézkedés (szükséges/javasolt feladat),
- c. intézkedés hatóköre (pl. szervezeti egység),
- d. kijelölt felelős,
- e. tervezett határidő.

A cselekvési tervben foglalt, a szükséges védelmi intézkedések bevezetéséhez szükséges erőforrásokat a Hivatalnak biztosítani kell.

A cselekvési tervet folyamatosan aktualizálni kell, a biztonsági értékelések, hatáselemzések és a folyamatos felügyelet eredményei alapján. A kitűzött feladatok megvalósulását a cselekvési tervben a Hivatal vezetője az elektronikus információs rendszer biztonságáért felelős közreműködésével követi nyomon.

A védelmi intézkedések megvalósulását a Hatóság számára a *NEIH-OVI Osztályba sorolás és védelmi intézkedés úrlappal* kell megküldeni. A nem teljesült/hibás kontrollokra létrehozott cselekvési tervet a Hatóság számára szintén meg kell küldeni.

Mivel ezek a tervek bizalmas információkat tartalmaznak, ezért ezt csak a jegyző, az elektronikus információs rendszer biztonságáért felelős, és az általuk kijelölt személyek (beleértve a kitűzött feladatok bevezetéséért felelősöket) ismerhetik meg.

3.2.4. Személyi biztonság

A Hivatalnak gondoskodnia kell arról, hogy az elektronikus információs rendszer felhasználói, a hozzáférési jogosultságot igénylők megismerjék a rájuk vonatkozó szabályokat, felelősségeket és a kötelező, illetve tiltott tevékenységeket az elektronikus információs rendszerben történő munkavégzés, felhasználás tekintetében.

Ennek értelmében minden munkatársnak és új belépőnek, jogosultságot igénylő személynek az alábbi képzésben szükséges részesülnie az elektronikus információs rendszer használatba vételét megelőzően:

- a. az elektronikus információs rendszer működése, funkciói, használata,
- b. az információk kezelése,

- c. az elektronikus információs rendszerhez kapcsolódó elvárások, vonatkozó szabályok, felelőségek,
- d. az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységek.

A képzést szükséges megtartani:

- a. az elektronikus információs rendszerhez jogosultságot igénylők számára a használatba vételt megelőzően, újonnan belépő felhasználók számára a kezdeti képzés részeként,
- b. amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi.

Az adatgazda az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezi a felhasználót, hozzáférési jogosultságot igénylő személyt, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja.

A szakrendszerhez kapcsolódó felhasználói jogosultság átadását követően, a betanulási időszakban, az új munkavállaló szakrendszerben végzett munkájának fokozott ellenőrzése szükséges. Az ellenőrzés a megbízott szervezeti egység vezető, vagy a jegyző által kijelölt munkatárs feladata.

Az új bevezetésű szakrendszerek felhasználóinak (pl. ASP keretrendszer és szakrendszerek) részt kell venni a központ által előírt oktatásokon.

A Hivatal elektronikus információs rendszer biztonságáért felelős a megbízott szervezeti egység vezetők együttműködésével legalább évente felülvizsgálja és frissíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelőségüket, az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységet a viselkedési szabályok betartását. Változás esetén a hozzáféréssel rendelkezőket tájékoztatja a követelményekről.

3.3. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS

Jelen eljárást abban az esetben kell alkalmazni, ha a Hivatal saját hatókörében informatikai szolgáltatást, vagy eszközöket (elektronikus információs rendszert, rendszerelemet) szerez be, rendszerfejlesztési tevékenységet végez, vagy végeztet. A beszerzésre vonatkozó követelmény alkalmazása szempontjából nem minősül beszerzésnek a jellemzően kis értékű, kereskedelmi forgalomban kapható általában irodai alkalmazások, szoftverek, vagy azok a hardver beszerzések, amelyek jellemzően a tönkrement eszközök pótlása, vagy az eszközpark addigiakkal azonos, vagy hasonló eszközökkel való bővítése céljából, valamint a javítás, karbantartás céljára történnek. Nem minősül fejlesztésnek a kereskedelmi forgalomban kapható szoftverek beszerzése és frissítése.

3.3.2. A rendszer fejlesztési életciklusa

Az elektronikus információs rendszerek biztonságáért felelős személy a saját hatókörben beszerzett rendszerekre, rendszerelemekre vonatkozóan az elektronikus információs rendszereinek teljes életútján, azok minden életciklusában figyelemmel kíséri informatikai biztonsági helyzetüket.

A Hivatal meghatározza és kijelöli az információbiztonsági szerepköröket és felelőségeket a fejlesztési életciklus egészére, szerződésben, munkaköri leírásban rögzíti ezekre a szerepkörökre vonatkozó tevékenységeket, felelőségeket.

A rendszer életciklus szakaszai során a következőket határozza meg:

- a. követelmény meghatározás:
a fejlesztéseket, beszerzéseket megelőzően a rendszerkövetelményeket meg kell határozni, amelyeket a szerződésben, fejlesztési dokumentációkban rögzíteni szükséges. Rögzíteni szükséges, a beszerzés, fejlesztés során alkalmazandó információbiztonsági követelményeket.
- b. fejlesztés vagy beszerzés:
a beszerzési, fejlesztési szerződésnek és dokumentációknak megfelelően az információbiztonsági követelmények betartása mellett a rendszer, rendszerelem beszerzése, fejlesztése.
- c. megvalósítás vagy értékelés:
A beszerzett, fejlesztett rendszer/rendszerelem értékelése annak céljából, hogy ellenőrzésre kerüljön az elvárt követelmények teljesülése. A rendszerek működési vizsgálatához minta adatbázisokat kell használni, a rendszerek teszteléséhez éles adatbázist használni tilos.
- d. üzemeltetés és fenntartás:
a beépítésre kerülő rendszerelem, bevezetésre kerülő elektronikus információs rendszer üzemeltetésére és frissítésére meghatározott követelményeket a szerződésben, rendszer dokumentációban rögzíteni kell. Meg kell követelni az üzemeltetéshez, frissítéshez szükséges dokumentációk naprakészen tartását, információbiztonsági elvárások megfogalmazását és betartását.
- e. kivonás (archiválás, megsemmisítés):
az elavult rendszereket, rendszerelemeket, egyéb eszközöket az információbiztonsági követelményeknek megfelelően kell kivonni, amelyet az érintettek felé kommunikálni szükséges.

3.6. KONFIGURÁCIÓKEZELÉS

3.6.1. Konfigurációkezelési eljárásrend

A konfigurációkezelés célja az informatikai infrastruktúra adatainak kézben tartása, az egyes komponensek beazonosítása, figyelemmel követése (incidensfelügyelet, problémakezelés) és karbantartása. A Hivatal életében bekövetkezett változások nyomon követése, hogy mindig naprakészen elérhető legyen, mely változás a rendszer mely pontjában/verziójában ment végbe. Ezáltal elkerülhető, hogy az infrastruktúrán elvégzett változtatások nem várt szolgáltatás kiesést okoznak.

A elektronikus információs rendszer biztonságáért felelős a rendszergazda közreműködésével megfogalmazza és dokumentálja a konfigurációkezelési eljárásrendet, mely szabályozza a konfigurációkezelési folyamatot (konfigurációs elemek kibocsátását és módosítását azok teljes életciklusára vonatkozóan) és elősegíti annak ellenőrzését.

A konfigurációkezelési eljárásrend változásainak nyomon követését az elektronikus információs rendszer biztonságáért felelős végzi, tartja naprakészen. Minden más esetben, legalább évente egyszer felül kell vizsgálni, mind az eljárásrendet, mind pedig a nyilvántartást.

3.6.2. Alap konfiguráció

A rendszergazdának vagy a Hivatal vezetője által kijelölt felelősnek szükség esetén az elektronikus információs rendszerek biztonságáért felelőssel együttműködve az információs rendszerekhez egy-egy alapkonfigurációt szükséges készítenie, amelyet dokumentáltan, bizalmasan naprakészen kell tartani. Az alapkonfiguráció frissítését az elektronikus információs rendszerelemek telepítésének és frissítéseinek szerves részeként kell elvégezni. Az alapkonfiguráció kiterjed valamennyi, hardver és szoftver elemre (beleértve a menedzselhető eszközöket is), valamint telepítő dokumentációkra /leírásra, azok változásaira. Bármilyen változásnak, ami módosítja a konfigurációs nyilvántartás tartalmát, felügyelet alatt kell lennie, amely a rendszergazda vagy a kijelölt felelős feladata. Ilyenek például az eszközökön, szoftvereken, és a hálózaton végzett változtatások.

Minden egyes fejlesztés/újítás, hibajavítás vagy módosítás esetében a változásokat rögzíteni szükséges és ennek megfelelően frissíteni kell az alapkonfigurációt, de meg kell őrizni az alapkonfiguráció frissítés/újítás előtti verzióját, hogy szükség esetén lehetőség legyen az erre való visszatérésre.

Biztonsági szempontokból meghatározott módon konfigurált elektronikus információs rendszerelemeket vagy eszközöket kell biztosítani azon személyek számára, akik az elektronikus információs rendszert külső helyszínen használják. Megfelelő biztonsági eljárásokat kell alkalmazni a külső helyszínen használt eszközök belső használatba vonásakor.

Az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet 2. melléklete tartalmazza az önkormányzati ASP rendszer szakrendszereinek használatához szükséges felhasználói (önkormányzati) munkaállomásokkal szembeni minimális elvárásokat. Ennek megfelelően kell kialakítani az informatikai infrastruktúra környezetet:

- a. Munkaállomás, laptop (szoftverekkel)
- b. Monitor
- c. Kártyaolvasó
- d. Nyomtató
- e. NTG csatlakozáshoz szükséges, hivatal oldali hálózati eszközök (rack szekrény, szünetmentes tápegység, switch)

Az ASP rendszerhez történő csatlakozáshoz kapcsolódóan el kell végezni a hálózat kiépítését, az eszközök beüzemelesét (munkaállomások, nyomtatók, hálózati aktív eszközök), szoftverek telepítése, beállítása (pl. tűzfal).

3.6.7. Legszűkebb funkcionalitás

Az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője ill. üzemeltetője az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa (pl. a jogszabályban előírt szolgáltató).

A Hivatal saját hatókörén belül meghatározza és biztosítja azokat a minimum konfigurációs beállításokat, amelyek a munkavégzéshez szükségesek. Ennek köszönhetően, semmilyen felesleges beállítás, plusz szolgáltatás/funkció nem kerül konfigurálásra.

A Hivatal korlátozza egyes szoftverek és szolgáltatások hozzáférését. Továbbá tiltja egyes portok, protokollok elérhetőségét elkerülve ezzel a külső támadásokat.

A legszűkebb funkcionalitás biztosítása érdekében szükséges feladatok:

- a. szakfeladatokhoz kapcsolódó, engedélyezett internetelési politika kialakítása, szabályozás, szükséges beállítások (fehérlista, szakfeladatok működtetéséhez nem szükséges portok tiltása)
- b. nyitott portok felülvizsgálata, a szükségtelen portok bezárása,
- c. a szükséges portok fokozott felügyelete, naplózása (operációs rendszer, tűzfal, tűzfalport, Router és egyéb eszköz beállítások: a szükséges portokon kívül ne legyen nyitva port, az adott porton honnan fogadjon bejövő és hova engedélyezzen kimenő forgalmat),
- d. tűzfal konfigurálás: a gyakori portok internet irányából történő elérésének korlátozása (csak Magyarországról elérhető, csak megadott IP címekről elérhető, csak bizonyos felhasználó vagy felhasználók számára elérhető),
- e. üzemeltetéshez használt portok (SSH, RDP, Telnet, LDAP, NTP, SMB, stb.) külső hálózathoz történő elérésének tiltása,
- f. IP alapú eszközök elkülönített címtartomány beállítása (IP telefonok, IP kamerák, stb.). Ha használatban van IP kamera, akkor IP címének a hivatali hálózatának IP címétől eltérő tartományba állítása szükséges (az eszközök nem használhatják a Hivatali IP cím tartományt). Javasolt dinamikus DNS szolgáltatás igénybevétele.
- g. nélkülözhető szoftverek, futtatói környezet eltávolítása (pl. JAVA)

Bármely módosítás esetén szükséges a konfigurációs beállításokat, szoftver és szolgáltatás korlátozásokat, valamint port és protokoll tiltásokat felülvizsgálni és frissíteni, amely a rendszergazda feladata.

3.6.8. Elektronikus információs rendszerelem leltár

A rendszergazdának vagy a Hivatal vezetője által kijelölt felelősnek szükséges:

- a. nyilvántartást készítenie az elektronikus információs rendszer(ek) elemeiről,
- b. azt rendszeres időközönként, minimálisan évente felülvizsgálja és frissítenie,
- c. az alapkoncepció nyilvántartásban vagy más dokumentumban kezelnie.

A leltár célja, hogy információval szolgáljon a Hivatalnál használt eszközökről, ahol lehetséges ezek alapkoncepcióiról, a bekövetkezett változásokról, valamint szükségessé válhatnak a Hivatal számára a hatékony személyes anyagi felelősségre vonhatóságához. Ennek érdekében úgy kell elkészíteni, hogy pontosan tükrözze az elektronikus információs rendszer aktuális állapotát, valamint az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftvelemet tartalmazza az elektronikus információs rendszerekhez vagy felhasználóhoz rendelve.

A leltárt szervezeti egységenként/önkormányzatonként szükséges elkészíteni (tartalmazni kell a rendszerelemek elhelyezési helyét), legalább a következőkre kell kiterjednie:

1. Felhasználói ICT eszközök: felhasználók által használt információs és kommunikációs technológia eszközök és az azokhoz kapcsolódó főbb információk (típus, operációs rendszer, elhelyezkedés, felhasználó).
2. Felhasználói alkalmazások, liszenszek: felhasználó oldali alkalmazások és azok funkciói, egyedi beállítások, liszenszek (szoftver megnevezése, liszensz típusa, liszenszszám).

Az eszközök hálózatba történő illesztéséről készüljön dokumentáció.

A nyilvántartás alapját képező, az elektronikus információs rendszerekhez kapcsolódó hardver és szoftver elemekről rendszerinformációs alkalmazással készített részletes elektronikus vagy papíralapú riportok megőrzése az azt készítő vagy tárolásért kijelölt felelős feladata.

Az elektronikus információs rendszer elem leltárt frissíteni kell az egyes rendszer elemek telepítésének, eltávolításának, frissítésének időpontjában. A frissítés elvégzése vagy a változás jelzése a kijelölt felelős felé a rendszergazda feladata.

3.1.3.3. Duplikálás elleni védelem

A rendszergazdának szükséges ellenőriznie, hogy az elektronikus információs rendszer leltárban nem szerepelnek-e olyan rendszer elemek, amelyek más elektronikus információs rendszer hatókörébe tartoznak.

3.6.10. A szoftver használat korlátozásai

A Hivatal kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak és a szerzői jogi, vagy más jogszabályoknak.

A szoftver használat főbb szabályai a következők:

- a. a telepítések során figyelembe kell venni a konfigurációs változáskezelési folyamatra vonatkozó irányelveket;
- b. a rendszergazda felelőssége a mindenkori üzleti követelményeknek, valamint információbiztonsági követelményeket teljesítő szoftverek, alkalmazások telepítése. Más felhasználók szoftvertelepítési jogot nem kaphatnak;
- c. minden új és meglévő szoftver telepítése/frissítése esetében a kiadott telepítési / frissítési útmutatók az irányadók;
- d. tilos a Hivatal által üzemeltetett munkaállomásokra olyan szoftvert telepíteni, melyhez nincs a Hivatalnak liszensze, vagy (ingyenes liszensz esetén) amelyet a Hivatal nem engedélyez;
- e. a Hivatal által vásárolt szoftverek (és a hozzájuk tartozó dokumentumok) másolása és átadása harmadik félnek tilos, hacsak megfelelő licenyszerződés ezt nem szabályozza másként, ebben az esetben viszont szükséges nyomon követni a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát;
- f. a biztonsági másolat használat létrehozása és tárolása megengedett az információbiztonsági követelmények betartása mellett (védett tárolás);
- g. minden, a felhasználók rendelkezésére bocsátott hardver és szoftver a Hivatal tulajdonát képezi, és mint ilyen eszköz előzetes bejelentés nélkül bármikor ellenőrizhető;
- h. megfelelő jogosultság nélkül a Hivatal alkalmazottja nem férhet hozzá a Hivatal rendszereihez, illetve olyan számítógépekhez, melyek ügyfél adatokat vagy a Hivatalra vonatkozó bizalmas információt tartalmaznak. Nem végezhetnek jogosulatlanul bármiféle változtatást a Hivatal rendszerein, beleértve az adatok törlését vagy megváltoztatását is;
- i. a szerverekre az operációsrendszer és a felhasználási módnak megfelelő alkalmazás csomag, valamint a megfelelő biztonsági beállítások telepítése a rendszergazda által történik.

A szabályok betartását a jegyző és az elektronikus információs rendszer biztonságáért felelős belső auditok keretében ellenőrzi. A Hivatal az elektronikus informatika biztonsággal kapcsolatos szoftverhasználatlaltal kapcsolatos további szabályokat Informatikai biztonsági eljárásrendben vagy egyéb dokumentumban kezelheti.

3.6.11. A felhasználó által telepített szoftverek

Rendszerprogramokat, illetve felhasználói alkalmazásokat kiszolgálókra és munkaállomásokra, infokommunikációs eszközökre csak a rendszergazda telepíthet, másolhat, távolíthat el.

Az eszközök firmware/driver/szoftverfrissítése a legutolsó stabil változatnak megfelelően történjen meg (kivéve a kompatibilitási problémákat okozó frissítéseket (pl. JAVA).

A felhasználók semmilyen szoftvert, alkalmazást nem telepíthetnek a munkaállomásaikra, az infokommunikációs eszköz használata során kizárólag, az eszközre telepített szoftvereket, alkalmazásokat használhatják. Új szoftver, alkalmazás telepítését vagy a meglévő alkalmazás jogosultságváltozását igényelni kell. A rendszergazda jogosult az igény felülvizsgálatára, és ha szükséges, biztonsági vagy gazdasági okból annak elutasítására.

A felhasználó az infokommunikációs eszközre telepített szoftvereket, alkalmazásokat a szoftverhez, alkalmazáshoz kiadott felhasználói leírás szerinti módon, szakszerűen köteles használni.

Azokon az eszközökön, amelyekön önkormányzati ASP rendszer van használatban, vagy adat továbbítódik rá, tilos olyan alkalmazást használni, amely az eszközt az ASP Központon kívüli harmadik féllel köti össze, és amellyel lehetőség van távoli támogatásra, vezérlésre, távoli hozzáférésre, képernyő átvételére stb. (pl. TeamViewer, rAdmin, VNC).

A külső felek által üzemeltetett alkalmazásokhoz kapcsolódó jogosultságokra vonatkozó igényléseket, változásjelentőket és levelezéseket a szervezeti egységek vezetői kötelesek másodpéldányban megküldeni a rendszergazdának. A külső fél által biztosított informatikai szolgáltatások használata során az általa kiadott előírások szerint kell eljárni.

A szoftvereket és adatokat arra nem jogosult harmadik fél számára másolni és továbbadni tilos.

A szoftverek adathordozóit, üzemeltetési és felhasználói dokumentációját, licencdokumentációját a rendszergazda tárolja és tartja nyilván.

3.7. KARBANTARTÁS

3.7.1. Rendszer karbantartási eljárásrend

A rendszeres karbantartás célja, hogy a Hivatal biztosítani tudja, az ügymenethez szükséges eszközök és szolgáltatások zavartalan működését, hiba esetén időben történő javítását. A rendszeres karbantartás során a karbantartásra jogosultaknak szükséges ellenőrizni a munkaállomások, szerverek, perifériák, hálózati eszközök fizikai és szoftveres állapotát, az esetlegesen felmerülő problémák megoldásáról gondoskodniuk kell. Az elektronikus információs rendszer biztonságáért felelős megfogalmazza és dokumentálja a rendszeres karbantartásra vonatkozó kontrollokat, mely szabályozza a rendszeres karbantartási folyamatot és elősegíti annak ellenőrzését.

A Hivatal az elektronikus információbiztonsággal kapcsolatos egyedi karbantartási szabályokat Informatikai biztonsági eljárásrendben vagy egyéb dokumentumban kezelheti.

3.7.2. Rendszeres karbantartás

A rendszeres karbantartásokat csak az arra jogosult személy(ek) végezheti(k) (a 2.1.14 *Karbantartók* fejezet szerint). A Hivatal a karbantartásokat és javításokat ütemezetten hajtja végre, dokumentáltatja, felülvizsgálja és jóváhagyja az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban.

A Hivatalnak a karbantartásokra karbantartási tervvel szükséges rendelkeznie, amelynek elkészítése a rendszergazda feladata. A karbantartási tervben meghatározásra kerül a munkaállomások, szerverek, perifériák, hálózati eszközök fizikai és szoftveres állapotát ellenőrző karbantartások ütemezése, felelőse. Külső személy/szolgáltató esetében a karbantartások ütemezését és azok feltételeit a szerződésben rögzíteni szükséges.

A hibákat, rendszerleállásokat, minden karbantartási tevékenységet dokumentálni szükséges (karbantartási napló/nyilvántartás).

A dokumentálásnak legalább az alábbiakra szükséges kitérnie:

- a. ütemezés (pl. előre ütemezett (tervezett), nem tervezett karbantartás),
- b. mikor történ a karbantartást (dátum, idő),
- c. a karbantartás megnevezése (ellenőrzés, javítás, frissítés stb.),
- d. az érintett eszköz/szoftver, rendszer megnevezése,
- e. módszer (pl. szemrevételezés),
- f. karbantartáshoz szükséges eszközök megnevezése,
- g. ki/kik végezte/ték a karbantartást,
- h. mennyi ideig tartott a karbantartás (ha lényeges),
- i. ha volt rendszerleállás, mennyi ideig tartott,
- j. a karbantartás ellenőrzés tényét (sikeres, sikertelen),
- k. intézkedés megjelölése sikertelen karbantartás esetén,
- l. aláírás.

A karbantartások utáni megfelelő működés ellenőrzése a rendszergazda, illetve külső személy/szolgáltató esetében a megbízott személy/szolgáltató feladata. Sikertelennek bizonyuló működés esetén, az adott eszközt, rendszert nem lehet újra üzembe helyezni, egészen addig, amíg a fennálló hibát ki nem javítják. A javításokért a rendszergazda illetve külső megbízott esetén a külső személy/szolgáltató felelős.

A karbantartások történhetnek munkaidőn kívül, vagy munkaidőn belül. A tervezett munkaidőn belüli karbantartásokat, ha azok az ügymenet kiesésével járnak, a karbantartás előtt 1 héttel közölni kell az ügyfelekkel.

A Hivatal birtokában lévő fizikai szerverek karbantartása a rendszergazda illetve külső személy/szolgáltató esetében a megbízott személy/szolgáltató feladata, szerződéses megállapodás szerint. A szerverek karbantartását ütemezetten, lehetőség szerint, munkaidőn kívül kell végrehajtani.

Adattartalommal bíró adathordozók, információs rendszer vagy rendszerelem szállítása esetén a megfelelő információbiztonsági intézkedések betartása kötelező a 3.6. *Adathordozók védelme* fejezetnek megfelelően. Karbantartás céljából az adathordozók, információs rendszer vagy rendszerelem szállítását a rendszergazda, külső személy/szolgáltató esetében a megbízott személy/szolgáltató végzi.

A Hivatal által használt szoftveres frissítéseket a rendszergazda végzi, figyelemmel kísérve egy-egy új patch megjelenését.

3.7.3.2. Adathordozó ellenőrzés

A rendszergazda a Hivatali munkaállomásokon lévő víruskeresőt úgy állítja be, hogy az automatikusan ellenőrizze a munkaállomásra csatlakoztatott diagnosztikai és teszt programokat tartalmazó adathordozókat a kártékony kódok tekintetében, mielőtt azt az elektronikus információs rendszerben használnák.

3.7.4. Távoli karbantartás

Azokon az eszközökön, amelyeken önkormányzati ASP rendszer van használatban, vagy adat továbbítódik rá, tilos olyan alkalmazást használni, amely az eszközt az ASP Központon kívüli harmadik féllel köti össze, és amellyel lehetőség van távoli támogatásra, vezérlésre, távoli hozzáférésre, képernyő átvételére stb. (pl. távoli asztal, TeamViewer, rAdmin, VNC).

Ha hatóság (pl. NISZ Zrt.) által nem tiltott, vagy technikailag lehetséges, akkor szükséges az engedélyezett hálózatok és hálózati szolgáltatások meghatározása, szükségesség/ engedélyezés esetén a meghatározott végpontok között VPN kapcsolat létrehozása, biztonságos protokollok (pl. üzemeltetési feladatok ellátásához a rendszerek VPN kapcsolaton keresztül történő elérés céljából).

Egyéb esetben (saját hatókörbe tartozó elektronikus információs rendszer, pl. levelező/webszerver stb.) a rendszergazda az alábbiak szerint jár el a távoli karbantartás tekintetében:

- a. jóváhagyja, nyomon követi és ellenőrzi a távoli karbantartási és diagnosztikai tevékenységeket,
- b. akkor engedélyezi a távoli karbantartási és diagnosztikai eszközök használatát, ha az összhangban áll az Informatikai Biztonsági Szabályzattal, és dokumentálva van az elektronikus információs rendszer rendszerbiztonsági tervében,
- c. hitelesítéseket alkalmaz a távoli karbantartási és diagnosztikai munkaszakaszok létrehozásánál,
- d. lezárja a munkaszakaszt és a hálózati kapcsolatokat, amikor a távoli karbantartás befejeződik,
- e. nyilvántartást vezet a távoli karbantartási és diagnosztikai tevékenységekről.

3.8. ADATHORDOZÓK VÉDELME

3.8.1. Adathordozók védelmére vonatkozó eljárásrend

A Hivatal jelen eljárásában rögzíti az adathordozók védelmére vonatkozó előírásait.

A Hivatali munka során használt adathordozók kezelésének szabályozása a megfelelő és biztonságos működés és rendelkezésre állás érdekében történik.

A munkavégzéshez a Hivatal tulajdonában lévő, nyilvántartott adathordozót lehet használni, illetve behozott adathordozó esetében a rendszergazda által ellenőrzött és engedélyezett eszközt (Lásd 2.1.12. *Be- és kiszállítás*). Az adathordozó használatára való igényt a szervezeti egység vezetőjéhez kell benyújtani. A rendeltetésszerű eszközhasználatot a Hivatal elektronikus információs rendszereihez történő csatlakoztatás után, a rendszergazda szűrőpróba szerűen ellenőrizheti.

Adathordozót, vagy adatot adathordozón/mobil eszközön (laptop, pendrive, floppyn, CD stb.) - otthoni munkavégzés és bármilyen más célból - a Hivatalból kijuttatni csak a szervezeti egység vezetője írásos engedélyével szabad az információbiztonsági előírásoknak megfelelően. A Hivatal az adathordozók használatát a Hivatal szakfeladatait támogató szakrendszerek munkaállomásain információbiztonsági megfontolásból utasítással, hardver, illetve szoftver úton korlátozza, szakrendszerek munkaállomásain kívüli minden előzetes értesítés nélkül figyelheti, monitorozhatja.

Az adathordozók információbiztonsági kezelésének általános irányelvei:

- a. informatikai eszközöket, adathordozókat tilos nyilvános helyen vagy harmadik félnél történő munkavégzés során őrizenlenül hagyni;
- b. munkavégzés közben nem lehet a használatban lévő mobil eszközöket felügyelet nélkül hagyni, a használaton kívüli eszközöket védett helyen kell tárolni („tisztasztal” szabálya);

- c. az informatikai infrastruktúra elemeit engedély nélkül, nem a munkaköri feladatba tartozó módon megváltoztatni, vagy eltávolítani nem lehet;
- d. tilos az olyan hordozható adathordozó használata az elektronikus információs rendszerben, melynek tulajdonosa nem azonosítható. Az adathordozókat sorszámmal és/vagy a felügyeletéért felelős nevével azonosítani kell, azokat a felhasználóhoz kell rendelni;
- e. az adathordozókat a felhasználók nem csatlakoztathatják egymás eszközeihez úgy, hogy az eszköz tulajdonosa nem tud róla;
- f. amennyiben kívülről érkezik adat valamilyen adathordozón, annak a megtekintése csak előzetes ellenőrzés és a vírus mentesség megállapítása után használható.

Bármely adathordozó eltűnését azonnal jelenteni kell a szervezeti egység vezetőjének azzal az információval együtt, hogy milyen Bizalmas/Szigorúan Bizalmas minőségű dokumentum kompromittálódott.

Az adathordozók védelme során figyelembe kell venni a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács (EU) 2016/679 rendeletét (GDPR). Ha személyes adatot tartalmazó, kriptográfiai védelemmel el nem látott adathordozó eltűnése, jogosulatlanokhoz jutása feltételezhető, akkor azonnal jelentést kell tenni az adatvédelmi tisztviselő felé.

3.8.2. Hozzáférés az adathordozókhoz

A megbízott szervezeti egység vezető meghatározza az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, jogosultságuk tartalmát.

A Hivatalból kilépő munkatársak vagy szerződéses viszony esetén a szerződés megszűnésében érintett megbízott harmadik felek kötelesek minden a birtokukban vagy használatukban lévő, a Hivatal tulajdonát képező eltávolítható adathordozót a rendszergazdának biztonságosan átadni, aki ellenőrzi, hogy az adathordozó állapota megegyezik-e a kiadáskori állapotával.

3.8.4. Adathordozók tárolása

Az adathordozókat fizikailag ellenőrizni kell és biztonságosan kell tárolni az arra engedélyezett vagy kijelölt helyen, védeni kell mindaddig, amíg jóváhagyott eszközökkel, technikákkal és eljárásokkal nem semmisítik meg, vagy nem törlik a rajtuk tárolt adatokat.

3.8.5. Adathordozók szállítása

Az adathordozók szállítása során az alábbi biztonsági szabályokat szükséges alkalmazni:

- a. a szállításhoz lehetőleg zárható és a káros környezeti hatásoktól védő tokot, dobozt, táskát kell használni;
- b. szállítás közben az adathordozót folyamatosan a munkatárs személyi felügyelete alatt kell tartani;
- c. szállítás során nem szabad az adathordozót másnak átadni, mások felügyeletére bízni,
- d. óvni kell a nagy melegtől, nagy hidegtől, gyors hőmérséklet változástól, közvetlen napsugárzástól, portól, nedvességtől;
- e. ha a készülék a szállítás során túlzottan lehűlt, vagy felforrósodott, használat előtt meg kell várni amíg szobahőmérsékletre kerül;

- f. a munkatársak kötelesek az általuk szállított fizikai adathordozókkal kapcsolatos minden eseményt (elvesztés, sérülés, lopás) felelőseknek vagy az elektronikus információs rendszer biztonságáért felelősnek haladéktalanul jelenteni;
- g. gépkocsival történő szállítás esetén az információs rendszerelemeket zárt/fedett csomagtartóban kell elhelyezni oly módon, hogy védve legyen a rázkódásból, sérülésből adódó károktól. Az információs rendszerelemeket és adathordozókat tilos (még rövid időre is) az autóban hagyni, a munkatársnak jármű elhagyásakor magával kell azokat vinnie;
- h. tilos az informatikai eszközök használatát harmadik feleknek átengedni, sem idegenek, sem családtagok, rokonok, ismerősök nem használhatják ezeket. A tiltás vonatkozik a saját tulajdonú eszközökre és a távmunka során használt eszközökre is.

A Hivatal az adathordozók szállításával kapcsolatos tevékenységeket azokra a személyekre korlátozza, akik általa az eszközök be- és kiszállítására engedélyt kaptak. Az adathordozók szállításával kapcsolatos engedélyeket, tevékenységeket dokumentálnia kell.

„Bizalmas” feletti besorolású adatokat tartalmazó adathordozót különös gondossággal kell szállítani. A mentési adathordozók szállítását csak a rendszergazda vagy az általa megbízott, vagy a szervezeti egység vezető által kijelölt személyek végezhetik.

3.8.5.2. Kriptográfiai védelem

Minden olyan hordozható eszközt, amelyet a Hivatal területén kívül használnak, szállítanak kriptográfiai (hardver titkosítási) mechanizmusokkal kell védeni a digitális adathordozókon tárolt információk bizalmosságának és sértetlenségének védelme érdekében (hordozható adattároló, pl. okostelefon, laptop, pendrive stb.).

A titkosítás elvégzése a rendszergazda feladata, az elektronikus információs rendszerek biztonságáért felelőssel egyeztetett eljárás alkalmazásával.

3.8.6. Adathordozók törlése

Az adathordozók törlésére vonatkozó biztonsági irányelvek:

- a. az adathordozókat elhasználódásuk esetén cserélni és selejtezni kell az adatvesztés elkerülése érdekében,
- b. az adathordozókat selejtezés, a hivatali ellenőrzés megszűnte, vagy újrafelhasználásra való kibocsátás előtt minden esetben adat mentesíteni kell ilyen célú megfelelő alkalmazással,
- c. a nem törölhető adathordozókat meg kell semmisíteni iratmegsemmisítőben vagy más módon össze kell törni,
- d. az adatmentesítés a rendszergazda feladata és felelőssége,
- e. a beépített, azaz nem mobil (nem cserélhető) lemez meghajtók szükség szerinti cseréje, és az elhasználódottak selejtezése a rendszergazda feladata.

A törlési mechanizmusokat a rendszergazda az információ minősítési kategóriájával arányos erősségnek és sértetlenségnek megfelelően alkalmazza:

- a. a „belső használatú” védelmi osztályba sorolt információkat tartalmazó adathordozót úgy kell megsemmisíteni, hogy ne legyen lehetőség a jogosulatlan hozzáférésre,

- b. a „bizalmas” védelmi osztályba sorolt információkat tartalmazó adathordozókat úgy kell megsemmisíteni, hogy az információk helyreállítása csak jelentős támogatással/eszközökkel, emberi erőforrással és időbefektetéssel legyen lehetséges,
- c. a „szigorúan bizalmas” védelmi osztályba sorolt információkat tartalmazó adathordozók helyreállítására nem lehet mód korszerű eszközökkel,
- d. adathordozó selejtezés céljára harmadik félnek, csak adat mentesítve adatható át.

Ha harmadik félnél történő javításra van szükség, és az elmentett adatok előzetes és biztonságos törlésére nem volt lehetőség, akkor a javítást külön megállapodás keretében helyszíni jelenlét betartásával kell elvégeztetni. A selejtezéssel, megsemmisítéssel megbízott 3. féllel titoktartási megállapodást kell kötni.

A törlésre alkalmazott eszközöket és módszereket hatékonyságát a rendszergazdának a szükséges gyakorisággal tesztelni szükséges (visszaállítás megkísérlésével).

A selejtezésről, a hivatali ellenőrzés megszűntéről, vagy újrafelhasználásra való kibocsátásról előtt minden esetben jegyzőkönyvet kell felvenni, melynek tartalmaznia kell a törlés megtörténtét.

3.8.7. Adathordozók használata

A szervezeti egység vezetője engedélyezheti, korlátozhatja vagy tilthatja bizonyos, vagy bármely adathordozó típusok használatát a kijelölt elektronikus információs rendszereken vagy rendszerelemeken működő biztonsági intézkedések használatával. A Hivatal szakfeladatait támogató szakrendszerek munkaállomásain az adathordozók használatát az engedélyezett jogosultságoknak megfelelően kell beállítani (csak az azonosított, a felügyeletéért felelőshöz rendelt adathordozó használható engedélyezett, az engedélyezett adathordozó használat dokumentálása szükséges). A szakrendszerek munkaállomásain információbiztonsági megfontolásból a nem engedélyezett adathordozó használatát technikai korlátozásokkal, beállításokkal meg kell akadályozni, melynek a felelőse a rendszergazda.

3.8.7.2. Ismeretlen tulajdonos

A Hivatal megtiltja az olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek tulajdonosa nem azonosítható. Az adathordozókat sorszámmal és/vagy a felügyeletéért felelős nevével azonosítani kell, azokat a felhasználóhoz kell rendelni.

3.9. AZONOSÍTÁS ÉS HITELESÍTÉS

3.9.1. Azonosítási és hitelesítési eljárásrend

A Hivatalnak gondoskodnia kell arról, hogy a felhasználók mindegyike egyedileg legyen azonosítva és hitelesítve, valamint egyedileg legyenek azonosítva és hitelesítve a felhasználók által végzett tevékenységek. Biztosítani kell ezt azért, hogy a tevékenységek és a hozzájuk tartozó felelősségek egyértelműen azonosíthatók legyenek, illetve, hogy elkerülhetővé váljanak a jogosulatlan hozzáférések, ezáltal csökkenthetőek a jogosulatlan hozzáférésekből származó információbiztonsági incidensek.

A szükséges jogosultságokat a felhasználóknak, az írásos jogosultság igénylését az adatgazdák hagyják jóvá és a rendszergazda/központi szolgáltató által kijelölt adminisztrátor osztja ki/állítja be.

A Hivatal felhasználóinak kiosztott jogosultságokról a nyilvántartás vezetésére kijelölt személynek nyilvántartást kell vezetnie, amelyet legalább évente egyszer az adatgazdákkal közösen felül kell vizsgálni, a nyilvántartást frissíteni kell bármilyen módosítást (pl. személyi változást, jogosultság kiosztását, visszavonását, módosítását) követően.

3.9.2. Azonosítás és hitelesítés (hivatalon belüli felhasználók)

A Hivatal a munkaállomásokon egyedileg azonosítja és hitelesíti a Hivatal felhasználóit, a felhasználók által végzett tevékenységeket/ szerepköröket.

A munkavégzéshez tartozó tevékenységi köröket és az azokhoz szükséges jogosultságokat az elektronikus információs rendszer biztonságáért felelős az adatgazdák és a rendszergazda közreműködésével határozza meg. Más, Hivatali rendszerhez (pl. szerver) való jogosultságokat és tevékenységi köröket az adott rendszerben kell megadni.

A központi szolgáltató rendszereinek használatához szükséges azonosítási és hitelesítési eljárást az üzemeltető határozza meg. ASP-ben a kétfaktoros azonosítás elvárás, amely a jelszó (tudás) alapú hitelesítés és a birtoklás alapú (E-személyi) hitelesítésből áll össze, elemei:

- a. E-személyi, kártyaolvasó, PIN kód
- b. felhasználónév-jelszó

A tenant szintű jogosításokat és eszköz alapú hitelesítéseket az ASP központ üzemeltetője osztja ki, módosítja és vonja vissza, a megfelelő igazgatásszervezési feladatok során meghatározott rend szerint.

A Hivatalnál tilos a csoportos felhasználói azonosítók használata.

3.9.4. Azonosító kezelés

A Hivatal a munkaállomásaihoz és az elektronikus információs rendszerhez, rendszerelemhez való hozzáféréshez szükséges azonosítókat szerepkörök vagy személyek jogosultságaihoz köti.

Az önkormányzati ASP rendszer használata során a jó áttekinthetőség érdekében összehangolt szerepkör-megnevezéseket szükséges alkalmazni. Ugyanannak a felhasználónak több szerepköre is lehet.

A munkaállomáshoz, rendszerelemhez, elektronikus információs rendszerhez, történő hozzáférést biztosító azonosítókat biztosítók:

- a. a rendszergazda (munkaállomáshoz, rendszerelemhez/eszközhöz),
- b. az önkormányzati ASP adminisztrátor (bérlő fiók, tenant szintű felhasználó kezelés)
- c. az önkormányzat szakrendszerei adminisztrátor(ok) (szakrendszer szintű jogosultságkezelés)
- d. egyéb központi szolgáltató (pl. anyakönyv) által kijelölt adminisztrátor

Az elektronikus információs rendszerekhez történő hozzáférést biztosító azonosítókat – informatikai rendszertől függően – a felhasználó vagy a rendszergazda hozza létre. Az azonosítók ismételt felhasználása tilos. A rendszer által meghatározott idő, vagy 3 hónap inaktivitás után az azonosítókat a rendszergazdának le kell tiltania, az azonosító ismételt engedélyezést követően aktiválható ismét.

3.9.5. A hitelesítésre szolgáló eszközök kezelése

Az ASP rendszer kétfaktoros azonosítást alkalmaz:

- a. jelszó (tudás) alapú hitelesítést,
- b. birtoklás alapú (token) hitelesítés (az e-Személyi igazolvánnyal)

Az Önkormányzati ASP Központ a felhasználói azonosításra egységes SSO (Single Sign-On, egyszeri bejelentkezés) szolgáltatást biztosít, melynek célja, hogy a felhasználónak egyszer kell magát azonosítva belépnie a Keretrendszerbe, majd sikeres bejelentkezés után eléri a hozzárendelt szakrendszereket.

Az elektronikus ügyintézéshez szükséges a Központi Azonosítási Ügynökön keresztüli azonosítás:

- a. Ügyfélkapu: olyan azonosítási szolgáltatás, amely lehetővé teszi, hogy a felhasználó biztonságosan léphessen kapcsolatba az elektronikus közigazgatási ügyintézészt nyújtó szervezetekkel
- b. Elektronikus személyazonosító igazolvány, e-Személyi

Amennyiben a felhasználó nem a fenti módon hitelesíti magát, a Hivatal:

- a. ellenőrzi a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát,
- b. meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát,
- c. biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat,
- d. dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket,
- e. megváltoztatja a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az elektronikus információs rendszer telepítése során,
- f. meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit,
- g. a hitelesítésre szolgáló eszköz típusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket,
- h. megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól,
- i. megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét,
- j. lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.

3.9.5.2. Jelszó (tudás) alapú hitelesítés

A jelszavak a felhasználó számítógépes szolgáltatásokhoz való hozzáférési jogosultságának hitelesítésére szolgálnak. A jelszókezelő rendszernek hatékonyan és interaktívan kell biztosítania a megfelelő színvonalú jelszavak használatát.

A Hivatal az alábbi elvárásokat érvényesíti a jelszavak kezelésével kapcsolatosan:

- a. a munkaadások, rendszerlemek, rendszerek hozzáféréséhez szükséges jelszavakat a jelszavak erősségének irányelve alapján kell megadni;
- b. a munkaadásokhoz, rendszerlemekhez, információs rendszerekhez kiadott kezdő jelszavakat kötelező az első bejelentkezés alkalmával megváltoztatni;
- c. a jelszavak erősségének irányelve: a jelszavak minimális hossza 6 karakter, tartalmazniuk kell kis- és nagybetűket, speciális és numerikus karaktereket egyaránt. Tilos olyan jelszavakat alkalmazni, melyek könnyen kitalálhatóak, mint például a személyes adatok, egyértelmű dátumok, gépnévre vagy a felhasználói névre utalóak vagy általános, szótári szavak (pl. „admin”, „password”), illetve amelyek gyári beállítású, alapértelmezett jelszavak;
- d. a felhasználók és megbízott harmadik felek felelősek a személyes jelszavaik megfelelő védelméért és annak következményeiért, ha a jelszavaik mások által ismertté válnak;

- e. a jelszavakat azonnal meg kell változtatni, ha a felhasználó úgy gondolja, hogy azok más tudomására jutottak, vagy valami szokatlant tapasztaltak a számítógépes rendszerükben (ezt követően értesíteni kell a rendszergazdát és az elektronikus információs rendszer biztonságáért felelős személyt);
- f. a jelszavakat rendszeres időközönként, legalább 3 havonta cserélni kell (lehetőség szerint automatikusan kikényszerítve), illetve az elektronikus információs rendszer által kikényszerített, vagy az üzemeltetők által meghatározott időközönként;
- g. új jelszónak nem szabad az utolsó 5 régebbi közül egyiket sem megadni;
- h. a jelszavakat alapvetően tilos leírni;
- i. nem tehető a jelszó egy automatikus bejelentkezési folyamat részévé;
- j. tilos a felhasználóknak bejelentkezni a Hivatal rendszereibe olyan felhasználónévvel, melyet eredetileg nem nekik bocsátottak ki, és amelyek használatára nem jogosultak;
- k. a felhasználók a személyes azonosítójukkal és jelszavukkal elkövetett cselekedetekért felelősséggel tartoznak;
- l. amennyiben a felhasználók által használt rendszerek valamelyike a fentieknél alacsonyabb biztonsági szintet követelne meg, a felhasználóknak minden esetben az itt szereplő szabályok szerint kell eljárni;
- m. ez a jelszó politika érvényes azokra a külső (nem a Hivatal által üzemeltetett) rendszerekre is, amelyeket a felhasználók a munkájukkal kapcsolatosan elérnek.

Szükséges meghatározni a szakrendszerekben a jogosítások kérdését, és a fluktuáció miatt a felhasználók jogosításának időszakos, Hivatali szintű ellenőrzését és esetleges korrekcióját. A folyamatos ügymenet biztosítása érdekében be kell állítani az egyes szakrendszerekben a helyettesítéseket, amennyiben erre lehetőség van, pl. ASP szakrendszerek esetén, vagy biztosítani kell, hogy az egyes szakrendszerekhez több felhasználónak legyen kiosztva jogosultsága.

Törekednie kell a legkisebb jogosultság kiosztásához a felhasználók körében, a *3.10.6. Legkisebb jogosultság elve* alapján. Valamennyi felhasználó munkavégzése során a szükséges és elégséges hozzáférés elve alapján kizárólag a feladat ellátásához szükséges hivatali adat, információ megismerésére, továbbá az adat- és rendszerhozzáférésre a munkavégzéséhez szükséges lehető legrövidebb ideig és szükséges legkisebb jogosultsági szint alkalmazásával jogosult.

A központi szolgáltató kötelező elvárásokat érvényesít a jelszó megadásával kapcsolatban. Az ASP Központ egy esetleges biztonsági incidens során a tenant adminisztrátoroknak privilégiumokkal járó jogosultság-kiosztását számon kérheti.

Azon informatikai rendszerei esetén, ahol jogosultság kizárólag egy felhasználó számára osztható ki, ott ezeket a jelszavakat – informatikai rendszerenként és felhasználónként – nyilván kell tartani, azokat zárt, a felhasználó által a lezárás mentén aláírt, dátummal és névvel ellátott, a jegyző által meghatározott, tűzbiztos, megfelelő mechanikai védelemmel ellátott páncélszekrényben kell tárolni. A folyamatos ügymenet biztosítása érdekében, indokolt esetben, a szervezeti vezető által engedélyezett esetekben, dokumentált módon történő felbontást követően a felhasználónak a megismert jelszavakat azonnal meg kell változtatni. Jelszavakat egyéb helyen tilos leírni.

A hitelesítésre vonatkozó követelményeket valamennyi rendszerelemre vonatkozóan érvényesíteni kell. A menedzselhető hálózati aktív eszköz tekintetében az eszköz gyári, alapértelmezett bejelentkezési azonosítói (név, password) kerüljenek megváltoztatásra.

Csak előre kijelölt, privilegizált felhasználóknak legyen lehetősége bejelentkezni a kérdéses eszközökbe.

A fenti szabályok az elektronikus információs rendszerek által technikailag kikényszeríthető részét a rendszergazdának kell beállítani.

3.9.5.3. Birtoklás alapú hitelesítés

A Hivatal az elektronikus információs rendszer hardver token alapú hitelesítése esetén olyan mechanizmusokat alkalmaz, amely megfelel a Hivatal által meghatározott minőségi követelményeknek, vagy az elektronikus információs rendszer nyilvános kulcsú infrastruktúra alapú hitelesítés esetén összekapcsolja a hitelesített azonosságot az egyéni vagy csoport fiókkal.

A hitelesítésre szolgáló hardver alapú eszközök kiosztását, visszavonását (az E-személyi kivételével) a rendszergazdának, az elektronikus információs rendszerek biztonságáért felelősnek vagy az erre kijelölt felelősnek nyilván kell tartani.

3.9.5.5. Személyes vagy megbízható harmadik fél általi regisztráció

A Hivatal szükség esetén meghatározott hitelesítő eszköz átvételéhez olyan regisztrációs eljárást követel meg, melyet meghatározott regisztrációs szervezet folytat le a Hivatal által meghatározott személyek vagy szereplők jóváhagyása mellett.

3.9.6. A hitelesítésre szolgáló eszköz visszacsatolása

Az elektronikus információs rendszernek fedett visszacsatolást kell biztosítani a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.

A Hivatalnál alkalmazott hitelesítési módszerek érdemi információval nem szolgálnak az esetleges támadóknak. A sikertelen belépést követően, a rendszer minimális üzenetet küld vissza a felhasználónak (pl. elrontott felhasználónév vagy jelszó esetén: „belépés sikertelen, elfelejtett jelszó” stb.)

3.9.8. Azonosítás és hitelesítés (hivatalon kívüli felhasználók)

Az elektronikus információs rendszernek egyedileg kell azonosítania és hitelesítenie a Hivatalon kívüli felhasználókat és a tevékenységüket.

Külső partnerek (szerződött partnerek, harmadik személyek) vonatkozásában a Hivatal IT rendszereihez való hozzáférés csak szerződés alapján biztosítható.

Külső partnerek esetén a hozzáférési jog maximum a szerződés lejáratáig adható.

A Hivatal IT rendszereihez hozzáférési jogot kapott természetes személyek, jogi személyek és jogi személyiséggel nem rendelkező szervezetek a hozzáférési jogot a velük kötött szerződés/ megállapodás és titoktartási nyilatkozatok alapján gyakorolhatják.

3.9.8. Hitelesítésszolgáltatók tanúsítványának elfogadása

A hálózati kapcsolatok titkosításához csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványokat lehet felhasználni.

3.10. HOZZÁFÉRÉS ELLENŐRZÉSE

3.10.1. Hozzáférés ellenőrzési eljárásrend

A Hivatal vezetője megfogalmazza, dokumentálja és kihirdeti a hozzáférés ellenőrzési eljárásrendet, mely a hozzáférés ellenőrzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. A jogosultság kezelés során figyelembe veszi a központi szolgáltató (a jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató) előírásait. Az elektronikus információbiztonsággal kapcsolatos egyedi engedélyezési hozzáférési szabályokat szükség esetén Informatikai biztonsági eljárásrendben kezeli.

Az elektronikus információs rendszer, rendszerelem használója kizárólag olyan munkatárs vagy a Hivatallal szerződéses jogviszonyban álló szerződött partner, harmadik személy lehet, aki a munkavégzéshez szükséges feltételekkel az 1.6.3. *A személyek ellenőrzése* fejezetnek megfelelően rendelkezik. Megismerte jelen szabályzatot, a rá vonatkozó rendelkezéseket, és ennek megfelelően hozzáférési jogosultságot kapott az elektronikus információs rendszerek használatához (a továbbiakban: felhasználó).

A központi szolgáltatók szakrendszereihez történő hozzáféréseket az üzemeltető által meghatározott szabályok alapján kell kezelni.

A hozzáférési jogosultságokat az adatgazda engedélyezi a hatáskörébe tartozó elektronikus információs rendszerek, rendszerelemek, adatok, tevékenységek tekintetében. A jogosultságok beállítását adott rendszertől függően a rendszergazda, vagy a központi szolgáltató által kijelölt adminisztrátor végzi. A kiadott jogosultságok engedélyezéséhez kapcsolódó feljegyzéseket meg kell őrizni.

A Hivatalnál jelenlévő felhasználóknak kiosztott jogosultságokról a rendszergazdának vagy a kijelölt felelősnek nyilvántartást kell vezetnie, amelyet legalább évente egyszer az adatgazdákkal közösen felül kell vizsgálni. Frissíteni kell továbbá, bármilyen módosítást követően.

A hozzáférési jogosultságok megszüntetéséről az alábbi esetekben szükséges intézkedni:

- a. dolgozó kilépése esetén,
- b. ha a Hivatal munkavállalóját a Hivatalon belül áthelyezték,
- c. ha a munkavállaló szervezeti egységen belül marad, de a munkaköre jelentősen megváltozott,
- d. ha a külső partner szerződése lejárt vagy megszűnt,
- e. tartós betegség, távollét, illetve helyettesítés esetén,
- f. visszaélés gyanúja vagy hasonló súlyos biztonsági esemény felmerülése esetén.

A jogosultságok visszavonását adott rendszertől függően a rendszergazda, a magasabb jogosultsággal rendelkező szervezeti egység vezető vagy a központi szolgáltató által kijelölt adminisztrátor végzi.

Az elektronikus információs rendszerekről, eszközökről, jogosultságokról kizárólag a jegyző, az általa kijelölt személy vagy az elektronikus információs rendszerek biztonságáért felelős szolgáltathat adatokat.

3.10.2. Felhasználói fiókok kezelése

A Hivatallal szerződéses jogviszonyban álló szereplők, a szerződésben meghatározott szerepkörökre kaphatnak jogosultságot. Kizárólag csak a 1.6.3. *A személyek ellenőrzése* fejezet követelményeinek teljesülése esetén lehet jogosultságot kiosztani.

Az elektronikus információs rendszer felhasználói fiókjait és típusait (ahol megengedett) a rendszergazda, vagy a központi szolgáltató által kijelölt adminisztrátor határozza meg.

A felhasználói fiókok kezelése a rendszergazda, vagy a központi szolgáltató által kijelölt adminisztrátor feladata. Meghatározzák a munkacsoportokhoz/ szerepkörökhöz tartozó felhasználói feltételeket. Meghatározzák és dokumentáltan kezelik az elektronikus információs rendszerhez hozzáférési jogosultsággal rendelkezők körét, a munkacsoportokhoz/ szerepkörökhöz tartozó jogosultságokat, valamint (szükség esetén) a felhasználói fiókok további jellemzőit.

Hozzáférést csak a szükséges mértékben és időtartamra lehet engedélyezni, figyelembe véve a szerepkörökhöz tartozó feladatokat. Tartományba léptetett eszközök esetén célszerű beállítani a fiókok automatikus tiltását, maximum 5 rontott jelszó, illetve 2 hét inaktivitást követően.

A rendszergazda, vagy a központi szolgáltató által kijelölt adminisztrátor létrehozza, engedélyezi, módosítja, letiltja és eltávolítja a felhasználói fiókokat a Hivatal, valamint a központi szolgáltató által meghatározott feltételekkel összhangban.

A rendszergazda, vagy a központi szolgáltató által kijelölt adminisztrátor ellenőrzi a felhasználói fiókok használatát.

A rendszergazdát, vagy a központi szolgáltató által kijelölt adminisztrátort értesíti kell, ha:

- a. a felhasználói fiókokra már nincsen szükség,
- b. a felhasználók kiléptek vagy áthelyezésre kerültek,
- c. az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak.

A munkaállomásokon a felhasználóknak nem lehet adminisztrátori joguk. Ha az elektronikus információs rendszerek zavartalan működéséhez szükségesek az emelt szintű jogok, a rendszergazdai jogosultságot a rendszergazda javaslatára a szervezeti egység vezető engedélyezheti a szükséges ideig, kizárólag a szakrendszerek használatához, mely nem használható programok telepítésére, beállítások megváltoztatására.

Minden felhasználónak saját felhasználói azonosítóval kell rendelkeznie, az ehhez szükséges jelszavakat az alkalmazott jelszó szabályoknak megfelelően kell képezni. Az első bejelentkezést követően a felhasználóknak meg kell változtatniuk a jelszavukat, a jelszó szabályokat figyelembe véve.

Tiltani kell a csoportos felhasználói azonosítók használatát.

A Hivatalnál több szerepkört betöltő személyek jogosultságai, a szerepköröknek megfelelően külön-külön kell, hogy kialakításra kerüljön.

A rendszergazda meghatározott gyakorisággal (a központi szolgáltató által kijelölt adminisztrátor a központi szolgáltató előírásai alapján), minimálisan évente felülvizsgálja a felhasználói fiókokat, ellenőrzi a fiókkezelési követelményekkel való összhangot.

3.10.3. Hozzáférés ellenőrzés érvényesítése

Az elektronikus információs rendszer és a szabályzatok közötti összhangot szükséges megteremteni annak érdekében, hogy az elektronikus információs rendszer érvényesítse a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

3.10.5. A felelőségek szétválasztása

A Hivatal meghatározza a felhasználók szerepköreit és az azokhoz tartozó feladatokat, felelőségeket, és ezt dokumentáltan a munkaköri leírásokban (külső szerződött partner esetében a szerződésben) kezeli. Minden szerepkörhöz külön-külön meghatározza a hozzáférés jogosultságait, a felelőségek szétválasztása érdekében.

3.10.6. Legkisebb jogosultság elve

A hozzáférés biztosításának alapelvei:

- a. hozzáférést csak a szükséges mértékben és időtartamra szabad engedélyezni, olyan személyek számára, akiknek a feladataik ellátása és/vagy jogaik gyakorlása érdekében indokolt. A szükséges mértékre és időtartamra történő korlátozás nemcsak a hozzáférés kockázatát minimalizálja, hanem a hozzáférő személy által viselt felelőséget is;
- b. a felhasználónak a tőle elvárható gondossággal kell eljárnia az adatkezelés során. Meg kell akadályoznia a kapott hozzáférési jogokkal való visszaélést azáltal, hogy megőrzi a hozzáférési adatok titkosságát;
- c. a Hivatal által használt rendszerekhez, rendszerelemekhez csak a jogosultságkezelési folyamat betartásával adható hozzáférés;
- d. külső partnerek (vállalkozók, hatóságok stb.) vonatkozásában a Hivatal rendszereihez, rendszeremeihez való hozzáférés csak szerződés alapján biztosítható;
- e. külső partnerek esetén a hozzáférési jog maximum a szerződés lejáratáig adható;
- f. a Hivatal rendszereihez, rendszeremeihez hozzáférési jogot kapott természetes személyek, jogi személyek és jogi személyiséggel nem rendelkező szervezetek a hozzáférési jogot a velük kötött szerződés, megállapodás vagy titoktartási nyilatkozatok alapján gyakorolhatják;
- g. a hozzáférési jogosultságokkal történő visszaélés gyanúja esetén a Hivatal minden dolgozója és szerződéses partnere köteles értesíteni az információbiztonsági felelőst,
- h. a felhasználó elszámoltatható minden olyan tevékenységért, amelyet a saját felhasználói azonosítójával végzett, vagy végeztek;
- i. az elektronikus információs rendszerekről és eszközökről kizárólag a jegyző, az általa kijelölt személy vagy az elektronikus információs rendszer biztonságáért felelős szolgáltatathat adatokat;
- j. jelen szabályzattól eltérni az elektronikus információs rendszer biztonságáért felelős engedélye esetén lehetséges (ilyen esetekben is szükséges a folyamat megfelelő dokumentálása).

A központi szolgáltató rendszereiben szintén törekedni kell a legkisebb jogosultság kiosztásosára a felhasználók körében. Az adminisztrátornak a jogosultságok kiosztásánál javasolt figyelembe vennie a Szervezeti és Működési Szabályzatot, amely nem kerülhet ellentmondásba sem jelen szabályzattal, sem a központi szolgáltató előírásaival.

Az ASP Központ egy esetleges biztonsági incidens során a tenant adminisztrátoroknak privilégiumokkal járó jogosultság-kiosztását számon kérheti. Biztonsági audit során, ha az indokoltnál magasabb hozzáférés állapítható meg egyes felhasználók esetében, annak oka jegyzőkönyvben kell, hogy szerepeljen. A jogosultságok kiosztója is felelőssé tehető a gondatlanságból bekövetkezett biztonsági események kapcsán.

3.10.6.2. Jogosult hozzáférés a biztonsági funkciókhoz

A Hivatal a szerepköröknek megfelelően hozzáférési jogosultságokat biztosít a biztonsági funkciókhoz és biztonságkritikus információkhoz.

3.10.6.3. Nem privilegizált hozzáférés a biztonsági funkciókhoz

A Hivatal kötelezővé teszi, hogy a Hivatal biztonsági funkcióihoz vagy biztonságkritikus információihoz hozzáférési jogosultsággal rendelkező felhasználói, a nem biztonsági funkciók használatához ne a különleges jogosultsághoz kötött - úgynevezett privilegizált - fiókjukat vagy szerepkörüket használják.

3.10.6.4. Privilegizált fiókok

A Hivatal az elektronikus információs rendszer privilegizált fiókjait meghatározott személyekre vagy szerepkörökre korlátozza. Minden olyan jogosultság ebbe a körbe tartozik, amely a felhasználói jogoknál több jogot jelent (pl. backup operátor, rendszeradminisztrátor stb.).

Főbb szabályok a privilegizált jogosultságokkal kapcsolatban:

- a. a rendszerek adminisztrációjához kellő rendszergazdai jogosultságot (előjogokat) csak a rendszergazdai feladatkörben foglalkoztatott munkatárs kaphat és csak a feladatkörnek megfelelő rendszerekre érvényesen. A rendszergazdai jogosultságok (előjogok), ahol ennek kifejezett műszaki akadálya nincsen, legyenek egyértelműen személyhez kötöttek, a csoportos azonosítók használata mindenképpen kerülendő;
- b. a rendszergazda az előjogokat biztosító azonosítóját csak a munkavégzéshez feltétlenül szükséges mértékben használja, minden más esetben a normál felhasználói azonosítójával dolgozzon;
- c. mindenképpen kerülni kell olyan rendszerek üzembeállítását, amelyek nem rendszergazda munkakörben dolgozó felhasználók rendszergazdai jogosultságokkal történő felruházását igényelnék;
- d. a központi szolgáltató egy esetleges biztonsági incidens során az adminisztrátoroknak privilégiumokkal járó jogosultság-kiosztását számon kérheti. Biztonsági audit során, ha az indokoltnál magasabb hozzáférés állapítható meg egyes felhasználók esetében, annak oka jegyzőkönyvben kell, hogy szerepeljen. Általánosságban megállapítható, hogy a jogosultságok kiosztója is felelőssé tehető a gondatlanságból bekövetkezett biztonsági események kapcsán.

3.10.10. A munkaszakasz zárolása

A rendszergazdának a munkaállomásokon szükséges automatikus képernyővédelmet beállítani, hogy kizárásra kerüljön az illetéktelen használat. A képernyővédelmet úgy kell beállítani, hogy felhasználói inaktivitást követően meghatározott időtartalom után automatikusan zárolja a munkaállomást. Az időtartamot kockázatelemzést követően a rendszergazda határozza meg, mely a hatóság által elvártaknak megfelelően alapesetben nem lehet több, mint 3 perc.

Az ismételt bejelentkezés kizárólag a felhasználó azonosításával és hitelesítésével történhet (felhasználónév és jelszó megadása).

3.10.10.2. Képernyőtakarás

A rendszergazda úgy állítja be a munkaállomást, hogy a munkaszakasz zárolásakor a képernyőn korábban látható információ egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel - ami a zároló személy nevét is tartalmazhatja - legyen eltakarva.

3.10.11. A munkaszakasz lezárása

A rendszergazda a Hivatal saját hatókörébe tartozó elektronikus információs rendszereket úgy állítja be, hogy az automatikusan lezárja a munkaszakaszt a Hivatal által meghatározott feltételek vagy a munkaszakasz szétkapcsolást igénylő események megtörténte után.

3.10.12. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

Az azonosítás és hitelesítés nélkül végrehajtható felhasználói tevékenységeket dokumentálni kell, indokolni kell a rendszerbiztonsági tervben, vagy más szabályzatban.

A Hivatalban jelenleg nincsenek azonosítás és hitelesítés nélkül engedélyezett tevékenységek.

3.10.14. Vezeték nélküli hozzáférés

Abban az esetben, ha a Hivatal engedélyezi a vezeték nélküli kapcsolaton keresztüli csatlakozást az elektronikus információs rendszeréhez, eljárásrendjében megjelöli a konfigurálásra és csatlakozásra vonatkozó követelményeket, valamint technikai útmutatót ad ki. A vezeték nélküli hozzáférés feltételeként engedélyezési eljárást folytat le, felhasználói korlátozásokat vezet be.

Azokon az eszközökön, amelyeken önkormányzati ASP rendszer van használatban, vagy adat továbbítódik rá, nem engedélyezhető vezeték nélküli hozzáférés.

3.10.15. Mobil eszközök hozzáférés ellenőrzése

A Hivatal belső eljárásrendben felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki az általa ellenőrzött mobil eszközökre, engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást.

A mobil eszközök használatát, Hivatalból történő kiszállítását minden esetben előzetes jegyzői vagy szervezeti egység vezetői engedélyezésnek kell megelőznie.

Az igénylést, kiadást, visszavételt, nyilvántartást, javítást, esetleges elvesztésére vagy a selejtezésére vonatkozó szabályokat eljárásrend tartalmazza.

3.10.15.2. Titkosítás

A Hivatal a mobil eszközök adattároló egységein (laptopok, adathordozók, pl. külső HDD) lehetőség szerint hardveres titkosítást, más esetben fizetett szoftveres titkosítást alkalmaz, a mobil eszközökön tárolt információk bizalmosságának és sértetlenségének a védelmére, illetve az információk hozzáférhetetlenné tételére. Továbbá a mobil eszközöket hitelesítési eljárással védi (pl. BIOS jelszó).

A Hivatalból kiszállított mobil eszközök esetén teljes eszköztitkosítást, tároló alapú titkosítást, vagy más technológiai eljárást kell alkalmazni (pl. Win10 Pro esetén BitLocker, ESET Endpoint Encryption).

Kizárólag hardveres titkosítású pendrive használat engedélyezett.

3.10.16. Külső elektronikus információs rendszerek használata

A Hivatal vezetője a rendszergazda és az elektronikus információs rendszer biztonságáért felelőssel együttműködve meghatározza, hogy milyen feltételek és szabályok betartása mellett jogosult a felhasználó külső rendszerből hozzáférni a Hivatal saját hatókörébe tartozó elektronikus információs rendszeréhez. Külső rendszerből való hozzáférés esetén is biztosítani kell azokat a feltételeket, amelyeket a Hivatal a Hivatali belső rendszerek biztonsága érdekében megvalósít (pl. naprakész víruskereső, naprakész operációsrendszer, tűzfal, biztonságos protokoll használat stb.).

Az engedélyezett külső rendszerek használatát dokumentálni szükséges.

Azokon az eszközökön, amelyeken önkormányzati ASP rendszer van használatban, vagy adat továbbítódik rá, tilos olyan alkalmazást használni, amely az eszközt az ASP Központon kívüli harmadik féllel köti össze, és amellyel lehetőség van távoli támogatásra, vezérlésre, távoli hozzáférésre, képernyő átvételére stb. (pl. TeamViewer, rAdmin, VNC).

3.10.16.2. Korlátozott használat

A Hivatal csak abban az esetben engedélyezi jogosult felhasználóknak egy külső elektronikus információs rendszer felhasználását az elektronikus információs rendszerhez való hozzáférésre, az általa ellenőrzött információk feldolgozására, tárolására vagy továbbítására, ha előzetesen ellenőrzi a szükséges biztonsági intézkedések meglétét a külső rendszeren saját eljárásrendjének megfelelő módon, vagy jóváhagyott, biztonságos kapcsolat van az elektronikus információs rendszerek között, vagy megállapodás született a külső elektronikus információs rendszert befogadó szervezettel.

3.10.16.3. Hordozható adattároló eszközök

A Hivatal szükség szerint korlátozza vagy megtiltja az ellenőrzött hordozható tárolóeszközök használatát külső elektronikus információs rendszerben is jogosultsággal rendelkező felhasználók számára.

3.10.17. Információ megosztás

A Hivatal elősegíti az információmegosztást azzal, hogy engedélyezi a jogosult felhasználóknak eldönteni, hogy a megosztásban résztvevő partnerhez rendelt jogosultságok megfelelnek-e az információra vonatkozó hozzáférési korlátozásoknak, olyan meghatározott információmegosztási körülmények esetén, amikor felhasználói megítélés szóba jöhet (tehát a jogosult felhasználó eldöntheti, hogy akivel az információt megosztaná, az jogosult-e arra, hogy az információ birtokába jusson). Lehetőség szerint automatizált mechanizmusokat vagy kézi folyamatokat alkalmaz arra, hogy segítséget nyújtson a felhasználóknak az információmegosztási vagy együttműködési döntések meghozatalában.

3.10.18. Nyilvánosan elérhető tartalom

Nyilvánosan hozzáférhető rendszerként definiálja a Hivatal a publikus weboldalát.

A Hivatal vezetője kijelöli a weblap tartalom felelőst, aki a jogszabályi követelményeknek és a Hivatal belső szabályainak megfelelően a tartalom feltöltési és karbantartási feladatok ellátásáért felelős. Tilos a hatályos törvénybe, jogszabályba, belső szabályzatba ütköző, vagy a Hivatal érdekeit, a jó ízlést és közérkölcset sértő tartalmat közzétenni.

A Hivatal weboldalán elsősorban hírközlő, információs, tájékoztató jellegű adatokat közöl, a települést mutatja be, aktuális híreket és információkat közöl az állampolgárok számára.

Havonta legalább egyszer, illetve adatfeltöltés után szükséges a honlapot átvizsgálni, és az esetlegesen nem nyilvános adattartalmakat eltávolítani.

Az elektronikus információs rendszer biztonságáért felelősfeladata, hogy a nyilvánosan közzé tehető adatokról oktatást tartson, a nem nyilvános adattartalmak közzétételének elkerülése érdekében.

Amennyiben a Hivatallal szerződéses jogviszonyban álló külső szolgáltató rendelkezik technikai hozzáféréssel, számára a jegyző vagy megbízottja adhat át dokumentált módon írásban – nyilvános közzétételre szánt, ellenőrzött – információt.

3.11. RENDSZER- ÉS INFORMÁCIÓ SÉRTETLENSÉG

3.11.2. Rendszer- és információsértetlenségre vonatkozó eljárásrend

Az elektronikus információs rendszerek, illetve az adatok sértetlenségére vonatkozóan a következő eljárásrendet kell alkalmazni.

Az eljárásrend célja, hogy a Hivatal által használt elektronikus információs rendszerben, rendszeremben bekövetkezett változások úgy, mint: hibajavítás, frissítés, új hardver üzembe helyezése, vagy a rendszerben bekövetkezett bármilyen módosítás esetén, az információsértetlenséget biztosítani tudja. A felsorolt változtatásokat a Hivatal saját hatáskörében kizárólag a rendszergazda végezheti. A rendszergazdának kell gondoskodnia arról, hogy a rendszer működéséhez szükséges alkalmazások, programok mindig naprakészen működjenek. Gondoskodnia kell a működéshez szükséges hardver elemekről, ezek bővítéséről, cseréjéről, selejtezéséről. Az ehhez szükséges frissítéseket, konfigurációs beállításokat/módosításokat/javításokat tervezetten kell elvégeznie.

A módosítások folyamán gondoskodnia kell arról, hogy a felhasználói adatok ne sérüljenek, és illetéktelenek ne tudjanak hozzáférni. A rendszerben bekövetkezett változásokat dokumentáltan kell kezelni, illetve a módosításoknak megfelelően a dokumentációkat is frissíteni kell. (pl. frissítési/telepítési útmutatók, konfigurációs beállítások).

Központi szolgáltatás esetében, a központi szolgáltató határozza meg, hogy ki jogosult fejlesztői, üzemeltetői, működtetői, tesztelési tevékenységet végezni a központi rendszer tekintetében.

3.11.3. Hibajavítás

A műszaki sebezhetőségek ellenőrzés alatt tartása érdekében, a rendszerek műszaki sebezhetőségeit jelentős késedelem nélkül, tervszerűen és ellenőrzött módon ki kell javítani a gyártók által biztosított frissítések (pl. operációs rendszer szintű patchek, BIOS, ROM, FIRMWARE), patchek, megkerülő megoldások használatával. A felhasználók haladéktalanul jelzik felettesüknek vagy a rendszergazdának, ha az informatikai rendszerben fennakadást, leállást, zavart észlelnek. Az ellenőrzést, azonosítást, javítást és jelentést a rendszergazda biztosítja.

Az operációs rendszerek vagy üzletileg kritikus alkalmazások verziófrissítése csak megtervezett módon történhet meg. A biztonságkritikus szoftvereket a frissítésük kiadását követő meghatározott időtartamon belül telepíteni szükséges (a frissítések történhetnek automatikusan is az adott operációs rendszer frissítési beállításainak megfelelően). Egyéb biztonsági kockázatot nem jelentő frissítéseket csak abban esetben kell telepíteni, ha azok üzleti szempontból lényeges hibák, sérülékenységek kijavítását, funkcióbővítést eredményeznek. A változást előzetesen tesztelni kell egy a Hivatali környezethez hasonló teszt rendszerben minden kritikus szolgáltatás és alkalmazás vonatkozásában a kompatibilitás, az alkalmazások helyes működése szempontjából. A változást követően ellenőrizni kell a változás eredményét és hatását.

A rendszerben bekövetkezett változásokat dokumentáltan kell kezelni, illetve a módosításoknak megfelelően a dokumentációkat is frissíteni kell. (pl. frissítési/telepítési útmutatók, konfigurációs beállítások).

A verzióváltással járó alapszoftver módosítással egy időben a változásokat a dokumentációban is át kell vezetni (Munkalap vagy egyéb feljegyzés alapján az Alapkonfiguráció nyilvántartásban). Ha nem a módosítást elvégző rendszergazda felelős a nyilvántartás aktualizálásáért, akkor a Munkalapot el kell juttatni az elektronikus információs rendszer biztonságáért felelős felé.

Egyes központi szolgáltatású rendszer esetében (ASP) a felhasználóknak lehetőségük van a rendszerrel kapcsolatos észrevételek, hibák bejelentésére. Ennek a bejelentési felülete a hibabejelentő rendszer.

3.11.4. Kártékony kódok elleni védelem

Információ feldolgozó rendszerek biztonságos üzemeléséhez és a feldolgozott információ biztonságos kezeléséhez, a sértetlenség és a bizalmasság megőrzéséhez nélkülözhetetlen, a hatékony védekezés a vírusok és a kémprogramok ellen, ezért:

- a. minden szolgáltatás fejlesztéséhez, üzemeltetéséhez, támogatásához stb. használt asztali és mobil számítógépet, valamint szervert védeni kell a vírusoktól folyamatosan frissülő vírusvédelmi rendszer működtetésével. Ezen felül, ha műszakilag lehetséges és információbiztonsági szempontból indokolt egyéb mobil eszközökre is megfelelő védelmet kell biztosítani (okos telefonok);
- b. a vírusvédelmi rendszer kiválasztása, és megfelelőségének ellenőrzése, a rendszergazda feladata, figyelembe véve, hogy az ingyenes alkalmazások nem teljesítik a követelményeket;
- c. a kiválasztásnál figyelembe kell venni, hogy a védendő rendszer eszközeinek teljesítményét csak elfogadható mértékben korlátozza, a hatékony munkavégzést ne gátolja;
- d. a vírusvédelmi rendszert úgy kell üzemeltetni, beállítani, és szabályokat (házirendeket) meghatározni, hogy az akadályozza meg a vírusok adathordozón, vezetékes vagy vezeték nélküli hálózaton, elektronikus levelezésben, vagy internet használat során történő bejutását a rendszerekbe;
- e. a kártékony kódok elleni védelmet úgy kell beállítani, hogy rendszeres ellenőrzéseket hajtson végre a belépési/kilépési pontokon, amikor a fájlokat letöltik, megnyitják, vagy elindítják;
- f. a vírusvédelmi rendszert úgy kell beállítani, hogy szükség esetén automatikusan riassza a rendszergazdát vagy a meghatározott további személy(eke)t
- g. az esetlegesen mégis bejutott vírusok kártételének meggátálása céljából a rendszereket lehetőleg automatikusan, a felhasználó beavatkozását nem igénylő módon, heti rendszerességgel át kell vizsgálni, és a bejutott kártékony kódokat meg kell semmisíteni;
- h. a kártékony kódok észlelése és megsemmisítése során jelentkező esetleges téves riasztásokat rendszergazda ellenőrzi;
- i. a rendszer konfigurálása a rendszergazda, a vonatkozó házirendek kialakítása, azok megfelelő működésének ellenőrzése és dokumentálása az elektronikus információs rendszer biztonságáért felelősfeladata;
- j. a szolgáltató által kiadott frissítéseket a rendszergazda a konfigurációkezelési eljárásnak megfelelően hajtja végre;
- k. a Hivatal minden munkatársa köteles az általa használt eszközökön a vírusvédelmet használni, azt semmiféle okból ki nem kapcsolhatja;

- l. kártékony kód észlelése esetén a kártékony kódokat azonnal karanténba kell helyezni, és jelezni kell a rendszergazdának;
- m. a rendszergazdának jelentenie kell az elektronikus információs rendszer biztonságáért felelős felé a kártékony kódok jelenlétét a rendszerben;
- n. a kártékony kódok megsemmisítése során, figyelembe kell venni annak, a rendszer rendelkezésre állására való kihatását;
- o. a kártékony kódok elleni intézkedéseket az információbiztonsági felelősnek dokumentáltan kell kezelnie és jelentenie kell azt a Kormányzati Eseménykezelő Központ felé.

Az elektronikus postafiókba érkező, ismeretlen feladótól származó, nem szokványos formátumú, gyanús csatolmányt tartalmazó, illetve idegen nyelvű küldeményekkel – a fennálló vírusveszély miatt – fokozott óvatossággal kell eljárni. Gyanús küldemény érkezésekor, illetve a vírusvédelmi rendszer riasztása esetén a csatolmányt megnyitni tilos. Tilos lánclevelek indítása vagy továbbítása.

A Hivatalnak meg kell őriznie az elektronikus információs rendszerek és az információ bizalmasságát, sértetlenségét és rendelkezésre állását a kártékony kódok és a kártékony üzenetek támadásaival szemben.

Az internethasználatra vonatkozó szabályokat az 1.6.9. *Viselkedési szabályok az interneten* fejezet tartalmazza.

3.11.4.3. Automatikus frissítés

A kártékony kódok elleni védelmi mechanizmusokat a rendszergazda úgy konfigurálja, hogy a víruskereső adatbázis automatikusan frissüljön.

3.11.5. Az elektronikus információs rendszer felügyelete

Felelősségi körén belül a rendszergazda vagy a szolgáltató felügyeli az elektronikus információs rendszert, hogy észlelje a kibertámadásokat vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat.

A rendszergazda vagy a megbízott felelős, szolgáltató a rendszer megfelelő működése érdekében figyelemmel kíséri az elektronikus információs rendszer, rendszerelemeinek rendelkezésre állását. Meghibásodás/rendszer hibaüzenet esetén meg kell oldania a problémát. Ellenőrzi, és valós esetben javítja a felhasználóktól érkezett észrevételeket (pl. mikor a felhasználó lassúnak észleli a rendszert), majd ezeket kommunikálja feléjük.

Azonosítja az elektronikus információs rendszer jogosulatlan használatát, és védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben. Az üzembiztonság érdekében a kiszolgálók operációs rendszereinek telepítőkészleteit tartalék adathordozón is tárolja, valamint rendszeresen menti az operációs rendszer beállításait.

Erősíteni kell a rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jel tapasztalható.

Meghibásodás/nem megfelelő üzemelés, esetleges támadás esetén közvetlenül az észlelést követően a rendszer felügyeletéből gyűjtött információkat az elektronikus információs rendszer biztonságáért felelős felé kell kommunikálni.

3.11.6. Biztonsági riasztások és tájékoztatások

Az elektronikus információs rendszer biztonságáért felelős folyamatosan figyeli a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket, folyamatosan figyelemmel kíséri a Nemzeti Kibervédelmi Intézet Kormányzati Eseménykezelő Központtól érkező értesítéseket, szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki, illetve a belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez.

Kialakítja és működteti a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, és kapcsolatot tart az érintett, külön jogszabályban meghatározott szervekkel, megfelelő ellenintézkedéseket és válaszlépéseket tesz. Az informatikai rendszert érintő biztonsági eseményeket a Hivatal e központ felé köteles jelenteni. Az információcsere és a központ kárenyhítő intézkedései során a Hivatal együttműködni köteles. Az ellenintézkedéseket a Hivatal az *1.5.8. Biztonsági eseménykezelési terv* fejezetnek megfelelően végzi el.

Az önkormányzati ASP-t ért incidensek észlelését jelenteni kell az ASP Központ felé is a Kormányzati Eseménykezelő Központ mellett (utóbbi esetén az észlelés nem feltétlenül jelentkezik a Hivatalnál, de kizárni sem lehet). Ennek a bejelentési felülete a hibabejelentő rendszer. A jelentés nem tartalmazhat olyan szenzitív adatot (pl. személyes adatot), elemeket, amelyet harmadik fél nem ismerhet meg.

Az elektronikus információs rendszer biztonságáért felelős a biztonsági riasztásokat és a kapcsolatos intézkedéseket elektronikus nyilvántartásban vagy egyéb dokumentumban rögzíti.

3.11.10. Bemeneti információ ellenőrzés

Az elektronikus információs rendszer ellenőrzi az információ belépési pontok érvényességét.

3.11.12. A kimeneti információ kezelése és megőrzése

A Hivatal az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

A kimeneti információk (pl.: nyomtatott dokumentumok) kezelésével és szétosztásával kapcsolatban a következők az előírások:

- a. gondoskodni kell a kimeneti információ tartalmi ellenőrzéséről,
- b. gondoskodni kell arról, hogy a kimeneti információhoz történő fizikai és logikai hozzáférés csak az arra jogosított személyekre korlátozódjon,
- c. gondoskodni kell arról, hogy a jogosult személyek időben megkapják az elkészült kimeneti információkat,
- d. biztosítani kell, hogy a megsemmisítési eljárások során az kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.

A kimeneti információk kezelése során figyelembe kell venni az információ minősítését. A mindenkori biztonsági osztályok függvényében kerülnek meghatározásra a szabályozások arra vonatkozóan, hogy miként kell eljárni a bizonyos adatokkal, dokumentumokkal.

További elvárásokat a 2.1.6. *A kimeneti eszközök hozzáférés ellenőrzése* és a Hivatal további szabályzatai tartalmaznak.

3.12. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG

3.12.1. Naplózási eljárásrend

Azért, hogy a Hivatal elektronikus információs rendszeréről, rendszerlemeiről naprakész információk álljanak rendelkezésre, gondoskodni kell a rendszer naplózási beállításairól. A naplózási beállítások elvégzése a rendszergazda feladata és felelőssége. A naplózási beállításokat legalább évente egyszer a rendszergazdának kell felülvizsgálni és szükség esetén módosítani, illetve akkor, ha az elektronikus információs rendszerben változás történik.

Ha a Hivatal az elektronikus információs rendszernek csak egyes elemeit vagy funkcióit üzemelteti vagy használja, a naplózás és elszámoltathatóság követelményeit ezen elemek és funkciók tekintetében kell teljesíteni. Amennyiben külső fél végzi a tevékenységet, a szolgáltatás részleteit szerződésben kell rögzíteni.

3.12.2. Naplózható események

A rendszergazda – az elektronikus információs rendszer biztonságáért felelőssel egyeztetve – meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét. A naplózható események meghatározásakor a rendszergazda lehetőség szerint vegye figyelembe az érintett munkatársak információigényeit is.

Az adminisztrátori tevékenységeket a rendszerek meglévő naplózási szolgáltatásai rögzítik, ezekről külön gondoskodni jelenleg nem szükséges.

A Hivatal által használt rendszerek legalább az alábbiakat naplózzák:

- a. a felhasználók be/ki jelentkezését és a profilmódosításokat,
- b. a rendszergazdai jogosultsággal végzett tevékenységeket,
- c. az adatbázisain történő változásokat,
- d. a konfigurációkezelésnek és a változáskövetésnek megfelelően a konfigurációs beállításokat,
- e. a rendszerben bekövetkezett hibákat, eseményeket,
- f. határvédelem logolása,
- g. vírusbeállítások.

A rendszergazdának és az információbiztonsági felelősnek közösen kell felülvizsgálnia a naplózott eseményeket, hogy azok elegendők-e, egy esetlegesen bekövetkezett biztonsági eseményt követő vizsgálat során.

3.12.3. Naplóbejegyzések tartalma

Az elektronikus információs rendszer a naplóbejegyzésekben gyűjtsön be elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele. (pl. felhasználó azonosítója, esemény időpontja, hibakód, vírustámadás stb).

3.12.8. Időbélyegek

A szerverek, a munkaállomások és a tűzfalak belső óráját a naplóbejegyzések követhetősége érdekében úgy kell beállítani, hogy azok az internetről automatikusan szinkronizálódjanak a szokásos internetes időszolgáltatások (NTP) egyikéről. Az óraszinkronizáláshoz szükséges protokoll átengedését a tűzfalakon biztosítani kell.

3.12.9. A naplóinformációk védelme

Az elektronikus információs rendszert, szervereket és munkaállomásokat úgy kell konfigurálni, hogy csak a rendszergazdai jogosultsággal rendelkezők tudjanak a naplóinformációkhoz hozzáférni. Továbbá az adatvédelemmel kapcsolatban az e szabályzatban foglaltak alapján kell mindenkor eljárni.

3.12.11. A naplóbejegyzések megőrzése

A rendszergazda gondoskodik a naplóbejegyzések megőrzéséről, hogy azok segítségül szolgáljanak az esetleges biztonsági események bekövetkeztét követő kivizsgáláskor. A naplózási szolgáltatásokat úgy kell beállítani, hogy azok lehetőség szerint (amennyiben a rendelkezésre álló tárhely lehetővé teszi) legalább 1 évre visszamenőleg rendelkezésre álljanak. Amennyiben nem áll rendelkezésre megfelelő méretű tárhely az eseménynaplók 1 évre visszamenő megőrzéséhez, úgy az eseménynaplót a biztonságos működést nem veszélyeztető maximumban kell beállítani.

3.12.12. Naplógenerálás

Az elektronikus információs rendszernek biztosítani kell a naplóbejegyzések előállítási lehetőségeit a 3.12.2 *Naplózható események* fejezetben meghatározottaknak megfelelően. Lehetővé kell tennie, hogy a rendszergazda kiválassza, mely naplózható események legyenek naplózva az információs rendszer egyes elemeire.

A rendszernek biztosítani kell a naplóbejegyzések előállítását a 3.12.2 *Naplózható események* fejezetben meghatározottak szerinti eseményekre, a 3.12.3 *Naplóbejegyzések tartalma* pontban meghatározott tartalommal.

3.13. RENDSZER- ÉS KOMMUNIKÁCIÓ VÉDELEM

3.13.1. Rendszer- és kommunikáció védelmi eljárásrend

A Hivatalon belüli kommunikáció, információáramlás célja, hogy a munkatársak hozzájussanak mindazon információkhoz, mely a Hivatal hatékony működéséhez szükséges. Különös tekintettel vonatkozik ez a szakmai jellegű információk, információbiztonsági előírások átadására, eljuttatására a Hivatal minden érintett munkatársa számára.

A Hivatalon belül az információk átadása az alábbi módszerekkel történhet:

- a. értekezletek, megbeszélések,
- b. elektronikus levelezési rendszerben küldött üzenetek,
- c. megosztott mappák.

Az értekeztet(ek)ről feljegyzés/jegyzőkönyv készül, amelyek esetében minden munkatárs saját felelőssége, hogy az értekezleten elhangzott információkat bizalmasan kezelje, munkája során alkalmazza, és a feladatokat végrehajtsa.

Az elektronikus információs rendszer biztonságáért felelős feladata, hogy minden érintett szereplővel kapcsolatban, a jelen szabályzatban leírt kommunikációra és rendszervédelemre vonatkozó biztonsági követelmények teljesülését ellenőrizze, ide értve az 1.6.9. *Viselkedési szabályok az interneten* fejezetben leírtakat is.

Jelen szabályozások felülvizsgálata és indokolt esetben történő frissítése az elektronikus információs rendszer biztonságáért felelős feladata, legalább évente egyszer.

A szolgáltatónak gondoskodnia kell a biztosított szolgáltatás elvártak szerinti működéséről, ehhez kártékony szoftvereket és illetéktelenek általi behatolásokat elhárító biztonsági határvédelmi megoldásokat, szükség esetén pedig a megfelelő incidenskezelési és analízisre szolgáló eszközöket kell alkalmaznia.

A szolgáltató feladata (ahol értelmezhető):

- a. virtuális gépek alkalmazása esetén a virtuális gépek más gépek felől, a fizikai hosztról és hálózat felől érkező támadások elleni védelme;
- b. nyomon követni a hálózati erőforrásokhoz, alkalmazásokhoz és adatokhoz való hozzáféréseket;
- c. az alkalmazási szintig elérő sebezhetőség esetén az alkalmazás-specifikus védelmi megoldásokat biztosítani (pl. levelezőprogram, spamszűrő, böngésző biztonsági frissítése);
- d. az alkalmazói szoftverek alatti rétegeket érintő sebezhetőségi pontokat megfelelő eszközökkel védeni (tűzfalak, böngészők frissítése stb.);
- e. az alkalmazás biztonságosan futtatható üzemmódra konfigurálása (pl. titkosítás kliens-szerver kommunikációban), és integrálása az alkalmazást igénybe vevő meglévő technikai biztonsági intézkedéseivel (azonosítás, hitelesítés, engedélyezési folyamatok). Az erre szolgáló technikai eszközök a széles körben használt szabványoknak megfelelőek legyenek (SSH, SFTP, SSL/TSL).

3.13.6. A határok védelme

Az informatikai hálózati határvédelem során a Hivatal informatikai hálózatában az internetkijárat, valamint minden külső, nem megbízhatónak ítélt hálózat felé történő kommunikáció során a belső hálózat és az ott elhelyezkedő elektronikus információs rendszerek és adatok védelme érdekében biztonsági és védelmi megoldásokat kell alkalmazni.

Gondoskodni kell a hálózat fizikai elemeinek védelméről, így különösen:

- a. vezetékek és végpontok illetéktelenek általi hozzáféréseinek megakadályozásáról,
- b. szükséges nem használt portok tiltásáról/porthasználat szűkítésről adott ip/ip tartományra, figyelembe véve a 3.3.6.7. *Legszűkebb funkcionalitás követelményeit*
- c. a vezeték nélküli kapcsolatok megfelelő titkosításáról (WPA2/PSK vezeték nélküli titkosítás szükséges)
- d. az eszközöz való illetéktelen hozzáférés megakadályozásáról

Az elektronikus információs rendszernek felügyelni és ellenőrizni kell a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt. A nyilvánosan hozzáférhető rendszer elemeket fizikailag vagy logikailag al-hálózatokban kell elhelyezni, elkülönítve a belső Hivatali hálózattól. A hatósági elvárásoknak megfelelően szükséges a szakrendszereket használó számítógépek, a nyílt internetet használó számítógépek és a nyilvános (vendég-) hálózatot használó számítógépek fizikai (Switch-el történő elszeparálással) vagy logikai elkülönítése (VLAN) külön, átjárhatatlan alhálózatokban.

Az elektronikus információs rendszer csak a Hivatal biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeket keresztül kapcsolódhat külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.

Mind a belső, mind a külső hálózati szolgáltatókhoz történő hozzáférést a következő módon kell ellenőrizni:

- a. megfelelő interfészt kell alkalmazni a Hivatal és más szervezet tulajdonában lévő, vagy nyilvános hálózat között;

- b. a felhasználókat jelszóval megfelelően hitelesíteni kell;
- c. ellenőrizni kell a felhasználók információszolgáltatáshoz való hozzáférését.

Az informatikai határvédelemmel, tűzfalal kapcsolatos elvárások:

- a. a szervezet internethez való csatlakoztatása a központi tűzfalon keresztül történjen meg
- b. a tűzfal szabályokat szükség esetén egyeztetni kell a központi szolgáltatóval (NISZ Zrt.)
- c. a tűzfal szabályok dokumentálása és azok zárható helyen történő tárolása legyen biztosítva

A rendszergazda feladata:

- a. határvédelmi rendszerek szoftvereinek naprakészen tartása, határvédelmi eszközök feketelistájának frissítése
- d. hálózati nyomtató megosztásának jelszavas védelme, vagy a szkennelt mappa ütemezett törlése
- e. tűzfal logok elemzése

3.13.10. Kriptográfiai kulcs előállítása és kezelése

A kriptográfiai eszközök bevezetése esetén ki kell dolgozni az eszközök biztonságos használatát garantáló szabályozást, melynek a következőket kell tartalmaznia:

- a. az eszközök védelmét biztosító előírások;
- b. az eszközök felhasználására vonatkozó követelmények;
- c. a kulcsok generálására, elosztására, tárolására és megsemmisítésére vonatkozó szabályok;

Titkosítás használata esetén a szolgáltatónak kriptográfiai kulcsok menedzselésére, védelmére, az azokhoz való hozzáférési szabályokra vonatkozó eljárásrendet kell kidolgoznia és alkalmaznia, igazodva az alkalmazott kulcsok jellegéből következő technikai követelményekhez (pl. nyilvános kulcsú titkosítás esetén a kulcspároknak megfelelő kezelése, szimmetrikus kulcsú titkosításnál a kulcskiosztás bizalmassága, az ezeket garantáló technikai eszközök igénybe vételével).

3.13.12. Együttműködésen alapuló számítástechnikai eszközök

Az elektronikus információs rendszernek meg kell gátolnia az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha a Hivatal engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszközöknél.

A Hivatal nem alkalmaz a központi szolgáltatású elektronikus információs rendszerben távolról elérhető eszközöket, következésképpen nincs lehetőség távoli aktiválásra. A rendszergazda feladata Házirendben a hozzáférések szabályozása, vagy driver-ek eltávolítása, hardvertiltás beállítása.

3.13.22. A folyamatok elkülönítése

Az elektronikus információs rendszernek elkülönített végrehajtási tartományt kell fenntartani minden végrehajtó folyamatra.

Az elektronikus információs rendszernek elkülönített végrehajtási tartományt kell fenntartani minden végrehajtó folyamatra (hálózati támadástól való védelem érdekében a szakrendszerei munkaállomások különálló védett hálózatba elhelyezése (vlan) lásd 3.13.6. *A határok védelme* fejezet).

Kapcsolódó melléletek

Melléklet száma	Melléklet megnevezése
1. sz. melléklet	Biztonsági osztályba és szintbe sorolás
2. sz. melléklet	Titoktartási és megismerési nyilatkozat minta

Alapfogalmak

adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;

adatgazda: annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik;

adatifeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik;

adatifeldolgozó: az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki/amely az adatkezelő részére adatifeldolgozást végez;

adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése;

adatkezelő: az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatifeldolgozóval végrehajtatja;

adminisztratív védelem: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás;

alapkonzfiguráció (baseline): egy adott időpillanatban a konfigurációs elemek jellemzőinek és azok kapcsolatának állapota, amely hivatkozási alapként felhasználható egy későbbi időpontban;

archiválás: a Hivatali alaptervékenység szempontjából lényeges azon információk és dokumentumok tárolásának célját szolgálja, amelyekre a folyamatban lévő feladatok teljesítéséhez már nincs szükség, de jogi követelmények miatt vagy más célokra bizonyos időpontig (tárolási időtartam) megőrzendők;

archivált adatok: információk és dokumentumok, amelyek archívumban kerültek elhelyezésre (Az archivált adatokat időállóan és igazolhatóan, alkalmas technológiák segítségével kell tárolni, pl. elektronikus, mágneses, optikai vagy kinyomtatott formában.);

archiválási rendszer: az archiváláshoz felhasznált, hardver- és szoftver-elemekből álló technikai rendszer;

auditálás: előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;

backup (adatmentés): az információknak az esetleges adatvesztéssel szembeni védelmét szolgáló kiegészítő tároló közegen történő mentése (Ily módon biztosítja a backup az információk rendelkezésre állását és integritását.);

bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;

biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége;

biztonsági osztályba sorolás: a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;

biztonsági szint: a Hivatal felkészültsége az lbtv. törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

biztonsági szintbe sorolás: a Hivatal felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

elektronikus információs rendszer (az lbtv. alkalmazásában): az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese;

elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy: állami és önkormányzati szervek esetében a szervezeti és működési szabályzat és a munkaköri leírások alapján, az lbtv. hatálya alá tartozó egyéb szervek esetében a munkaköri leírásban vagy egyéb módon a feladatok ellátásával megbízott személy;

elektronikus információs rendszerek védelméért felelős vezető: az állami és önkormányzati szervek esetében a szervezeti és működési szabályzat alapján, az lbtv. hatálya alá tartozó egyéb szervek esetében munkaköri leírásban vagy egyéb módon kijelölt vezető;

életciklus: az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam, az állapotváltozások meghatározott menete, amely jellemző az adott konfigurációs elem típusra;

észlelés: a biztonsági esemény bekövetkezésének felismerése;

éves továbbképzés: az elektronikus információs rendszerek védelméért felelős vezető, az elektronikus információs rendszer biztonságáért felelős személy és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy iskolarendszeren kívüli továbbképzése;

felhasználó: egy adott elektronikus információs rendszert igénybe vevők köre;

felhasználó-felismerés: a felhasználó-felismerés a hálózatokon vagy alkalmazásokon belül a felhasználó egyértelmű beazonosítására szolgál. A felhasználó-felismeréshez felhasználói jogok hozzárendelésére kerül sor;

fenyegetés: olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;

fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;

folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;

globális kibertér: a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese;

illegális szoftverhasználat: egy számítógépes program jogtalan lemásolása és használata - megsértve a szerzői jogi törvényt, valamint a szerzőnek a szoftver licenz szerződésben leírt feltételeit (aki szoftvert illegálisan használ, az a szerzői jogi törvény értelmében büntetőjogi törvénybe ütköző cselekedetet követ el);

információ: bizonyos tényekről, tárgyokról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti;

jogosultság, hozzáférési jogosultság: az informatikai rendszer védelmi mechanizmusainak azon eleme, amely meghatározza, hogy a kezelésre jogosult egyed (személy, program, folyamat stb.) milyen erőforrást (adatot, adathordozót, szolgáltatást, eszközt) milyen módon kezelhet (olvashat, írhat, módosíthat, törölhet, használhat stb. illetve ezek kombinációja);

jogosulatlan másolás: a szoftver licenz szerződés, amennyiben eltérően nem rendelkezik, a vevőnek csak egyetlen "biztonsági" másolat készítését engedélyezi, arra az esetre, ha az eredeti szoftver lemeze meghibásodna, vagy megsemmisülne (Az eredeti szoftver bármely további másolása jogosulatlan másolásnak minősül, és megsérti a szoftvert védő és használatát szabályozó licenz szerződést, valamint a szerzői jogi törvényt.);

kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez;

kibervédelem: a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését;

kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;

kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;

kockázatkezelés: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása, intézkedések kiválasztására és végrehajtására a kockázat csökkentése érdekében;

kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;

korai figyelmeztetés: valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;

kritikus adat: az Infotv. szerinti személyes adat, különleges adat vagy valamely jogszabállyal védett adat;

létfontosságú információs rendszerelem: az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené;

létfontosságú információs rendszerelem: az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené;

logikai védelem: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;

magas biztonsági követelményű elektronikus információs rendszerek: jelen Informatikai biztonsági szabályzatban használt meghatározás szerint: 3-as vagy magasabb biztonsági osztályba sorolt elektronikus információs rendszerek (nem jogszabályi definíció);

magyar kibertér: a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarország felé irányulnak, illetve Magyarország érintett benne;

megelőzés: a fenyegetés hatása bekövetkezésének elkerülése;

megőrzési időtartam: az azon időtartam, amely azzal a nappal záródik le, amelyen a törvényi vagy egyéb, a megőrzésre vonatkozó követelmény véget ér;

munkahely: a felhasználók által használt végponti készülék és mobil adathordozó;

reagálás: a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;

rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;

sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvártnal megegyeznek, ideértve a bizonyosságot abban, hogy az, az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

sérülékenység: az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;

sérülékenység vizsgálat: az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;

súlyos biztonsági esemény: olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;

számítógépes eseménykezelő központ: az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik [(európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)];

szellemi tulajdon: törvények szerint egy eredeti számítógépes program az azt létrehozó személy vagy vállalat szellemi tulajdona és engedély nélküli másolásuk törvénybe ütköző cselekedet;

szoftver licenz szerződés: egy adott szoftver esetében a licenz szerződés határozza meg a szerzői jog tulajdonosa által megengedett szoftverhasználat feltételeit (A szoftverhez adott licenz szerződésre külön utalás történik a szoftver dokumentációjában, vagy a program indításakor megjelenő képernyőn is. A szoftver ára tartalmazza a szoftver licenzjét, és megfizetése kötelezi a vevőt, hogy a szoftvert kizárólag a licenz szerződésben leírt feltételek szerint használja.);

tudás alapú hitelesítés: olyan hitelesítési eljárás, mód, mely során a felhasználó az általa mások előtt titokban tartott ismeret alapján hitelesíti a rendszerben magát (például jelszó, PIN kód);

szervezet: az adatkezelést végző, illetve az adatfeldolgozást végző vagy végeztető jogi személy vagy egyéni vállalkozó, valamint az üzemeltető;

teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;

üzemeltető: az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős;

üzemzavar: az a helyzet, amelyben az üzleti folyamatok és/vagy üzleti rendszerek nem az előirányzottak szerint működnek. Az ebből adódó potenciális károk csekély mértékűek, mivel a feladat-teljesítés csak lényegtelen mértékben sérül (pl. Üzemzavar a helyi IT rendszerek lokalizált olyan mértékű hibája, amelyet a normál IT support a normál SLA időközön belül elhárítani képes. Az elhárítás ideje előre jelezhető és nem igényli üzleti oldali kényszerintézkedések, speciális eljárások használatát.);

technikai számlák: a személyhez nem kötött felhasználó-felismeréseket technikai számláknak nevezzük. Elsősorban olyan funkciók és feladatok számára kerülnek bevetésre, amelyek nem igénylik a mindenkori felhasználó interaktív tevékenységét, hanem pl. az IT rendszerek közötti adatcseréhez szükségesek;

teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem,

üzemeltető: az elektronikus információs rendszer vagy annak részeinek működtetését végzi;

válság: összetett és átláthatatlan helyzet rendkívül magas kárpotenciállal, amely a Hivatal létét veszélyezteti. A meglévő vészhelyzeti tervek csak feltételesen hatékonyak. (A válság eseti, egyedi kezelést és azonnali ad-hoc döntések meghozatalát követelheti a Hivatal vezetésének bevonásával.);

változat (variant): egy olyan konfigurációs elem, amely alapvetően egy adott konfigurációs elem szerint épül fel, attól csak kis mértékben tér el.

védelmi feladatok: megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés;

vészhelyzet: az IT folyamatok, eszközök vagy rendszerek nem az előírásoknak megfelelően működnek és funkcióik nem állíthatók helyre a szükséges időtartamon belül, és az ügymenet oly mértékben sérül, hogy nagy kárszint állhat elő, a Hivatal alaptevékenységének végzése, azonban nem kerül veszélybe (pl. üzemzavar elhárításának határideje nem látható előre, vagy a várható határidő túlmutat az SLA szerinti vállaláson és az üzemzavar következtében a kár enyhítése üzleti oldali lépések megtételét, rendkívüli intézkedéseket, vészhelyzeti forgatókönyvek aktiválását teszi szükségessé);

zárt célú elektronikus információs rendszer: jogszabályban meghatározott elkülönült nemzetbiztonsági, honvédelmi, rendészeti, igazságszolgáltatási, külügyi feladatokat ellátó elektronikus információs, informatikai vagy hírközlési rendszer;

zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem.

Szirmabesenyői Polgármesteri Hivatal

Cselekvési terv (NEIH adatszolgáltatáshoz)

a 2013. évi L. törvényben meghatározott követelmények teljesítésére
41/2015. (VII. 15.) BM rendelet szerinti védelmi intézkedések

Követelmény-azonosító	Követelmény a 41/2015. (VII. 15.) BM rendelet szerint	Követelmény bevezetésének elvárt határideje	Meghatározott intézkedés határideje (ha nem az elvárt)	Felelős
3.1.4.8.1.4.	Az elektronikus információs rendszer mentései	2018.06.30		Jegyző
3.1.4.9.	Az elektronikus információs rendszer helyreállítása és újraindítása	2018.06.30		Jegyző
3.2.1.3.1.2.	Fizikai belépési engedélyek	2018.06.30		Jegyző
3.2.1.4.1.8.	A fizikai belépés ellenőrzése	2018.06.30		Jegyző
3.2.1.4.1.9.	A fizikai belépés ellenőrzése	2018.06.30		Jegyző
3.3.7.2.1.1.	Rendszeres karbantartás	2018.06.30		Jegyző
3.3.7.2.1.2.	Rendszeres karbantartás	2018.06.30		Jegyző
3.3.7.2.1.4.	Rendszeres karbantartás	2018.06.30		Jegyző
3.3.7.2.1.6.	Rendszeres karbantartás	2018.06.30		Jegyző
3.3.10.2.1.1.	Felhasználói fiókok kezelése	2018.06.30		Jegyző
3.3.10.2.1.2.	Felhasználói fiókok kezelése	2018.06.30		Jegyző
3.3.10.2.1.3.	Felhasználói fiókok kezelése	2018.06.30		Jegyző
3.3.10.2.1.4.	Felhasználói fiókok kezelése	2018.06.30		Jegyző
3.3.10.2.1.5.	Felhasználói fiókok kezelése	2018.06.30		Jegyző
3.3.10.2.1.6.	Felhasználói fiókok kezelése	2018.06.30		Jegyző
3.3.10.2.1.7.1.	Felhasználói fiókok kezelése	2018.06.30		Jegyző
3.3.10.2.1.7.2.	Felhasználói fiókok kezelése	2018.06.30		Jegyző
3.3.10.2.1.7.3.	Felhasználói fiókok kezelése	2018.06.30		Jegyző
3.3.10.2.1.8.1.	Felhasználói fiókok kezelése	2018.06.30		Jegyző
3.3.10.2.1.8.2.	Felhasználói fiókok kezelése	2018.06.30		Jegyző
3.3.10.2.1.8.3.	Felhasználói fiókok kezelése	2018.06.30		Jegyző
3.3.10.2.1.9.	Felhasználói fiókok kezelése	2018.06.30		Jegyző
3.3.10.2.1.10.	Felhasználói fiókok kezelése	2018.06.30		Jegyző
3.3.11.4.1.1.	Kártékony kódok elleni védelem	2018.06.30		Jegyző
3.3.11.4.1.3.2.	Kártékony kódok elleni védelem	2018.06.30		Jegyző
3.3.11.5.1.1.	Az elektronikus információs rendszer felügyelete	2018.06.30		Jegyző
3.3.11.5.1.2.	Az elektronikus információs rendszer felügyelete	2018.06.30		Jegyző
3.3.11.5.1.3.	Az elektronikus információs rendszer felügyelete	2018.06.30		Jegyző
3.3.11.5.1.4.	Az elektronikus információs rendszer felügyelete	2018.06.30		Jegyző
3.3.11.5.1.5.	Az elektronikus információs rendszer felügyelete	2018.06.30		Jegyző
3.3.11.5.1.6.	Az elektronikus információs rendszer felügyelete	2018.06.30		Jegyző
3.3.12.8.1.1.	Időbélyegek	2018.06.30		Jegyző

Követelmény-azonosító	Követelmény a 41/2015. (VII. 15.) BM rendelet szerint	Követelmény bevezetésének elvárt határideje	Meghatározott intézkedés határideje (ha nem az elvárt)	Felelős
3.3.12.9.1.	A naplóiinformációk védelme	2018.06.30		Jegyző
3.3.12.11.	A naplóbejegyzések megőrzése	2018.06.30		Jegyző
3.3.13.6.1.1.	A határok védelme	2018.06.30		Jegyző
3.3.13.6.1.2.	A határok védelme	2018.06.30		Jegyző
3.3.13.6.1.3.	A határok védelme	2018.06.30		Jegyző
3.3.13.12.	Együttműködésen alapuló számítástechnikai eszközök	2018.06.30		Jegyző

Kelt.:

Dr. Szakos Judit

Jegyző

#	Rendszer/alkalmazás neve	Rendszer/alkalmazás rövid neve	Biztonsági osztály
1	ASP Adó szakrendszer (bevezetés alatt álló informatikai rendszer)	ASP_adó	4
2	ASP Gazdálkodási szakrendszer (bevezetés alatt álló informatikai rendszer)	ASP_gazd	3
3	ASP Ingatlan-kataszter szakrendszer (bevezetés alatt álló informatikai rendszer)	ASP_ing	3
4	ASP Iratkezelő szakrendszer (bevezetés alatt álló informatikai rendszer)	ASP_irat	3
5	ASP Keretrendszer (bevezetés alatt álló informatikai rendszer)	ASP_keret	4
6	ASP Portálrendszer (bevezetés alatt álló informatikai rendszer)	ASP_portál	3
7	ASZA Anyakönyvi szolgáltató rendszer	ASZA	2
8	Cím és körzetnyilvántartás	CIMNYILV	2
9	CSTINFO	CSTINFO	2
10	E-adat	E_ADAT	2
11	EAK Elektronikus Anyakönyvi Rendszer	EAK	2
12	Ebnyilvántartó - nebih.gov.hu	EB NEBIH	2
13	EBR 42	EBR_42	1
14	EPER (csak lekérdezésre)	EPER	2
15	Gépjármű havi változás feldolgozása	Gj Havi	2
16	Helyi Vizual Regiszter	H_VIZUAL_REG	2
17	Hivatali kapu	HKP	2
18	IPL KEK KH Integrált Portál-alapú Lekérdező Rendszer	IPL KEK KH	2
19	Karton	KARTON	2
20	Katawin (lekérdezésre)	KATAWIN	2
21	KCR	KCR	2
22	KGR K11	KGR_K11	2
23	KIR (oktatas.hu)	KIR	1
24	KIRA	KIRA	2
25	Kormányhivatali webfelület	BORSOD_GOV_HU	2
26	Korona Takarékszövetkezet Electra	Korona_Electra	2
27	Közigállás	KOZIGA	1
28	KSA Közszolgálati Statisztikai Adatgyűjtő	KSA	1
29	KSH Elektra	KSH_ELEKTRA	1
30	KTK Közfoglalkoztatási Támogatások Keretrendszere	KTK	2
31	Nemzeti Választási Rendszer	NVR	2
32	NJT	NJT	2
33	NRSZH Támop projekt igénylés Kezelő Rendszer	NRSZH_TAMOP	2
34	OBP	OBP	1
35	Önegm	ONEGM	2
36	ONKADO (csak lekérdezésre)	ONKADO	2
37	PROBONO	PROBONO	2
38	PTR	PTR	2
39	Takarnet	TAKARNET	2
40	TARTINFO Tartalékállomány információs rendszer	TARTINFO	2
41	TelR Országos Területfejlesztési és Területrendezési Információs Rendszer	TEIR	1
42	TÉR Teljesítmény Értékelő Rendszer	TÉR	2
43	TEVADMIN	TEVADMIN	2

#	Rendszer/alkalmazás neve	Rendszer/alkalmazás rövid neve	Biztonsági osztály
44	TKKI Helyi esélyegyenlőségi program	TKKI	1
45	TSZR	TSZR	2
46	VÁKIR	VAKIR	2
47	Vizuális Közfoglalkoztatási Piac	VIZUAL_KOZFOG_PIAAC	1
48	Winszoc	WINSZOC	2

Készítette: Szűcsné Tóth Éva Zsuzsanna - elektronikus információs rendszerek biztonságáért felelős

Kilencedik napirendi pont:

Husztai Gábor polgármester:

Juhászné Molnár Mária képviselő-asszony ajánlja fel képviselői alapját a római katolikus templom külső felújításához.

Hozzászólások:

Asztalos Erika képviselő, a Pénzügyi Bizottság elnöke:

A Bizottság elfogadásra javasolta a határozat-tervezetet.

A napirendi pont keretében egyéb hozzászólás, kérdés nem volt, annak megtárgyalását a polgármester lezárta, indítványára a Képviselő-testület egyhangúlag, 6 fő igen szavazatával, ellenszavazat és tartózkodás nélkül meghozta a következő határozatot:

Szirmabesenyő Nagyközség Önkormányzata Képviselő-testületének

72/2018. (VI.20.) Kt. határozata a képviselői alap terhére benyújtott támogatási döntésről

Szirmabesenyő Nagyközség Önkormányzata Képviselő-testülete egyhangúlag, 6 fő igen szavazatával, ellenszavazat és tartózkodás nélkül hozzájárul Juhászné Molnár Mária képviselő asszony képviselői alapjából 150.000,-Ft felhasználásához a Szirmabesenyői Római Katolikus Templom külső felújítási munkálatai költségeihez.

A határozat utasítja a Gazdálkodási Csoport vezetőjét az előirányzat átcsoportosítására.

Határidő: 2018. december 31.

Felelős: Gazdálkodási Csoport vezetője

Husztai Gábor s.k.
polgármester

dr. Szakos Judit s.k.
jegyző

Tizedik napirendi pont:

Husztai Gábor polgármester:

A térítési díjak nem emelkednek. A lakosság felé ez a legfontosabb.

dr. Szakos Judit jegyző:

A térítési díjak felülvizsgálata, azokkal kapcsolatban számítások végzése minden évben kötelezettség, akkor is, ha nem változnak a díjak.

A bölcsődében emelkedik a támogatás mértéke.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

A Bizottság elfogadásra javasolta a rendelet-tervezetet.

Asztalos Erika képviselő, a Pénzügyi Bizottság elnöke:

A Bizottság elfogadásra javasolta a rendelet-tervezetet.

A napirendi pont keretében egyéb hozzászólás, kérdés nem volt, annak megtárgyalását a polgármester lezárta, indítványára a Képviselő-testület egyhangúlag, 6 fő igen szavazatával, ellenszavazat és tartózkodás nélkül megalkotta a következő rendeletet:

Szirmabesenyő Nagyközség Önkormányzata Képviselő-testületének

14/2018. (VI.20.) önkormányzati rendelete

az intézményi térítési díjakról szóló 5/2012. (III.29.) önkormányzati rendelet módosításáról

Szirmabesenyő Nagyközség Önkormányzata Képviselő-testülete a szociális igazgatásról és szociális ellátásokról szóló 1993. évi III. törvény 92 § (1) bekezdés a.) pontjában és a 115 § (1) bekezdésében, valamint a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény 29 § (1) és (2) bekezdés e.) pontjában kapott felhatalmazás alapján, Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény 13 § (1) bekezdésében meghatározott feladatkörében eljárva, a Képviselő-testület Szervezeti és Működési Szabályzatáról szóló 13/2016. (VI. 24.) önkormányzati rendelet 29 § (3) bekezdésben biztosított véleményezési jogkörében eljáró Szirmabesenyő Nagyközség Önkormányzata Képviselő-testület Pénzügyi és Humánterületi Bizottságai véleményének kikérésével a következőket rendeli el:

1.§

(1) A rendelet 2 § helyébe a következő rendelkezés lép:

„2 § A Képviselő-testület, mint fenntartó a Napsugár Óvoda és Bölcsőde bölcsődés korú ellátottjai részére a gondozási intézményi térítési díjhoz 1.500.-Ft/fő/nap kedvezményt biztosít.

Az étkezésért fizetendő bruttó díj 400.-Ft/fő/nap.

A gondozási díj összege 0.-Ft/fő/nap.”

2.5

A rendelet 2018. július 1-jén lép hatályba.

Husztí Gábor s.k.
polgármester

dr. Szakos Judit s.k.
jegyző

Tizenegyedik napirendi pont:

A napirendi pont keretében a következő bejelentések hangzottak el:

Szakos István képviselő, a Területfejlesztési Bizottság elnöke:

Kérdésem, hogy az Állomás utca belterületi szakaszának felújítása mikor kezdődik?

Jól mondjuk-e a lakosság felé, hogy a buszmegállók megépítése után fog a felújítás megtörténni.

Husztí Gábor polgármester:

Igen, jól. Most beszéltem a főépítésvezetővel és kértem, hogy vonuljanak fel a mi projektünkötől függetlenül. 3 ajánlatot kértünk és a tervezett 42 millió forint helyett 57 millió forint a legalacsonyabb ajánlati ár, itt tartanak az árak az építőiparban.

Sikerült lealkudnunk 43 millió forintra az egyik ajánlatot.

Megpróbáljuk első körben letenni a szegélyköveket, amik az út és az öblök elválasztására szolgálnak, a sport melletti parkolónál is.

Fontos lenne, hogy haladjon a projekt. Elméletileg az az ígéret, hogy akármikor fel tudnak vonulni.

Ha másképp nem megy, az iskola előtt utólag berakjuk a járdaszigetet.

Az ajánlatokra is nagyon sokat kell várni, leterheltek a cégek.

Juhásznő Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

Kérdésem, hogy a református templom előtti parkoló elkészülése mikorra várható?

Lesz ott zebra is?

Ojtozi Attila műszaki vezető:

Igen. Még egy átereszt kell betenni a túlsó oldalra.

Husztí Gábor polgármester:

Felfestett zebra lesz, hogy ne legyen burkolatváltás. De ez a hosszú távú cél, mert az is forgalomlassító. Nehézkesen megy a gyártás, nincs emberünk, most költöztetjük az egészségügyet. Nincs sofőrünk. A kőművesünk közmunkás segítőkkel ennyire tud haladni.

Ojtozi Attila műszaki vezető:

Egy kőművesünk van, 62 éves.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

Az egészségügy költözéséről a lakosságot postai úton is tájékoztatni szükséges, mert az idősebbek számára az fontos.

Huszi Gábor polgármester:

Plakátok is készülnek, az intézménybe is, A/5 méretben szórólapok, amelyeket eljuttatunk minden postaládába.

A Művelődési Házba a beköltözés megtörtént, a fogászat pedig a Csabai kapui Rendelőintézetben fog ideiglenesen működni. Azt fogjuk bérelni 120 napon keresztül. Ez a rendelő régen is fogászati rendelő volt.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

A temetőn nagyon szépen látnak a fű.

Huszi Gábor polgármester:

Igen és a temető mögötti úton a kátyúzás is megvan.

A nonprofit kft-be lett vásárolva egy másfél tonnás padkahenger.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

Ezt a hengert bérebe is lehet venni?

Huszi Gábor polgármester:

Igen, ezt szeretnénk volna, de sajnos nincs közmunkásunk és a saját településünk fenntartása is nehézségekbe fog ütközni. Dolgozókat kell jövőre felvennünk normális fizetésért, kertészt, festőt, asztalost, kőművest.

Bodnár Krisztián képviselő:

Néhány frekventált helyen az útpadkát meg kell igazítani.

Huszi Gábor polgármester:

Melyek a frekventált helyek?

Bodnár Krisztián képviselő:

A butiksonon előtti másik oldalon, a Vörösmarty-Állomás utca között.

Huszi Gábor polgármester:

A régi olajkút felé is a Kossuth utcán is nagyon rossz az út széle.

Ojtozi Attila műszaki vezető:

3 hét múlva lehet körülbelül dolgozni a padkahengerrel, mert akkor lesz a szállításához jármű.

Asztalos Erika képviselő, a Pénzügyi Bizottság elnöke:

A Segítő Szolgálat előtti fák kivágásáért nagyon sokan elmarasztalnak bennünket.

Megnézték sokan a fákat és azt mondták, hogy nem is voltak betegek.

Husztai Gábor polgármester:

Nem azért vágtuk ki, mert betegek voltak, hanem mert ment be a gyökerük az épületek és a járda alá, a vízelvezetőárokba.

Két idős elesett a kiálló gyökerekben.

Asztalos Erika képviselő, a Pénzügyi Bizottság elnöke:

Ezt nem így kellett volna csinálni. Mellé kellett volna ültetni kis fát és a régit kivágni, amikor az új megerősödik. Ez így a faluközpontban nagyon csúnya.

Husztai Gábor polgármester:

Azt úgy nem lehet, mert a fa kivágása mindig okoz sérülést a környezetében.

Meg kell nézni egy hatvanas évekbeli fényképet, ott akkor nem volt fa.

Asztalos Erika képviselő, a Pénzügyi Bizottság elnöke:

De most volt és szép volt.

Husztai Gábor polgármester:

A vasúti parkot tervező kertészmérnökkel konzultáltunk és hatféle javaslatot adott, hogy milyen fát tegyünk oda. Ma elkezdődött a tuskók visszamarása, ezzel a héten végzünk és helyre tudjuk állítani a parkolót és tudunk még virágokat is ültetni. Elnyert pályázatunk van a Szolgálat épületének felújítására és napelemek is lesznek ott.

Juhászné Molnár Mária képviselő, a Humánterületi Bizottság elnöke:

Az iskola közbeszerzése hogyan áll?

Husztai Gábor polgármester:

Jelenleg hiánypótlásra került, tehát rendkívüli testületi ülés lesz, amire be fogjuk hozni a Rendezési Terv módosítását is, mert a mai postával jött meg a jóváhagyása a Kiemelt Fejlesztési Terület II-nek.

A cél, hogy a gépészeti felújítás történjen meg először, fűtéskorszerűsítés, kazáncsere, világítás és működés alatt meg lehet csinálni a nyílászárócserét és a homlokzati hőszigetelést.

Győrfi Lászlóné iskolaigazgató:

Mi lesz, ha az önkormányzat által eldöntött 42 millió forintnál többbe fog kerülni a külső munkálat?

Husztai Gábor polgármester:

Nem tudjuk még az ajánlatokat, van erre vonatkozóan önkormányzati döntés, de az ajánlatok függvényében az újra gondolható.

Talán a kormányzat is fogja kompenzálni az áremelkedéseket a TOP pályázatok kapcsán. Kiemelkedő tényező a minimálbér emelkedése.

Amit igazgató asszony említett, az épület külső felújítása, azt célozza, hogy az épület külső megjelenése olyan legyen, mint a terven és magában hordozza az aula megnagyobbításának lehetőségét is.

Győrfi Lászlóné iskolaigazgató:

A szülők felé is azt kommunikáltuk, hogy a belső munkálatok a nyár folyamán lemennek és a külsők majd azután folyamatosan.

dr. Szakos Judit jegyző:

Igazgató asszony mit tud a tankerületi központ megígért 25 millió forintos támogatásáról?

Győrfi Lászlóné iskolaigazgató:

Nem fogjuk megkapni, ez lett a döntés.

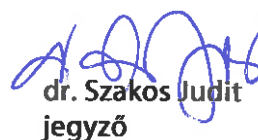
A napirendi pont keretében egyéb hozzászólás, bejelentés nem volt, annak megtárgyalását a polgármester lezárta.

Az ülés keretében egyéb hozzászólás, kérdés nem volt, az ülést a polgármester bezárta.

kmf

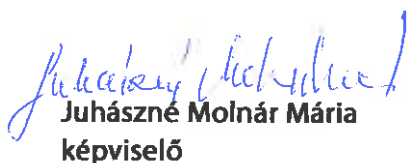


Husztai Gábor
polgármester



dr. Szakos Judit
jegyző

Jegyzőkönyv hitelesítők:



Juhászné Molnár Mária
képviselő



Asztalos Erika
képviselő

A jegyzőkönyv mellékletét képező előterjesztések és dokumentumok:

- 1.) Meghívó
- 2.) Jelenléti ív
- 3.) Jelentés a lejárt határidejű határozatok végrehajtásáról és a két ülés közötti időszak eseményeiről
- 4.) Javaslat a Szirmabesenyői Napsugár Óvoda és Bölcsőde alapítóokiratának módosítására
- 5.) Tájékoztató az iskola oktató-nevelő munkájáról
- 6.) Beszámoló az óvoda-bölcsőde nevelő munkájáról
- 7.) Tervezet Szirmabesenyő Nagyközség Önkormányzata Képviselő-testületének .../2018. (...) önkormányzati rendelete a közszolgálati tisztviselők napjáról
- 8.) Javaslat a hulladékgazdálkodással kapcsolatos határozatok elfogadására
- 9.) Javaslat Önkormányzati étkeztetési fejlesztések támogatására szóló pályázat benyújtására
- 10.)Javaslat a Szirmabesenyői Polgármesteri Hivatal Informatikai Biztonsági Szabályzatának elfogadására
- 11.)Javaslat a képviselőtestületi alap felhasználására
- 12.) Tervezet az intézményi térítési díj megállapításáról szóló 5/2012.(III.29.) önkormányzati rendelet módosítására