CDSYS
COMPLIANCE DATA SYSTEMS Kft,

A LESENCETOMAJI KÖZÖS ÖNKORMÁNYZATI HIVATAL
INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Lesencetomaj

2018

Kiadva / hatályos: 2018. január 24-től.

Készítette: Compliance Data Systems Kft. az Albacomp információbiztonsági partnere

TARTALOM

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 Lesencetomaji Közös Önkormányzati Hivatal (továbbiakban: Hivatal) információbiztonsága, rendeltetésszerű és biztonságos működése, továbbá a Hivatal által használt elektronikus információs rendszerek (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 (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 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, ezek dokumentálása, továbbá hatósági bejelentése a Jegyző feladata és felelőssége. A kijelölés, illetve visszavonás az alábbi dokumentumokban kerül rögzítésre:

- 3. számú melléklet – Az elektronikus információs rendszerek biztonságáért felelős személy kijelölési dokumentuma
- 4. számú melléklet – Az elektronikus információs rendszerek biztonságáért felelős személy megbízásának visszavonási dokumentuma

Az információbiztonsági felelős a kijelöléssel, illetve annak visszavonásával kapcsolatban előírt bejelentési kötelezettségét a Hivatal által rendelkezésére bocsátott fenti dokumentumok alapján teljesíti.

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: **3**.

A biztonsági szintbe sorolás indoklása:

A Hivatal szakfeladatait támogató elektronikus információs rendszert használ, de nem 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 INTÉZKEDÉSI TERV

A Hivatal a megvalósítandó biztonsági intézkedéseket és azok megvalósításának sorrendjét az elvárt biztonsági szint elérése céljából intézkedési, illetve 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 ELEKTORNIKUS INFORMÁCIÓS RENDSZEREK NYILVÁNTARTÁSA

A Hivatal az általa használt EIR-ekről jelen szabályzat 5. 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 kezdeményezni, illetve 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 (6. számú melléklet – Változáskezelési adatlap) megőrzéséről a Jegyző köteles gondoskodni.

12 KOCKÁZATELEMZÉS

A kockázatok elemzésének rendje, az azzal összefüggő tevékenységek, feladatok és felelősségek ***a Lesencetomaji Közös Önkormányzati Hivatal által használt elektronikus információs rendszerek kockázatelemzési és kockázatkezelési eljárásrendjében*** kerültek rögzítésre.

13 RENDSZER ÉS SZOLGÁLTATÁSBESZERZÉS

A Hivatal saját hatókörében 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-) FOLYTONSSÁG 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 alternatív (tartalék) intézkedéseket, a helyreállításhoz szükséges feladatokat és az azokhoz kapcsolódó prioritásokat, 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 tartalék intézkedéseket;
- 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 alternatív eljárások bevezetésének szükségességét, továbbá az azok alkalmazásához biztosítandó feltételeket (8. 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 (pl.: van az adott eszközből tartalék vagy helyettesíthető mással).

Az informatikai erőforrások kiesésére vonatkozó üzletmenet-folytonossági terv kiadása (hatályba léptetése), az érintettekkel történő megismertetése, a végrehajtásban 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 tartalék intézkedések, 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 és 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:

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

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 (7. számú melléklet – Az elektronikus információs rendszerek mentése) az IT üzemeltető feladata és felelőssége. Az eseti biztonsági mentések, valamint a helyreállítási, illetve tesztelési célú visszatöltések végrehajtásáról az IT üzemeltető köteles a 7. számú melléklet – Az elektronikus információs rendszerek mentése dokumentumban 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