Előterjesztés

Javaslat a Kislángi Polgármesteri Hivatal Elektronikus Információs Rendszerek Kockázatelemzési és kockázatkezelési Eljárásrendjének és Információbiztonsági Szabályzatának elfogadására

Az előterjesztést készítette: dr. Berta Edina
jegyző

Az Informatikai Biztonsági Szabályzat célja

Az Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) célja a Hivatalnak az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (továbbiakban: Ibtv.), valamint az ASP szakrendszeri kapcsolódás okán a 257/2016. (VIII. 31.) Korm. rendeletben foglalt információbiztonsági követelményeknek való megfelelőségét biztosítani.

Az Ibtv. és végrehajtási rendelete – 41/2015. (VII. 15.) BM rendelet (továbbiakban: Vhr.) – a Hivatal által használ informatikai rendszerek, az azokban kezelt adatok védelmét célozza, közvetve pedig ez által a kormányzati szervek által biztosított központi szakrendszerek, így például az ASP-ben kezelt adatok biztonságát is hivatott garantálni.

Az informatikai rendszereket hatékonyan úgy lehet megvédeni, ha annak minden veszélyeztetett pontján megfelelő védelmet alakítunk ki, minden kiskaput becsukunk, emiatt fontos, hogy minden, a központi rendszerekhez hozzáférő, azokat használó Önkormányzatnál, Hivatalnál és egyéb szervezetnél – kvázi minden számítógépen, minden csatlakozó hálózaton – egyformán és jól működő informatikai biztonsági megoldásokat alkalmazzunk.

A szabályzat céljából kiindulva hatálya mindenkire kiterjed, aki bármilyen módon részt vesz a Hivatalnál keletkező, felhasznált, feldolgozott, tárolt, illetve továbbított adatok kezelésében. Így minden munkavállalóra, tisztviselőre, az IT üzemeltetőre, informatikusra, az információbiztonsági felelősre (IBF), a Hivatal weboldalának fejlesztőjére, illetve karbantartójára, valamint a számítógépek, nyomtatók, stb. javítását végző szervizes szakemberekre egyaránt.

Kiterjed továbbá minden a Hivatalnál a munkavégzéshez használt informatikai és infokommunikációs eszközre, így a számítógépekre, szerverekre, az azokon futtatott programokra, a nyomtatókra, hálózati eszközökre, az okostelefonokra és még a vagyonvédelmi rendszerekre is, úgymint a riasztó, a beléptető vagy a kamerás megfigyelő rendszerek.

Mindenre és mindenkire, ami vagy aki részt vesz a Hivatalnál az adatok kezelésében, feldolgozásában vagy továbbításában. Ezt a nagy halmazt hívja a törvény elektronikus információs rendszernek (továbbiakban: EIR).

A fenti szabályzatok elkészítését és elektronikus információs rendszer biztonságáért felelős személy (a továbbiakban: információbiztonsági felelős) kötelező kinevezését (megbízását) feladatait az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) írja elő a hatálya tartozó szervezetek, így a Hivatal számára is.

Kisláng Község Önkormányzat Képviselő-testülete a Kislángi Közös Önkormányzati Hivatal tekintetében 2017-ben kötött megállapodást a Közinformatika Nonprofit Kft-vel, aki biztosította az információbiztonsági felelőst és a szabályzatok elkészítését.

Kisláng Község Önkormányzata 2020. január 1. napjától önálló Polgármesteri Hivatalt működtet, a közös önkormányzati hivatal megszűnt.

Mindezek alapján Kisláng Község Önkormányzat Képviselő-testülete a 2020. január 30. napján megtartott ülésén a 18/2020.(I.30.) számú határozatával döntött arra vonatkozóan, hogy a **HANGANOV Korlátolt Felelősségű Társaságot (2730 Albertirsa, BA-KO u. 6., képviseli: Kedves Zoltán ügyvezető)** az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (Info tv.), illetve az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló rendeletében (GDPR: General Data Protection Regulation = általános adatvédelmi rendelet) meghatározott követelményeknek megfelelő külső adatvédelmi tisztviselőt biztosítása tekintetében, valamint a Kislángi Polgármesteri Hivatal Informatikai Biztonsági Szabályzatának és Elektronikus Információs Rendszerek Kockázatelemzési és Kockázatkezelési Eljárásrendjét szabályozó dokumentáció elkészítésével.

A Hanganov Kft. elkészítette Kislángi Polgármesteri Hivatal Informatikai Biztonsági Szabályzatát és Elektronikus Információs Rendszerek Kockázatelemzési és Kockázatkezelési Eljárásrendjét szabályozó dokumentációt.

Az Informatikai Biztonsági Szabályzat és Elektronikus Információs Rendszerek Kockázatelemzési és Kockázatkezelési Eljárásrendjét szabályozó dokumentáció az előterjesztés 1. számú mellékletét képezi.

Mindezek alapján szükséges a Szabályzatok elfogadása.

A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról 2011. évi CXXVIII. törvény 46. § (4) bekezdésében foglaltak szerint veszélyhelyzetben a települési önkormányzat képviselő-testületének, a fővárosi, megyei közgyűlésnek feladat- és hatáskörét a polgármester, illetve a főpolgármester, a megyei közgyűlés elnöke gyakorolja. Ennek keretében nem foglalhat állást önkormányzati intézmény átszervezéséről, megszüntetéséről, ellátási, szolgáltatási körzeteiről, ha a szolgáltatás a települést is érinti.

Kisláng, 2020. június 9.

Rumpler Tibor sk.
polgármester

1. HATÁROZATI JAVASLAT

KISLÁNG KÖZSÉG ÖNKORMÁNYZAT POLGÁRMESTERÉNEK
...../2020.(VI.10.) HATÁROZATA
A Kislángi Polgármesteri Hivatal Elektronikus Információs Rendszerek Kockázatelemzési és Kockázatkezelési Eljárásrendjének elfogadásáról

Kisláng Község Polgármestere a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény 46. §-ának (4) bekezdésében foglalt feladat- és hatáskörömben eljárva az alábbi döntést hoztam.
Kisláng Község Önkormányzat nevében elfogadtam a Kislángi Polgármesteri Hivatal Elektronikus Információs Rendszerek Kockázatelemzési és Kockázatkezelési Eljárásrendjét, mely a határozat szoros mellékletét képezi.

A Kislángi Polgármesteri Hivatal Elektronikus Információs Rendszerek Kockázatelemzési és Kockázatkezelési Eljárásrendjének aláírásáról gondoskodom.

Határidő: azonnal
Felelős: Rumpler Tibor polgármester

2. HATÁROZATI JAVASLAT

KISLÁNG KÖZSÉG ÖNKORMÁNYZAT POLGÁRMESTERÉNEK

……/2020.(VI.10.) HATÁROZATA

A Kislángi Polgármesteri Hivatal Informatikai Biztonsági Szabályzatának elfogadásáról

Kisláng Község Polgármestere a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény 46. §-ának (4) bekezdésében foglalt feladat- és hatáskörömben eljárva az alábbi döntést hoztam.

Kisláng Község Önkormányzat nevében elfogadtam a Kislángi Polgármesteri Hivatal Informatikai Biztonsági Szabályzatát, mely a határozat szoros mellékletét képezi.

A Kislángi Polgármesteri Hivatal Informatikai Biztonsági Szabályzatának aláírásáról gondoskodom.

Határidő: azonnal
Felelős: Rumpler Tibor polgármester

Szám: 1709-2/2020.

A KISLÁNGI POLGÁRMESTERI HIVATAL

ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK KOCKÁZATELEMZÉSI ÉS KOCKÁZATKEZELÉSI ELJÁRÁSRENDJE

Kisláng

2020

Kiadva / hatályos:

Készítette:

HANGANOV Kft.
Az információbiztonság és az adatvédelem szakértője
www.hanganov.hu

TARTALOM

1 AZ ELJÁRÁSREND CÉLJA 2
2 AZ ELJÁRÁSREND HATÁLYA 3
2.1 AZ ELJÁRÁSREND SZEMÉLYI HATÁLYA 3
2.2 AZ ELJÁRÁSREND TÁRGYI HATÁLYA 3
2.3 AZ ELJÁRÁSREND IDŐBELI HATÁLYA 3
3 AZ ELJÁRÁSREND KIADÁSA, KEZELÉSE, FELÜLVIZSGÁLATA 3
4 DOKUMENTUMVÉDELEM 3
5 AZ INFORMÁCIÓBIZTONSÁGI KOCKÁZATMENEDZSMENT SZEREPLŐI 4
6 AZ INFORMÁCIÓBIZTONSÁGI KOCKÁZATMENEDZSMENT 4
6.1 KOCKÁZATFELMÉRÉS 4
6.1.1 Kockázatok azonosítása 5
6.1.2 Kockázatok elemzése 5
6.1.3 Kockázatok értékelése 7
6.2 KOCKÁZATKEZELÉS 7
6.2.1 A kockázat elfogadása, felvállalása 8
6.2.2 A kockázat elkerülése 8
6.2.3 A kockázat áthárítása 8
6.2.4 A kockázat módosítása 9
6.2.5 Maradvány kockázat felvállalása 9
6.2.6 A kockázatkezelési javaslat és végrehajtása 9
6.3 KOCKÁZATMENEDZSMENT KOMMUNIKÁCIÓ 10
1. SZÁMÚ MELLÉKLET – KOCKÁZATELEMZÉSI JELENTÉS 11

1 AZ ELJÁRÁSREND CÉLJA

A Kislángi Polgármesteri Hivatal (a továbbiakban: Hivatal) elektronikus információs rendszerek (a továbbiakban: EIR) kockázatelemzési és kockázatkezelési eljárásrendjének célja a Hivatal által használt EIR-ekre ható információbiztonsági kockázatok felmérésével, elemzésével, valamint kezelésével összefüggő tevékenységek, feladatok és felelősségek meghatározása.
Célja továbbá fentiek rögzítésével biztosítani azt, hogy a Hivatal által használt EIR-ekre ható kockázatok kezelése a vonatkozó, hatályos jogszabályokban, úgymint különösen az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (a továbbiakban: Ibtv.), valamint a végrehajtására kiadott 41/2015. (VII. 15.) BM rendeletben (a továbbiakban: Vhr.) megfogalmazott információbiztonsági követelményeknek megfelelően és elvárt minőségben történjen.

2 AZ ELJÁRÁSREND HATÁLYA

2.1 Az eljárásrend személyi hatálya

Az eljárásrend személyi hatálya kiterjed a Hivatal munkavállalóira, valamint azokra a személyekre, akik részt vesznek a Hivatalnál keletkező, felhasznált, feldolgozott, tárolt, illetve továbbított adatok kezelésében.

Kiterjed továbbá mindazon, a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban lévő személyekre, akik a Hivatal által működtetett informatikai rendszerek kezelésében (üzemeltetésében, karbantartásában, javításában, illetve felügyeletében) részt vesznek.

2.2 Az eljárásrend tárgyi hatálya

Az eljárásrend tárgyi hatálya kiterjed a Hivatalnál keletkezett és a Hivatal által kezelt információk teljes életciklusukon át történő kezelésével, védelmével kapcsolatos eszközökre és tevékenységekre, valamint az informatikai rendszerben üzemeltetett valamennyi hardver és szoftver elemre, amely felhasználja, feldolgozza, felügyeli, ellenőrzi, tárolja, továbbítja a Hivatalnál keletkező, illetve felhasznált adatokat.

2.3 Az eljárásrend időbeli hatálya

Az eljárásrend a kiadása napján lép hatályba és jelenlegi verziója visszavonásig – vagy a következő kiadásra kerülő verzió hatályba lépéséig – hatályos.

3 AZ ELJÁRÁSREND KIADÁSA, KEZELÉSE, FELÜLVIZSGÁLATA

Az eljárásrend kiadása, Hivatalon belüli kihirdetése és rendelkezésre állásának biztosítása (megőrzése) a Jegyző feladata és felelőssége.

Az eljárásrend felülvizsgálatát és frissítését a következő gyakorisággal kell elvégezni:

- a Hivatal kockázatmenedzsment folyamataiban, az alkalmazott módszertanban bekövetkező változás, vagy
- a Hivatal szervezetében, illetve a szerepkörökben történő jelentős változás esetén, illetve
- amennyiben biztonsági értékelés, illetve biztonságelemzés által indokolt.

Az eljárásrend felülvizsgálatának kezdeményezése, a felülvizsgálat eredményeként esetlegesen keletkezett új vagy módosított eljárásrend kiadása, valamint a felülvizsgálat megtörténtét igazoló feljegyzés megőrzése a Jegyző feladata és felelőssége.

Az eljárásrend felülvizsgálatára javaslatot tehet az információbiztonsági felelős.

Az eljárásrend felülvizsgálatát az információbiztonsági felelős köteles végrehajtani és eredményét dokumentáltan átadni a Jegyző számára.

4 DOKUMENTUMVÉDELEM

Az eljárásrend és mellékletei, az általa előírt elkészítendő és megőrzendő dokumentumok jogosulatlanok számára való megismerhetőségük és módosíthatóságuk elleni védelméről a Hivatal elektronikus formában történő tárolásuk, illetve vezetésük esetén hozzáférés- és jogosultsági rendszerrel védett tárterületen történő elhelyezéssel, illetve kizárólag a Hivatal belső hálózatán engedélyezett terjesztéssel, papír alapon a Hivatal iratkezelésre vonatkozó előírásai alapján gondoskodik.

Az eljárásrendben előírt dokumentumok elektronikus, illetve papír alapú formában egyaránt kezelhetők a Jegyző erre vonatkozó döntése szerint.

Minden dokumentum esetében biztosítani szükséges annak folyamatos rendelkezésre állását, változás esetén kinyomtatott másodpéldányának az iratkezelési szabályoknak megfelelő helyi tárolásával. A dokumentum új verziójának készítője köteles azt, illetve annak nyomtatható, elektronikus példányát a Jegyző rendelkezésére bocsátani, aki gondoskodik az aktuálisan érvényes nyomtatott példánynak a Hivatal iratkezelésre vonatkozó előírásainak megfelelő módon történő kezeléséről és megőrzéséről.

5 AZ INFORMÁCIÓBIZTONSÁGI KOCKÁZATMENEDZSMENT SZEREPLŐI

A jelen kockázatelemzési és kockázatkezelési eljárásrendben foglaltak végrehajtásának folyamatában a Hivatal információbiztonsági szervezetének alábbi szerep-, illetve felelősségi körei érintettek:

Felelősségi szint	Szerepkör
Vezetői általános felelősség, benne koordinációs, kommunikációs felelősség (Hivatal és hatóság, Hivatal és információbiztonsági felelős között)	Jegyző
Információbiztonsági tevékenységek tervezéséért, menedzseléséért való felelősség	Információbiztonsági felelős
Informatikai rendszerelemek működési, üzemeltetési felelőssége	IT üzemeltető
Információbiztonsági szabályok és előírások betartása	Jelen eljárásrend személyi hatálya alá tartozók (a Hivatal munkavállalói, a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban lévők)

6 AZ INFORMÁCIÓBIZTONSÁGI KOCKÁZATMENEDZSMENT

Az információbiztonsági kockázatmenedzsment célja, hogy a Hivatal által a folyamatait érintően végzett általános kockázatelemzési és kezelési tevékenységhez igazodó módszertan alkalmazásával biztosítsa a Hivatal által használt elektronikus információs rendszerek, valamint az általuk kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzéséhez szükséges egyenszilárd, kockázatokkal arányos védelmi intézkedések kialakítását és működtetését.

A Hivatal által használt EIR-ek esetében a kockázatmenedzsment folyamataihoz kapcsolódó feladatok végrehajtását jelen módszertan szerint kell elvégezni.

6.1 Kockázatfelmérés

Az információbiztonsági kockázatok felmérésének folyamata az alábbi lépéseket foglalja magában:

- a kockázatok azonosítása,
- a kockázatok elemzése,
- a kockázatok értékelése.

A kockázatfelmérést, illetve annak aktualizálását az információbiztonsági felelős hajtja végre – a Jegyző, illetve a hivatali munkatársak közreműködésével és szükség szerint az IT üzemeltető bevonásával – a Hivatal által használt EIR-ek és működési környezetük alábbi változásai esetében:

- új EIR bevezetése,
- új rendszerelem meglévő EIR-be illesztése, illetve
- meglévő EIR más (helyi, illetve külső) elektronikus információs rendszerekhez történő kapcsolódása,

amennyiben a változás (beleértve az új fenyegetések és sebezhetőségek megjelenését is), a megváltozott körülmény vagy a tervezett változtatás az EIR-ben, illetve működési környezetében olyan jelentős eltéréssel vagy módosítással jár, amely befolyásolja az EIR biztonsági állapotát, s az alkalmazott védelmi intézkedéseket.

6.1.1 Kockázatok azonosítása

A kockázatok azonosítása során meg kell határozni azokat a fenyegetettségeket (eseményeket, veszélyeket, gyenge pontokat, sérülékenységeket, illetve védelmi intézkedést érintő hiányosságokat), amelyek a Hivatal által használt EIR-ek, illetve a kezelt adatok bizalmasságát, sértetlenségét vagy rendelkezésre állását bármilyen okból fenyegetik, függetlenül attól, hogy a Hivatalnak az adott fenyegetettségre, a fennállását előidéző helyzetre, illetve körülményre van-e ráhatása vagy sem.

Érintett adatkörök azonosítása

Az EIR által kezelt, tárolt adatok típusa és mennyisége a fenyegetettség kihasználásának lehetséges következményeit, azok hatásait, mértékét jelentősen befolyásolja, emiatt az azonosítás során meg kell határozni, hogy jogszabály által védett adatot (pl.: személyes, különleges vagy minősített), közérdekű vagy közérdekből nyilvános adatot érinthet-e és milyen mennyiségben.

Fenyegetések és forrásaik azonosítása

A fenyegetések azonosítása az iparági tapasztalatok, a fenyegetésekre, azok kihasználásának gyakoriságára vonatkozó kutatások, statisztikák, illetve trendek, valamint a korábbi biztonsági incidensek tapasztalatai alapján történhet, az informatikai infrastruktúra esetében a rendszerelem típusának megfelelő, jellemző sérülékenységek figyelembe vételével.

A fenyegetések azonosítása során az alábbi területeket kell vizsgálni:

- hardver-, szoftver, illetve hálózati- (kommunikációs) eszközök,
- fizikai környezet,
- szervezet és működése (folyamatok, eljárások),
- vezetői (menedzsment) tevékenységek,
- munkavállalók (pl.: kulcsfelhasználók),
- külső felek (pl.: szolgáltatók), tőlük való függőség.

A fenyegetés forrását tekintve lehet:

- véletlen vagy szándékos károkozás következménye,
- belső vagy külső forrásból származó,
- a műszaki paraméterekből adódó.

Kontroll környezet vizsgálata

Egy adott EIR fenyegetettségét a meglévő kontrollok hiánya vagy nem megfelelő alkalmazása (pl.: hibás vagy hiányos konfigurációs beállítás) szintén okozhatja. A kockázatok azonosítása során emiatt célszerűen a Hivatal szervezeti biztonsági szintbe sorolásának, illetve az általa használt EIR biztonsági osztály besorolásának megfelelően jogszabályban meghatározott adminisztratív, fizikai, illetve logikai védelmi intézkedések megvalósításának státuszát, működésének, hatékonyságának megfelelőségét kell elsődlegesen figyelembe venni.

Az azonosított kockázatok adatait a védelmi intézkedések típusának (adminisztratív, fizikai, logikai) megfelelő tagolásban az 1. számú melléklet – Kockázatelemzési jelentés 2 – 4. soraiban kell rögzíteni.

6.1.2 Kockázatok elemzése

A kockázatelemzés célja, hogy feltárja és értékelje a Hivatal által használt EIR-ekre vonatkozóan az azonosított kockázatok bekövetkezése esetén a lehetséges következményeket, azok kiterjedését, hatásait, a várható kár mértékét, az azonosított kockázatok bekövetkezésének reális valószínűségét, s ezek alapján meghatározza a kockázati besorolási értékeket.

A következmények értékeléséhez, az azokhoz kapcsolódó kockázati besorolási értékek meghatározásához a Vhr.-ben alkalmazott szempontrendszer alkalmazása javasolt, az alábbiak szerint:

Hatás (kár) értéke	Következmények

Hatás (kár) értéke	Következmények
1	az elektronikus információs rendszer nem kezel jogszabályok által védett (pl.: személyes) adatot;
	nincs bizalomvesztés, a probléma az érintett szervezeten belül marad, és azon belül meg is oldható;
	a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez képest jelentéktelen;
2	személyes adat sérülhet;
	az érintett szervezet üzlet-, vagy ügymenete szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat vagy elektronikus információs rendszer sérülhet;
	a lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető;
	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 1%-át.
3	különleges személyes adat sérülhet, személyes adatok nagy mennyiségben sérülhetnek;
	az érintett szervezet üzlet-, vagy ügymenete szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett adat sérülhet;
	a lehetséges társadalmi-politikai hatás: bizalomvesztés állhat elő az érintett szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek;
	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 5%-át.
4	különleges személyes adat nagy mennyiségben sérülhet;
	személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket);
	az érintett szervezet üzlet-, vagy ügymenete szempontjából nagy értékű, üzleti titkot, vagy különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet;
	a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében, vagy vezetésében személyi felelősségre vonást kell alkalmazni;
	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 10%-át.
5	különleges személyes adat kiemelten nagy mennyiségben sérülhet;
	emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be;
	a nemzeti adatvagyon helyreállíthatatlanul megsérülhet;
	az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;
	a lehetséges társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;
	az érintett szervezet üzlet- vagy ügymenete szempontjából nagy értékű üzleti titkot, vagy kiemelten érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet;
	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 15%-át.

A bekövetkezési valószínűséget a támadási potenciál [CommonCriteriaCommonEvaluationMethodology (CEM)] implicit ismeretének segítségével, szakértői tapasztalatokon alapuló becslés elvégzésének módszerével kell meghatározni. A támadási potenciál a sikeres támadás esélyét fejezi ki, és függ a támadási cél értékétől, a támadáshoz szükséges szakértelemtől, eszköztől és időtől, valamint a védelem erősségétől is.

A bekövetkezési valószínűség lehetséges értékei az alábbiak lehetnek:

Jelölése	Jelentése	Gyakoriság, illetve támadási potenciál
A	alacsony	Bekövetkezhet, de nem valószínű.
K	közepes	Elképzelhető, hogy bekövetkezik a jövőben (előfordulhat visszaélés vagy károkozás).
M	magas	1-2 éven belül bekövetkezhet.
N	nagyon magas	Várhatóan bekövetkezik a közeljövőben (pl.: bárki által kihasználható, ismert sérülékenység).

A kockázatelemzés eredményét az 1. számú melléklet – Kockázatelemzési jelentés adott kockázatra vonatkozó táblázatának 5. és 6. soraiban kell rögzíteni.

6.1.3 Kockázatok értékelése

A kockázatelemzés eredményeinek értékelése során az összevethetőség biztosítása, valamint a kockázati kritérium mátrixban történő megjeleníthetőségük érdekében a bekövetkezési valószínűség értékeit az alábbiak szerint számszerűsítjük:

Jelölése	Jelentése	Értéke
A	alacsony	1
K	közepes	2
M	magas	3
N	nagyon magas	4

A következmények várható hatása (kár mértéke), valamint a bekövetkezési valószínűség értékeiből az alábbiak szerint számítható a kockázati érték:

Hatás (kár) értéke / Bekövetkezési valószínűség	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	
3	3	6	9		
4	4	8			

Fenti kockázati kritériumrendszer (mátrix) alapján a becsült kockázat értéke szolgál a kockázatkezelési intézkedésekre vonatkozó javaslat, illetve döntés alapjául.

A Hivatalnál alkalmazott kockázati szintek:

Kockázat értéke	Kockázati szint
1 – 2	alacsony kockázat
3 – 9	közepes kockázat
10 vagy több (10+)	

A kockázatértékelés eredményét az 1. számú melléklet – Kockázatelemzési jelentés adott kockázatra vonatkozó táblázatának 7. sorában kell rögzíteni.

6.2 Kockázatkezelés

A kockázatkezelés azon tevékenységek összessége, amely az adott EIR, illetve az általa kezelt adatok bizalmasságát, sértetlenségét, illetve rendelkezésre állását veszélyeztető kockázat megszüntetésére vagy elfogadható szintre való csökkentésére irányul. A kockázatkezelés módját a kockázat nagysága, a megvalósítás költsége és várható hatása alapján kell meghatározni.

A kockázatkezelés végrehajtásának lehetőségei:

- kockázat elfogadása, felvállalása,
- kockázat elkerülése,
- kockázat áthárítása,
- kockázat módosítása,
- maradvány kockázatok felvállalása.

6.2.1 A kockázat elfogadása, felvállalása

A Hivatal a kockázat tudatos elfogadását, felvállalását kizárólag abban az esetben alkalmazhatja, amennyiben a kockázat megfelel az alábbi elfogadási kritériumokban foglaltaknak:

- a megállapított kockázati szint alacsony;
- nem történik külső vagy belső normatíva (jogszabály, szabályozó) megsértése;
- a közvetlen, illetve közvetett kár értéke nem haladja meg a Hivatal költségvetésének 1%-át;
- a társadalmi-politikai hatás a Hivatalon belül kezelhető, nem romlik a Hivatal jó hírneve, reputációja;
- a kockázat megszüntetése vagy mérséklése nagyobb költséggel vagy erőforrás igénnyel jár, mint amekkora kár a bekövetkezésekor keletkezik vagy a helyreállításhoz szükséges;
- közvetve vagy közvetlenül testi épséget vagy emberi életet nem veszélyeztet.

Fenti kritériumok alapján a Hivatal jelen eljárásrend tárgyában – az általa használt EIR-ek kockázataival kapcsolatban – megállapított ***kockázati tűréshatára az alacsony kockázati szint*** besorolásnál került kijelölésre.

A jogszabályi nem megfelelés automatikusan magas kockázati szintnek minősül, amelynek elfogadása, felvállalása kizárólag az arra jogosult Jegyző felelőssége, melyet írásban köteles rögzíteni.

A kockázat elfogadásáról, felvállalásáról a kockázatkezelési javaslat alapján a Jegyző dönt.

6.2.2 A kockázat elkerülése

Amennyiben a kockázat költségarányos kezelésére, csökkentésére nincs reális lehetőség, akkor a kockázat előfordulásának elkerülését biztosítandó javasolható a kockázatos tevékenység, az érintett EIR vagy rendszerelem használatának megszüntetése, illetve korlátozása, amennyiben az hatékonyan kivitelezhető és megfelelő védelmet garantál.

A kockázat elkerülése kizárólag az alacsony és közepes kockázatok esetén alkalmazható kockázatkezelési eljárás.

A kockázat elkerüléséről a kockázatkezelési javaslat alapján a Jegyző dönt.

6.2.3 A kockázat áthárítása

A kockázat csökkenthető a következmények, a bekövetkezett kár vagy a felelősség áthárításával, megosztásával. A Hivatal a számára kockázatos szolgáltatással, eszközzel vagy körülménnyel kapcsolatos kockázatokat átháríthatja harmadik félre, külső partnerre (pl.: szolgáltató, beszállító, biztosító, stb.). Ebben az esetben szerződésben kell meghatározni a felelősségeket, azok elhatárolását, valamint a kockázat átvállalás mértékét (pl.: felelősségbiztosítás összege).

A kockázat áthárítása, megosztása esetén új kockázati tényezők jelenhetnek meg, meglévő kockázatok módosulhatnak. Az új kockázatokat be kell vonni a kockázatmenedzsment folyamatba, a módosult kockázatokat ismételten elemezni és kezelni szükséges.

A kockázat áthárítása az alacsony és közepes kockázatok esetén alkalmazható kockázatkezelési eljárás, amennyiben a kockázat áthárítását, megosztását követően a fennmaradó kockázat teljesíti a 6.2.1 A kockázat elfogadása, felvállalása pontban meghatározott elfogadási kritériumokat.

A kockázat áthárításáról a kockázatkezelési javaslat alapján a Jegyző dönt.

6.2.4 A kockázat módosítása

A kockázatmódosítás célja meghatározni mindazon intézkedéseket, amelyekkel a kockázat megszüntethető, megelőzhető, csökkenthető, hatása az elfogadható szintre mérsékelhető, felismerhető, illetve az azzal kapcsolatos tudatosság növelhető.

A javasolt intézkedés lehet már meglévő védelmi intézkedés módosítása vagy új kontroll bevezetése (pl.: EIR vagy rendszerelem konfigurációjának, biztonsági beállításainak módosítása; új, szigorúbb szabályozó elem előírása, stb.).

A nem vagy csak részben hatékony védelmi intézkedések esetében meg kell vizsgálni azok kivezetésének lehetőségét vagy más, esetleg már meglévő, működő kontrollokkal való helyettesíthetőségét.

A kockázat módosítása bármely kockázati szint esetén alkalmazható és preferált kockázatkezelési eljárás.

A kockázat módosításáról a kockázatkezelési javaslat alapján a Jegyző dönt.

6.2.5 Maradvány kockázat felvállalása

Amennyiben a kockázat kezelésével a kockázat szintjének a 6.2.1 A kockázat elfogadása, felvállalása pontban meghatározott elfogadási kritériumok alá csökkentése sikertelen, maradvány kockázat keletkezik.

Maradvány kockázat kizárólag abban az esetben vállalható fel, ha az a Hivatal szervezeti biztonsági szint besorolásával, illetve az érintett EIR biztonsági osztályba sorolásával kapcsolatban az Ibtv.-ben, illetve a Vhr.-ben meghatározott biztonsági követelménnyel vagy egyéb vonatkozó jogszabályi előírással nem ütközik.

A maradvány kockázat felvállalásáról a Jegyző dönt, melyet minden esetben írásban köteles rögzíteni.

6.2.6 A kockázatkezelési javaslat és végrehajtása

A kockázatkezelési javaslat tartalmazza a kockázatfelmérés eredménye alapján kiválasztott kockázatkezelési módot, valamint a megvalósításához szükséges intézkedéseket, amelyekkel az adott kockázat megszüntethető, illetve a kockázati szint a 6.2.1 A kockázat elfogadása, felvállalása pontban meghatározott elfogadási kritériumok alá csökkenthető.

A kockázat kezelésére vonatkozó javaslatot az 1. számú melléklet – Kockázatelemzési jelentés adott kockázatra vonatkozó táblázatának 8. sorában kell rögzíteni.

A kockázatkezelési javaslat végrehajtásáról a Jegyző dönt, a javaslatban meghatározott intézkedések végrehajtása – a feladatok kiosztása, intézkedés elrendelése – a Jegyző feladata és felelőssége.

Amennyiben a kockázatfelmérés új EIR bevezetését megelőzően a vonatkozó biztonsági osztály meghatározásánál hiányosságokat állapít meg, illetve abban az esetben, ha a feltárt kockázatok számossága miatt indokolt, a kockázatkezelési javaslat a kockázatkezelés elvégzésére Cselekvési Terv elkészítését írja elő.

A Cselekvési Terv tartalmazza a javasolt intézkedések konkrét megvalósítására vonatkozó részletes előírásokat, a feladatokat, határidőket és a végrehajtásukért felelős szerepköröket.

A Cselekvési Terv jóváhagyása, végrehajtásának elrendelése a Jegyző feladata és felelőssége. A tervben foglalt feladatok végrehajtásában köteles minden jelen eljárásrend személyi hatálya alát tartozó személy (hivatali munkavállaló, IT üzemeltető, stb.) közreműködni.

Új EIR bevezetése során a megállapított biztonsági osztályhoz tartozó követelményeket a rendszer használatba vételéig kötelező teljesíteni.

6.3 Kockázatmenedzsment kommunikáció

A kockázatkezelés sikeres megvalósítása érdekében a kockázatmenedzsment folyamattal kapcsolatos információk cseréje és megosztása kiemelten fontos, mely által

- az érintettek információt kapnak a Hivatal kockázatmenedzsment eredményeiről;
- megismerik a kockázatkezelés lehetséges módjait, hatékony eljárásait;
- biztonsági tudatosságuk szintje növelhető;
- felelősen lesznek képesek részt venni a kockázatkezelés végrehajtásában;
- az információk hiánya miatt bekövetkező vétlen károkozás megelőzhető, elkerülhető vagy csökkenthető.

Fentiek biztosítása céljából az 1. számú melléklet – Kockázatelemzési jelentés alapján elkészített kockázatelemzési jelentés megőrzéséről, valamint tartalmának a kockázatkezelésben érintettekkel történő megismertetéséről a Jegyző köteles a 4. Dokumentumvédelem fejezetben előírtak szerint gondoskodni.

1. SZÁMÚ MELLÉKLET – KOCKÁZATELEMZÉSI JELENTÉS

Hivatal megnevezése:	Kislángi Polgármesteri Hivatal

Azonosított kockázatonként külön táblázat kitöltése szükséges!

I. Adminisztratív védelmi intézkedésekkel kapcsolatos kockázatok

1	**Sorszám / Azonosító** (pl.: sorfolytonos számozással, pl.: K01, K02, K03, stb.)	K01
2	**Kockázat megnevezése, leírása** (az azonosított kockázat megnevezése, leírása: a fenyegetés és forrása, esetlegesen hiányzó kontrollok meghatározása)	
3	**Érintett adatok** (az adatkör típusa: személyes / különleges / minősített / közérdekű vagy közérdekből nyilvános adatok / egyéb és mennyisége, nagyságrendje)	
4	**Fenyegetés típusa** (az azonosított kockázat az EIR-ben kezelt adatok mely tulajdonságát – vagy többet is – fenyegeti: B: bizalmasság, S: sértetlenség, R: rendelkezésre állás)	
5	**Hatás (kár) értéke** (a következmény kockázati szint besorolása: 1 – 5)	
6	**Bekövetkezés valószínűsége** (A: alacsony / 1, K: közepes / 2, M: magas / 3, N: nagyon magas / 4)	
7	**Kockázat értéke** (A kockázat értékelésének eredménye: A: alacsony / 1-2; K: közepes / 3-9; M: magas / 10+)	
8	**Kockázatkezelési javaslat** (A kockázat kezelésére vonatkozó szakértői javaslat, pl.: új védelmi intézkedés bevezetése, az adott EIR vagy rendszerelem kivezetése, cseréje, stb.)	

1	**Sorszám / Azonosító** (pl.: sorfolytonos számozással, pl.: K01, K02, K03, stb.)	K02
2	**Kockázat megnevezése, leírása** (az azonosított kockázat megnevezése, leírása: a fenyegetés és forrása, esetlegesen hiányzó kontrollok meghatározása)	
3	**Érintett adatok** (az adatkör típusa: személyes / különleges / minősített / közérdekű vagy közérdekből nyilvános adatok / egyéb és mennyisége, nagyságrendje)	
4	**Fenyegetés típusa** (az azonosított kockázat az EIR-ben kezelt adatok mely tulajdonságát – vagy többet is – fenyegeti: B: bizalmasság, S: sértetlenség, R: rendelkezésre állás)	
5	**Hatás (kár) értéke** (a következmény kockázati szint besorolása: 1 – 5)	
6	**Bekövetkezés valószínűsége** (A: alacsony / 1, K: közepes / 2, M: magas / 3, N: nagyon magas / 4)	
7	**Kockázat értéke** (A kockázat értékelésének eredménye: A: alacsony / 1-2; K: közepes / 3-4; M: magas / 5+)	
8	**Kockázatkezelési javaslat** (A kockázat kezelésére vonatkozó szakértői javaslat, pl.: új védelmi intézkedés bevezetése, az adott EIR vagy rendszerelem kivezetése, cseréje, stb.)	

II. Fizikai védelmi intézkedésekkel kapcsolatos kockázatok

1	**Sorszám / Azonosító** (pl.: sorfolytonos számozással, pl.: K01, K02, K03, stb.)	K03
2	**Kockázat megnevezése, leírása** (az azonosított kockázat megnevezése, leírása: a fenyegetés és forrása, esetlegesen hiányzó kontrollok meghatározása)	
3	**Érintett adatok** (az adatkör típusa: személyes / különleges / minősített / közérdekű vagy közérdekből nyilvános adatok / egyéb és mennyisége, nagyságrendje)	
4	**Fenyegetés típusa** (az azonosított kockázat az EIR-ben kezelt adatok mely tulajdonságát – vagy többet is – fenyegeti: B: bizalmasság, S: sértetlenség, R: rendelkezésre állás)	
5	**Hatás (kár) értéke** (a következmény kockázati szint besorolása: 1 – 5)	
6	**Bekövetkezés valószínűsége** (A: alacsony / 1, K: közepes / 2, M: magas / 3, N: nagyon magas / 4)	
7	**Kockázat értéke** (A kockázat értékelésének eredménye: A: alacsony / 1-2; K: közepes / 3-4; M: magas / 5+)	
8	**Kockázatkezelési javaslat** (A kockázat kezelésére vonatkozó szakértői javaslat, pl.: új védelmi intézkedés bevezetése, az adott EIR vagy rendszerelem kivezetése, cseréje, stb.)	

1	**Sorszám / Azonosító** (pl.: sorfolytonos számozással, pl.: K01, K02, K03, stb.)	K04
2	**Kockázat megnevezése, leírása** (az azonosított kockázat megnevezése, leírása: a fenyegetés és forrása, esetlegesen hiányzó kontrollok meghatározása)	
3	**Érintett adatok** (az adatkör típusa: személyes / különleges / minősített / közérdekű vagy közérdekből nyilvános adatok / egyéb és mennyisége, nagyságrendje)	
4	**Fenyegetés típusa** (az azonosított kockázat az EIR-ben kezelt adatok mely tulajdonságát – vagy többet is – fenyegeti: B: bizalmasság, S: sértetlenség, R: rendelkezésre állás)	
5	**Hatás (kár) értéke** (a következmény kockázati szint besorolása: 1 – 5)	
6	**Bekövetkezés valószínűsége** (A: alacsony / 1, K: közepes / 2, M: magas / 3, N: nagyon magas / 4)	
7	**Kockázat értéke** (A kockázat értékelésének eredménye: A: alacsony / 1-2; K: közepes / 3-4; M: magas / 5+)	
8	**Kockázatkezelési javaslat** (A kockázat kezelésére vonatkozó szakértői javaslat, pl.: új védelmi intézkedés bevezetése, az adott EIR vagy rendszerelem kivezetése, cseréje, stb.)	

III. Logikai védelmi intézkedésekkel kapcsolatos kockázatok

1	**Sorszám / Azonosító** (pl.: sorfolytonos számozással, pl.: K01, K02, K03, stb.)	K05
2	**Kockázat megnevezése, leírása** (az azonosított kockázat megnevezése, leírása: a fenyegetés és forrása, esetlegesen hiányzó kontrollok meghatározása)	
3	**Érintett adatok** (az adatkör típusa: személyes / különleges / minősített / közérdekű vagy közérdekből nyilvános adatok / egyéb és mennyisége, nagyságrendje)	
4	**Fenyegetés típusa** (az azonosított kockázat az EIR-ben kezelt adatok mely tulajdonságát – vagy többet is – fenyegeti: B: bizalmasság, S: sértetlenség, R: rendelkezésre állás)	
5	**Hatás (kár) értéke** (a következmény kockázati szint besorolása: 1 – 5)	
6	**Bekövetkezés valószínűsége** (A: alacsony / 1, K: közepes / 2, M: magas / 3, N: nagyon magas / 4)	
7	**Kockázat értéke** (A kockázat értékelésének eredménye: A: alacsony / 1-2; K: közepes / 3-4; M: magas / 5+)	
8	**Kockázatkezelési javaslat** (A kockázat kezelésére vonatkozó szakértői javaslat, pl.: új védelmi intézkedés bevezetése, az adott EIR vagy rendszerelem kivezetése, cseréje, stb.)	

1	**Sorszám / Azonosító** (pl.: sorfolytonos számozással, pl.: K01, K02, K03, stb.)	K06
2	**Kockázat megnevezése, leírása** (az azonosított kockázat megnevezése, leírása: a fenyegetés és forrása, esetlegesen hiányzó kontrollok meghatározása)	
3	**Érintett adatok** (az adatkör típusa: személyes / különleges / minősített / közérdekű vagy közérdekből nyilvános adatok / egyéb és mennyisége, nagyságrendje)	
4	**Fenyegetés típusa** (az azonosított kockázat az EIR-ben kezelt adatok mely tulajdonságát – vagy többet is – fenyegeti: B: bizalmasság, S: sértetlenség, R: rendelkezésre állás)	
5	**Hatás (kár) értéke** (a következmény kockázati szint besorolása: 1 – 5)	
6	**Bekövetkezés valószínűsége** (A: alacsony / 1, K: közepes / 2, M: magas / 3, N: nagyon magas / 4)	
7	**Kockázat értéke** (A kockázat értékelésének eredménye: A: alacsony / 1-2; K: közepes / 3-4; M: magas / 5+)	
8	**Kockázatkezelési javaslat** (A kockázat kezelésére vonatkozó szakértői javaslat, pl.: új védelmi intézkedés bevezetése, az adott EIR vagy rendszerelem kivezetése, cseréje, stb.)	

Szám: 1709-1/2020.

A KISLÁNGI POLGÁRMESTERI HIVATAL

INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Kisláng

2020

Kiadva / hatályos:

Készítette:

HANGANOV Kft.
Az információbiztonság és az adatvédelem szakértője
www.hanganov.hu

TARTALOM

1 A SZABÁLYZAT CÉLJA 5
2 A SZABÁLYZAT HATÁLYA 5
2.1 A SZABÁLYZAT SZEMÉLYI HATÁLYA 5
2.2 A SZABÁLYZAT TÁRGYI HATÁLYA 5
2.3 A SZABÁLYZAT IDŐBELI HATÁLYA 5
3 A SZABÁLYZAT KIADÁSA, KEZELÉSE, FELÜLVIZSGÁLATA 6
4 DOKUMENTUMVÉDELEM 6
5 ÁLTALÁNOS ADAT- ÉS INFORMÁCIÓVÉDELMI SZABÁLYOK 6
6 AZ INFORMÁCIÓBIZTONSÁG SZERVEZETE 7
7 AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGÁÉRT FELELŐS SZEMÉLY 7
8 BIZTONSÁGI OSZTÁLYBA SOROLÁS 7
8.1 A HIVATAL ÁLTAL HASZNÁLT EIR-EK BIZTONSÁGI BESOROLÁSA 7
8.2 A HIVATAL SZERVEZETÉNEK BIZTONSÁGI BESOROLÁSA 7
9 CSELEKVÉSI TERV 8
10 AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK NYILVÁNTARTÁSA 8
11 AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGGAL KAPCSOLATOS ENGEDÉLYEZÉSI ELJÁRÁS 8
12 KOCKÁZATELEMZÉS 9
13 RENDSZER ÉS SZOLGÁLTATÁSBESZERZÉS 9
14 ÜZLETMENET- (ÜGYMENET-) FOLYTONOSSÁG TERVEZÉSE 9
14.1 ÜZLETMENET-FOLYTONOSSÁGI TERV INFORMATIKAI ERŐFORRÁS KIESÉSEKRE 10
14.2 ÜZLETMENET-FOLYTONOSSÁGRA VONATKOZÓ ELJÁRÁS 11
14.2.1 Esemény felismerése, jelzése 11
14.2.2 Döntés az erőforrás kiesés kezelésének módjáról 11
14.2.3 Vészhelyzet elhárítása, visszatérés a normál működési folyamathoz 11
14.3 A FOLYAMATOS MŰKÖDÉSRE FELKÉSZÍTŐ KÉPZÉS 11
14.4 AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER MENTÉSEI 12
14.5 AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER HELYREÁLLÍTÁSA ÉS ÚJRAINDÍTÁSA 12
15 A BIZTONSÁGI ESEMÉNYEK KEZELÉSE 12
15.1 A BIZTONSÁGI ESEMÉNYEK FIGYELÉSE 12
15.2 A BIZTONSÁGI ESEMÉNYEK JELENTÉSE 12
15.3 SEGÍTSÉGNYÚJTÁS A BIZTONSÁGI ESEMÉNYEK KEZELÉSÉHEZ 13
15.4 BIZTONSÁGI ESEMÉNYKEZELÉSI TERV 13
15.5 KÉPZÉS A BIZTONSÁGI ESEMÉNYEK KEZELÉSÉRE 13
16 EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY-BIZTONSÁG 13
16.1 SZEMÉLYBIZTONSÁGI FELTÉTELEK 13
16.2 A HIVATALLAL SZERZŐDÉSES JOGVISZONYBAN ÁLLÓ (KÜLSŐ) SZERVEZETRE VONATKOZÓ KÖVETELMÉNYEK 14
16.3 ELJÁRÁS A JOGVISZONY MEGSZŰNÉSEKOR 16
16.4 AZ ÁTHELYEZÉSEK, ÁTIRÁNYÍTÁSOK ÉS KIRENDELÉSEK KEZELÉSE 16
16.5 FEGYELMI INTÉZKEDÉSEK 17
16.6 VISELKEDÉSI SZABÁLYOK AZ INTERNETEN 17
17 TUDATOSSÁG ÉS KÉPZÉS 17
17.1 KAPCSOLATTARTÁS AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁG JOGSZABÁLYBAN MEGHATÁROZOTT SZERVEZETRENDSZERÉVEL ÉS AZ E CÉLT SZOLGÁLÓ ÁGAZATI SZERVEZETEKKEL 17
17.2 KÉPZÉSI ELJÁRÁSREND 18
17.3 BIZTONSÁG TUDATOSSÁG KÉPZÉS 18
17.4 SZEREPKÖR VAGY FELADAT ALAPÚ BIZTONSÁGI KÉPZÉS 18
17.5 A BIZTONSÁGI KÉPZÉSRE VONATKOZÓ DOKUMENTÁCIÓK 19
18 FIZIKAI ÉS KÖRNYEZETI VÉDELEM 19
18.1 FIZIKAI VÉDELMI ELJÁRÁSREND 19
18.2 FIZIKAI BELÉPÉSI ENGEDÉLYEK 20
18.3 A FIZIKAI BELÉPÉS ELLENŐRZÉSE 21
18.4 A FIZIKAI HOZZÁFÉRÉSEK FELÜGYELETE 22
18.5 A LÁTOGATÓK ELLENŐRZÉSE 22

18.6 Vészvilágítás 22
18.7 Tűzvédelem 22
18.8 Hőmérséklet és páratartalom ellenőrzés 22
18.9 Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem 22
18.10 Be- és kiszállítás 23
18.11 Karbantartók 23
19 ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK 23
19.1 Engedélyezés 23
19.2 Az elektronikus információs rendszer kapcsolódásai 23
19.3 Külső kapcsolódásokra vonatkozó korlátozások 24
20 TERVEZÉS 24
20.1 Rendszerbiztonsági terv 24
20.2 Cselekvési terv készítése 25
20.3 Személyi biztonság 25
21 BIZTONSÁGI ELEMZÉS 25
21.1 Biztonságelemzési eljárásrend 25
21.2 Biztonsági értékelések 25
21.3 A biztonsági teljesítmény mérése 26
22 TESZTELÉS, KÉPZÉS ÉS FELÜGYELET 26
22.1 Tesztelési, képzési és felügyeleti eljárások 26
22.2 Sérülékenység-teszt 26
23 KONFIGURÁCIÓKEZELÉS 27
23.1 Konfigurációkezelési eljárásrend 27
23.2 Alapkonfiguráció 27
23.3 A konfigurációváltozások felügyelete (változáskezelés) 27
23.4 Előzetes tesztelés és megerősítés 28
23.5 Biztonsági hatásvizsgálat 28
23.6 Konfigurációs beállítások 28
23.7 Legszűkebb funkcionalitás 28
23.8 Elektronikus információs rendszerelem leltár 29
23.9 A szoftverhasználat korlátozásai 29
23.10 A felhasználó által telepített szoftverek 29
24 KARBANTARTÁS 30
24.1 Rendszer karbantartási eljárásrend 30
24.2 Rendszeres karbantartás 30
25 ADATHORDOZÓK VÉDELME 30
25.1 Adathordozók védelmére vonatkozó eljárásrend 30
25.2 Hozzáférés az adathordozókhoz 31
25.3 Adathordozók törlése 31
25.4 Adathordozók használata 31
26 AZONOSÍTÁS ÉS HITELESÍTÉS 32
26.1 Azonosítási és hitelesítési eljárásrend 32
26.2 Azonosítás és hitelesítés 32
26.3 Hálózati hozzáférés privilegizált fiókokhoz 32
26.4 Azonosító kezelés 32
26.5 A hitelesítésre szolgáló eszközök kezelése 33
26.6 A hitelesítésre szolgáló eszköz visszacsatolása 34
26.7 Hitelesítés kriptográfiai modul esetén 34
26.8 Azonosítás és hitelesítés (szervezeten kívüli felhasználók) 34
26.9 Hitelesítésszolgáltatók tanúsítványának elfogadása 34
27 HOZZÁFÉRÉS ELLENŐRZÉSE 34
27.1 Hozzáférés ellenőrzési eljárásrend 34
27.2 Felhasználói fiókok kezelése 35
27.3 Hozzáférés ellenőrzés érvényesítése 35
27.4 Sikertelen bejelentkezési kísérletek 35
27.5 A rendszerhasználat jelzése 36

27.6 Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek 36
27.7 Távoli hozzáférés 36
27.8 Vezeték nélküli hozzáférés 37
27.9 Mobil eszközök hozzáférés ellenőrzése 37
27.10 Külső elektronikus információs rendszerek használata 37
27.11 Nyilvánosan elérhető tartalom 38
28 RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG 38
28.1 Rendszer- és információsértetlenségre vonatkozó eljárásrend 38
28.2 Hibajavítás 38
28.3 Kártékony kódok elleni védelem 38
28.4 Az elektronikus információs rendszer felügyelete 39
28.5 Biztonsági riasztások és tájékoztatások 40
28.6 A kimeneti információ kezelése és megőrzése 40
29 NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG 40
29.1 Naplózási eljárásrend 40
29.2 Naplózható események 40
29.3 Naplóbejegyzések tartalma 41
29.4 Napló tárkapacitás 41
29.5 Naplózási hiba kezelése 42
29.6 Naplóvizsgálat és jelentéskészítés 42
29.7 Időbélyegek 42
29.8 A naplóinformációk védelme 42
29.9 A naplóbejegyzések megőrzése 43
29.10 Naplógenerálás 43
30 RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM 43
30.1 Rendszer- és kommunikációvédelmi eljárásrend 43
30.2 Túlterhelés – szolgáltatás megtagadás alapú támadás – elleni védelem 43
30.3 A határok védelme 44
30.4 Kriptográfiai kulcs előállítása és kezelése 44
30.5 Kriptográfiai védelem 44
30.6 Együttműködésen alapuló számítástechnikai eszközök 44
30.7 Biztonságos név/cím feloldó szolgáltatások (úgynevezett hiteles forrás) 45
30.8 Biztonságos név/cím feloldó szolgáltatás (úgynevezett rekurzív vagy gyorsító tárat használó feloldás) 45
30.9 Architektúra és tartalékok név/cím feloldási szolgáltatás esetén 45
30.10 A folyamatok elkülönítése 45
31 ZÁRÓ RENDELKEZÉSEK 46
1. SZÁMÚ MELLÉKLET – AZ INFORMÁCIÓBIZTONSÁG SZEREPLŐI 47
2. SZÁMÚ MELLÉKLET – MEGISMERÉSI NYILATKOZAT 48
3. SZÁMÚ MELLÉKLET – AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK NYILVÁNTARTÁSA 49
4. SZÁMÚ MELLÉKLET – VÁLTOZÁSKEZELÉSI ADATLAP 52
5. SZÁMÚ MELLÉKLET – AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK MENTÉSE 53
6. SZÁMÚ MELLÉKLET – ÜZLETMENET-FOLYTONOSSÁGI TERV INFORMATIKAI ERŐFORRÁS KIESÉSEKRE 55
7. SZÁMÚ MELLÉKLET – BELÉPÉSRE JOGOSULTAK NYILVÁNTARTÁSA 59
8. SZÁMÚ MELLÉKLET – BELÉPÉSI NAPLÓ 60
9. SZÁMÚ MELLÉKLET – INFORMÁCIÓS RENDSZERELEMEK BE- ÉS KISZÁLLÍTÁSÁNAK NYILVÁNTARTÁSA 61
10. SZÁMÚ MELLÉKLET – ELEKTRONIKUS INFORMÁCIÓS RENDSZERELEM LELTÁR 62
11. SZÁMÚ MELLÉKLET – TITOKTARTÁSI NYILATKOZAT 64
12. SZÁMÚ MELLÉKLET – HELYISÉGEK BIZTONSÁGI BESOROLÁSA 65

1 A SZABÁLYZAT CÉLJA

Az Informatikai Biztonsági Szabályzat célja mindazon rendszerszintű követelmények, előírások és eljárások, feladatok és tevékenységek meghatározása és egységes, magas szintű szabályozási keretbe foglalása, melyek által a Kislángi Polgármesteri Hivatal (a továbbiakban: Hivatal) információbiztonsága, rendeltetésszerű és biztonságos működése, továbbá a Hivatal által használt elektronikus információs rendszerek (a továbbiakban: EIR) sértetlensége és rendelkezésre állása, valamint a Hivatal által kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása folyamatosan fenntartható módon megvalósítható, megőrizhető, illetve továbbfejleszthető.

Célja emellett a vonatkozó jogszabályoknak, különösen az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (továbbiakban: Ibtv.), a végrehajtására kiadott 41/2015. (VII. 15.) BM rendelet (továbbiakban: Vhr.), valamint a 257/2016. (VIII. 31.) Korm. rendeletben foglalt információbiztonsági követelményeknek való megfelelés biztosítása.

Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) a fenti célok teljesülése érdekében rögzíti a Hivatal elvárt biztonsági szintjének és az általa használt EIR-ek biztonsági osztályba sorolásának megfelelő adminisztratív, fizikai és logikai védelmi intézkedésekkel kapcsolatos követelmények teljesítésével összefüggő folyamatokat, eljárásokat, feladatokat és felelősségeket.

A feladatok végrehajtása a 6. Az információbiztonság szervezete című fejezetben meghatározott szerepkörökhöz kapcsolódik, mely szerepkört betöltő személyek adatai, elérhetőségei az 1. számú melléklet – Az információbiztonság szereplői dokumentumban kerültek rögzítésre.

2 A SZABÁLYZAT HATÁLYA

2.1 A szabályzat személyi hatálya

A szabályzat személyi hatálya kiterjed a Hivatal köztisztviselőire, munkavállalóira, valamint azokra a személyekre, akik részt vesznek a Hivatalnál keletkező, felhasznált, feldolgozott, tárolt, illetve továbbított adatok kezelésében.

Kiterjed továbbá mindazon, a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban lévő személyekre, akik a Hivatal által működtetett informatikai rendszerek kezelésében (üzemeltetésében, karbantartásában, javításában, illetve felügyeletében) részt vesznek.

2.2 A szabályzat tárgyi hatálya

A szabályzat tárgyi hatálya kiterjed a Hivatalnál keletkezett és a Hivatal által kezelt információk teljes életciklusukon át történő kezelésével, védelmével kapcsolatos eszközökre és tevékenységekre, valamint az informatikai rendszerben üzemeltetett valamennyi hardver és szoftver elemre, amely felhasználja, feldolgozza, felügyeli, ellenőrzi, tárolja, továbbítja a Hivatalnál keletkező, illetve felhasznált adatokat. Kiterjed továbbá a Hivatal által használt EIR-ek, illetve rendszerelemeik dokumentációira.

2.3 A szabályzat időbeli hatálya

A szabályzat kiadása napján lép hatályba és jelenlegi verziója visszavonásig – vagy a következő kiadásra kerülő verzió hatályba lépéséig – hatályos.

3 A SZABÁLYZAT KIADÁSA, KEZELÉSE, FELÜLVIZSGÁLATA

Az IBSZ kiadása, Hivatalon belüli kihirdetése és rendelkezésre állásának biztosítása (megőrzése) a Jegyző feladata és felelőssége.

Az IBSZ személyi hatálya alá tartozók munka- illetve feladatkörüknek megfelelő mértékben kötelesek az IBSZ tartalmát, a benne foglalt előírásokat, különösen a számukra meghatározott feladatokat és felelősségeket megismerni, s ezek tudomásul vételéről nyilatkozatot tenni (2. számú melléklet – Megismerési nyilatkozat). A nyilatkozatok megőrzéséről a Jegyző köteles gondoskodni.

Az IBSZ felülvizsgálatát és frissítését a következő gyakorisággal kell elvégezni:

- események hiányában 1 év múlva, vagy
- információbiztonsággal kapcsolatos jogszabályi változásokat követően, vagy
- az érintett szervezetben, illetve a szerepkörökben történő jelentős változás esetén, vagy
- új elektronikus információs rendszer bevezetését, használatba vételét megelőzően, illetve
- a védelmi intézkedésekben bekövetkezett jelentős technológiai változásokat követően.

Az IBSZ felülvizsgálatának kezdeményezése, a felülvizsgálat eredményeként esetlegesen keletkezett új vagy módosított szabályozó kiadása, valamint a felülvizsgálat megtörténtét igazoló feljegyzés megőrzése a Jegyző feladata és felelőssége.

Az IBSZ felülvizsgálatára javaslatot tehet az információbiztonsági felelős.

Az IBSZ felülvizsgálatát az információbiztonsági felelős köteles végrehajtani és eredményét dokumentáltan átadni a Jegyző számára.

4 DOKUMENTUMVÉDELEM

Az IBSZ és kapcsolódó eljárásrendjei, mellékletei, elkészítendő és megőrzendő dokumentumai, valamint az előírt nyilvántartások jogosulatlanok számára való megismerhetőségük és módosíthatóságuk elleni védelméről a Hivatal elektronikus formában történő tárolásuk, illetve vezetésük esetén hozzáférés- és jogosultsági rendszerrel védett tárterületen történő elhelyezéssel, illetve kizárólag a Hivatal belső hálózatán engedélyezett terjesztéssel, papír alapon a Hivatal iratkezelésre vonatkozó előírásai alapján gondoskodik.

Az IBSZ-ben előírt nyilvántartások elektronikus, illetve papír alapú dokumentumban egyaránt vezethetők a Jegyző erre vonatkozó döntése szerint.

Minden dokumentum esetében biztosítani szükséges annak folyamatos rendelkezésre állását, változás esetén kinyomtatott másodpéldányának az iratkezelési szabályoknak megfelelő helyi tárolásával. A dokumentum új verziójának készítője köteles azt, illetve annak nyomtatható, elektronikus példányát a Jegyző rendelkezésére bocsátani, aki gondoskodik az aktuálisan érvényes nyomtatott példánynak a Hivatal iratkezelésre vonatkozó előírásainak megfelelő módon történő kezeléséről és megőrzéséről.

5 ÁLTALÁNOS ADAT- ÉS INFORMÁCIÓVÉDELMI SZABÁLYOK

Az illetéktelen hozzáférés (megismerés, betekintés) elleni védelem biztosítása céljából a személyes adatot tartalmazó adathordozók, dokumentumok biztonságos kezeléséről minden hivatali munkavállaló a „Tiszta asztal, tiszta képernyő"-elv alkalmazásával köteles gondoskodni.

Az ügyfelek, illetve látogatók által látható területen az ügyintézés időtartama alatt a papír alapú adathordozók kezelése során kizárólag az aktuális ügyhöz szükséges iratok lehetnek elől (pl.: az íróasztalon), az elektronikus dokumentumok, valamint a Hivatal által használt EIR-ekben kezelt

adatok esetében kizárólag az aktuális ügyintézéshez szükséges alkalmazások, programablakok lehetnek megnyitva a képernyőn.

Az ügyintézés, illetve a munkavégzés befejezését követően minden iratot az eredeti tárolási helyére kell visszahelyezni, illetve a már nem szükséges alkalmazásokat, programablakokat be kell zárni.

Fenti szabályok a rálátásvédelem helyszíni kialakításától függetlenül kötelezően betartandók!

6 AZ INFORMÁCIÓBIZTONSÁG SZERVEZETE

A Hivatalban az információbiztonság szervezete az alábbi szerepkörök és felelősségi szintek szerint került kialakításra:

Felelősségi szint	Szerepkör
Vezetői általános felelősség, benne koordinációs, kommunikációs felelősség (Hivatal és hatóság, Hivatal és információbiztonsági felelős között)	Jegyző
Információbiztonsági tevékenységek tervezéséért, menedzseléséért való felelősség	Információbiztonsági felelős
Informatikai rendszerelemek működési, üzemeltetési felelőssége	IT üzemeltető
Információbiztonsági szabályok és előírások betartása	Jelen szabályzat személyi hatálya alá tartozók (a Hivatal munkavállalói, a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban lévők)

7 AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGÁÉRT FELELŐS SZEMÉLY

Az információbiztonsági felelős megbízása, kinevezése, illetve szükség esetén megbízásának visszavonása, dokumentálása, továbbá hatósági bejelentése a Jegyző feladata és felelőssége.

A megbízott információbiztonsági felelős adatai az 1. számú melléklet – Az információbiztonság szereplői dokumentumban kerülnek rögzítésre.

8 BIZTONSÁGI OSZTÁLYBA SOROLÁS

8.1 A Hivatal által használt EIR-ek biztonsági besorolása

Az Ibtv. alkalmazásában egy elektronikus információs rendszernek kell tekinteni adott adatgazda által, adott cél érdekében az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttesét.

A Hivatal az általa használt EIR-ek biztonsági osztályba sorolását a 10. Az elektronikus információs rendszerek nyilvántartása fejezetben előírt nyilvántartásban jelöli.

8.2 A Hivatal szervezetének biztonsági besorolása

A Hivatal elvárt biztonsági szintjét az Ibtv. és a Vhr. előírásai alapján az információbiztonsági felelős állapítja meg és a Jegyző az IBSZ (jelen szabályzat) kiadásával hagyja jóvá.

Az Ibtv. és a Vhr. előírásai alapján a Hivatal, mint szervezet elvárt biztonsági szintje: **4.**

A biztonsági szintbe sorolás indoklása:

A Hivatal szakfeladatait támogató elektronikus információs rendszert használ és üzemelteti azt, továbbá központi üzemeltetésű és több szervezetre érvényes biztonsági megoldásokkal védett elektronikus információs rendszerek felhasználója, illetve feladatai támogatására más külső szolgáltatót is igénybe vesz.

9 CSELEKVÉSI TERV

A Hivatal a megvalósítandó biztonsági intézkedéseket és azok megvalósításának sorrendjét az elvárt biztonsági szint elérése céljából cselekvési tervben határozza meg. A terv elkészítésében közreműködik az információbiztonsági felelős.

A terv jóváhagyása, a felügyeleti hatóság számára történő megküldése, valamint végrehajtásának elrendelése a Jegyző feladata és felelőssége.

A tervben foglalt feladatok végrehajtásában köteles minden érintett hivatali munkavállaló és az IT üzemeltető közreműködni. A tervben foglaltak végrehajtását az információbiztonsági felelős köteles – a tervben megállapított mérföldkövekhez, határidőkhöz igazodva – szükség szerint a Hivatal munkavállalói, az IT üzemeltető, illetve az egyéb közreműködők (pl.: szerződéses szolgáltató partnerek) bevonásával ellenőrizni, s annak eredményéről a Jegyzőt tájékoztatni, indokolt esetben a terv felülvizsgálatát, módosítását kezdeményezni, továbbá abban közreműködni.

10 AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK NYILVÁNTARTÁSA

A Hivatal az általa használt EIR-ekről jelen szabályzat 3. számú melléklet – Az elektronikus információs rendszerek nyilvántartása mellékletében foglalt tartalommal naprakész nyilvántartást vezet. A nyilvántartás vezetése, aktualizálása és megőrzése a Jegyző feladata és felelőssége, kitöltéséhez az információbiztonsági felelős és az IT üzemeltető szakmai, módszertani támogatást biztosít, illetve javaslatot tehet.

11 AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGGAL KAPCSOLATOS ENGEDÉLYEZÉSI ELJÁRÁS

A Jegyző jogosult és köteles a Hivatal hatáskörébe tartozó – jelen IBSZ-ben engedélyezéshez kötött – minden információbiztonsággal kapcsolatos tevékenységgel, intézkedéssel kapcsolatban a szükséges engedélyezési eljárást lefolytatni, különösen az alábbiak esetében:

a) az irányítása alá tartozó munkavállalók munkavégzéséhez szükséges infokommunikációs eszközök biztosítása;
b) a használt, illetve használandó, új rendszerek és azokhoz szükséges jogosultságok, hozzáférések beállítása (a kapcsolódó felhasználói fiókok létrehozása, módosítása, illetve törlése), illetve a rendszer vagy rendszerelem konfigurációjának módosítása;
c) az elektronikus információs rendszereknek helyt adó létesítményekbe, helyiségekbe történő belépés;
d) információs rendszerelemek be- és kiszállítása;
e) az elektronikus információs rendszeren, illetve elemein karbantartás, javítás végrehajtása, a munkavégzés engedélyezése;
f) elektronikus adathordozók használata;
g) távoli, illetve vezeték nélküli hozzáférések;
h) együttműködésen alapuló számítástechnikai eszközök használata;

i) új elektronikus információs rendszer bevezetése;
j) új rendszerelem meglévő EIR-be illesztése;
k) elektronikus információs rendszerének más (helyi, illetve külső) elektronikus információs rendszerekhez történő kapcsolódása.

Az f - k) pontokban fentiekben felsorolt, információbiztonsági engedélyezéshez kötött új igény, illetve változás jelzése az információbiztonsági felelős felé a Jegyző feladata és felelőssége.

Az információbiztonsági felelős feladata a változásra vonatkozóan rendelkezésre álló információk alapján megvizsgálni és értékelni a tervezett változtatás információbiztonságra gyakorolt várható hatását, lehetséges kockázatait, s ennek alapján a változtatás – esetleg kiegészítő védelmi intézkedésekkel történő – jóváhagyására, illetőleg a változtatási igény elutasítására javaslatot tenni a Jegyző felé.

Az engedélyezési eljárás, valamint annak eredményét is tartalmazó dokumentáció (4. számú melléklet – Változáskezelési adatlap) megőrzéséről a Jegyző köteles gondoskodni.

12 KOCKÁZATELEMZÉS

A kockázatok elemzésének rendje, az azzal összefüggő tevékenységek, feladatok és felelősségek az ***Elektronikus információs rendszerek kockázatelemzési és kockázatkezelési eljárásrendjében*** kerültek rögzítésre.

13 RENDSZER ÉS SZOLGÁLTATÁSBESZERZÉS

A Hivatal saját hatáskörében nem szerez be olyan informatikai szolgáltatást vagy eszközöket, valamint nem végez vagy végeztet olyan rendszerfejlesztési tevékenységet, amely a Vhr.-ben meghatározott védelmi követelmények teljesítési kötelezettségét vonná maga után.

A Vhr. előírásai szerint a jellemzően kis értékű, kereskedelmi forgalomban kapható, általában irodai alkalmazások, szoftverek beszerzése, illetve azok a hardver beszerzések, amelyek jellemzően a tönkrement eszközök pótlása vagy az eszközpark addigiakkal azonos vagy hasonló eszközökkel való bővítése céljából történnek, valamint a javítás, karbantartás céljára történő beszerzések esetében az érintett szervezet nem köteles alkalmazni a rendszer és szolgáltatásbeszerzésre meghatározott követelményeket. Szintén ebbe a körbe tartozik, azaz nem minősül fejlesztésnek a Vhr. szerint a kereskedelmi forgalomban kapható szoftverek beszerzése és frissítése.

A Hivatal informatikai rendszerének működtetéséhez és biztonságos üzemeltetéséhez kapcsolódó szolgáltatások (pl.: internet kapcsolat, informatikai eszközök üzemeltetése, karbantartása, stb.) beszerzése során a Jegyző köteles gondoskodni arról, hogy a szolgáltatási szerződés tartalma, illetve a szolgáltatás nyújtása összhangban legyen a Hivatal által elvárt információbiztonsági követelményekkel (lásd: 16.2 A Hivatallal szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények).

14 ÜZLETMENET- (ÜGYMENET-) FOLYTONOSSÁG TERVEZÉSE

A Hivatal által használt EIR-ek rendelkezésre állásának, valamint az EIR-ekben tárolt, illetve kezelt adatok sértetlenségének és rendelkezésre állásának megőrzése érdekében a Hivatal az alábbi, megelőző védelmi intézkedéseket teszi:

- gondoskodik a működéséhez szükséges helyben tárolt adatok, információk megfelelő és rendszeres biztonsági mentéséről a 14.4 Az elektronikus információs rendszer mentései fejezetben meghatározottak szerint;

- megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását; ennek érdekében a mentési adathordozók tárolására elsődleges és másodlagos tárolási helyszínt jelöl ki, továbbá kialakítja a mentési adathordozók biztonságos tárolásának feltételeit (pl.: zárható lemezszekrény vagy páncélszekrény, elektronikus védelemmel ellátott helyiség, stb.);
- gondoskodik az informatikai eszközök rendszeres karbantartásáról, szükség szerinti javításáról;
- a kieső informatikai erőforrások (pl.: hardvereszközök) pótlásáról szükség esetén rendkívüli beszerzéssel gondoskodik;
- a működése, a hivatali ügymenet folyamatosságának biztosítása érdekében a munkavégzéshez szükséges informatikai erőforrások kiesésére vonatkozóan tervet készít, amely tartalmazza az érintett EIR-eket, az alapfeladatokat és funkciókat, a problémakezeléshez szükséges azonnali intézkedéseket, valamint a helyreállítási idő függvényében szükséges helyettesítő eljárásokat, a helyreállításhoz szükséges erőforrásokat, feladatokat, az intézkedések végrehajtásáért felelős szerepköröket, feladataikat, továbbá a normál működési folyamathoz történő visszatérés feltételeit.

14.1 Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

Az üzletmenet-folytonossági terv szabályozza a Hivatal ügymenetéhez tartozó folyamatait veszélyeztető informatikai erőforrás kiesésekkel kapcsolatos hibák vagy egyéb események esetén megteendő intézkedéseket, úgymint:

- az azonnali intézkedéseket;
- a hivatali folyamatok, az ügymenet folyamatosságának (szükség esetén) alternatív módon történő biztosítását célzó helyettesítő eljárásokat;
- a normál működési folyamathoz való visszatéréssel kapcsolatos feladatokat.

A Hivatal az üzletmenet-folytonossági tervben határozza meg és rögzíti az ügymenete, illetve folyamatai informatikai szolgáltatásoktól való függősége alapján az általa használt rendszerekkel szemben támasztott rendelkezésre állási és visszaállítási követelményeket (mennyi ideig tudják az adott rendszert nélkülözni), valamint az informatikai támogatás nélküli időszakra helyettesítő eljárások bevezetésének szükségességét, továbbá az azok alkalmazásához biztosítandó feltételeket (6. számú melléklet – Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre).

Az üzletmenet-folytonossági tervben nem szerepelnek azon EIR-ek, illetve rendszerelemeik, amelyek a Hivatal által elfogadható kiesési, illetve helyreállítási időn belül pótolhatók.

Az informatikai erőforrások kiesésére vonatkozó üzletmenet-folytonossági terv kiadása (hatályba léptetése), az érintettekkel történő megismertetése, a végrehajtásában érintettek számára hozzáférhető helyen, nyomtatott formában történő tárolásának biztosítása, továbbá rendszeres, illetve szükség szerinti felülvizsgálatának elrendelése a Jegyző feladata és felelőssége.

A terv szakmai tartalmának ellenőrzése, jóváhagyása és felülvizsgálata az információbiztonsági felelős feladata. Az üzletmenet-folytonossági terv elkészítésében, végrehajtásában, rendszeres tesztelésében és felülvizsgálatában feladatellátása keretében részt vesz, illetve közreműködik az IT üzemeltető.

Az IT üzemeltető feladata gondoskodni arról, hogy minden, a tervben szereplő rendszer és erőforrás vonatkozásában rendelkezésre álljanak azok a dokumentált eljárások, amelyek alapján a helyreállítás elvégezhető.

Az IT üzemeltető feladata a visszaállítási eljárások dokumentált tesztelése, valamint változás esetén a mentési rend aktualizálása a 14.4 Az elektronikus információs rendszer mentései fejezetben előírtak szerint az alábbi rendszerességgel:

- új EIR bevezetése során;
- a mentési eljárásrendet érintő változás esetén (pl.: mentendő információk körének vagy a mentési gyakoriságnak a változása);

- az alkalmazott mentési technológia változása esetén;
- a rendelkezésre állási és visszaállítási követelmények változásakor;
- az előző pontokban felsorolt változások hiányában évente legalább egy alkalommal.

14.2 Üzletmenet-folytonosságra vonatkozó eljárás

14.2.1 Esemény felismerése, jelzése

Amennyiben olyan esemény következik be, amely a Hivatal munkavégzéshez szükséges informatikai eszközöket, illetve rendszereit részben vagy teljesen működésképtelenné teszi, a Jegyzőt haladéktalanul értesíteni kell. Az értesítés az eseményt észlelő munkavállaló vagy IT üzemeltető feladata és kötelessége.

14.2.2 Döntés az erőforrás kiesés kezelésének módjáról

A Jegyző – szükség szerint az IT üzemeltetővel, központi vagy külső szolgáltatás esetén annak üzemeltetési kapcsolattartójával, illetve az információbiztonsági felelőssel konzultálva – a bekövetkezett erőforráskieséses állapot körülményeiről és hatásairól, az erőforráskiesés megszüntetésére vonatkozó intézkedések végrehajtásának becsült időtartamáról (helyreállítási idő) rendelkezésre álló információk mérlegelését követően dönt az esemény kezelési módjáról, amely lehet:

- kisebb hatású, az informatikai erőforrások szűk körét érintő vagy várhatóan rövid idejű erőforráskiesés esetén (pl.: olyan hibajelenség előfordulásakor, amely helyben – esetleg távoli segítségnyújtás igénybe vételével – kezelhető, mint például egy eszköz újraindítása) a szükséges intézkedés megtételének;
- az informatikai erőforrások széles körét vagy egészét érintő (vészhelyzet) esetén az üzletmenet-folytonossági tervben szereplő helyettesítő eljárások, illetve helyreállító tevékenységek végrehajtásának elrendelése.

Amennyiben a bekövetkezett esemény kapcsán, illetve a probléma kezelése során megállapítható, hogy a Hivatal által használt EIR-ekben kezelt, tárolt vagy feldolgozott adatok bizalmassága, sértetlensége vagy rendelkezésre állása megsérült, úgy a Jegyző köteles a 15. A biztonsági események kezelése fejezetben foglaltak szerint eljárni.

14.2.3 Vészhelyzet elhárítása, visszatérés a normál működési folyamathoz

A helyzet kezeléséről hozott döntésnek megfelelően a helyreállításban kompetens (pl.: IT üzemeltető) végrehajtja a szükséges intézkedést, majd annak eredményéről tájékoztatja a Jegyzőt, illetve az információbiztonsági felelőst.

A Jegyző az üzletmenet-folytonossági tervben foglalt, az erőforrás kiesés sikeres megszüntetésére vonatkozó feltételek fennállása esetén rendelheti el a normál működési folyamathoz történő visszatérést, s tájékoztatja erről az érintett személyeket.

14.3 A folyamatos működésre felkészítő képzés

Az Üzletmenet-folytonossági terv végrehajtásához kapcsolódó feladatokat minden, a terv végrehajtásában érintett személlyel dokumentált módon meg kell ismertetni. A szükséges képzési forma kiválasztása, a képzés megszervezése, valamint a tervezett képzés tartalmáról, lebonyolításáról az információbiztonsági felelős tájékoztatása a Jegyző feladata és felelőssége. A képzés szakmai tartalmának megfelelőségét a tájékoztatás alapján az információbiztonsági felelős ellenőrzi, illetve hagyja jóvá.

Az üzletmenet-folytonossághoz kapcsolódó további előírások, dokumentumok:

- 5. számú melléklet – Az elektronikus információs rendszerek mentése.
- 6. számú melléklet – Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre,

Az üzletmenet-folytonosságot érintő előírások dokumentált felülvizsgálatát az információbiztonsági felelős évente köteles elvégezni, s ennek eredményéről a Jegyzőt tájékoztatni.

14.4 Az elektronikus információs rendszer mentései

A biztonsági mentések konfigurálása és rendszeres végrehajtása a dokumentált mentési rend alapján (5. számú melléklet – Az elektronikus információs rendszerek mentése) az IT üzemeltető feladata és felelőssége. A rendszeres biztonsági mentésekre vonatkozó információkat (mentendő adatok köre, mentési gyakoriság, megőrzési idő, elsődleges és másodlagos tárolási helyszín, stb.) az 5. számú melléklet – Az elektronikus információs rendszerek mentésedokumentum tartalmazza.

Az eseti biztonsági mentések, valamint a helyreállítási, illetve tesztelési célú visszatöltések végrehajtásáról az IT üzemeltető köteles a szintén az 5. számú melléklet – Az elektronikus információs rendszerek mentésedokumentumban meghatározott mentési napló tartalommal nyilvántartást vezetni.

14.5 Az elektronikus információs rendszer helyreállítása és újraindítása

Amennyiben a Hivatal által használt EIR-eket, rendszerelemeiket érintő hiba vagy biztonsági esemény kezelése biztonsági mentésből történő helyreállítási, illetve újraindítási tevékenységet igényel, azok végrehajtása az IT üzemeltető feladata és felelőssége. Kivételt képezhet ez alól a kisebb – nem kiszolgáló szintű – újraindítási feladatok végrehajtása (pl.: munkaállomás esetén), melyet – szükség szerint az IT üzemeltető szakmai támogatása mellett – az eszköz használatára feljogosított hivatali munkavállaló is végrehajthat.

15 A BIZTONSÁGI ESEMÉNYEK KEZELÉSE

A Hivatal annak érdekében, hogy a biztonsági események által okozható kár minimális legyen, az információbiztonsági incidensek tervezett kezelésére jelen fő fejezetben meghatározott eljárásrendet lépteti életbe.

15.1 A biztonsági események figyelése

A Hivatal által használt EIR-ekhez hozzáféréssel rendelkező munkatársak és a Hivatallal egyéb munkavégzésre irányuló jogviszonyban álló személyek egyaránt kötelesek hibás működés vagy rendellenes esemény észlelése esetén jelezni. A jelzés formájától és tartalmától függően az esemény a kezelése során különböző eszkalációs szinteken kerülhet dokumentálásra. Elektronikus (pl.: email) jelzés esetén az észlelő, egyéb esetekben az IT üzemeltető, hatósági bejelentést igénylő biztonsági esemény kapcsán az információbiztonsági felelős által.

15.2 A biztonsági események jelentése

A Hivatal által használt EIR-ek bármely rendszerelemének, hardver- illetve szoftver komponenseinek rendellenes vagy hibás működéséről, működési zavarairól vagy hibajelzéseiről lehetőség szerint elektronikus formában (email) – vagy ha az nem működik, akkor telefonon keresztül – minden munkavállaló köteles tájékoztatni az IT üzemeltetőt, aki biztonsági incidens gyanújának felmerülésekor köteles haladéktalanul tájékoztatni az információbiztonsági felelőst és a Jegyzőt.

Amennyiben a Hivatal által használt EIR-ek bármely eleme vonatkozásában egyértelműen azonosítható biztonsági esemény következik be vagy annak gyanúja felmerül (pl.: sérül a bizalmasság, indokolatlan adatmódosítás látható vagy nem áll rendelkezésre valamely rendszerelem), elektronikus formában (email) – vagy ha ez nem működik, akkor telefonon keresztül – haladéktalanul tájékoztatni kell az információbiztonsági felelőst, aki javaslatot tesz a Jegyző számára az incidens kezelési módjára, illetve a 15.4 Biztonsági eseménykezelési terv alapján bejelentési kötelezettség körébe

tartozó biztonsági eseményt jelenti az Ibtv.-ben meghatározott eseménykezelő felé. Ebben az esetben fenti eszkalációs rendből az IT üzemeltető kihagyható.

Az információbiztonsági felelős a bejelentett biztonsági eseményeket figyelemmel kíséri és dokumentálja.

15.3 Segítségnyújtás a biztonsági események kezeléséhez

A biztonsági incidens kezelésének támogatását a 15.4 Biztonsági eseménykezelési terv fejezetben meghatározottak szerint, feladat- illetve felelősségi körének megfelelően az IT üzemeltető, illetve az információbiztonsági felelős végzi.

15.4 Biztonsági eseménykezelési terv

A biztonsági események kezelésének előfeltétele azok felismerése, amelynek érdekében a Hivatal minden munkavállalója, illetve az általa használt EIR-ekhez hozzáféréssel rendelkező, a Hivatallal egyéb munkavégzésre irányuló jogviszonyban álló személy köteles a tapasztalt rendellenességeket a 15.2 A biztonsági események jelentése fejezetben meghatározott eszkalációs rend szerint jelezni.

Amennyiben a bekövetkezett esemény hatására a Hivatal által használt EIR-ek, illetve a bennük kezelt adatok, továbbá azok helyben tárolt bemeneti vagy kimeneti információinak bizalmassága, sértetlensége vagy rendelkezésre állása sérül vagy sérülhetett, akkor azt minden esetben biztonsági eseményként kell kezelni.

Az adott esemény biztonsági eseménnyé minősítését kérdéses esetben, illetve annak kiértékelése során az információbiztonsági felelős támogatja, illetve végzi el az eset összes körülményéről rendelkezésre álló információk alapján.

A biztonsági esemény értékeléséhez, kivizsgálásához, illetve bejelentéséhez esetlegesen szükséges további információk (pl.: log fájlok) begyűjtésében az IT üzemeltető köteles közreműködni.

A Hivatal által használt EIR-ek bizalmasságát, sértetlenségét, illetve rendelkezésre állását közvetlenül veszélyeztető biztonsági eseményt az információbiztonsági felelős köteles a jogszabályban meghatározott eseménykezelő felé bejelenteni.

A biztonsági esemény jellegétől és várható hatásaitól függően a bekövetkezett vagy okozható kár, kockázat mérséklése, illetve a fenyegetettség vagy veszélyhelyzet elhárítása, megszüntetése érdekében az információbiztonsági felelős által javasolt és szükséges, illetve a Jegyző által meghatározott intézkedések végrehajtásában minden érintett köteles együttműködni.

Az informatikai erőforrások kiesésével járó esemény bekövetkezése esetén a 14.2 Üzletmenet-folytonosságra vonatkozó eljárás, vírustámadás esetén a 28.3 Kártékony kódok elleni védelem fejezetben meghatározott intézkedések alkalmazandók.

A biztonsági esemény kezelésének lezárását követően szükség esetén új megelőző védelmi intézkedések bevezetésével kell a hasonló incidensek jövőbeni előfordulásának kockázatát csökkenteni. A biztonsági eseményről rendelkezésre álló információk vizsgálata alapján az információbiztonsági felelős jogosult az indokolt új, illetve meglévő védelmi intézkedések módosítására vonatkozó javaslat elkészítése, s a Jegyző számára történő megküldése.

15.5 Képzés a biztonsági események kezelésére

A Hivatal által használt EIR-ekhez, illetve a Hivatal által kezelt adatokhoz hozzáféréssel rendelkező személyek biztonsági események kezelésével kapcsolatos képzése a rendszeres éves biztonsági képzés részeként, a 17.4 Szerepkör vagy feladat alapú biztonsági képzés fejezetben meghatározottak szerint történik.

16 EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY-BIZTONSÁG

16.1 Személybiztonsági feltételek

A munkaköri alkalmasság jogszabályban meghatározott vizsgálata, illetve az ezzel kapcsolatos feladatok elvégzése, úgymint az adott hivatali munkakör betöltéséhez szükséges iskolai végzettség, szakképzettség, szakképesítés, illetve gyakorlati idő meglétének, valamint – amennyiben indokolt – egészségi és pszichikai alkalmasságra vonatkozó vizsgálatról szóló igazolások ellenőrzése a munkáltatói jogkört gyakorló vezető, azaz a Jegyző feladata és felelőssége.

A Hivatal nemzetbiztonsági ellenőrzés hatálya alá tartozó munka- illetve feladatkörrel nem rendelkezik.

A Hivatal által használt EIR-ekhez hozzáféréssel rendelkező munkatársak biztonsági szempontból azonos követelményeknek kell, hogy megfeleljenek. Esetükben a munkaköri alkalmassági követelményeknek történő megfelelés, a munkavégzésükre vonatkozó hivatali előírások, szabályozók, illetve eljárásrendek megismerése és maradéktalan betartása, valamint a titoktartási nyilatkozatban vállalt felelősségük képezik a biztonsági besorolásuknak megfelelő kötelezettségek alapját, az ezzel kapcsolatos garanciális feltételeket. Ennek megfelelően a Hivatal informatikai rendszereihez, illetve kezelt adataihoz történő hozzáférés biztosítása, a tényleges munkavégzés megkezdése előtt kötelesek a tevékenységüket érintő előírások, szabályozók, illetve eljárásrendek megismerésével és betartásával kapcsolatos felelősségükről, valamint titoktartási kötelezettségükről nyilatkozatot tenni (11. számú melléklet – Titoktartási nyilatkozat).

A Hivatal által használt EIR-ekhez, illetve a Hivatal által kezelt adatokhoz hozzáféréssel rendelkező, a Hivatallal egyéb munkavégzésre irányuló jogviszonyban álló személyek (pl.: üzemeltetési, karbantartási vagy egyéb, információbiztonsággal kapcsolatos szolgáltatást végzők) esetében a Jegyző feladata és felelőssége a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során fenti kötelezettségeket érvényesíteni. A Hivatal informatikai rendszereihez, illetve kezelt adataihoz történő hozzáférés biztosítása, a tényleges munkavégzés megkezdése előtt az e körbe tartozó személyek kötelesek a tevékenységüket érintő előírások, szabályozók, illetve eljárásrendek megismerésével és betartásával kapcsolatos felelősségükről (szerződésben foglalva, annak aláírásával), valamint titoktartási kötelezettségükről a 11. számú melléklet – Titoktartási nyilatkozat szerinti nyilatkozatot tenni. A vonatkozó belső előírásoknak, szabályozóknak a szerződésben meghatározott feladatok által indokolt mértékben történő megismertetése, továbbá a nyilatkozatok meglétének ellenőrzése és megőrzése a Jegyző feladata és felelőssége.

16.2 A Hivatallal szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények

A Hivatallal szerződéses jogviszonyban álló külső szervezet (pl.: üzemeltető, karbantartó, polgári jogi szerződés alapján a Hivatal számára feladatot végrehajtó vagy szolgáltatást nyújtó) esetében a Jegyző feladata és felelőssége gondoskodni arról, hogy minimálisan az alábbi biztonsági követelmény elemek a szerződésben előírásra kerüljenek.

Minden információbiztonságot érintő szerződésben rögzíteni kell mind a Hivatal, mind pedig a külső, szerződő fél részéről legalább egy-egy közvetlen kapcsolattartásra kijelölt személyt, valamint annak elérhetőségeit (telefonszám, elektronikus levelezési cím) abból a célból, hogy a szerződés időtartama alatt a szerződés teljesítésével, az ellátott feladatokkal vagy a nyújtott szolgáltatásokkal összefüggő kommunikáció, továbbá a biztonsági eseményekkel kapcsolatos jelzési kötelezettség teljesíthetősége folyamatosan biztosított legyen. Kivételt képeznek ez alól azok a – jellemzően infokommunikációs szolgáltatási – szerződések (pl.: vonalas telefon vagy internet kapcsolat előfizetés), amelyek teljesítése során a szolgáltató nem kap(hat) hozzáférést a Hivatal által használt EIR-ekhez, illetve az általa kezelt adatokhoz. Ezek esetében nem szükséges természetes személyhez kötött kapcsolattartói információkat

biztosítania a szolgáltatónak, elegendő a hibabejelentéshez általánosan használt központi elérhetőségeinek szerepeltetése.

Abban az esetben, ha a szerződés teljesítése során a külső szerződő fél, illetve az azt képviselő személy a Hivatal által használt EIR-ekhez, illetve a Hivatal által kezelt adatokhoz hozzáféréssel kell, hogy rendelkezzen munkavégzésével kapcsolatban, akkor a szerződésnek jelen, valamint a 16.1 Személybiztonsági feltételek fejezeteiben előírtak mellett tartalmaznia kell a következőket:

1. Szerződő fél kijelenti, hogy a Hivatal Informatikai Biztonsági Szabályzatában előírt biztonsági követelményeket és feladatokat megismerte és a szerződés teljesítése során az abban meghatározott szabályok maradéktalan betartására kötelezettséget vállal.
2. Szerződő fél kijelenti, hogy a szerződés teljesítésében részt vevő személyek a feladatok magas szakmai színvonalon történő ellátásához szükséges iskolai végzettséggel, szakképzettséggel, szakképesítéssel, illetve szakmai gyakorlattal rendelkeznek, valamint büntetlen előéletűek.
3. Szerződő fél vállalja, hogy a szerződés teljesítésében részt vevők személyében bekövetkező változás esetén – ismert vagy tervezett változás esetén a személyi változást megelőzően minimum 8 munkanappal, előre nem látható változás esetén soron kívül, haladéktalanul – tájékoztatja a Hivatalt annak érdekében, hogy a szükséges intézkedéseket, a hozzáférés-, illetve jogosultság beállításokat időben meg tudja tenni.
4. Szerződő fél vállalja, hogy személyi változás esetén a Hivatal által az érintett személy számára biztosított, személyhez kötötten kiadott eszközöket visszaszolgáltatja a Hivatal számára.
5. A szerződő fél képviseletében a Hivatal számára munkát végző személyek kötelesek bármely általuk észlelt vagy tudomásukra jutott, a Hivatal által használt elektronikus információs rendszert (EIR) vagy általa kezelt adatot érintő biztonsági incidensről haladéktalanul tájékoztatni a Hivatal szerződésben meghatározott kapcsolattartóját. A tájékoztatás történhet szóban, telefonon, de minden ilyen esetben elvárás, hogy a szóbeli tájékoztatást ésszerű időn belül követően írásban (pl.: elektronikus levélben) is köteles azt megtenni.
6. Szerződő fél vállalja, hogy amennyiben hatáskörébe tartozik, akkor a Hivatal által használt EIR-eket érintő biztonsági események kezelésében, illetve a biztonsági eseményt kiváltó okok megszüntetésében, szükség szerint az új, megelőző védelmi intézkedések bevezetésében közreműködik, illetve az ezekkel, valamint a Kormányzati Eseménykezelő Központ (GovCert) vagy a felügyeleti hatóság (NEIH) által kiadott biztonsági riasztásokkal kapcsolatban az információbiztonsági felelős által meghatározott, a Hivatal által számára jelzett feladatokat, tevékenységeket végrehajtja.
7. Szerződő fél tudomásul veszi, hogy a Hivatal kijelölt információbiztonsági felelőse jogosult a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében bekérheti a követelményeknek való megfelelőség alátámasztásához szükséges, a tevékenységével kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot. Szerződő fél az információbiztonsági felelőssel köteles együttműködni, az általa kért tájékoztatást, illetve információkat számára a szerződésben meghatározott kapcsolattartási szabályoknak megfelelően megadni.
8. Szerződő fél vállalja, hogy legkésőbb a szerződés záró időpontjában a Hivatal számára dokumentált módon átadja az elektronikus információs rendszerek biztonsága tárgyában a szerződés teljesítése során keletkezett valamennyi dokumentumot és a Hivatal elektronikus információs rendszereinek folyamatos működtetéséhez szükséges minden információt (pl.: hozzáférési adatot).

Amennyiben a külső szerződő fél a Hivatal számára adatkezelést is végez, szerződéses feltételként kell szerepeltetni fentieken túl a külső szervezet Ibtv.-ben foglalt előírásoknak történő megfelelési kötelezettségét is.

Minden szerződésnek tartalmaznia kell a nem megfelelő teljesítésre, a szándékos vagy vétlen károkozásra, továbbá büntetőjogi felelősségre vonatkozó előírásokat. A nem megfelelő teljesítés esetén a szankcionálás formái az alábbiak lehetnek:

- szerződéses kötelezettség teljesítésére való írásbeli felszólítás,

- kötbér vagy pönálé érvényesítése,
- szerződés felmondása.

Az információbiztonsági felelős jogosult minden információbiztonságot érintő szerződés tartalmának megismerésére és véleményezésére, valamint szükség esetén további biztonsági tárgyú szerződéses feltételekre, garanciális elemekre vonatkozó javaslatot tenni a Jegyző felé.

16.3 Eljárás a jogviszony megszűnésekor

A Hivatal által használt EIR-ekhez hozzáféréssel rendelkező hivatali munkatársak munkaviszonyának, illetve a hasonló hozzáféréssel rendelkező, a Hivatallal szerződéses jogviszonyban álló külső szervezet szerződésének megszűnése esetén a Jegyző feladata kezdeményezni a számukra kiadott fizikai és logikai hozzáférési jogosultságok (az EIR-ekben beállított hozzáféréseken kívül ilyenek, különösen: a beléptető rendszer, riasztó, kulcsfelvételi jog) visszavonását (felfüggesztését), valamint gondoskodni a kiadott, a Hivatal tulajdonát képező minden eszköz (pl.: infokommunikációs eszközök, belépőkártya, kulcsok, hitelesítési eszközök, hozzáférési kódok, stb.) visszavételéről hivatali munkavállaló esetében annak munkavégzés alóli felmentésének, külső szerződő fél esetében legkésőbb a szerződés lezárásának időpontjában.

A jogviszony megszűnésének záró időpontját követően a távozó munkatárs felhasználói fiókjának végleges törlését a Jegyző feladata és felelőssége kezdeményezni, amennyiben az ahhoz kapcsolódó információkra sem jogszabályi kötelezettségek teljesítése, sem pedig bármely folyamatban lévő hatósági vizsgálat vagy eljárás, illetve biztonsági események kivizsgálása céljából nem lehet szükség.

Hivatali munkatárs jogviszonyának megszűnése (megszüntetése) esetén a Jegyző kijelöli – és a munkakör átadás-átvételi folyamatba bevonja – azt a munkatársat, aki a jogviszony megszűnését követően átveszi a kilépő munkavállaló feladatait, tevékenységeit és munkaadatait; valamint gondoskodik a dokumentált munkakör, illetve feladat átadás-átvételi eljárás lefolytatásáról a munkavállaló munkavégzés alóli felmentésének időpontját megelőzően, amellyel

- gondoskodik a jogviszonyt megszüntető személynek a Hivatal által használt EIR-ekkel, illetve azok biztonságával kapcsolatos munkaköri feladatainak folytatólagosan történő ellátásáról;
- gondoskodik a kilépő személy által korábban használt, kezelt EIR-ekhez és szervezeti információkhoz való hozzáférés folyamatosságának biztosításáról;
- továbbá amelynek során tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről.

A jogviszony megszűnéséről a Jegyző a helyben szokásos módon tájékoztatja a Hivatal érintett munkavállalóit, illetve a szerződésben meghatározott módon azon szerződéses partnereit, amelyek esetében a kilépő munkaköri feladatai a Hivatal érvényes szerződéseinek teljesítését befolyásolják (pl.: kapcsolattartó személyének megváltozása). Értesíti továbbá a központi üzemeltetésű EIR-ek ismert kapcsolattartóit, amennyiben a kilépő személyhez kötődő magasabb szintű jogosultságok (pl.: kiemelt felhasználó, tenant admin, stb.) megszüntetése, illetve azok megváltoztatása, átruházása az adott EIR hozzáférési- és jogosultsági rendszere, biztonsági beállításai miatt ezt szükségessé teszi (pl.: nincs jogosultsága a Hivatalnak az ezzel kapcsolatos konfigurációt módosítani).

A Hivatal által használt EIR-ben magasabb szintű jogosultsággal (privilegizált hozzáféréssel) rendelkező, illetve információbiztonsággal kapcsolatos feladatot végző kilépő személyről, valamint a Hivatal által használt EIR-ekhez, illetve a Hivatal által kezelt adatokhoz hozzáféréssel rendelkező, a Hivatallal egyéb munkavégzésre irányuló jogviszonyban álló személyek (pl.: üzemeltetési, karbantartási vagy egyéb, információbiztonsággal kapcsolatos szolgáltatást végzők), illetve szervezetek szerződéses jogviszonyának megszűnéséről a Jegyző feladata és felelőssége tájékoztatni az információbiztonsági felelőst, a jogviszony megszűnésének ismertté válásának időpontjában vagy ahhoz képest ésszerű időn belül (pl.: szerződés felbontására vonatkozó döntés meghozatalát követően).

16.4 Az áthelyezések, átirányítások és kirendelések kezelése

Hivatali munkatárs munkakörének vagy feladatainak megváltozása, illetve áthelyezése, átirányítása esetében az előző, a 16.3 Eljárás a jogviszony megszűnésekor fejezetben foglaltakat az alábbi eltérésekkel kell alkalmazni:

Az új munka-, illetve feladatkör által nem igényelt korábbi, meglévő fizikai és logikai hozzáférések megszüntetését, illetve az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását vagy megszüntetését, továbbá az ahhoz nem szükséges eszközök visszavételét követően a Jegyző feladata gondoskodni arról, hogy a használandó, új rendszerek és azokhoz szükséges jogosultságok, hozzáférések beállítása, valamint a kapcsolódó felhasználói fiókok létrehozása, módosítása, illetve indokolt esetben törlése megtörténjen.

16.5 Fegyelmi intézkedések

A biztonsági szabályok szándékos megsértőivel szemben a Hivatal fegyelmi eljárást indít. Ha felmerül a lehetősége annak, hogy a biztonsági eseményt kiváltó ok számítógépes bűncselekmény elkövetéséhez kötődik, abban az esetben a Hivatal jogi képviselője, valamint a Jegyző jogosult büntetőjogi feljelentést is tenni.

Amennyiben a biztonsági szabályokat nem a Hivatal személyi állományába tartozó személy sérti meg, akkor a Jegyző a Hivatal jogi képviselőjének bevonásával megvizsgálja a jogi lépések megtételének indokoltságát és megteszi a szükséges intézkedéseket. A Hivatallal munkavégzésre irányuló egyéb jogviszonyban vagy szerződéses kapcsolatban álló személy esetén a Jegyző érvényesíti a vonatkozó szerződésben meghatározott következményeket.

A fegyelmi, illetve hatósági eljárásban felhasználni kívánt evidenciák begyűjtéséhez az információbiztonsági felelős szakmai iránymutatást, támogatást biztosít, az IT üzemeltető közreműködik, megőrzésükről a Jegyző köteles gondoskodni.

A biztonsági szabályok megsértése esetén alkalmazott eljárás, illetve intézkedések során figyelembe kell venni a 15. A biztonsági események kezelése fejezetben foglalt előírásokat is.

16.6 Viselkedési szabályok az interneten

A Hivatal a munkatársai számára az informatikai eszközöket és erőforrásokat, így az internet elérését szintén a hivatali munkavégzés céljára biztosítja.

A hivatali internet használata során tilos

- a 27.11 Nyilvánosan elérhető tartalom fejezetben meghatározott weboldalak kivételével a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele;
- a hivatali email cím magáncélú használata, azzal történő regisztráció nem a munkavégzéshez kapcsolódó internetes szolgáltatások (pl.: hírlevél, levelező lista feliratkozás; webáruház, stb.) igénybevételéhez;
- fájlcserélő vagy chat szolgáltatás használata, valamint a munkavégzéshez nem kapcsolódó letöltések végrehajtása.

A Jegyző a munkavégzés által indokolt esetben fenti szabályok betartása alól 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben foglaltak szerint felmentést adhat.

Az engedély nélküli tevékenységet végrehajtó, szabályszegő személy felelősségre vonására a 16.5 Fegyelmi intézkedések fejezetben meghatározottak szerint a Jegyző jogosult.

17 TUDATOSSÁG ÉS KÉPZÉS

17.1 Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és az e célt szolgáló ágazati szervezetekkel

Az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével való kapcsolattartás – a Hivatal számára az Ibtv.-ben, illetve kapcsolódó rendeleteiben előírt bejelentési és adatszolgáltatási kötelezettségek teljesítésének kivételével – elsődlegesen az információbiztonsági felelős feladata és felelőssége. Ennek keretében a NEIH, illetve a GovCert által kiadott biztonságtudatosító, ismeretterjesztő és oktatóanyagokra felhívja a Hivatal munkatársainak figyelmét, illetve számukra elérhetővé teszi azokat folyamatos oktatásuk, képzésük elősegítése érdekében, továbbá jelzi az aktuális, a Hivatal által használt EIR-eket érintő fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információkat, az e szervezetek által kiadott biztonsági riasztásokat a Hivatal, illetve az IT üzemeltető felé.

Az információbiztonsági felelős feladata emellett az információbiztonsággal foglalkozó hazai, illetve nemzetközi szakmai ismeretek és trendek, módszertani kutatások és fejlesztések, valamint az elektronikus információbiztonsággal kapcsolatos eljárások, technikák és technológiák figyelemmel kísérése, s a lehetőségek függvényében gyakorlati alkalmazásuk elősegítése, támogatása.

17.2 Képzési eljárásrend

A Hivatal által használt EIR-ekhez hozzáféréssel rendelkező munkatársakat a munkavégzés megkezdése előtt – az új munkavállalók kezdeti képzésének részeként – az IBSZ tartalmára épülő, a munkavégzésükhöz kapott infokommunikációs eszközök rendeltetésszerű használatára, az információbiztonsággal kapcsolatos előírások, szabályok betartására, valamint a biztonsági események jelentési kötelezettségére vonatkozó feladataik és felelősségeik megismertetését célzó, továbbá az általuk munkaköri feladataik ellátása során használandó EIR-ek alapvető biztonsági követelményeiről szóló képzésben kell részesíteni.

Az információbiztonságra vonatkozó jogszabályi környezet megváltozásakor, valamint amikor a Hivatal informatikai biztonságát vagy az IBSZ tartalmát érintő, illetve az általa használt EIR-ekben jelentős változás következik be, a jogszabályváltozás hatályba lépését, illetve a jelentős változást követő 60 napon belül a Hivatal fentiekben meghatározott, képzésre kötelezett munkatársait a változásokkal kapcsolatos továbbképzésben, illetve tájékoztatásban kell részesíteni.

A képzés, továbbképzés, tájékoztatás tematikájának meghatározásáért, szakmai tartalmának saját tananyag esetén összeállításáért, külső forrásból származó tananyag esetén jóváhagyásáért az információbiztonsági felelős, lebonyolításáért és a részvétel feltételeinek biztosításáért, illetve a tájékoztatás megtartásáért a Jegyző felelős.

Minden hivatali munkatárs köteles részt venni az információbiztonsággal kapcsolatos számára előírt képzéseken.

A Hivatal által használt EIR-ekhez, illetve a Hivatal által kezelt adatokhoz hozzáféréssel rendelkező, a Hivatallal egyéb munkavégzésre irányuló jogviszonyban álló személyek és szervezetek (pl.: üzemeltetési, karbantartási vagy egyéb, információbiztonsággal kapcsolatos szolgáltatást végzők) esetében a vonatkozó belső előírásoknak, szabályozóknak a szerződésben meghatározott feladataik által indokolt mértékben történő megismertetése céljából, amennyiben szerzői-, felhasználási- vagy terjesztési jogok azt nem korlátozzák, akkor a képzés, tájékoztatás kiterjeszthető, tananyaga, illetve az abból készített kivonat a szerződő fél rendelkezésére bocsátható. Ennek feltételeinek biztosítása, továbbá a szerződő fél által a tevékenységét érintő előírások, szabályozók, illetve eljárásrendek megismerésével és betartásával kapcsolatos felelősségéről szerződésben meghatározott módon tett nyilatkozata meglétének ellenőrzése és megőrzése a Jegyző feladata és felelőssége.

17.3 Biztonság tudatosság képzés

Az információbiztonsági felelős feladata az új információbiztonsági tudatosító programok, oktatások kezdeményezése és azok szakmai tartalmának meghatározása.

Évente legalább egy alkalommal minden, a Hivatal által használt EIR-ekhez, illetve a Hivatal által kezelt adatokhoz hozzáféréssel rendelkező munkavállaló köteles a számára előírt biztonságtudatosító programon, illetve oktatáson részt venni.

17.4 Szerepkör vagy feladat alapú biztonsági képzés

A Hivatal minden, munkaköri feladatai ellátása során valamely általa használt EIR felhasználására kötelezett munkavállalója számára biztosítja feladatainak és szerepkörének megfelelő mértékben az adott EIR felhasználására, annak biztonsági követelményeire vonatkozóan rendelkezésre álló információkat, dokumentációkat, továbbá az ezzel kapcsolatban esetlegesen elérhető (pl.: központi üzemeltető által biztosított) képzésen történő részvételt.

A Hivatal által használt EIR-ekhez, illetve a Hivatal által kezelt adatokhoz hozzáféréssel rendelkező, a Hivatallal egyéb munkavégzésre irányuló jogviszonyban álló személyek és szervezetek szerepkör, illetve feladat alapú biztonsági képzésére vonatkozó általános előírásokat a 17.2 Képzési eljárásrend, a szakmai alkalmasságukra vonatkozó feltételeket és garanciális szerződéses elemeket pedig a 16.2 A Hivatallal szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények fejezet tartalmazza.

17.5 A biztonsági képzésre vonatkozó dokumentációk

Az IBSZ esetében a hivatali munkavállalók a 2. számú melléklet – Megismerési nyilatkozat aláírásával igazolják, hogy az információbiztonsági előírásokat, szabályokat megismerték és azok betartását magukra nézve kötelezőnek ismerik el.

Az egyéb információbiztonsági tárgyú képzéseken, biztonságtudatosító programokon, oktatásokon történő részvétel igazolása az adott képzés, oktatás jellegétől és lebonyolítási módjától függően történhet a képzést, oktatást szervező szervezet – amennyiben az nem a Hivatal – által kiadott igazolás, illetve jelenléti ív formájában.

A nyilatkozatok, illetve a részvételt igazoló dokumentumok megőrzéséről a Jegyző köteles gondoskodni.

18 FIZIKAI ÉS KÖRNYEZETI VÉDELEM

18.1 Fizikai védelmi eljárásrend

A Hivatal az általa használt EIR-ek szempontjából érintett létesítményekre, épületekre és helyiségekre érvényes fizikai védelmi eljárásrendet jelen fő fejezetben, az alábbiak szerint határozza meg.

A Hivatal a helyiségek biztonsági szempontú besorolását az alábbi kategóriák alapján, a 12. számú melléklet – Helyiségek biztonsági besorolása dokumentumban rögzíti:

Biztonsági zóna megnevezése	Biztonsági zóna leírása
Nyitott terület	Ügyfelek és látogatók számára nyitott, általuk szabadon hozzáférhető, látogatható helyiségek.
Zárt terület	Ügyintézésre, munkavégzésre használt és egyéb zárható, illetve az ügyfelek és látogatók elől elzárt helyiségek. Ide tartoznak a Hivatal által használt EIR-ek elemeinek helyt adó helyiségek.

Védett terület	A zárt területen belül az informatikai erőforrásokat koncentráltan tartalmazó, fokozottan védendő helyiségek. Ide tartozik minden, a Hivatal által használt EIR-ek központi elemeinek helyt adó helyiség (pl.: szerver szoba).

Nyitott területen a Hivatal által használt EIR-ekhez közvetlenül vagy közvetett módon hozzáférést biztosító hálózati végpont vagy egyéb informatikai eszköz esetében gondoskodni kell az adott eszköz típusának megfelelő hozzáférésvédelem kialakításáról (pl.: hálózati végpont letiltása, fizikai csatlakozásának megszüntetése a központi hálózati elosztón, nyomtató vagy multifunkciós berendezés kizárólag azonosítást követően történő használatának kikényszerítése, beállítása jelszavas vagy PIN kódos védelem alkalmazásával, stb.). Amennyiben a hozzáférésvédelem nem alakítható ki, a Hivatal a végpont fizikai megszüntetéséről, illetve az eszköz zárt területre történő áthelyezéséről köteles gondoskodni.

A Hivatal Szervezeti és Működési Szabályzatában meghatározott nyitvatartási (ügyfélfogadási) időn belül a Hivatal minden épületének ügyfelek és látogatók számára nyitott területeire (pl.: ügyfélváró, folyosó, stb.) bárki szabadon beléphet.

A Hivatal ügyintézésre használt helyiségeibe, irodáiba az ügyfelek ügyintézési célból az ügyintézésben eljáró munkatárs engedélyét követően; ezen helyiségekbe, továbbá a Hivatal egyéb, ügyfelek elől elzárt területeire, köztük a Hivatal által használt EIR-ek elemeinek helyt adó helyiségekbe a látogatók és munkavégzés céljából a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban álló személyek (pl.: üzemeltető, karbantartó, stb.) a kíséretükkel, illetve felügyeletükkel a Jegyző által megbízott munkavállaló engedélyével léphetnek be.

Nyitvatartási időn kívül a Hivatal épületeiben ügyfél, látogató vagy a Hivatal számára munkát végző, szerződött partner kizárólag a Jegyző erre vonatkozó külön írásos – rendkívüli, indokolt esetben szóbeli – engedélyével, s az általa e feladattal megbízott munkavállaló felügyelete mellett tartózkodhat. A nyitvatartási időn kívül történő belépési igényről – vészhelyzet, például tűzeset kivételével – a Jegyzőt minden esetben előzetesen tájékoztatni kell.

Minden munkatárs kötelessége, hogy a Hivatalban kialakított fizikai és elektronikus védelem elemeit (zárható nyílászárók, riasztó rendszer, stb.) rendeltetésüknek és a jelen fejezetben meghatározott szabályoknak megfelelően használja.

Tilos a védelmi eszközök funkcionalitásának megváltoztatása, mint például:

- az automatikusan záródó, illetve a folyamatosan zárt állapotban tartandó nyílászárók kitámasztása;
- az elektronikus védelmi rendszerek érzékelőinek (pl.: mozgásérzékelő szenzor) letakarása, pozíciójának megváltoztatása (pl.: elforgatása) vagy leszerelése, megbontása.

A zárható helyiségeket azok elhagyását követően minden alkalommal zárt állapotba kell helyezni.

Minden munkatárs köteles azonnal jelezni a Jegyző felé, ha a védelmi rendszerek működésében rendellenességet vagy hibát észlel.

18.2 Fizikai belépési engedélyek

A Hivatal épületeibe belépésre jogosult hivatali munkavállalók és a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban álló személyek listájának elkészítéséről és kezeléséről, valamint naprakész állapotban tartásáról a Jegyző, illetve az általa e feladat ellátásával megbízott munkatárs gondoskodik (7. számú melléklet – Belépésre jogosultak nyilvántartása). A belépésre jogosultak listájának jóváhagyása, valamint a jogosultak körében történő jogviszony változás esetén (pl.: új munkavállaló belépése, munkaviszony, illetve szerződés megszűnése) felülvizsgálata a Jegyző, illetve az általa e feladat ellátásával megbízott munkatárs feladata és felelőssége. A Jegyző által jóváhagyott lista írásos belépési engedélynek minősül.

A belépésre alkalmas nyílászárók kulcsainak, illetve a bejutáshoz szükséges további eszközök (pl.: egyéni belépőkártya, hozzáférési vagy riasztókód) védelméről a Hivatal az alábbi szabályok szerint gondoskodik:

a) a Hivatal épületeibe belépést lehetővé tevő kulcs, illetve egyéb eszköz kizárólag belépési engedéllyel rendelkező személynek, s dokumentált átadás-átvételi folyamat keretében adható ki (az átadás-átvételt igazoló dokumentum egy példányának megőrzése a Jegyző feladata);

b) a kulcsok és egyéb eszközök biztonságos kezeléséről, megőrzéséről az átvevő köteles gondoskodni;

c) egy-egy kulcspéldányt minden nyílászáró esetében letétbe kell helyezni a Jegyzőnél (mesterpéldány biztosítása);

d) a kulcs, egyéb eszköz elvesztése vagy ellopása, illetve a kód kompromittálódása biztonsági incidensnek minősül, amely esetben birtokosa haladéktalanul értesíteni köteles a Jegyzőt a szükséges intézkedések (zárszerkezet cseréje, kód visszavonása, megváltoztatása) megtétele érdekében;

e) azon hozzáférési kódok megváltoztatásáról, amelyek esetében év közben kilépő munkavállaló jogviszony változása vagy a d) pontban meghatározott biztonsági incidens bekövetkezése azt nem tette az év folyamán szükségessé a Jegyző köteles évente legalább egy alkalommal gondoskodni.

Az állandó belépésre jogosultak számára a Jegyző köteles gondoskodni a Hivatalban újonnan bevezetésre kerülő belépési jogosultságot igazoló dokumentum (pl.: kitűző, azonosító kártya, intelligens kártya) kibocsátásáról, valamint jogosultság, illetve jogviszonyt érintő változás esetén annak visszavonása, érvénytelenítése, törlése vagy megsemmisítése ügyében.

18.3 A fizikai belépés ellenőrzése

A Hivatal épületeinek minden oldalról zárható határfelülettel kell rendelkeznie. Minden munkatárs köteles ellenőrizni a felügyelete alatt álló hivatali helyiség nyílászáróinak megfelelő működését, zárhatóságát. Rendellenesen működő, nem zárható nyílászáró javításáról haladéktalanul intézkedni kell, emiatt azt soron kívül jelezni köteles a hibát észlelő vagy arról értesülő munkatárs a Jegyző felé.

A Hivatal épületeinek ügyfelek, illetve látogatók számára biztosított bejáratain, valamint az ügyfelek és látogatók számára nyitott területein és az ügyintézésre használt, az ügyintéző munkatárs által felügyelt helyiségein kívül minden más be- és kilépésre alkalmas nyílászárót használaton kívül nyitvatartási időben is zárt állapotban kell tartani. A Hivatal ezzel biztosítja, hogy a belépésre jogosultak kizárólag az engedélyezett be-, és kilépési pontokon keresztül közlekedjenek, illetve haladhassanak át, továbbá csak azokba a helyiségekbe léphessenek be, ahol személyes felügyelet nélkül jogosultak tartózkodni.

A belépésre jogosultak által elérhető helyiségek folyamatos ellenőrzésének biztosítása érdekében a Hivatal ügyintézésre használt helyiségeiben ügyfelek, továbbá a Hivatal egyéb, ügyfelek elől elzárt területeire, köztük a Hivatal által használt EIR-ek elemeinek helyt adó helyiségeiben a látogatók és munkavégzés céljából a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban álló személyek (pl.: üzemeltető, karbantartó, stb.) kizárólag felügyelet mellett tartózkodhatnak. A felügyelet biztosítása ügyfél esetében az ügyében eljáró ügyintéző, látogató és szerződéses partner esetében a Jegyző által ezzel megbízott munkavállaló feladata.

A Hivatal által használt EIR-ek elemeinek helyt adó helyiségekbe történő belépésekkel kapcsolatban a belépési jogosultság ellenőrzése a nem a Hivatal állományába tartozó személyek esetében az ügyintézésben eljáró munkatárs, illetve az adott személy kíséretével, felügyeletével a Jegyző által megbízott munkavállaló feladata.

Az állandó belépésre nem jogosult, nem a Hivatal állományába tartozó személyek (ügyfelek, látogatók, a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban álló üzemeltetők,

karbantartók, stb.) belépésének adatait a felügyeletet biztosító munkatárs köteles a 8. számú melléklet – Belépési napló alapján készített nyilvántartásban rögzíteni. A belépési napló vezetésére vonatkozó kötelezettség betartását a Jegyző jogosult ellenőrizni.

Ha az adott hivatali épületben élőerős védelmet alkalmaz a Hivatal, abban az esetben a belépési jogosultság ellenőrzésével és dokumentálásával, továbbá amennyiben a személy- és vagyonvédelmi feladatok folyamatos ellátását az nem akadályozza vagy lehetetleníti el, akkor a kíséret, illetve felügyelet ellátásával a vagyonőr megbízható.

Amennyiben az adott hivatali épületben a fizikai belépések felügyeletére, illetve az egyéni belépési engedélyek ellenőrzésére elektronikus eszközt (pl.: megfigyelő, beléptető rendszer, stb.) vezet be vagy alkalmaz a Hivatal, az ellenőrző eszközök nyilvántartásba vételéről a Jegyző köteles gondoskodni.

18.4 A fizikai hozzáférések felügyelete

A Hivatal által használt EIR-ek elemeinek helyt adó helyiségekben ügyfelek, látogatók és munkavégzés céljából a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban álló személyek (pl.: üzemeltető, karbantartó, stb.) kizárólag felügyelet mellett tartózkodhatnak, illetve végezhetnek munkát.

A személyes felügyelet keretében a fizikai hozzáférés ellenőrzése, a fizikai biztonsági esemény észlelése folyamatosan biztosított.

A Hivatal épületeinek nyitvatartási időn kívüli, kockázatokkal arányos védelméről a Hivatal fizikai védelmi intézkedésekkel (pl.: mechanikai védelem eszközei), illetve elektronikus védelmi rendszer (pl.: távfelügyeleti riasztó, jelző rendszer) alkalmazásával gondoskodik.

Fizikai hozzáféréssel kapcsolatos biztonsági incidens bekövetkezése esetén a 15. A biztonsági események kezelése fejezetben meghatározottakkal összhangban a Jegyző gondoskodik az információbiztonsági felelős javaslata alapján a hozzáférésekről rendelkezésre álló naplóadatok (pl.: belépési napló, riasztó rendszer naplóállományai) átvizsgálásáról, indokolt esetben (pl.: hatósági eljárás kezdeményezése) az eljáró hatóság számára történő átadásáról.

18.5 A látogatók ellenőrzése

A Hivatal a látogatói belépéseket a 18.3 A fizikai belépés ellenőrzése fejezetben előírtak alapján dokumentálja, s azt indokolt esetben, biztonsági esemény bekövetkezését követően a 18.4 A fizikai hozzáférések felügyelete fejezetben meghatározottak szerint vizsgálja.

18.6 Vészvilágítás

A Hivatal a hatályos tűzvédelmi előírásoknak megfelelően biztosítja a vészkijáratokat és a menekülési útvonalakat, illetve azok láthatóságát.

18.7 Tűzvédelem

A Hivatal a hatályos tűzvédelmi előírásoknak megfelelő tűzoltó-technikai termékeket alkalmaz és tart karban.

18.8 Hőmérséklet és páratartalom ellenőrzés

A Hivatal az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl.: szerver szoba) a hőmérsékletnek és a páratartalomnak az erőforrások biztonságos működéséhez szükséges szinten tartása és folyamatos figyelemmel kísérése, ellenőrzése céljából erre alkalmas légkondicionáló berendezést üzemeltet.

A hőmérséklet és páratartalom ellenőrzéséhez kapcsolódó konkrét paramétereket (elfogadható, optimális értéktartomány, riasztási érték) a helyiségben üzemeltetett eszközök gyártói ajánlásainak figyelembe vételével a Hivatal rendszer üzemeltetési leírásban rögzíti.

A légkondicionáló berendezés vagy egyéb telepített felügyeleti mérőeszköz helyi riasztásjelzésének észlelése esetén minden munkavállaló köteles a Jegyzőt, illetve az IT üzemeltetőt haladéktalanul értesíteni.

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

A Hivatal az informatikai erőforrásokat koncentráltan tartalmazó helyiségek tervezése során gondoskodik arról, hogy az a víz-, és más csővezetéken szállított anyagok által okozható károktól védett legyen, szükség esetén a csővezetékek kiváltásával, áthelyezésével biztosítva a megfelelő védelmet.

A Hivatal által használt EIR elemeit képező informatikai eszközök elhelyezése során a Hivatal gondoskodik arról, hogy azok a csővezetékek rongálódásból származó károkkal szemben védettek legyenek. Ennek érdekében az informatikai eszközöket a csővezetékektől lehetőség szerint minél távolabbra és magasabbra kell elhelyezni, illetve a talajszint alatti helyiségek esetén vizsgálni kell a helyiség falainak megfelelő vízszigetelését.

A Jegyző köteles gondoskodni arról, hogy a főelzárócsapok hozzáférhetősége, működtetésének módja minden hivatali munkatárs számára ismert legyen. Működőképességük biztosításáról, ellenőrzéséről a Hivatal épületeinek vagyonkezelője köteles állagmegóvási, karbantartási feladatainak ellátása keretében gondoskodni.

18.10 Be- és kiszállítás

A Hivatal a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben meghatározottak szerint engedélyezi vagy tiltja a létesítménybe bevitt, illetve onnan kivitt információs rendszerelemeket. A be- és kiszállítás felügyeletét, figyelemmel kísérését a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban álló személy felügyeletével megbízott munkatárs látja el, szakmai ellenőrzésében szükség szerint közreműködik az IT üzemeltető.

A Hivatal a be- és kiszállítások dokumentálásáról a 9. számú melléklet – Információs rendszerelemek be- és kiszállításának nyilvántartása vezetésével gondoskodik. A nyilvántartás vezetése, az új bejegyzés rögzítése a be- és kiszállítás felügyeletét ellátó munkatárs feladata. A nyilvántartás rendelkezésre állásának biztosításáról, továbbá a vezetésére vonatkozó kötelezettség betartásáról, illetve annak ellenőrzéséről a Jegyző gondoskodik.

18.11 Karbantartók

A Hivatal által használt, felügyelete alá tartozó EIR-ek, illetve rendszerelemeik karbantartását kizárólag a Hivatallal e feladat ellátására vonatkozóan szerződéses jogviszonyban álló szervezetek, illetve személyek a 18. Fizikai védelmi eljárásrend fejezetben meghatározottak szerint, s minden esetben csak felügyelet mellett végezhetik. A hozzáférési jogosultság igazolásának ellenőrzése a felügyeletet ellátó munkatárs feladata.

A Hivatal által használt EIR-ek karbantartását végzők adatait a Hivatal a E10. Az elektronikus információs rendszerek nyilvántartásában vezeti.

19 ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK

19.1 Engedélyezés

Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, a Hivatal hatókörébe tartozó emberi, fizikai és logikai erőforrásra, eljárási és védelmi szintre, valamint folyamatra.

Az engedélyezés részletes szabályait a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás fejezet tartalmazza.

19.2 Az elektronikus információs rendszer kapcsolódásai

A Hivatal által használt EIR-ek más EIR-ekhez történő kapcsolódása a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben meghatározott engedélyezési eljárás alapján történhet.

A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR-ek esetében a kapcsolódás szabályait, úgymint a rendszer kapcsolatait, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát a rendszer tulajdonosa határozza meg és dokumentálja. Új, saját fejlesztésű EIR használatba vétele esetén a Hivatal gondoskodik arról, hogy ugyanezen információk a rendszer dokumentációiban szerepeljenek. Saját üzemeltetésű EIR-ek esetében az IT üzemeltető felelős a meglévő rendszerdokumentációk fenti, esetleg hiányzó információkkal történő kiegészítéséért.

A Jegyző feladata gondoskodni arról, hogy a Hivatal által használt EIR-ekkel kapcsolatba kerülő munkatársai, valamint a Hivatallal munkavégzésre irányuló egyéb szerződéses jogviszonyban lévő személyek a feladatellátásukhoz szükséges mértékben az EIR-ekről rendelkezésre álló rendszer-, illetve felhasználói dokumentációkat megismerjék.

19.3 Külső kapcsolódásokra vonatkozó korlátozások

A Hivatal által használt EIR-ek, illetve rendszerelemeik külső elektronikus információs rendszerhez történő kapcsolódása kizárólag a Hivatal által igénybe vett vagy jóváhagyott hálózati kommunikációs csatornán (internet kapcsolat, adathálózat) keresztül a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben meghatározottak szerint a Jegyző jóváhagyásával engedélyezett.

A végrehajtható programok, script-ek (pl.: Java Applet, JavaScript, VB Script, CGI, stb.) letöltését, futtatásának lehetőségét, valamint web és alkalmazásba csomagolt ActiveX objektumok működését le kell tiltani az internet böngésző programokban, továbbá gondoskodni kell arról, hogy a böngésző alkalmazás biztonsági frissítése rendszeresen megtörténjen.

Az internet csatlakozásra használt böngészőprogram biztonsági beállításait az IT üzemeltető a 23. Konfigurációs beállítások fejezetben előírtak szerint köteles elvégezni.

A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR-ek esetében a kapcsolódás biztonsági követelményeit – fentieknél esetenként szigorúbb korlátozását, illetve az attól való eltérést – a rendszer tulajdonosa határozza meg, a Hivatal gondoskodik annak alkalmazásáról.

20 TERVEZÉS

20.1 Rendszerbiztonsági terv

Amennyiben a Hivatal új EIR tervezési feladatait látja el, gondoskodik arról, hogy az EIR-hez a szükséges dokumentációk, köztük a rendszerbiztonsági terv is elkészüljön minimálisan az alábbi tartalmi elemekkel:

- meghatározza az EIR hatókörét, alapfeladatait (biztosítandó szolgáltatásait), biztonságkritikus elemeit és alapfunkcióit;
- meghatározza az EIR és az általa kezelt adatok jogszabály szerinti biztonsági osztályát;
- meghatározza az EIR működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait;
- a vonatkozó rendszerdokumentáció keretébe foglalja az EIR biztonsági követelményeit;
- meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedés bővítéseket.

A Jegyző feladata gondoskodni arról, hogy a Hivatal új EIR-el kapcsolatba kerülő munkatársai, valamint a Hivatallal munkavégzésre irányuló egyéb szerződéses jogviszonyban lévő személyek a feladatellátásukhoz szükséges mértékben a rendszerbiztonsági tervet és a kapcsolódó rendszerdokumentációkat megismerjék.

A Jegyző a 4. Dokumentumvédelem fejezetben leírtak szerint gondoskodik a rendszerbiztonsági terv védelméről, továbbá gondoskodik arról, hogy a rendszerbiztonsági tervben a Hivatal számára meghatározott biztonsági feladatok, védelmi intézkedések végrehajtása megtörténjen.

A Jegyző feladata kezdeményezni a rendszerbiztonsági terv készítőjénél annak felülvizsgálatát és szükség szerinti aktualizálását, frissítését az EIR-ben vagy annak üzemeltetési környezetében történt változások, illetve a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén, illetve ezek hiányában legalább évente egy alkalommal.

A rendszerbiztonsági terv felülvizsgálatában az információbiztonsági felelős jogosult – szükség szerint az IT üzemeltető bevonásával – közreműködni.

20.2 Cselekvési terv készítése

A Hivatal a 9. Cselekvési terv fejezetben előírtakkal összhangban a szükséges védelmi intézkedések megtételére tervet készít, amennyiben az új EIR-ére vonatkozó biztonsági osztály meghatározásánál (a kockázatelemzés, illetve helyzetfelmérés során) hiányosságot állapít meg. A tervben dokumentálja a megállapított hiányosság javítására, valamint az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányuló tervezett tevékenységeit, továbbá gondoskodik azok végrehajtásáról, annak ellenőrzéséről és a terv rendszeres felülvizsgálatáról.

20.3 Személyi biztonság

A Hivatal által használt EIR-ekhez hozzáférési jogosultságot igénylő személyekkel kapcsolatos elvárások, az EIR használatára vonatkozó biztonsági szabályok és kötelezettségek megismertetéséről és annak dokumentálásáról a Hivatal a 17.2 Képzési eljárásrend, a 17.4 Szerepkör vagy feladat alapú biztonsági képzés, továbbá a 16.1 Személybiztonsági feltételek fejezetekben meghatározottak szerint gondoskodik.

A személyi biztonsággal kapcsolatban meghatározott követelmények felülvizsgálatát az információbiztonsági felelős az IBSZ felülvizsgálata alkalmával a 3. A szabályzat kiadása, kezelése, felülvizsgálata fejezetben meghatározottak szerint végzi el.

21 BIZTONSÁGI ELEMZÉS

21.1 Biztonságelemzési eljárásrend

A Hivatal által használt EIR-ek és működési környezetük védelmi intézkedéseit, a bevezetett intézkedések működőképességét, valamint tervezettnek, az előírt biztonsági követelményeknek megfelelő működését az információbiztonsági felelős felülvizsgálati tevékenysége keretében jogosult ellenőrizni, illetve értékelni:

- új elektronikus információs rendszer bevezetése;
- a kockázatelemzés, illetve helyzetfelmérés;
- a cselekvési, illetve intézkedési tervek végrehajtásának ellenőrzése;
- valamint az IBSZ felülvizsgálata során.

Az értékelés eredményétől függően az információbiztonsági felelős javaslatot tehet a Jegyző számára új védelmi intézkedések bevezetésére, meglévő intézkedések, továbbá a tervek módosítására.

21.2 Biztonsági értékelések

Az információbiztonsági felelős feladata a biztonságértékelés eredményét összefoglaló jelentés elkészítése és megküldése a Jegyző számára.

A biztonsági értékelésről készült jelentés minimálisan az alábbi elemeket kell, hogy tartalmazza:

- az értékelendő (adminisztratív, fizikai és logikai) védelmi intézkedések;
- a biztonsági ellenőrzések eredményességét meghatározó eljárásrendek;
- az értékelési környezet, az értékelő csoport, az értékelés célja, az értékelést végzők feladata.

A Jegyző feladata gondoskodni arról, hogy a jelentést a Hivatal által használt EIR-ekkel kapcsolatba kerülő munkatársai, valamint a Hivatallal munkavégzésre irányuló egyéb szerződéses jogviszonyban lévő személyek a feladataik által indokolt mértékben megismerjék.

21.3 A biztonsági teljesítmény mérése

A Hivatal az általa használt EIR-ek biztonsági teljesítményének, illetve az alkalmazott védelmi intézkedések hatékonyságának mérésére az alábbi mutatókat alkalmazza:

Mérőszám	Mérés módja
biztonsági események száma	a biztonsági eseményekről, bejelentésükről készült feljegyzések adott időszakra vonatkozó összesítése
az EIR-ek rendelkezésre állása	a rendelkezésre állás elvesztésével járó biztonsági események időtartama, illetve a központilag biztosított szolgáltatások üzemeltetői által rendelkezésre bocsátott mérések alapján
az EIR-ekkel kapcsolatba kerülő személyek biztonsági képzésének lefedettsége	a képzésekről készült dokumentumok alapján a részvételi arány meghatározása

A mérések végrehajtásában az IT üzemeltető, a Hivatal munkatársai, valamint a Hivatallal szerződéses jogviszonyban álló szervezetek (pl.: szolgáltatást nyújtók) kötelesek közreműködni, ahhoz információkat nyújtani. Az információbiztonsági felelős az adott biztonsági értékelés alkalmával a releváns mérőszámok értékeit figyelembe veszi és felhasználja.

22 TESZTELÉS, KÉPZÉS ÉS FELÜGYELET

22.1 Tesztelési, képzési és felügyeleti eljárások

A Hivatal a saját fejlesztésű és általa üzemeltetett, a felügyelete, irányítása alatt lévő EIR-ek esetében az EIR üzembe helyezését megelőzően, valamint az EIR, illetve rendszerelemeinek, működési környezetének jelentős megváltozása esetén a fejlesztő, illetve az IT üzemeltető bevonásával gondoskodik az adott rendszer dokumentált funkcionális és biztonsági tesztelésének végrehajtásáról.

A Jegyző feladata gondoskodni arról, hogy a tesztelés eredményét biztonsági elemzés, értékelés céljából az információbiztonsági felelős megkapja (lásd: 21.1 Biztonságelemzési eljárásrend).

Az EIR-hez kapcsolódó képzésekről a Hivatal a 17.2 Képzési eljárásrend, felügyeletéről a 28.4 Az elektronikus információs rendszer felügyelete fejezetekben meghatározottak szerint gondoskodik.

22.2 Sérülékenység-teszt

A Hivatal a saját fejlesztésű és általa üzemeltetett, a felügyelete, irányítása alatt lévő EIR-ek esetében, amennyiben az adott EIR rendszerfejlesztési, üzemeltetési és használati körülményei lehetővé teszik, külső szervezet bevonásával gondoskodik a rendszer sérülékenységi vizsgálatának elvégzéséről az EIR üzembe helyezését megelőzően, illetve új, lehetséges sérülékenységek felmerülésekor.

A sérülékenységi teszt dokumentált végrehajtása kapcsán megköveteli, hogy azt szakmailag elismert és elfogadott, naprakész fenyegetettségi adatbázist használó sérülékenységvizsgálati eszközök és technikák alkalmazásával végezzék el, továbbá a vizsgálati jelentés tartalmazza az alábbiakat:

- a feltárt hibákat, valamint a nem megfelelő konfigurációs beállításokat;
- a végrehajtott ellenőrzési listákat és tesztelési eljárásokat;
- a feltárt sérülékenység(ek) lehetséges hatásait;
- egy támadó milyen információkat képes elérni az elektronikus információs rendszerben, és ennek elhárítására milyen javítások végrehajtása szükséges;
- a sérülékenység teszt eredményét, annak szakmai, módszertani elemzését.

A sérülékenységi teszt végrehajtásához az EIR-hez, illetve rendszerelemeihez szükséges különleges jogosultsághoz kötött – úgynevezett privilegizált – hozzáférést a Hivatal biztosítja.

A Jegyző feladata gondoskodni arról, hogy a sérülékenységi teszt eredményét az információbiztonsági felelős megkapja, továbbá a vizsgált EIR-rel kapcsolatba kerülő munkatársai, valamint a Hivatallal munkavégzésre irányuló egyéb szerződéses jogviszonyban lévő személyek a feladataik által indokolt mértékben megismerjék.

Az információbiztonsági felelős feladata ellenőrizni és felügyelni, hogy a sérülékenységi vizsgálatról készített jelentésben javasolt és szükséges javító intézkedések az adott EIR biztonságának felülvizsgálata, illetve az EIR vagy rendszerelemeinek, működési környezetének megváltoztatása folyamán (pl.: a programkód, a rendszerbiztonsági terv, stb. módosítása) végrehajtásra kerüljenek, továbbá gondoskodni arról, hogy a feltárt új sérülékenységek az EIR következő tesztelése, illetve vizsgálata során a vizsgálandó sérülékenységek körében szerepeljenek.

23 KONFIGURÁCIÓKEZELÉS

23.1 Konfigurációkezelési eljárásrend

Konfigurációmódosítást kizárólag a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben meghatározottak szerint arra felhatalmazást, engedélyt kapott, a Hivatallal munkaviszonyban, illetve munkavégzésre irányuló egyéb (pl.: szerződéses) jogviszonyban álló személy hajthat végre.

A konfiguráció megváltozását az IT üzemeltető minden esetben köteles dokumentálni a hardver és szoftver komponensekről vezetett nyilvántartásban (lásd: 23.8 Elektronikus információs rendszerelem leltár), illetve az érintett rendszer dokumentációjában vagy a rendszer üzemeltetési leírásában.

23.2 Alapkonfiguráció

A Hivatal a saját fejlesztésű és általa üzemeltetett, a felügyelete, irányítása alatt lévő EIR-ek esetében az EIR megfelelő és üzembiztos működtetéséhez szükséges alapkonfiguráció paramétereit a rendszer dokumentációjában (rendszer üzemeltetési leírás) rögzíti és tartja karban. A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR-ek esetében a rendszer tulajdonosa határozza meg és dokumentálja az adott EIR használatához szükséges konfiguráció tartalmát, a kompatibilitási, illetve a minimális hardver- és szoftverkövetelményeket és ezek beállításait.

A Hivatal fentiek alapján, továbbá figyelembe véve, hogy az egyes rendszerelemek több EIR részeként egyaránt funkcionálhatnak, alakítja ki az EIR-ek működési környezetét képező informatikai eszközök alapkonfigurációit, amelyek komponenseit a 23.8 Elektronikus információs rendszerelem leltárban tartja nyilván és jelöli. A több EIR által közösen használt rendszerelemek esetében az alapkonfiguráció megegyezhet a nyilvántartás (konfiguráció menedzsment adatbázis) kezdeti, kiinduló állapotában rögzített leltáradatokkal.

23.3 A konfigurációváltozások felügyelete (változáskezelés)

A Hivatal a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben felsorolt változástípusok esetén az engedélyezési eljárás részeként gondoskodik a változás hatásainak vizsgálatáról, valamint a változtatásra vonatkozó döntés dokumentálásáról.

A változtatás végrehajtása az engedély birtokában a kijelölt felelős (pl.: IT üzemeltető) feladata. A változtatást az IT üzemeltető hardver és szoftver komponensek esetében a 23.8 Elektronikus információs rendszerelem leltárban, beállítások módosítása esetén az érintett rendszer dokumentációjában, illetve a rendszer üzemeltetési leírásában köteles rögzíteni.

Az információbiztonsági felelős jogosult a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységek ellenőrzésére, illetve felülvizsgálati tevékenysége során – minimum éves rendszerességgel – auditálja azt.

23.4 Előzetes tesztelés és megerősítés

A Hivatal a saját fejlesztésű és általa üzemeltetett, a felügyelete, irányítása alatt lévő EIR-ek esetében a konfiguráció megváltoztatása előtt a 22.1 Tesztelési, képzési és felügyeleti eljárások fejezetben meghatározottak szerint hajtja végre és a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben leírtak alapján engedélyezi és dokumentálja a változást.

Hardver meghibásodás miatt szükséges rendszerelem csere esetében a beépítésre kerülő új hardverelem műszaki megfelelőségének vizsgálata az IT üzemeltető feladata. Karbantartás, illetve hibajavítás céljából kizárólag olyan hardverelem építhető be, amely a használt EIR-ek ismert kompatibilitási és konfigurációs igényeinek megfelel.

23.5 Biztonsági hatásvizsgálat

Az információbiztonsági felelős a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben meghatározottak szerint végzi el a Hivatal saját fejlesztésű és általa üzemeltetett, a felügyelete, irányítása alatt lévő EIR-ek esetében a tervezett változtatások előzetes biztonsági hatásvizsgálatát.

23.6 Konfigurációs beállítások

A Hivatal a saját fejlesztésű és általa üzemeltetett, a felügyelete, irányítása alatt lévő EIR-ek esetében meghatározza a működési követelményeknek még megfelelő, ugyanakkor biztonsági szempontból a lehető leginkább korlátozott módon – a „szükséges minimum" elv alapján – az EIR-ben alkalmazandó konfigurációs beállításokat, s ezeket a rendszer dokumentációjában rögzíti. A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR-ek esetében a rendszer tulajdonosa határozza meg és dokumentálja az adott EIR használatához szükséges konfigurációs beállításokat.

A beállítások elvégzése, a konfigurációs követelményekről rendelkezésre álló rendszer dokumentációk alapján az IT üzemeltető feladata. Amennyiben a konfiguráció során a meghatározott beállításokhoz képest eltérést tapasztal, úgy azt köteles a 23.3 A konfigurációváltozások felügyelete (változáskezelés) fejezetben előírtak szerint jelezni, valamint a rendszer dokumentációjában, illetve a rendszer üzemeltetési leírásában rögzíteni.

Az információbiztonsági felelős a konfigurációs beállítások változtatásait a 23.3 A konfigurációváltozások felügyelete (változáskezelés) fejezetben meghatározott tevékenysége keretében kíséri figyelemmel, illetve ellenőrzi.

23.7 Legszűkebb funkcionalitás

A Hivatal a saját fejlesztésű és általa üzemeltetett, a felügyelete, irányítása alatt lévő EIR-ek konfigurációs beállításait a legszűkebb funkcionalitás elvének megfelelően, a nem szükséges funkciók, portok, protokollok, szolgáltatások korlátozásával, illetve tiltásával határozza meg és dokumentálja. A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR-ek esetében a rendszer tulajdonosa határozza meg és dokumentálja az adott EIR használatához szükséges és elégséges konfigurációs beállításokat.

A beállítások végrehajtását az IT üzemeltető a 23.6 Konfigurációs beállítások fejezetben előírtak szerint köteles elvégezni.

A Hivatal által használt EIR-ek működési környezetét képező kiszolgálókon és munkaállomásokon telepíthető, illetve használható szoftverekre vonatkozó szabályokat a 23.9 A szoftverhasználat korlátozásai, valamint a 23.10 A felhasználó által telepített szoftverek fejezetek tartalmazzák.

23.8 Elektronikus információs rendszerelem leltár

A Hivatal által használt EIR-ek rendszerelemeiről, a hardver és szoftver komponensekről az IT üzemeltető köteles naprakész nyilvántartást vezetni. A nyilvántartásnak minimálisan a 10. számú melléklet – Elektronikus információs rendszerelem leltár mellékletben meghatározott tartalommal kell rendelkeznie, s biztosítania kell a nyilvántartott rendszerelemek egyértelmű beazonosíthatóságát.

A nyilvántartás elektronikus formában (pl.: konfigurációkezelési adatbázis), illetve automatizált változásfelügyeleti megoldással aktualizálható módon egyaránt vezethető, amennyiben képes biztosítani a komponensek változásainak időbeni visszakereshetőségét.

A nyilvántartás formájától függetlenül biztosítani kell a Hivatal számára az adatokhoz történő folyamatos hozzáférést: papír alapú nyilvántartás esetén az iratkezelésre vonatkozó, valamint a 4. Dokumentumvédelem fejezetben meghatározott előírásoknak megfelelően, elektronikus formában a Jegyző és az információbiztonsági felelős részére.

23.9 A szoftverhasználat korlátozásai

A Hivatal informatikai rendszereiben kizárólag a Jegyző által engedélyezett, jogtiszta, a Hivatal által megvásárolt kereskedelmi és/vagy szabad felhasználású, valamint jogszabályban előírt központi szolgáltató által biztosított szoftver termékeket lehet alkalmazni.

Az IT üzemeltető feladata ellenőrizni a Hivatal informatikai rendszereiben telepített és futtatott programokat és alkalmazásokat, a mennyiségi licencekkel védett szoftverek használatát a 10. Az elektronikus információs rendszerek nyilvántartásában, illetve kereskedelmi szoftver esetén a felhasználásra vonatkozó szerződésben szereplő engedélyezett licence szám alapján, valamint az állomány megosztásokat az esetlegesen szerzői joggal védett tartalmak jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására irányuló tevékenységek szűrése céljából.

Nem engedélyezett tevékenység vagy szoftverhasználat észlelése esetén az IT üzemeltető köteles a Jegyzőt haladéktalanul tájékoztatni, valamint az utasításának megfelelően a szükséges intézkedéseket (pl.: nem engedélyezett szoftver vagy jogvédett tartalom eltávolítása) megtenni.

Az engedély nélküli tevékenységet végrehajtó, szabályszegő személy felelősségre vonására a 16.5 Fegyelmi intézkedések fejezetben meghatározottak szerint a Jegyző jogosult.

23.10 A felhasználó által telepített szoftverek

A Hivatal a munkatársai, az általa használt EIR-ek felhasználói számára az informatikai eszközöket és erőforrásokat a hivatali munkavégzés céljára biztosítja, azokon kizárólag az IT üzemeltető által telepített szoftverek, alkalmazások és szolgáltatások használatára jogosultak. A munkaállomásokra a felhasználók nem telepíthetnek programokat, továbbá nem módosíthatják a telepített szoftverek konfigurációját, működését és nem távolíthatják el azokat!

A munkavégzés, az ügymenet, illetve az adott folyamat hatékonyságát javító szoftverek használatára a Hivatal munkatársai javaslatot tehetnek a Jegyző felé, aki ebben az esetben a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás alapján dönt a szoftver beszerzésének, illetve telepítésének engedélyezéséről.

A munkaállomásokra telepített szoftvereket az IT üzemeltető ellenőrzi a 23.9 A szoftverhasználat korlátozásai fejezetben meghatározottak szerint.

24 KARBANTARTÁS

24.1 Rendszer karbantartási eljárásrend

A Hivatal által használt EIR-ek folyamatos működésének biztosítása, rendelkezésre állásának megőrzése érdekében az IT üzemeltető feladata az informatikai eszközök, a rendszerelemek hardver, illetve szoftver komponenseinek rendszeres és dokumentált karbantartásáról, szükség szerinti javításáról gondoskodni.

24.2 Rendszeres karbantartás

A karbantartásról az IT üzemeltető az adott rendszerelemre vonatkozó gyártói ajánlásoknak megfelelő módon és rendszerességgel köteles gondoskodni.

A tervezett karbantartási, illetve a szükséges javítási feladatok végrehajtásáról az IT üzemeltető köteles a Jegyzőt előzetesen tájékoztatni. A Jegyző a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás alapján dönt a tevékenység jóváhagyásáról.

Amennyiben a karbantartás, illetve javítás a helyszínen nem végezhető el és emiatt az érintett rendszerelem kiszállítására van szükség, ennek engedélyezését, felügyeletét és dokumentálását a Hivatal a 18.10 Be- és kiszállítás fejezetben meghatározottak szerint végzi.

Adathordozót is tartalmazó rendszerelem (eszköz) esetén az elszállítás előtt az IT üzemeltető feladata az adathordozón található adatok és információk szükség szerinti eseti biztonsági mentéséről a 5. számú melléklet – Az elektronikus információs rendszerek mentése dokumentumban meghatározottak szerint, s az adathordozóról történő visszaállíthatatlan módú törléséről gondoskodni.

A Jegyző a Hivatal munkatársainak közreműködésével ellenőrzi, hogy a rendszerelem, illetve az EIR a karbantartási vagy javítási tevékenységek után is megfelelően működik-e. A Jegyző és az információbiztonsági felelős jogosult az IT üzemeltetőtől minden olyan információt (hozzáférést, adatot, dokumentációt, stb.) bekérni, az IT üzemeltető pedig köteles biztosítani, amely a funkcionális, illetve biztonsági ellenőrzés végrehajtásához szükséges.

A karbantartási, illetve javítási tevékenységekről az IT üzemeltető köteles nyilvántartást vezetni, s ezzel kapcsolatban keletkező dokumentációk hozzáférhetőségét azok megjelenési formájától függően a Hivatal számára biztosítani a 4. Dokumentumvédelem fejezetben meghatározott szabályok szerint.

25 ADATHORDOZÓK VÉDELME

25.1 Adathordozók védelmére vonatkozó eljárásrend

A Hivatal az elektronikus adathordozók védelméről hozzáférésük, továbbá teljes életciklusukra kiterjedő biztonságos kezelésük jelen IBSZ-ben történő szabályozásával, papír alapú adathordozók esetében a Hivatal iratkezelésre vonatkozó előírásai alapján gondoskodik.

A Hivatal által használt EIR-ek beépített adathordozót tartalmazó rendszerelemeinek biztonságos elhelyezéséről és felügyeletéről a Hivatal a 18. Fizikai és környezeti védelem, jogosulatlan hozzáférés elleni védelméről annak a 18.4 A fizikai hozzáférések felügyelete fejezetében előírt módon gondoskodik.

A hivatali munkavégzéshez a Hivatal által biztosított, beépített adathordozót tartalmazó mobil eszközök (pl.: laptop, tablet, okostelefon) és mobil adattároló eszközök (pl.: memóriakártya, külső háttértároló eszköz vagy merevlemez, optikai adathordozó lemez, stb.) fizikai védelméről, biztonságos tárolásáról és kezeléséről a használatára jogosult személy/munkavállaló köteles gondoskodni. Használaton kívül az eszközt, adattárolót el kell zárni, illetve illetéktelenek számára hozzáférhető helyen folyamatos felügyelet nélkül, őrizetlenül hagyni (pl.: közterületen parkoló zárt gépjárműben is) TILOS!

Az adathordozó vagy eszköz elvesztése, ellopása biztonsági eseménynek minősül, melyet minden munkavállaló az észlelést követően haladéktalanul köteles jelenteni a Jegyző számára, aki a 15. A biztonsági események kezelése fejezetben meghatározottak szerint jár el ilyen esetben.

25.2 Hozzáférés az adathordozókhoz

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomások és kiszolgálók (pl.: fájl szerver) adathordozóihoz kizárólag a használatára jogosult személy/munkavállaló férhet hozzá. Az illetéktelen hozzáférés elleni védelem biztosítása céljából az adott számítógépet minimum egytényezős hitelesítéssel, egyedi hozzáférési azonosító és hitelesítő eszköz (pl.: felhasználónév és jelszó) alkalmazásával kell ellátni.

A munkavégzéshez a Hivatal által biztosított mobil adattároló vagy beépített adathordozót tartalmazó mobil eszközön munkavégzéshez kapcsolódó információkat az adathordozó típusának megfelelően lehetőség szerint fájl- vagy tárolószintű titkosítással ellátva kell tárolni. Az eszköz biztonságát – amennyiben technológiai oldalról támogatott – további hozzáférés védelmi megoldás (pl.: jelszó, PIN kód, stb.) alkalmazásával is biztosítani kell.

A kriptográfiai védelem kialakításában és beállításában az IT üzemeltető feladata közreműködni, a titkosításhoz használt kulcsok, egyedi azonosítók és hitelesítő eszközök (pl.: jelszó) biztonságos kezelése és megőrzése az eszköz, illetve adathordozó használatára jogosult feladata és felelőssége.

Adathordozó előállítására alkalmas eszköz, berendezés (pl.: nyomtató) a Hivatal nyitvatartási idejében az ügyfelek és látogatók által hozzáférhető, felügyelet nélkül lévő helyiségben nem helyezhető el, kivéve, ha az adott eszköz képes felügyelt nyomtatást biztosítani, s beállításra kerül rajta, hogy nyomtatási feladat kizárólag a nyomattulajdonos helyi hitelesítését követően hajtható végre. Az eszköz

konfigurálása, a beállítások dokumentálása az IT üzemeltető feladata. A beállított védelmi intézkedések megfelelőségét az információbiztonsági felelős felügyeleti tevékenysége keretében jogosult ellenőrizni.

25.3 Adathordozók törlése

Az IT üzemeltető feladata az adathordozó típusának megfelelő, helyreállíthatatlanságot biztosító törlési technikát (pl.: többszörös felülírás, roncsolás, stb.) alkalmazva törölni a Hivatal által használt EIR-ek és a munkavégzéshez a Hivatal által biztosított mobil eszközök beépített adathordozóit, továbbá a mobil elektronikus adathordozókat azok leselejtezése vagy újrafelhasználásra való kibocsátása előtt.

Amennyiben javítási, karbantartási célból adathordozót is tartalmazó rendszerelem (eszköz) ideiglenesen kikerül a Hivatal felügyelete alól, a kiszállítás előtt az IT üzemeltető feladata az adathordozón található adatok és információk szükség szerinti eseti biztonsági mentéséről, s az adathordozóról történő visszaállíthatatlan módú törléséről gondoskodni.

25.4 Adathordozók használata

A Hivatal által használt EIR-ekhez, illetve rendszerelemeihez kizárólag a Hivatal által biztosított és/vagy ellenőrzött mobil eszközök és adathordozók csatlakoztatása engedélyezett. Eltérni ettől indokolt esetben, a Jegyző jóváhagyását (lásd: 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás) és a szükséges biztonsági ellenőrzések lefolytatását követően lehet. A nem a Hivatal tulajdonát képező, idegen adathordozó vagy mobil eszköz csatlakoztatását megelőzően az IT üzemeltető feladata az adathordozó megbízhatóságának ellenőrzése (pl.: vírusellenőrzés). Idegen eszköz csatlakoztatási igényét a Jegyző számára engedélyezés céljából az igénylő köteles előzetesen jelezni.

Adathordozó vagy mobil eszköz engedély nélküli csatlakoztatása biztonsági eseménynek minősül, amely a 15. A biztonsági események kezelése, továbbá a 16.5 Fegyelmi intézkedések fejezetekben meghatározott eljárást, illetve következményeket vonja maga után.

26 AZONOSÍTÁS ÉS HITELESÍTÉS

26.1 Azonosítási és hitelesítési eljárásrend

A Hivatal által a hivatali munkavégzés támogatása céljából használt EIR-ekhez történő felhasználói hozzáférés kizárólag azonosítást és hitelesítést követően engedélyezett, jelen fő fejezetben megállapított szabályok szerint. A munkavégzéshez szükséges azonosítók, felhasználói fiókok létrehozását és konfigurálását, a jogosultságok beállítását a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás alapján a Jegyző engedélyezi, s az IT üzemeltető hajtja végre.

26.2 Azonosítás és hitelesítés

A felhasználók által végzett tevékenységek nyomon követhetőségének biztosítása érdekében a hivatali munkavégzés támogatása céljából kizárólag olyan EIR használata engedélyezett, amely képes a felhasználók egyedi azonosítására és hitelesítésére. Új EIR fejlesztése, bevezetése, illetve használatba vétele előtt az engedélyezési eljárás során az információbiztonsági felelős jogosult az adott rendszer azonosítási, hitelesítési megoldásának vizsgálatára, s javaslatot tenni a Jegyző számára annak jóváhagyására vagy elutasítására.

Csoportszintű hozzáférés csak a munkavégzés folyamatosságának, valamint a munkavégzéshez szükséges információkhoz történő hozzáférés biztosítása céljából és kizárólag abban az esetben engedélyezhető és képezhető ilyen azonosító, amennyiben a csoport nevében az érintett rendszerben

önálló művelet (változtatás) nem hajtható végre (pl.: egyirányú, passzív kommunikáció: csoportos levelezési cím, terjesztési lista).

26.3 Hálózati hozzáférés privilegizált fiókokhoz

Új EIR fejlesztése, bevezetése során a Hivatal a különleges jogosultsághoz kötött – úgynevezett privilegizált – felhasználói fiókokhoz (pl.: rendszer adminisztrátor, rendszergazda) való hálózaton keresztüli hozzáféréshez többtényezős hitelesítés alkalmazását követeli meg.

A meglévő, általa használt EIR-ek esetében, amennyiben az a hatáskörébe, felügyelete alá tartozik és technológiai szempontból megvalósítható, akkor a Hivatal gondoskodik a többtényezős hitelesítés kialakításáról a privilegizált hálózati hozzáférésekhez. Amennyiben az adott EIR-ben a többtényezős hitelesítés megvalósítására nincs lehetőség, a Hivatal gondoskodik a rendszer követelményeknek megfelelő, tervezett kiváltásáról.

26.4 Azonosító kezelés

A munkaállomásokon, szerver kiszolgáló gépeken, valamint a Hivatal kezelésében, felügyelete alatt álló informatikai eszközökön (pl.: hálózati eszközök, nyomtatók, stb.) a helyi, illetve címtár használata esetén a tartományi felhasználói azonosítók létrehozása, hozzárendelése a meghatározott egyénhez, csoporthoz, szerepkörhöz vagy eszközhöz, továbbá az azonosítók adminisztrálása, nyilvántartása az IT üzemeltető feladata. A Hivatal által használt EIR-ek esetében, amennyiben azok önálló azonosítási megoldással rendelkeznek és a felhasználói azonosítók kezelése a Hivatal hatáskörébe tartozik, akkor azok kezelése az erre feljogosított szerepkört (pl.: alkalmazás adminisztrátor, tenant admin, stb.) betöltő, a Jegyző által e feladat végrehajtásával megbízott munkatárs feladata.

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomásokon a felhasználó 15 perc időtartamú inaktivitása esetén azonosítóját le kell tiltani (pl.: számítógép zárolása, számítógép üresjárati korlátja). A munkaállomás újbóli használatát ismételt hitelesítéshez kell kötni. Az ezekhez szükséges beállítások végrehajtását az IT üzemeltető a 23.6 Konfigurációs beállítások fejezetben előírtak szerint köteles elvégezni.

Új EIR fejlesztése, bevezetése során a Hivatal az azonosítók kezelésével kapcsolatban megköveteli, hogy az paraméterezhető módon, meghatározott időtartamig legyen képes megakadályozni az azonosító ismételt felhasználását, továbbá meghatározott időtartamú inaktivitás esetén tiltsa le az azonosítót. Meglévő EIR-ek esetében, amennyiben az a hatáskörébe, felügyelete alá tartozik és technológiai szempontból megvalósítható, akkor az IT üzemeltető feladata ennek dokumentált konfigurálása.

26.5 A hitelesítésre szolgáló eszközök kezelése

A hitelesítésre szolgáló eszközök kiosztását, továbbá a felhasználásának megfelelő jogosultságok beállítását 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás alapján a Jegyző engedélyezi, s a 26.4 Azonosító kezelés fejezetben előírtak szerint az azonosítók kezelésével megbízott (IT üzemeltető, tenant admin, stb.) hajtja végre.

A Hivatal a saját fejlesztésű és általa üzemeltetett, a felügyelete, irányítása alatt lévő EIR-ek, illetve rendszerelemeik esetében a tudásalapú hitelesítő eszközök (jelszavak) képzésével és használatával kapcsolatban az alábbi szabályokat állapítja meg:

A jelszavas hitelesítést alkalmazó rendszerelemeken kötelező a jelszavas védelem beállítása és alkalmazása.

A felhasználói jelszavakra vonatkozó minimálisan alkalmazandó általános jelszó követelmények:

- a jelszó minimális hossza (legrövidebb jelszó): 8 karakter;
- a jelszó bonyolultsága (komplexitás): tartalmaznia kell legalább egy kis- és nagybetűs, speciális karaktert, valamint számjegyet;

- előző jelszavak megőrzése: legutolsó 5 jelszó tárolása;
- a jelszavak minimális és maximális élettartama: 5 és 90 nap.

A meghatározott jelszóképzési szabálytól eltérni a jelszó hosszát, bonyolultságát illetően a magasabb védelmi szintet jelentő irányba, felfelé lehet (pl.: „jelszó helyett jelmondat"-elv alkalmazásával).

A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR-ek esetében a Hivatal a rendszer tulajdonosa által meghatározott jelszóképzési szabályokat alkalmazza.

A felhasználói jelszavakat tilos papír alapon, felírva tárolni! Kivételt képeznek ez alól a privilegizált hozzáférésekhez tartozó azonosítók és jelszavaik, melyeket rendelkezésre állásuk folyamatos biztosítása érdekében az azonosító kezelője (pl.: IT üzemeltető) köteles létrehozásuk és minden módosításuk alkalmával egy példányban beazonosítható módon dokumentálni, s azt átadni a Jegyző számára, aki gondoskodik azok biztonságos megőrzéséről és kezeléséről (lezárt borítékban, páncélszekrényben).

A felhasználói azonosítók és jelszavak elektronikus tárolása, nyilvántartása kizárólag önálló és biztonságos hitelesítési megoldással rendelkező (pl.: jelszavas védelemmel ellátott dokumentum, jelszó menedzsment alkalmazás) vagy egyéb kriptográfiai védelemmel ellátott (pl.: titkosított partíció vagy adatbázis, adattábla) módon, offline tárolással engedélyezett; nyílt formában vagy mobil infokommunikációs eszközön (pl.: okostelefon, tablet), valamint online (interneten keresztül elérhető, felhő alapú) jelszótároló rendszerben tilos!

Az internetkapcsolaton keresztül elérhető EIR-ek, illetve rendszerelemeik esetében az internet böngészőprogramok beépített kényelmi funkciójának, a bejelentkezési adatok tárolásának (pl.: automatikus kiegészítés, felhasználói jelszavak megjegyzése) a használata tilos, a funkciót ki kell kapcsolni!

A felhasználói jelszavakkal kapcsolatos szabályok (jelszó házirend, böngésző program, stb.) beállítását az IT üzemeltető a 23.6 Konfigurációs beállítások fejezetben előírtak szerint köteles elvégezni. Felhasználói fiók, hozzáférés, illetve jogosultság változás esetén a hitelesítő eszköz módosításáról a 16.1 Személybiztonsági feltételek fejezetben meghatározottak szerint az IT üzemeltető feladata gondoskodni.

A privilegizált hozzáférések alapértelmezett jelszavait (pl.: hálózati eszközök esetében) az IT üzemeltető köteles a rendszerelem első konfigurációja, telepítése alkalmával megváltoztatni és dokumentálni, valamint a beállított hozzáférés adatait a Jegyző rendelkezésére bocsátani.

Amennyiben a Hivatal által használt EIR birtoklás alapú (pl.: hardver token, PKI tanúsítvány, kódkártya) hitelesítést alkalmaz, s az e célra szolgáló eszközök kiosztása, visszavonása, illetve cseréje a Hivatal hatáskörébe tartozik, akkor azt minden esetben átadás-átvételi bizonylattal dokumentálja. Az átadás-átvétel dokumentumainak megőrzéséről a Hivatal a hatályos iratkezelési szabályainak megfelelően gondoskodik.

A Hivatal a birtoklásalapú hitelesítésre szolgáló eszközök használati idejét, továbbá ismételt felhasználhatóságának feltételeit az érintett EIR igénybevételére vonatkozó szabályok, valamint a kibocsátó, illetve a gyártó ajánlásainak megfelelően alakítja ki, illetve alkalmazza.

A hitelesítésre szolgáló eszköz felhasználójának feladata és felelőssége a kapott eszköz bizalmasságának és sértetlenségének megőrzése. Bármely hitelesítésre szolgáló eszköz kompromittálódását (pl.: a jelszó illetéktelen személy általi megismerése) vagy sérülését, az eszköz elvesztését, ellopását a használó az észlelést követően haladéktalanul köteles a 15. A biztonsági események kezelése fejezetben meghatározottak szerint a Jegyzőnek jelenteni.

26.6 A hitelesítésre szolgáló eszköz visszacsatolása

A Hivatal a saját fejlesztésű és általa üzemeltetett, a felügyelete, irányítása alatt lévő EIR-ek esetében kizárólag olyan rendszerelemek alkalmazását engedélyezi, amelyek a hitelesítési folyamat során képesek fedett visszacsatolást biztosítani. A követelmények teljesülését az információbiztonsági

felelős a 22.1 Tesztelési, képzési és felügyeleti eljárások fejezetben meghatározottak szerint jogosult ellenőrizni.

26.7 Hitelesítés kriptográfiai modul esetén

Új EIR fejlesztése, bevezetése során a Hivatal megköveteli, hogy a rendszer egy adott kriptográfiai modulhoz való hitelesítésre olyan mechanizmusokat használjon, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának.

26.8 Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

A Hivatal által használt EIR-ekhez, illetve a Hivatal által kezelt adatokhoz hozzáféréssel rendelkező, a Hivatallal egyéb szerződéses, munkavégzésre irányuló jogviszonyban álló személyek számára, tevékenységük nyomon követhetőségének biztosítása érdekében minden esetben egyedi azonosítót képez, s ez alapján hitelesíti őket. Az azonosítók létrehozása és a használatukhoz szükséges hitelesítő eszközök kiosztása a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás alapján a Jegyző engedélyével, a 26.4 Azonosító kezelés fejezetben előírtak szerint az azonosítók kezelésével megbízott (IT üzemeltető, tenant admin, stb.) feladata.

26.9 Hitelesítésszolgáltatók tanúsítványának elfogadása

Új EIR fejlesztése, bevezetése során a Hivatal előírja, hogy a rendszer csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványokat fogadhatja el a szervezeten kívüli felhasználók hitelesítéséhez.

27 HOZZÁFÉRÉS ELLENŐRZÉSE

27.1 Hozzáférés ellenőrzési eljárásrend

A Hivatal az általa használt EIR-ekkel kapcsolatban a hozzáférések ellenőrzésének eljárásrendjét jelen fő fejezetben, az alábbiak szerint határozza meg.

Az információbiztonsági felelős jogosult a hozzáférések, illetve felhasználói fiókok kezelésével kapcsolatos beállítások és tevékenységek ellenőrzésére, illetve felülvizsgálati tevékenysége során – minimum éves rendszerességgel – auditálja azt. Az eseti, illetve rendszeres ellenőrzések lefolytatásában, a felülvizsgálatban az IT üzemeltető köteles közreműködni, ahhoz információkat nyújtani.

27.2 Felhasználói fiókok kezelése

A Hivatal által használt EIR-ekben, valamint az azokhoz hozzáférést biztosító munkaállomásokon a hivatali munkavégzéshez szükséges azonosítók, felhasználói fiókok létrehozását, a jogosultságok beállítását, továbbá ezek módosítását a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás alapján a Jegyző engedélyezi, s a 26.4 Azonosító kezelés fejezetekben meghatározottak szerint kijelölt felelős hajtja végre.

A fiók kezelőjét a Jegyző köteles értesíteni, amennyiben az adott

- felhasználói fiókra már nincs szükség;
- felhasználó kilépett vagy áthelyezésre került;
- EIR használata vagy az ehhez szükséges ismeretek megváltoztak.

Az adott fiók kezelője a felhasználói fiók, hozzáférés, illetve jogosultság megváltozása esetén a hitelesítő eszköz módosításáról a 16.1 Személybiztonsági feltételek fejezetben meghatározottak szerint köteles gondoskodni.

27.3 Hozzáférés ellenőrzés érvényesítése

A Hivatal által használt EIR-ekhez hozzáférést biztosító, a Hivatal által felügyelt kiszolgálókhoz és munkaállomásokhoz a hozzáférés kizárólag a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben meghatározott jóváhagyást, valamint azonosítást és hitelesítést követően engedélyezett.

A Hivatal által használt EIR-ek esetében a hivatali munkavégzéshez szükséges azonosítók, felhasználói fiókok létrehozását, a jogosultságok beállítását, továbbá ezek módosítását szintén minden esetben a Jegyző engedélyezi, s ez alapján a 26.4 Azonosító kezelés fejezetben meghatározottak szerint kijelölt felelős hajtja végre. A jóváhagyott jogosultságok érvényesítése az azonosítás és hitelesítés során történik meg.

A Hivatal által használt EIR-ekhez hozzáférést biztosító, a Hivatal által felügyelt kiszolgálók és munkaállomások biztonsági beállításait az IT üzemeltető jogosult módosítani.

27.4 Sikertelen bejelentkezési kísérletek

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomások és kiszolgálók biztonsági beállításait (fiókzárolási házirend) az IT üzemeltető a 23.6 Konfigurációs beállítások fejezetben előírt eljárás szerint, az alábbi szabályoknak megfelelően köteles végrehajtani:

- a felhasználó 3 egymást követő sikertelen bejelentkezési kísérlete esetén a munkaállomás automatikusan zárolja a felhasználói fiókot (pl.: fiókzárolási küszöb);
- a fiók zárolása automatikusan 30 perc elteltével kerüljön feloldásra (pl.: fiókzárolás időtartama, fiókzárolási számlázó nullázása).

Új EIR fejlesztése, bevezetése során a Hivatal a sikertelen bejelentkezési kísérletek kezelésével kapcsolatban minimális feltételként fenti szabályoknak történő megfelelést követeli meg. Meglévő EIR-ek esetében, amennyiben az a hatáskörébe, felügyelete alá tartozik és technológiai szempontból megvalósítható, akkor az IT üzemeltető feladata ennek dokumentált konfigurálása.

A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR-ek esetében a Hivatal a rendszer tulajdonosa által meghatározott szabályokat alkalmazza.

27.5 A rendszerhasználat jelzése

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomásokon az IT üzemeltető feladata a 23.6 Konfigurációs beállítások fejezetben előírt eljárás szerint az alábbi tartalmi elemekkel bíró, a rendszerhasználat jelzésére vonatkozó interaktív bejelentkezési üzenet beállítása:

- Ön a Kislángi Polgármesteri Hivatal informatikai rendszerét használja;
- a rendszer használatát figyelhetik, rögzíthetik, naplózhatják;
- a rendszer jogosulatlan használata tilos és büntetőjogi vagy polgárjogi felelősségre vonással jár;
- a bejelentkezéssel fentieket tudomásul veszi és azokhoz hozzájárul.

Új EIR fejlesztése, bevezetése során a Hivatal a rendszerhasználat jelzésével kapcsolatban fenti szabályoknak történő megfelelést követeli meg. Meglévő EIR-ek esetében, amennyiben az a hatáskörébe, felügyelete alá tartozik és technológiai szempontból megvalósítható, akkor az IT üzemeltető feladata ennek dokumentált konfigurálása.

A Hivatal nyilvánosan elérhető EIR üzemeltetése esetén gondoskodik arról, hogy az

- kijelezze a rendszer használatának feltételeit, mielőtt további hozzáférést biztosít;
- amennyiben felügyelet, adatrögzítés vagy naplózás történik, kijelezze, hogy ezek megfelelnek az adatvédelmi szabályoknak;
- leírást biztosítson a rendszer engedélyezett felhasználásáról.

27.6 Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

A Hivatal által használt EIR-ekhez hozzáférést biztosító, a Hivatal által felügyelt munkaállomások és kiszolgálók kizárólag azonosítást és hitelesítést követően vehetők igénybe.

A Hivatal saját fejlesztésű és általa üzemeltetett, a felügyelete, irányítása alatt lévő, nyilvánosan elérhető (közzétett) tartalmakat kezelő EIR esetében a tartalom adminisztrálásához, illetve a rendszer üzemeltetéséhez szükséges privilegizált hozzáférések szintén csak azonosítás és hitelesítés után érhetők el.

Az azonosítás és hitelesítés nélküli hozzáférést vagy anonim bejelentkezést lehetővé tevő beépített fiókok (pl.: vendég) letiltásáról az IT üzemeltető köteles gondoskodni.

27.7 Távoli hozzáférés

A Hivatal a saját fejlesztésű és általa üzemeltetett, a felügyelete, irányítása alatt lévő EIR-ek esetében a távoli hozzáférést kizárólag akkor és azon személynek engedélyezi és hagyja jóvá, amennyiben az maradéktalanul megfelel a jelen IBSZ-ben meghatározott biztonsági követelményeknek.

A Hivatal az informatikai rendszeréhez történő hálózaton keresztüli, üzemeltetési célú (pl.: távsegítség biztosítása) hozzáférés kapcsán minimálisan a titkosított adatátviteli csatorna alkalmazását (pl.: VPN) követeli meg. A távoli hozzáférésre használt megoldás biztonsági követelményeknek történő megfelelőségét az információbiztonsági felelős jogosult megvizsgálni. Amennyiben a távoli hozzáférésre rendszeresített megoldás, illetve technológia olyan biztonsági funkciókat valósít meg, amelyek garantálják a hálózati hozzáférés megfelelő szintű biztonságát, akkor a Jegyző az információbiztonsági felelős javaslata alapján dönt az alkalmazott megoldás használatának engedélyezéséről, illetve ellenkező esetben a követelményeknek megfelelő rendszerrel történő kiváltásáról.

A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR-ek esetében a Hivatal a rendszer tulajdonosa által meghatározott felhasználásra vonatkozó korlátozásokat, konfigurálási vagy kapcsolódási követelményeket és megvalósítási útmutatókat alkalmazza.

A Jegyző a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben meghatározottak szerint engedélyezi vagy tiltja a Hivatal által használt EIR-ekhez történő távoli hozzáférést.

27.8 Vezeték nélküli hozzáférés

A Hivatal épületeiben vezeték nélküli hálózati hozzáférést a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben meghatározottak szerint a Jegyző engedélyével lehet létesíteni, illetve igénybe venni. Kivételt képez ez alól – amennyiben az adott telephelyen elérhető – a Hivatal által biztosított, a Hivatal hálózatáról leválasztott, szeparált nyilvános hálózati hozzáférés (pl.: „vendég" wifi), amelyhez a Hivatal munkatársai is csatlakoztathatják saját mobil eszközeiket.

Hivatali munkavégzés céljára biztosított vezeték nélküli hálózat hozzáférésvédelemmel (minimum jelszavas védelemmel) ellátottan és a csatlakoztatható eszközök – például fizikai hálózati címének (MAC address filter) – szűrésével létesíthető. A hivatali munkavégzés céljára biztosított vezeték nélküli hálózathoz kizárólag a Hivatal tulajdonát képező, a Hivatal által felügyelt mobil infokommunikációs eszköz csatlakoztatható.

A Hivatal vezeték nélküli hálózati beállításainak kezelése, dokumentálása az IT üzemeltető feladata. A beállítások ellenőrzésére az információbiztonsági felelős felügyeleti tevékenysége keretében jogosult.

27.9 Mobil eszközök hozzáférés ellenőrzése

A Hivatal által a munkavégzéshez biztosított, a Hivatal tulajdonát képező mobil eszközök használatba vétele előtt az IT üzemeltető köteles gondoskodni a 25. Adathordozók védelme és a 28.3 Kártékony kódok elleni védelem fejezetekben előírt védelmi funkciók, valamint a titkosított adatátvitel megvalósításához szükséges alkalmazások (pl.: VPN) beállításáról.

Mobil eszköz használatát, továbbá annak a Hivatal által használt EIR-ekhez történő kapcsolódását a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben meghatározottak szerint a Jegyző engedélyezheti.

27.10 Külső elektronikus információs rendszerek használata

A Hivatal a saját fejlesztésű és általa üzemeltetett, a felügyelete, irányítása alatt lévő EIR-ek esetében egy külső rendszerből hozzáférést az EIR-hez, illetve annak használatával a Hivatal által ellenőrzött információk feldolgozását, tárolását vagy továbbítását kizárólag akkor és azon személynek engedélyezhet és hagyhat jóvá, amennyiben

- előzetesen ellenőrzi tudja a szükséges biztonsági intézkedések meglétét a külső rendszeren, vagy
- jóváhagyott kapcsolat van az EIR-ek között, illetve megállapodás született a külső EIR-t befogadó szervezettel.

A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR-ek esetében a Hivatal a rendszer tulajdonosa által meghatározott feltételeket és szabályokat alkalmazza.

Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (E-ügyintézési tv.) szerinti szabványos információátadási felületeket a Hivatal Információátadási Szabályzata tartalmazza.

A Jegyző a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben meghatározottak szerint engedélyezi vagy tiltja a Hivatal által használt EIR-ekhez külső rendszerből történő hozzáférést, illetve külső elektronikus információs rendszerek segítségével a Hivatal által ellenőrzött információk feldolgozását, tárolását vagy továbbítását.

27.11 Nyilvánosan elérhető tartalom

A Hivatalban kizárólag a Jegyző által engedélyezett információkat lehet közzétenni. Minden más információ közzététele TILOS!

A Hivatal kezelésében lévő, nyilvánosan elérhető tartalom közzététele az alábbi formában valósulhat meg:

- a Hivatal honlapján vagy jogszabályban meghatározott központi kiszolgálón történő közzététel – a Jegyző eseti engedélyével;
- a bárki számára kiadható információ (jellemzően pl.: kitöltetlen űrlap, ügyintézéshez köthető folyamatleírás, közérdekű tájékoztató anyag) hivatali munkavállaló általi továbbítása korlátozás nélküli megtekintésre, illetve felhasználásra – a Jegyző általános engedélyével.

A Jegyző feladata és felelőssége a közzétételre javasolt tartalom ellenőrzése, valamint a közzétételre feljogosított munkavállalók képzése a közzététel tartalmával kapcsolatban (általánosan közzétételre engedélyezett információk köre, nem nyilvános információk köre, stb.).

A Jegyző jogosult és köteles évente legalább egy alkalommal átvizsgálni a nyilvánosan hozzáférhető és a honlapon közzétett információkat, s amennyiben nem nyilvános információtartalmat talál,

intézkedni annak eltávolításáról, valamint tájékoztatni a vizsgálat eredményéről az információbiztonsági felelőst.

A közzétételre alkalmazott kiszolgálón a nyilvánosan hozzáférhető információk elhelyezésében, törlésében az IT üzemeltető, illetve a honlap adminisztrálásával megbízott felelős köteles közreműködni.

28 RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG

28.1 Rendszer- és információsértetlenségre vonatkozó eljárásrend

A Hivatal az általa üzemeltetett, felügyelete, irányítása alá tartozó EIR-ekre, illetve amennyiben értelmezhető, rendszerelemeikre vonatkozó rendszer- és információsértetlenségi eljárásrendet jelen fő fejezetben, az alábbiak szerint határozza meg.

28.2 Hibajavítás

A Hivatal informatikai infrastruktúrájába, üzemeltetés felügyeleti hatáskörébe tartozó rendszerelemek hibáinak javításáról, illetve rendszeres karbantartásáról az IT Üzemeltető a 23. Konfigurációkezelés és a 24.1 Rendszer karbantartási eljárásrend fejezetekben előírtak szerint köteles gondoskodni.

A 28.5 Biztonsági riasztások és tájékoztatások fejezet alapján az információbiztonsági felelős által a biztonságkritikus szoftverekre, frissítéseikre vonatkozóan jelzett tevékenységek dokumentált végrehajtása az IT üzemeltető feladata és felelőssége.

28.3 Kártékony kódok elleni védelem

A Hivatal minden interneteléréssel rendelkező munkaállomásán és a Hivatal által munkavégzés céljára biztosított mobil infokommunikációs eszközén (pl.: laptop, tablet, telefon, stb.) víruskereső és vírusirtó funkcionalitással bíró védelmi szoftvert kell működtetni, amelynek telepítése, biztonsági beállításainak konfigurálása az IT üzemeltető feladata és felelőssége.

A védelmi szoftvernek minimálisan az alábbi funkciókkal kell rendelkeznie:

- legyen képes a külső forrásokból származó fájlok valós idejű ellenőrzését végrehajtani a végpontokon, a hálózati belépési vagy kilépési pontokon, amikor a fájlokat letöltik, megnyitják, vagy elindítják (pl.: email csatolt állományát);
- legyen képes előzetes konfigurációt követően időzített módon, rendszeresen automatikus ellenőrzéseket végrehajtani;
- legyen képes a vírusdefiníciós adatbázis automatikus frissítésére;
- kártékony kód észlelése esetén blokkolja vagy helyezze karanténba azt és jelenítsen meg riasztást a felhasználó számára.

A megfelelő védelmi szoftver kiválasztása az IT üzemeltető feladata, a működési feltételek (pl.: szükséges licencek) biztosításáról a Hivatal köteles gondoskodni. Az információbiztonsági felelős felülvizsgálati tevékenysége keretében ellenőrzi és javaslatot tehet a kártékony kódok elleni védelemre alkalmazott megoldás cseréjére, kiváltására, amennyiben az nem képes megfelelően biztosítani a Hivatal által használt EIR-ek egyenszilárd és kockázatokkal arányos védelmét (pl.: kritikus sérülékenységei válnak ismertté, gyártói támogatása nem biztosítja valamely elvárt funkcionalitást vagy megszűnik, stb.).

Minden munkavállaló köteles a védelmi szoftver által megjelenített riasztásról az IT üzemeltetőt haladéktalanul értesíteni.

Az IT üzemeltető feladata a védelmi szoftver által generált riasztások kivizsgálása, s indokolt esetben a 15. A biztonsági események kezelése fejezetben meghatározottak szerint a Jegyző, illetve az információbiztonsági felelős tájékoztatása.

Vírusfertőzés tényének fennállása esetén az IT üzemeltető jelzése nyomán a Jegyző kihirdeti a vírusriadó állapotot, s erről tájékoztatja a hivatali munkatársakat és az információbiztonsági felelőst.

A vírusriadó időtartama alatt minden munkavállaló köteles együttműködni a vírusfertőzés továbbterjedését, valamint a helyreállítási tevékenységeket érintően az IT üzemeltető, illetve az információbiztonsági felelős által meghatározott intézkedések (pl.: munkaállomások ideiglenes leállítása, internet használat felfüggesztése, stb.) végrehajtásában.

A helyreállítási tevékenység keretében az IT üzemeltető gondoskodik – szükség szerint a hivatali munkavállalók közreműködésével – a fertőzött eszköznek a hivatali belső hálózatról történő leválasztásáról, a vírusfertőzés megszüntetéséről, a veszélyeztetett munkaállomások (pl.: azonos alhálózatban lévő gépek), rendszerelemek vírusellenőrzéséről, illetve a vírus eltávolítását követően adatvesztés vagy sérülés esetén az állományok, illetve konfigurációk mentésből történő visszaállításáról.

A sikeres helyreállítást követően az IT üzemeltető jelzése nyomán a Jegyző hirdeti ki a vírusriadó állapot, valamint az annak időtartama alatt esetlegesen bevezetett ideiglenes védelmi intézkedések alkalmazásának megszüntetését.

28.4 Az elektronikus információs rendszer felügyelete

A Hivatal az általa használt, a felügyelete, irányítása alatt lévő EIR-ek, illetve rendszerelemeik esetében a 29.1 Naplózási eljárásrend, a 29.6 Naplóvizsgálat és jelentéskészítés, valamint a 27. Hozzáférés ellenőrzése fejezetekben meghatározott tevékenységekkel biztosítja az EIR felügyeletét.

Az EIR rendellenes működése, jogosulatlan használat, illetve hozzáférés észlelése vagy gyanúja esetén a Hivatal a 15. A biztonsági események kezelése fejezetben előírt eljárásrendet követi. Fokozott kockázatra utaló jel észlelése esetén a Hivatal az EIR felügyeletét a naplóvizsgálati gyakoriság növelésével erősíti meg.

A hálózat védelmére alkalmazott eszközökből (pl.: tűzfal) kinyert információk jogosulatlan hozzáférés, módosítás és törlés elleni védelmét a Hivatal a 29.8 A naplóinformációk védelme fejezetben meghatározott módon biztosítja.

Az EIR-ek felügyeletével kapcsolatban rendelkezésre álló felügyeleti információkhoz történő hozzáférést az információbiztonsági felelős számára, annak éves felülvizsgálati tevékenységéhez, illetve eseti jelleggel a bekövetkezett biztonsági esemény értékeléséhez, kivizsgálásához, illetve bejelentéséhez az IT üzemeltető, illetve az adott EIR felügyeleti információihoz hozzáféréssel rendelkező, azok kezelésével megbízott (pl.: tenant admin, honlap adminisztrátora, stb.) köteles biztosítani.

28.5 Biztonsági riasztások és tájékoztatások

Az információbiztonsági felelős folyamatosan figyelemmel kíséri a GovCert, illetve a NEIH által kiadott, a Hivatal által használt EIR-eket és rendszerelemeket érintő fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információkat, az e szervezetek által kiadott biztonsági riasztásokat, s jelzi a Hivatal, illetve az IT üzemeltető felé a szükséges védelmi intézkedések megtétele céljából.

Az információbiztonsági felelős feladata a fenti, illetve a jogszabályban meghatározott további szervekkel való kapcsolattartás a 17.1 Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és az e célt szolgáló ágazati szervezetekkel fejezetben, valamint a bejelentési kötelezettség teljesítése és az incidens kezelésének szakmai irányítása a 15. A biztonsági események kezelése fejezetben meghatározottak szerint.

28.6 A kimeneti információ kezelése és megőrzése

A Hivatal az általa használt EIR-ek kimeneti információinak kezelését, megőrzését, illetve archiválását a hatályos és vonatkozó jogszabályi előírásoknak, illetve az adott EIR tulajdonosa által meghatározott üzemeltetési és felhasználási követelményeknek megfelelően köteles végezni. Az információbiztonsági felelős jogosult felülvizsgálati tevékenysége keretében ezek megfelelő betartását ellenőrizni.

29 NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG

29.1 Naplózási eljárásrend

A Hivatal az általa használt EIR-ek naplózásával kapcsolatos eljárásrendet jelen fő fejezetben, az alábbiak szerint határozza meg.

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomások, kiszolgálók és a felügyelete alá tartozó további (pl.: hálózati) eszközök esetében az IT üzemeltető, illetve az adott EIR vagy rendszereleme naplózási beállításaihoz hozzáféréssel rendelkező, azok kezelésével megbízott (pl.: tenant admin, honlap adminisztrátora, stb.) jogosult és köteles a jelen fejezetben meghatározott naplózási beállításokat a 23. Konfigurációkezelés fejezetben előírt szabályok szerint végrehajtani.

29.2 Naplózható események

A Hivatal az általa üzemeltetett, a felügyelete, irányítása alatt lévő EIR-ek, illetve rendszerelemeik esetében a naplózható, illetve naplózandó biztonsági események körét az alábbiakban határozza meg:

Rendszeresemények:

- indítás,
- leállás/leállítás,
- hiba,
- szoftver telepítés,
- szoftver eltávolítás,
- konfiguráció módosítása.

Felhasználói hozzáféréssel kapcsolatos események:

- sikeres bejelentkezés,
- sikertelen bejelentkezés,
- kijelentkezés,
- jelszóváltoztatás.

Felhasználói hozzáféréseken (fiók, csoport) végzett műveletek:

- létrehozás,
- módosítás,
- engedélyezés,
- letiltás,
- törlés.

Hálózati forgalommal kapcsolatos események:

- megvalósult kapcsolat,
- blokkolt kapcsolat.

Naplózással kapcsolatos események (sikeres és sikertelen):

- elindítás,

- leállítás,
- újraindítás,
- beállítások módosítása,
- napló kiürítése, törlése,
- naplóvesztés lehetősége (pl.: tárhely kapacitás elfogyás).

Az információbiztonsági felelős jogosult a naplózható események, illetve az adott EIR-ben naplózásra beállított események körének (naplórend) felülvizsgálatára, s a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához szükség szerint további események naplózására, a naplórend módosítására javaslatot tenni.

29.3 Naplóbejegyzések tartalma

A Hivatal az általa üzemeltetett, a felügyelete, irányítása alatt lévő EIR-ek, illetve rendszerelemeik esetében kizárólag olyan naplózási funkcionalitással rendelkező rendszerelem beszerzését, illetve alkalmazását engedélyezi, amely biztosítja, hogy a naplóbejegyzés tartalmazza legalább az alábbi információkat:

- minden eseménnyel kapcsolatban az esemény időpontját, típusát, keletkezésének helyét (mely komponens generálta az eseményt), kimenetelét (siker vagy hiba), s amennyiben lehetséges, akkor a műveletet kezdeményező, illetve végrehajtó (felhasználói, szolgáltatás, stb.) fiók azonosító adatait;
- hibaeseménnyel kapcsolatban a hibát okozó komponens vagy művelet megnevezését, a hiba következményeit;
- hálózati eseménnyel kapcsolatban a forrás és cél beazonosításához szükséges adatokat (pl.: hálózati cím, port).

A Hivatal a saját fejlesztésű új EIR esetében követelményként előírja, hogy az a naplóbejegyzésekben az esemény vizsgálatához szükséges és elégséges fent meghatározott minimális információkat legyen képes rögzíteni. A követelmények teljesülését az információbiztonsági felelős a 22.1 Tesztelési, képzési és felügyeleti eljárások fejezetben meghatározottak szerint jogosult ellenőrizni.

29.4 Napló tárkapacitás

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomások, kiszolgálók és a felügyelete alá tartozó további (pl.: hálózati) eszközök konfigurálását az IT üzemeltetőúgy kell, hogy elvégezze, hogy azokon a naplóinformációk helyi eseménynaplóban történő rögzítéséhez, a naplóállományok helyben történő tárolásához szükséges tárkapacitás rendelkezésre álljon a 29.9 A naplóbejegyzések megőrzése fejezetben meghatározott időtartamig.

29.5 Naplózási hiba kezelése

A Hivatal a saját fejlesztésű új EIR esetében követelményként előírja, hogy az naplózási hiba esetén legyen képes riasztást küldeni (pl.: email) a felügyeletével megbízott személy számára, illetve biztosítsa a legrégebbi naplóbejegyzések felülírását, a naplózási folyamat leállítását vagy újraindítását. A követelmények teljesülését az információbiztonsági felelős a 22.1 Tesztelési, képzési és felügyeleti eljárások fejezetben meghatározottak szerint jogosult ellenőrizni.

A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR-ek esetében a Hivatal (az EIR naplózási beállításaihoz hozzáféréssel rendelkező, azok kezelésével megbízott) a rendszer tulajdonosa által meghatározott naplózási hibakezelési szabályokat, illetve funkciókat alkalmazza.

29.6 Naplóvizsgálat és jelentéskészítés

Az IT üzemeltető köteles a naplóbejegyzések felülvizsgálatát, elemzését a nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából legalább havi rendszerességgel elvégezni, s amennyiben problémát tapasztal, akkor az információbiztonsági felelőst tájékoztatni.

A 28.5 Biztonsági riasztások és tájékoztatások fejezetben foglaltak szerint, fokozott kockázatra utaló jelzés esetén az információbiztonsági felelős kérheti a naplózandó események körének kibővítését, a naplóbejegyzések vizsgálatának gyakrabban történő végrehajtását, illetve a rendelkezésre álló felügyeleti információkhoz történő hozzáférés biztosítását, melyben az IT üzemeltető, illetve az adott EIR felügyeleti információihoz hozzáféréssel rendelkező, azok kezelésével megbízott (pl.: tenant admin, honlap adminisztrátora, stb.) köteles közreműködni.

29.7 Időbélyegek

A Hivatal az általa üzemeltetett, a felügyelete, irányítása alatt lévő EIR-ek, illetve rendszerelemeik esetében kizárólag olyan rendszerelem beszerzését, illetve alkalmazását engedélyezi, amely belső rendszerórát használ a naplóbejegyzések időbélyegeinek előállításához, saját fejlesztésű új EIR esetében pedig követelményként írja elő, hogy az rendelkezzen e funkcióval. A követelmények teljesülését az információbiztonsági felelős a 22.1 Tesztelési, képzési és felügyeleti eljárások fejezetben meghatározottak szerint jogosult ellenőrizni.

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomások, kiszolgálók és a felügyelete alá tartozó további (pl.: hálózati) eszközök esetében annak érdekében, hogy azok rendszerórái folyamatosan szinkronban legyenek az IT üzemeltető feladata minden eszközre egységesen megbízható, központi időforrás alkalmazásának konfigurálása.

29.8 A naplóinformációk védelme

A naplóinformációk jogosulatlan hozzáféréssel, módosítással és törléssel szembeni védelmét a Hivatal azon felügyelete alá tartozó EIR-ek, illetve rendszerelemeik esetében, amelyeknél a naplózási beállítások, illetve a naplóinformációk kezelése a hatáskörébe tartozik, a naplóbejegyzésekhez történő hozzáférést, illetve a naplózási beállítások módosítását magasabb – kiemelt vagy privilegizált felhasználói – hozzáféréshez, jogosultsághoz kötésével, továbbá e hozzáférésekhez tartozó azonosító, illetve hitelesítő eszközök szabályozott (lásd: 26.5 A hitelesítésre szolgáló eszközök kezelése, illetve 27.3 Hozzáférés ellenőrzés érvényesítése fejezetek), a biztonsági követelményeknek megfelelő kezelésével biztosítja.

A Hivatal az archivált naplóinformációk védelmét elektronikus formában történő tárolásuk esetén hozzáférés- és jogosultsági rendszerrel védett tárterületen történő elhelyezésükkel biztosítja. Mobil adathordozón történő tárolásuk, illetve továbbításuk esetén a 25. Adathordozók védelme, illetve a 30.5 Kriptográfiai védelem fejezetekben előírt vonatkozó védelmi intézkedéseket alkalmazza.

29.9 A naplóbejegyzések megőrzése

A Hivatal által használt, általa üzemeltetett, illetve felügyelete alá tartozó EIR-ek és azon rendszerelemeik esetében, amelyeknél a naplóinformációk kezelése a hatáskörébe tartozik, a biztonsági események utólagos kivizsgálásának biztosítása érdekében a naplóbejegyzések megőrzéséről a Hivatal az alábbiak szerint gondoskodik:

a) a naplóinformációkat helyi eseménynaplóban rögzítő EIR-ek és elemeik esetében a naplózási beállításokat az IT üzemeltető úgy kell, hogy konfigurálja, hogy a naplóállományok helyben tároltan – amennyiben jogszabály a megőrzési időt nem korlátozza – legalább 30 napra visszamenőleg rendelkezésre álljanak;
b) amennyiben a helyi eseménynapló beállításai, illetve a rendelkezésre álló, e célra dedikáltan fenntartható tároló kapacitás a naplózandó események mennyisége miatt ezt nem teszi

lehetővé, abban az esetben a naplózást archiválásra kell beállítani (az idő előtti felülírás elkerülése érdekében), s gondoskodni szükséges az archív naplóállományok legalább 90 napig történő megőrzéséről (hálózati- vagy külső tárolón, illetve a mentési eljárás keretein belül a mentési gyakoriság figyelembe vételével), ha jogszabály a megőrzési időt nem korlátozza;

c) központi naplógyűjtő rendszer alkalmazása esetén, amennyiben a gyűjtés automatizált módon, online vagy ütemezett rendszerességgel biztosított, a helyi (számítógépen történő) naplóállomány archiválás mellőzhető, a naplógyűjtő rendszerben kell – amennyiben jogszabály a megőrzési időt nem korlátozza – legalább 90 napig megőrizni a naplóbejegyzéseket.

29.10 Naplógenerálás

A Hivatal a saját fejlesztésű új EIR esetében megköveteli, illetve új rendszerelem beszerzése során követelményként írja elő, hogy az a 29.2 Naplózható események fejezetben meghatározott, a rendszer típusától függően alkalmazható naplózható eseményekre vonatkozó naplóinformációkat szabványos formában, visszakereshető módon legyen képes előállítani és tárolni, továbbá az audit események naplózásának be-, illetve kikapcsolására biztosítson lehetőséget. A követelmények teljesülését az információbiztonsági felelős a 22.1 Tesztelési, képzési és felügyeleti eljárások fejezetben meghatározottak szerint jogosult ellenőrizni.

30 RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM

30.1 Rendszer- és kommunikációvédelmi eljárásrend

A Hivatal az általa használt EIR-ekkel kapcsolatban a rendszer- és kommunikációvédelmi eljárásrendet jelen fő fejezetben, az alábbiak szerint határozza meg.

30.2 Túlterhelés – szolgáltatás megtagadás alapú támadás – elleni védelem

A Hivatal a szolgáltatás megtagadás alapú támadások elleni védelem érdekében a hálózati-, illetve internet szolgáltatást nyújtó szerződéses partnere kiválasztása során előnyben részesíti azon szolgáltatókat, amelyek a hálózati túlterheléses támadások kivédésére saját megoldással, illetve megfelelő kapacitásokkal rendelkeznek.

A Hivatal a 23.7 Legszűkebb funkcionalitás, a 23.9 A szoftverhasználat korlátozásai, a 23.10 A felhasználó által telepített szoftverek, valamint a 28.3 Kártékony kódok elleni védelem fejezetekben meghatározott védelmi intézkedésekkel gondoskodik a felhasználói tevékenységek korlátozásáról és az általa használt EIR-ek védelméről, hogy belső hálózatából ne indíthassanak szolgáltatás megtagadás típusú támadásokat más rendszerek vagy hálózatok ellen.

Szolgáltatás megtagadás jellegű, túlterheléses támadás gyanúja, illetve észlelése esetén a Hivatal a 15. A biztonsági események kezelése fejezetben foglaltak szerint jár el.

30.3 A határok védelme

A Hivatal a belső hálózat védelmének biztosítása érdekében határvédelmi megoldást (tűzfal) alkalmaz a hálózati forgalom felügyeletére, irányítására. A határvédelmi eszköznek minimálisan az alábbi biztonsági funkciókat kell ellátnia:

- végezzen címfordítást a belső, nem nyilvános és a külső hálózati címek között;
- a 23.7 Legszűkebb funkcionalitás fejezetben előírtakkal összhangban alapból tiltania kell és csak kivételként engedélyezhet bármely hálózati forgalmat;
- csak a protokoll és port szinten jóváhagyott kommunikációt engedheti át;

- utólag visszakereshető módon, szabványos formátumban naplózza a sikeres, engedélyezett, illetve a blokkolt hálózati forgalom leíró adatait (forrás-, cél cím; port, protokoll, időpont, stb.).

A naplózás, illetve naplóállományok kezelésére vonatkozó részletes előírásokat a 29. Naplózás és elszámoltathatóság fejezet tartalmazza.

A határvédelmi eszköz adminisztrálása a védett, belső hálózatból, illetve távoli hozzáférés esetén csak biztonságos kommunikációs csatornán keresztül engedélyezett.

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomások és kiszolgálók kizárólag a határvédelmi eszközön felügyelt interfészeken keresztül kapcsolódhatnak külső hálózatokhoz vagy külső elektronikus információs rendszerekhez (lásd: 19.3 Külső kapcsolódásokra vonatkozó korlátozások).

Amennyiben a Hivatal nyilvánosan hozzáférhető rendszerelemeket (pl.: web kiszolgáló szervert) üzemeltet, azt a belső hivatali hálózattól elkülönített, logikailag szeparált alhálózatban helyezi el, hálózati irányonként – belső, illetve külső – külön fizikai csatoló interfészekkel. A rendszerelemek, valamint a logikai elválasztás konfigurálása az e célra szolgáló, menedzselhető hálózati eszközön az IT üzemeltető feladata.

30.4 Kriptográfiai kulcs előállítása és kezelése

Amennyiben a Hivatal által használt EIR nyilvános kulcsú infrastruktúrát (PKI) alkalmaz, a kulcsok generálása és kezelése a 26.5 A hitelesítésre szolgáló eszközök kezelése fejezetben előírtaknak megfelelően történhet.

A követelmények teljesülését az információbiztonsági felelős felülvizsgálati tevékenysége keretében jogosult ellenőrizni.

30.5 Kriptográfiai védelem

A Hivatal az általa üzemeltetett, a felügyelete, irányítása alatt lévő EIR-ek, illetve rendszerelemeik esetében kriptográfiai védelmet biztosító megoldást a mobil adattároló és beépített adathordozót tartalmazó mobil eszközök esetében a 25.2 Hozzáférés az adathordozókhoz, a felhasználói azonosítók és jelszavak elektronikus tárolása, nyilvántartása esetén a 26.5 A hitelesítésre szolgáló eszközök kezelése, valamint a távoli hozzáféréshez használt titkosított adatátviteli csatorna esetében, a 27.7 Távoli hozzáférés fejezetben meghatározottak szerint alkalmaz.

A kriptográfiai védelem megvalósítása az eszköz e célt szolgáló funkciójának használatával történhet (pl.: BitLocker meghajtótitkosítás, VPN), melyek esetében a technológia (pl.: OpenVPN, SSTP, stb.), illetve az általa alkalmazott rejtjelezési algoritmus (pl.: AES) megfelelősége nemzetközileg elismert információbiztonsági szabvány alapján (pl.: CC, FIPS) igazolt.

30.6 Együttműködésen alapuló számítástechnikai eszközök

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomásokon kizárólag abban az esetben engedélyezett együttműködésen alapuló számítástechnikai eszközök (pl.: kamera, mikrofon) használata, amennyiben a hivatali munkavégzés, illetve az adott EIR használata (pl.: kommunikáció) céljából indokolt. A funkciót biztosító eszközzel (alkalmazás, szoftver) szembeni követelmény, hogy közvetlen kijelzést nyújtson a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.

Az alkalmazni kívánt eszköz megfelelőségét az IT üzemeltető közreműködésével az információbiztonsági felelős jogosult előzetesen ellenőrizni, s a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben meghatározottak szerint a Jegyző engedélyezi.

30.7 Biztonságos név/cím feloldó szolgáltatások (úgynevezett hiteles forrás)

A Hivatal név/cím feloldási szolgáltatást külső, informatikai, illetve telekommunikációs szolgáltató partnertől vesz igénybe.

A Hivatal saját fejlesztésű új EIR esetében követelményként előírja, hogy az a név/cím feloldási kérésekre a hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozó kiegészítő adatokat is biztosítson, illetve amennyiben egy elosztott, hierarchikus névtár részeként működik, akkor jelezze az utódtartományok biztonsági állapotát is, és (ha azok támogatják a biztonságos feloldási szolgáltatásokat) hitelesítse az utód- és elődtartományok közötti bizalmi láncot.

30.8 Biztonságos név/cím feloldó szolgáltatás (úgynevezett rekurzív vagy gyorsító tárat használó feloldás)

A Hivatal név/cím feloldási szolgáltatást külső, informatikai, illetve telekommunikációs szolgáltató partnertől vesz igénybe.

A Hivatal saját fejlesztésű új EIR esetében követelményként előírja, hogy az eredethitelesítést és adatsértetlenség ellenőrzést kérjen és hajtson végre a hiteles forrásból származó név/cím feloldó válaszokra.

30.9 Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

A Hivatal név/cím feloldási szolgáltatást külső, informatikai, illetve telekommunikációs szolgáltató partnertől vesz igénybe. A szolgáltatás igénybe vételének feltétele, hogy a szolgáltató biztosítson elsődleges és másodlagos (tartalék) kiszolgálót. A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomásokon, kiszolgálókon, illetve hálózati eszközökön a szolgáltatás igénybevételéhez szükséges beállítások dokumentált elvégzése a 23.6 Konfigurációs beállítások fejezet előírásainak alkalmazásával az IT üzemeltető feladata.

30.10 A folyamatok elkülönítése

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomásokon és kiszolgálókon kizárólag olyan rendszer (operációs rendszer) működtetése engedélyezett, amely elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára, azaz képes több különböző biztonsági szinten, egymástól szeparáltan a folyamatok futtatására (pl.: user, system, kernel, stb.). Az ismert, kereskedelmi forgalomban kapható operációs rendszerek (Microsoft, MacOS, illetve Linux verziók) alkalmazzák e technológiát, illetve további kernel- és/vagy memóriavédelmi megoldásokat szintén (pl.: DEP, ASLR, NX, stb.).

A Hivatal saját fejlesztésű új EIR esetében követelményként írja elő, hogy az legyen funkcionálisan kompatibilis a fentiek szerinti védelmet biztosító alaprendszerrel (operációs rendszer).

31 ZÁRÓ RENDELKEZÉSEK

Az IBSZ kiadása napján lép hatályba és visszavonásig érvényes.

Az IBSZ rendelkezéseit minden, a személyi hatálya alá tartozó köteles betartani. A szabályzatban foglaltak be nem tartása esetén a Hivatal jogosult hátrányos jogkövetkezményeket alkalmazni.

Jelen Informatikai Biztonsági Szabályzat hatálybalépésével egyidejűleg a korábban kiadott Informatikai Biztonsági Szabályzat hatályát veszti.

1. SZÁMÚ MELLÉKLET – AZ INFORMÁCIÓBIZTONSÁG SZEREPLŐI

Szerepkör	**Név, elérhetőség** (telefonszám, email cím)
Jegyző	dr. Berta Edina +36 30/2329-450 jegyzo@kislang.hu
Információbiztonsági felelős	Bihari Emil +36 70/6036-604 bihari.emil@hanganov.hu
IT üzemeltető	
Az IBSZ hatálya alá tartozó és végrehajtásáért felelős további, a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban lévő szervezetek, személyek	A Hivatal munkavállalói a Belépésre jogosultak nyilvántartásában szerepelnek (7. számú melléklet), a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban lévő szervezetek, személyek pedig Az elektronikus információs rendszerek nyilvántartásában (3. számú melléklet) kerülnek rögzítésre.

2. SZÁMÚ MELLÉKLET – MEGISMERÉSI NYILATKOZAT

Az Informatikai Biztonsági Szabályzatban foglalt előírásokat, szabályokat megismertem és tudomásul veszem, hogy azokat munkavégzésem során köteles vagyok betartani.

Dátum	Név	Beosztás/munkakör	Aláírás

3. SZÁMÚ MELLÉKLET – AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK NYILVÁNTARTÁSA

Hivatal megnevezése:	Kislángi Polgármesteri Hivatal

Sorszám / Azonosító (pl.: sorfolytonos számozás: 1, 2, 3…)		
EIR megnevezése (szakrendszer, szoftver neve és/vagy elérési útja: URL)		
EIR alapfeladatai (pl.: a szervezet mely szakterületi feladatát / ügycsoportját támogatja)		
Az EIR által biztosítandó szolgáltatások (a rendszer rendeltetése, hivatali folyamat rövid leírása)		
Licence darabszám (amennyiben a szervezet kezeli)		
EIR felügyeletét gyakorló személy adatai (név, beosztás, elérhetőség: telefonszám, email cím)		
EIR típusa (helyi / központi) (központi: jogszabályban előírt, illetve központi közreműködő szolgáltatótól igénybe vett; helyi: a szervezet által üzemeltetett rendszer)		
EIR működési környezete (számítógépre telepített kliens alkalmazással működik / hálózaton keresztül elérhető: internetböngésző programban)		
EIR adatkezelése (helyi / központi / mindkettő) (helyi gépen tárol adatokat / nem tárol: központi, online adatkezelés)		
EIR adattartalma (személyes / különleges adatot tartalmaz / nem tartalmaz)		
Az EIR biztonsági osztály besorolása (az EIR-ben kezelt adatokért felelős, az „adatgazda" köteles a besorolást elvégezni és megadni)	**Bizalmasság**	
	Sértetlenség	
	Rendelkezésre állás	
EIR szállító, fejlesztő és karbantartó szervezet(ek) és kapcsolattartó személyek azonosító és elérhetőségi adatai (név, email cím, telefonszám)		

Kitöltési útmutató

Elektronikus információs rendszerenként kötelező kitölteni!

Sorszám / Azonosító

Az EIR-ek Hivatalon belüli egyértelmű azonosítását, megkülönböztetését szolgálhatja – az EIR hivatkozható a sorszám/azonosító használatával más dokumentumokban, nyilvántartásokban.

EIR megnevezése

Az EIR megnevezése lehet a szoftver vagy rendszer általánosan használt neve, nevének rövidítése (pl.: ÖNKADÓ) és/vagy az internetes elérési útja (pl.: njt.hu), ami egyértelműen meghatározza, hogy mely rendszerről van szó.

EIR alapfeladatai

Azon önkormányzati – a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény 13.§-ban meghatározott vagy a Hivatal Alapító Okiratában, illetve SZMSZ-ben nevesített – kötelező vagy önként vállalt feladat(ok), melyekhez az EIR használata támogatást biztosít (pl.: szociális szolgáltatások és ellátások – gyermekvédelmi támogatásban részesülők természetbeni juttatása).

Az EIR által biztosítandó szolgáltatások

A rendszer rendeltetése, hivatali folyamat rövid leírása (pl.: új szociális ellátási igénylés adatainak rögzítése, nyilvántartása és kezelése).

Licence darabszám

Abban az esetben töltendő, ha a Hivatal vásárolt vagy fejlesztetett valamilyen programot, amelyhez felhasználói licence-ket kapott (pl.: az elsőfokú építésügyi hatóság és a hozzá tartozó települések teljes építésügyi feladatainak számítógépes támogatását, nyilvántartását, az építéshatósági eljárás lefolytatásához szükséges iratok, határozatok, értesítések, végzések, megkeresések előállítását, tárolását végző Tégla2 nevű kereskedelmi szoftver).

EIR felügyeletét gyakorló személy adatai

Azon munkavállaló adatai kerülhetnek ide, aki például az adott rendszer használatához kiemelt jogosultságokkal rendelkezik (pl.: felvehet új felhasználókat, ellenőrizheti a rögzített adatokat vagy a végrehajtott módosításokat; ASP esetében ilyen funkció például a tenant admin hozzáférés).

EIR típusa (helyi / központi)

Központinak minősül, amennyiben a Hivatal jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltatót, illetve központi adatkezelőt és adatfeldolgozó szolgáltatót vesz igénybe. Jellemzően központi minden olyan központi szerv által fejlesztett, illetve biztosított alkalmazás és rendszer, amelyek használata a Hivatal számára kötelezően előírt vagy ajánlott (pl.: amiatt, mert az abban készült jelentést vagy az azon keresztül beküldött adatokat fogadja el az adott központi szerv vagy hatóság), mint például a KSH Elektra, a Takarnet. Helyi általában a Hivatal által vásárolt kereskedelmi szoftver (pl.: Tégla2), esetleg hasonló célra fejlesztetett egyedi alkalmazás.

EIR működési környezete

Számítógépre telepített kliens alkalmazáson keresztül működik például az ÁNYK (Abevjava) vagy az ONKADO. Hálózatos (internetes) működésűek például a KIR, a KSH Elektra, a Takarnet, stb.

EIR adatkezelése (helyi / központi / mindkettő)

Az előző ponttal jellemzően összefüggő módon a számítógépre telepített programok általában tárolnak helyben is adatokat (lásd pl.: ÁNYK kitöltött nyomtatványai, törzsadatai, mellékelt dokumentumai vagy a beküldött .kr fájlok), míg az interneten keresztül elérhetőek általában nem, azoknál jellemzőbb a központi adattárolás, viszont kimeneti fájlok (pl.: kinyomtatott vagy letölthető, illetve PDF állományba menthető) ezeknél is előfordulhatnak, amely esetekben a „mindkettő" érték megadása szükséges!

EIR adattartalma

Azt kell itt megadni, hogy milyen típusú adatok kezelése történik az adott EIR-ben? Ennek jelentősége az adott EIR biztonsági osztályba sorolása, az EIR-rel összefüggő kockázatok elemzése során jelentkezik.

Az EIR biztonsági osztály besorolása

A központilag biztosított szakrendszerek (pl.: ASP) esetében a működtető végzi el az EIR biztonsági osztályba sorolását, majd azt közzéteszi a felhasználók, így a Hivatal felé. Ennek megfelelően a működtető által adott besorolást kell itt szerepeltetni. A saját működtetésű, a Hivatal által fejlesztetett, illetve üzemeltetett rendszerek esetében – függetlenül attól, hogy esetleg a központilag biztosított szakrendszerhez automatikus adatátadással kapcsolódik-e vagy sem – a Hivatal köteles elvégezni a biztonsági osztályba sorolást.

EIR szállító, fejlesztő és karbantartó szervezet(ek) és kapcsolattartó személyek azonosító és elérhetőségi adatai

A „Szállító" központilag biztosított szakrendszer esetén a működtető (pl.: ASP esetében a MÁK), saját működtetésű rendszer esetén az adott rendszert, illetve szoftvert biztosító (kereskedelmi szoftver esetén az eladó vagy disztribútor). Előfordulhat, hogy adott esetben a „Szállító" és a „Fejlesztő" is ugyanaz a szereplő vagy cég. Amennyiben szoftver követés, felhasználói támogatás is együtt jár az adott rendszer felhasználására kötött, fennálló megállapodásban, szerződésben, illetve licence-ben, akkor itt az ismert kapcsolattartó (ha van külön kijelölt, dedikált személy), annak hiányában az adott cég vagy szervezet felelős vezetőjének adatait megjeleníteni. Ha nem nevesített a támogató személye (pl.: Helpdesk vagy Ügyfélszolgálat), akkor annak elérhetőségeit kell itt szerepeltetni.

4. SZÁMÚ MELLÉKLET – VÁLTOZÁSKEZELÉSI ADATLAP

I. Változás/igény bejelentés adatai *(a változást kezdeményező/igénylő tölti ki)*

Változást kezdeményező/igénylő/bejelentő adatai	
Név	***Beosztás/munkakör***
Változás/igény adatai	
Változás/igény típusa (a megfelelőt jelölje X-szel)	
1. Új infokommunikációs eszköz igénylése (pl.: számítógép, telefon)	
2. Hozzáférés, jogosultság beállítása/módosítása, konfiguráció megváltoztatása (pl.: felhasználói fiók létrehozása, törlése, rendszer vagy rendszerelem beállításainak módosítása)	
3. Hivatali – az elektronikus információs rendszereknek helyt adó – létesítményekbe, helyiségekbe történő belépés engedélyezése (pl.: karbantartás céljából eseti belépés – lásd: 5. pont)	
4. Információs rendszerelem be- és kiszállítása (pl.: hardver szállítás – 3. pont is kell hozzá!)	
5. Karbantartás, javítás (pl.: hardver csere, bővítés), valamint a munkavégzés engedélyezése (3. pont is kell hozzá!)	
6. Elektronikus adathordozók használata (pl.: CD/DVD írás, USB pendrive használat, stb.)	
7. Távoli, illetve vezeték nélküli hozzáférés biztosítása	
8. Együttműködésen alapuló számítástechnikai eszközök használata (pl.: audio és/vagy video kommunikációra alkalmas eszköz használatának engedélyezése)	
9. Új elektronikus információs rendszer bevezetése	
10. Új rendszerelem meglévő elektronikus információs rendszerbe illesztése (pl.: program telepítése, hardver bővítés, stb.)	
11. Az alkalmazott elektronikus információs rendszer más (helyi, illetve külső) elektronikus információs rendszer(ek)hez történő kapcsolódása	
A változás/igény részletes leírása (pl.: igényelt eszköz, szoftver típusa, paraméterei vagy a belépés tervezett időpontja, stb.)	
Változás/igény bejelentés időpontja (dátum):	

II. Változás/igény engedélyezésének adatai *(a változást jóváhagyó, engedélyező tölti ki)*

A változást/igényt **engedélyezem / nem engedélyezem**.	
(a megfelelő aláhúzandó)	
Az engedélyezett változás végrehajtásáért felelős neve (pl.: IT üzemeltető vagy a belépést felügyelő munkatárs, stb.):	
Változás végrehajtásának határideje (dátum):	
Dátum:	
aláírás	

5. SZÁMÚ MELLÉKLET – AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK MENTÉSE

I. Rendszeres mentés adatai

(EIR-enként kötelező kitölteni az alábbi tartalommal!)

EIR azonosítója (amennyiben az EIR nyilvántartásban alkalmazták)		
EIR megnevezése		
Mentendő adatok köre (pl.: rendszer fájlok, konfigurációs állományok, napló állományok, alkalmazás adatok, adatbázis fájlok, teljes partíció, stb.)		
Mentendő adatok elérési útja (pl.: gépnév/könyvtár felsorolás)		
Mentési gyakoriság		óra/nap/hét/hónap *(a megfelelő aláhúzandó)*
Megőrzési idő (online tárolás: a mentésre használt eszközön gyorsan elérhető módon)		nap/hét/hónap/év *(a megfelelő aláhúzandó)*
Online mentés célja, adathordozó típusa (pl.: fájl szerver, NAS, belső vagy külső merevlemez, szalagos média, optikai adathordozó: DVD, CD)		
Archivált állományok, illetve mentési adathordozók megőrzési ideje (offline tárolás)		nap/hét/hónap/év *(a megfelelő aláhúzandó)*
Archiválásra használt adathordozó típusa (pl.: külső merevlemez, szalagos média, optikai adathordozó: DVD, CD)		
Elsődleges tárolási helyszín (az archiválásra használt, offline adathordozók tárolásának helye, pl.: Jegyző páncélszekrénye)		
Másodlagos tárolási helyszín (üzemeltetési szerződés tartalma alapján lehet például a Kormányzati Adattrezor vagy az IT üzemeltető székhelye, telephelye)		

II. Mentési/visszatöltési napló

A mentési naplóban minden eseti biztonsági mentés, minden sikertelen rendszeres mentés, valamint helyreállítási vagy tesztelési célból végrehajtott visszatöltési művelet adatait kötelező rögzíteni.

Dátum	**Művelet iránya** (mentés / visszatöltés)	**Adatok köre***	**Adatok elérési útja**	**Mentési adathordozó típusa****	**Mentési adathordozó azonosítója (címkéje)****	**Mentési adathordozó megőrzési ideje****	**Művelet eredménye** (sikeres / sikertelen)

** Amennyiben az I. Rendszeres mentés adatai nyilvántartásban az EIR egyedi azonosítóval került rögzítésre, itt elegendő az azonosító hivatkozása.*

*** Eseti biztonsági mentés alkalmával kötelező kitölteni!*

6. SZÁMÚ MELLÉKLET – ÜZLETMENET-FOLYTONOSSÁGI TERV INFORMATIKAI ERŐFORRÁS KIESÉSEKRE

I. Az informatikai erőforrás kiesés által érintett EIR adatai

(EIR-enként kötelező kitölteni az alábbi tartalommal!)

Sorszám			
I.1	**EIR azonosítója**		
I.2	**EIR megnevezése**		
I.3	Informatikai erőforrás kiesés által érintett alapfeladatok, funkciók, a probléma leírása (pl.: mely, az adott EIR által támogatott hivatali feladat ellátását akadályozza az adott rendszer, illetve rendszerelem kiesése).		
I.4	A kiesés, illetve helyreállítás Hivatal által elfogadható, tolerálható maximális időtartama (helyreállítási idő: H)		perc/óra/nap *(a megfelelő aláhúzandó)*

A tervben az üzletmenet-folytonossági, illetve az alternatív hivatali folyamatokra való átállás intézkedéseire adott határidők a hiba vagy esemény észlelésétől, az eredeti hivatali folyamat visszaállításához szükséges határidők a hiba vagy esemény elhárításától számítva értendők (T-vel az esemény bekövetkezésének időpontja, H-val pedig a helyreállításhoz szükséges, illetve maximálisan tolerálható időtartam került jelölésre).

II. Üzletmenet-folytonossági intézkedések

Sorszám	Intézkedés	Felelős	Határidő
II.1	Helyettesítő eljárás alkalmazásának elrendelése	Jegyző	T
II.2	Az IT üzemeltető értesítése	Észlelő (munkatárs) / Jegyző	T+15 perc
II.3	Helyettesítő eljárások alkalmazása	Kijelölt hivatali munkatársak	T+H
II.4	Helyreállítás	IT Üzemeltető	T+H

III. Alternatív üzletmenet

Előfeltételek:

- megfelelően felkészített, képzett hivatali munkatársak, akik képesek a III.1. Helyettesítő eljárás táblázatban jelölt feladatok (pl.: kézi adatrögzítés, illetve iktatás) végrehajtására;
- a helyreállításhoz szükséges tartalék erőforrások;

III.1. Helyettesítő eljárás(ok)

Helyettesítő eljárás megnevezése, leírása	**Végrehajtásért felelős** (kijelölt hivatali munkatárs neve vagy minden hivatali munkatárs)

III.2. Tartalék erőforrások

Tartalék erőforrás megnevezése	**Felelős** (az erőforrás rendelkezésre állásáért felelős neve)

III.3. Helyreállítás

Sorszám	**Intézkedés megnevezése, leírása**
1	
2	
3	
4	
5	
6	

Sorszám	**Intézkedés**	**Felelős**	**Határidő**
III.3.1	A tartalék erőforrások használatával a helyreállítás végrehajtásának megkezdése.	IT Üzemeltető	T+15 perc
III.3.2	Helyreállítással kapcsolatos intézkedések végrehajtása – az erőforrás kiesés típusának, jellegének függvényében (pl.: telekommunikációs szolgáltató értesítése, tartalék munkaállomás beüzemelése, szoftver telepítés, mentésből történő adat helyreállítás, tesztelés, stb.)	IT Üzemeltető	T+H

IV. Visszaállás a normál folyamatokra

Előfeltétel:

- az informatikai erőforrás kiesés megszűnése (a hiba kijavítása), az érintett rendszer, rendszerelem helyreállítása, működésének tesztelése, ismételt rendelkezésre állása.

Sorszám	Intézkedés	Felelős	Határidő
IV.1	Visszaállás elrendelése	Jegyző	H+15 perc
IV.2	A helyettesítő eljárás alkalmazása során keletkezett információk normál folyamatok számára történő biztosítása (pl.: utólagos rögzítés).	Kijelölt hivatali munkatársak	A rendelkezésre álló kapacitás függvényében a lehető legrövidebb időn belül.

Megismerési záradék

Az üzletmenet-folytonossági tervben foglalt előírásokat megismertem és tudomásul veszem, hogy azokat munkavégzésem során köteles vagyok betartani.

Dátum	Név	Beosztás/munkakör	Aláírás

7. SZÁMÚ MELLÉKLET – BELÉPÉSRE JOGOSULTAK NYILVÁNTARTÁSA

Hivatal megnevezése:	Kislángi Polgármesteri Hivatal
Épület, telephely megnevezése, címe:	
Dátum:	

Név	**Beosztás**	**Szervezet** (belső: KÖH; külső: szervezet megnevezése)

8. SZÁMÚ MELLÉKLET – BELÉPÉSI NAPLÓ

Hivatal megnevezése:	Kislángi Polgármesteri Hivatal
Épület, telephely megnevezése, címe:	
Dátum:	

Név	**Belépés időpontja:**(óra, perc)	**Kilépés időpontja:**(óra, perc)	**Belépés célja:** **Ü**: ügyfél ügyintézés; **L**: látogató (vendég); **SZ**: szerződött partner (pl.: IT üzemeltető, karbantartó)

9. SZÁMÚ MELLÉKLET – INFORMÁCIÓS RENDSZERELEMEK BE- ÉS KISZÁLLÍTÁSÁNAK NYILVÁNTARTÁSA

(Telephelyenként vezetendő!)

Hivatal megnevezése:	Kislángi Polgármesteri Hivatal
Épület, telephely megnevezése, címe:	

Dátum	**Hardver eszköz, rendszerelem megnevezése** (azonosító/sorozatszám/leltári szám – ha van!)	**Szállítás iránya** (jelölje X-el)		**Szállítást végző adatai** (Név/beosztás/szervezet)
		Be	**Ki**	

10. SZÁMÚ MELLÉKLET – ELEKTRONIKUS INFORMÁCIÓS RENDSZERELEM LELTÁR

I. Hardver és vezérlő szoftver eszközök

I.1. Munkaállomások (PC, Notebook)

Azonosító (gépnév)	
Gyártó, típus (brand PC, illetve notebook esetén)	
Processzor (gyártó, típus, órajel)	
Memória (gyártó, típus, méret)	
Tároló kapacitás (gyártó, típus, méret)	
Hálózati csatoló (gyártó, típus, sebesség)	
Operációs rendszer jogtulajdonosa (gyártó / fejlesztő pl.: Microsoft)	
Operációs rendszer megnevezése (pl.: Windows 10 Pro x64)	
A munkaállomásról hozzáférhető EIR-ek megnevezése (amennyiben az EIR nyilvántartásban alkalmazásra került, elegendő az EIR azonosítók felsorolása)	
Beszerzés éve	
Munkaállomás helye (telephely)	

I.2. Központi kiszolgálók (Szerver, NAS)

Azonosító (gépnév)	
Gyártó, típus	
Processzor (gyártó, típus, órajel)	
Memória (gyártó, típus, méret)	
Tároló kapacitás (gyártó, típus, méret)	
Hálózati csatoló 1. (gyártó, típus, sebesség)	
Hálózati csatoló 2. (gyártó, típus, sebesség)	
Hálózati csatoló 3. (gyártó, típus, sebesség)	
Operációs rendszer jogtulajdonosa (gyártó / fejlesztő pl.: Microsoft)	
Operációs rendszer megnevezése (pl.: Windows Server 2012 Std R2)	
Kiszolgáló funkciói (pl.: fájl-, alkalmazás-, nyomtató-,web-, címtár-, névfeloldási-, mentési-, stb.)	
A kiszolgálón üzemeltetett EIR-ek megnevezése (amennyiben az EIR nyilvántartásban alkalmazásra került, elegendő az EIR azonosítók felsorolása)	
Beszerzés éve	
Kiszolgáló helye (telephely)	

I.3. Nyomtatók

Azonosító (eszköz neve)	
Gyártó, típus	
Beszerzés éve	
Eszköz helye (telephely)	

I.4. Hálózati eszközök (switch, router, hardveres tűzfal)

Azonosító (eszköz neve)		
Gyártó, típus		
Vezérlő szoftver verziója (amely az adott eszközön van)	bootware	
	appware	
	firmware	
Beszerzés éve		
Eszköz helye (telephely)		

I.5. Egyéb eszközök (Storage, Tape Library, stb.)

Azonosító (eszköz neve)	
Gyártó, típus	
Beszerzés éve	
Eszköz helye (telephely)	

II. Szoftver licencek

Szoftver jogtulajdonosa (gyártó / fejlesztő)	
Szoftver megnevezése, típusa (pl.: Windows 10 Pro x64)	
Nyelv	
Licence típusa (Felhasználói vagy Eszköz – Per User vagy Per Device)	
Licence száma (db vagy korlátlan)	
Licence érvényessége, lejárata (Pl.: 1 év – pontos lejárati dátum megadásával vagy örökös: nem jár le)	
Eredeti licence konstrukció (OEM / Dobozos / Mennyiségi / Refurbished)	
Számítógép(ek) vagy felhasználó(k) azonosítója (amelyre telepítésre került vagy aki használatára engedélyt kapott) – több esetén felsorolandó	

III. Weboldalak

Weboldal elérhetősége, domain neve (URL)	
Weboldal üzemeltetésének helye (saját szerver, tárhely szolgáltató neve)	
Webmotor típusa (pl.: Drupal, Wordpress, Joomla vagy egyedi fejlesztés)	
Webmotor verzió	
Webadmin neve	
Webadmin telefonszáma	
Webadmin email	

11. SZÁMÚ MELLÉKLET – TITOKTARTÁSI NYILATKOZAT

TITOKTARTÁSI NYILATKOZAT

Alulírott

Név	
Születési hely	
Születési idő	
Anyja neve	
Lakcím	

büntetőjogi és polgári jogi felelősségem tudatában kijelentem, hogy a munkavégzés során tudomásomra jutott, előttem ismertté vált olyan információkról és adatokról illetéktelen szervnek vagy személynek tájékoztatást nem adok, amelyek kiszolgáltatása a Kislángi Polgármesteri Hivatal(a továbbiakban: Hivatal) számára hátrányos vagy jogellenesen előnyös következményekkel járna.

Kijelentem továbbá, hogy tudatában vagyok annak, hogy titoktartási kötelezettségem a munkavégzésre irányuló szerződéses jogviszonyom ideje alatt, valamint annak megszűnését követően időbeli korlátozás nélkül fennáll, valamint, hogy a titoktartási kötelezettség megszegése esetén a hatályos jogszabályok szerint meghatározott jogkövetkezmények alkalmazhatóak velem szemben.

Jelen titoktartási kötelezettség alól felmentést a hatályos jogszabályok figyelembe vételével, kizárólag az adott információ vagy adat tulajdonosának (titokbirtokos) engedélyével, írásos formában a Hivatal erre feljogosított képviselője adhat.

Kelt: Kisláng, 20_____

_____

nyilatkozattevő

12. SZÁMÚ MELLÉKLET – HELYISÉGEK BIZTONSÁGI BESOROLÁSA

Hivatal megnevezése:	Kislángi Polgármesteri Hivatal
Épület, telephely megnevezése, címe:	

Biztonsági zóna[1]	**Biztonsági zónába tartozó helyiség(ek) megnevezése**
Nyitott terület	
Zárt terület	
Védett terület	

[1] Nyitott terület: ügyfelek és látogatók számára nyitott, általuk szabadon hozzáférhető, látogatható helyiségek.
Zárt terület: ügyintézésre, munkavégzésre használt és egyéb zárható, illetve az ügyfelek és látogatók elől elzárt helyiségek. Ide tartoznak a Hivatal által használt EIR-ek elemeinek helyt adó helyiségek.
Védett terület: a zárt területen belül az informatikai erőforrásokat koncentráltan tartalmazó, fokozottan védendő helyiségek. Ide tartozik minden, a Hivatal által használt EIR-ek központi elemeinek helyt adó helyiség (pl.: szerver szoba).