Bodrogkeresztúri Közös Önkormányzati Hivatal

INFORMÁCIÓBIZTONSÁGI SZABÁLYZATA

Jóváhagyta / Kiadta: 2025.11.15.

Dávid Zoltán
jegyző

Verziókövetés			
Kiadás / Hatályba lépés dátuma	**Szerző(k) / Véleményező(k) / Jóváhagyó(k)**	**Verzió**	**Leírás**
2025.11.10.	Bihari Emil, IBF (HANGANOV Kft.)	1.0	Első változat.
2025.11.15.	Dávid Zoltán, jegyző	1.1	Jóváhagyott, kiadott változat.

TARTALOM

A SZABÁLYZAT CÉLJA 4
A SZABÁLYZAT HATÁLYA 4
Személyi hatály 4
Tárgyi hatály 4
Időbeli hatály 4
A SZABÁLYZAT KIADÁSA, KEZELÉSE, FELÜLVIZSGÁLATA 4
INFORMÁCIÓ- és DOKUMENTUMVÉDELEM 5
AZ INFORMÁCIÓBIZTONSÁG SZERVEZETE 5
AZ INFORMÁCIÓBIZTONSÁGGAL KAPCSOLATOS ENGEDÉLYEZÉSI ELJÁRÁS 6
KOCKÁZATMENEDZSMENT 7
Kockázatkezelési stratégia 8
ÜGYMENET-FOLYTONOSSÁG 8
Ügymenet-folytonosságra vonatkozó eljárásrend 9
Esemény felismerése, jelzése 9
Döntés az erőforrás kiesés kezelésének módjáról 9
Veszélyhelyzet elhárítása, visszatérés a normál működési folyamathoz 9
BIZTONSÁGI MENTÉSEK 9
BIZTONSÁGI ESEMÉNYEK KEZELÉSE 10
A biztonsági események jelzése, jelentése 10
A biztonsági események kivizsgálása, értékelése és kezelése (biztonsági eseménykezelési terv) 10
TUDATOSSÁG ÉS KÉPZÉS 11
Biztonságtudatossági képzési eljárásrend 11
RENDSZER- ÉS SZOLGÁLTATÁSBESZERZÉS 12
Fejlesztésre vonatkozó szabályok 12
TERVEZÉS 13
Rendszerbiztonsági terv 13
Viselkedési szabályok 14
NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG 14
Naplózási képesség vizsgálata 14
Naplóbejegyzések tartalma 15
Naplóinformációk megőrzése, védelme 15
Naplózás beállítása, kezelése 16
Naplóbejegyzések vizsgálata 16
Naplózás felülvizsgálata 16
HOZZÁFÉRÉS-FELÜGYELET 16
Felhasználói fiókok kezelése 16
Sikertelen bejelentkezési kísérletek 17
A rendszerhasználat jelzése 17
Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek 17
Távoli hozzáférés 18
Vezeték nélküli hozzáférés 18

Mobil eszközök hozzáférés-ellenőrzése 18
Külső rendszerek használata 18
Nyilvánosan elérhető tartalom 19
AZONOSÍTÁS ÉS HITELESÍTÉS 19
Privilegizált fiókok 20
Azonosító kezelés 20
A hitelesítésre szolgáló eszközök kezelése 20
Újrahitelesítés 21
KONFIGURÁCIÓKEZELÉS 21
Alapkonfiguráció 21
Konfigurációs beállítások 21
Rendszerelem leltár 22
A szoftverhasználat korlátozásai 22
Felhasználó által telepített szoftverek 22
ÉRTÉKELÉS, ENGEDÉLYEZÉS ÉS MONITOROZÁS 23
Biztonsági értékelések 23
Az intézkedési terv és mérföldkövei 24
Engedélyezés 24
Folyamatos felügyelet 24
RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG 24
Kártékony kódok elleni védelem 24
Az elektronikus információs rendszer monitorozása 25
Biztonsági riasztások és tájékoztatások kezelése 25
RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM 26
Szolgáltatásmegtagadással járó támadások elleni védelem 26
A határok védelme 26
Együttműködésen alapuló informatikai eszközök 27
A folyamatok elkülönítése 27
KARBANTARTÁS 27
ADATHORDOZÓK VÉDELME 28
Az adathordozók használati szabályai 28
Az adathordozók törlése 29
FIZIKAI ÉS KÖRNYEZETI VÉDELEM 29
Belépési engedélyek 29
Belépések ellenőrzése 29
Fizikai hozzáférések felügyelete 29
Rendszerelemek be- és kiszállítása 30
Környezeti károk elleni védelem 30
SZEMÉLYI BIZTONSÁG 30
Személybiztonsági feltételek 30
Kiemelt kockázatú munkakörök 31
Eljárás a jogviszony megszűnésekor 31

Az áthelyezések, átirányítások és kirendelések kezelése 32
Fegyelmi intézkedések 32
ZÁRÓ RENDELKEZÉSEK 32

A SZABÁLYZAT CÉLJA

Az Információbiztonsági Szabályzat (a továbbiakban: IBSZ vagy Szabályzat) célja mindazon szervezeti- és rendszerszintű követelmények és szabályok általános meghatározása és egységes, magas szintű szabályozási keretbe foglalása, melyek által a **Bodrogkeresztúri Közös Önkormányzati Hivatal** (a továbbiakban: Hivatal vagy Szervezet) rendeltetésszerű, a mindenkori hatályos jogszabályi előírásoknak megfelelő, eredményes és biztonságos működése, valamint az általa az alaptevékenysége végzéséhez használt elektronikus információs rendszerek (a továbbiakban: EIR), az azokban kezelt adatok és az EIR-ek által nyújtott vagy azokon keresztül elérhető szolgáltatások bizalmassága, sértetlensége és rendelkezésre állása, továbbá az EIR-ek elemeinek sértetlensége és rendelkezésre állása vonatkozásában azok zárt, teljes körű, folytonos és kockázatokkal arányos védelme, s mindezek által a Szervezet kiberbiztonsága folyamatosan fenntartható módon megvalósítható, megőrizhető, illetve továbbfejleszthető.
A Hivatal vezetője elkötelezett a fentiekben rögzített cél eléréséhez, az információbiztonság tervezéséhez, szervezéséhez, irányításához, kockázatokkal arányos megvalósításához, felügyeletéhez, folyamatos fenntartásához és továbbfejlesztéséhez indokolt és megfelelő intézkedések végrehajtása, megvalósítása, valamint az ehhez szükséges erőforrások biztosítása iránt.

A SZABÁLYZAT HATÁLYA

Személyi hatály

A Szabályzat személyi hatálya kiterjed a Hivatal minden foglalkoztatottjára. Kiterjed továbbá mindazon, a Hivatallal munkavégzésre irányuló bármely szerződéses jogviszonyban álló személyekre, akik a Hivatal által használt és rendelkezésében lévő EIR-ek kezelésében (üzemeltetésében, karbantartásában, javításában, fejlesztésében, illetve felügyeletében) részt vesznek.

Tárgyi hatály

A Szabályzat tárgyi hatálya kiterjed a Hivatal rendelkezésében lévő EIR-re, azok rendszerelemeire, valamint az EIR-ekben kezelt adatokra. Kiterjed továbbá a Hivatal által használt EIR-ek, illetve rendszerelemeik dokumentációira.

Időbeli hatály

A Szabályzat a kiadása napján lép hatályba és visszavonásáig hatályos.

A SZABÁLYZAT KIADÁSA, KEZELÉSE, FELÜLVIZSGÁLATA

A Szabályzat előkészítése, szakmai tartalmának az IBSZ-ben rögzített biztonsági szerepkört betöltő személyekkel együttműködve a jogszabályban rögzített követelményekhez és a Hivatal működéséhez egyaránt igazodó kialakításának koordinálása az IBF feladata.
A Szabályzat jóváhagyása és kiadása a jegyző feladata és felelőssége.
A Szabályzat kihirdetéséről és a személyi hatálya alá tartozókkal történő megismertetéséről a jegyző köteles gondoskodni.
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.
Az IBSZ felülvizsgálatát és frissítését a következő gyakorisággal kell elvégezni:

- a Hivatal működésében, alaptevékenységében, illetve szervezetében, a biztonsági szerepkörökben, a használt EIR-ekben vagy a vonatkozó, hatályos jogszabályi előírásokban bekövetkezett olyan jelentős változás esetén, amely a Szabályzat értelmezését és megfelelő alkalmazását, következetes végrehajtását annak módosítása nélkül akadályozhatja vagy gátolhatja;

- olyan változás esetén, amely érinti az EIR-ek biztonságát, bizalmasságát, rendelkezésre állását, sértetlenségét vagy a Hivatal alaptevékenységét;
- az újonnan felmerülő kockázat kezelése érdekében, ha a bekövetkezett kiberbiztonsági incidenssel vagy incidensközeli helyzettel összefüggő kockázatot a kockázatelemzés során nem vizsgálták;
- az ellenőrzés vagy a kiberbiztonsági gyakorlat alkalmával feltárt hiányosságok alapján, a nemzeti kiberbiztonsági hatóság által előírtak szerint;
- fentiek hiányában annak érdekében, hogy a változó kiberfenyegetettségi környezetben a Szabályzat relevanciája és hatékonysága biztosítható legyen, legalább 2 évenkénti rendszerességgel.

Az IBSZ felülvizsgálatára javaslatot tehet, illetve azt kezdeményezheti bármely, a Szabályzatban rögzített biztonsági szerepkört betöltő személy.

INFORMÁCIÓ- ÉS DOKUMENTUMVÉDELEM

Az IBSZ és az ahhoz kapcsolódó szabályzatok és eljárásrendek, az ezekben előírt elkészítendő és megőrzendő dokumentumok tartalmának jogosulatlan megismerés és módosítás elleni védelméről a Hivatal elektronikus formában történő kezelésük esetén hozzáférés- és jogosultsági rendszerrel védett tárterületen történő elhelyezésükkel, papír alapon történő kezelésük esetében pedig a Szervezet iratkezelési szabályai szerint eljárva gondoskodik.

AZ INFORMÁCIÓBIZTONSÁG SZERVEZETE

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

Biztonsági szerepkör általános megnevezése	**Hozzárendelt felelősségi szint**	**Szervezetnél a szerepkör betöltője**
Első számú vezető	Általános vezetői és az információbiztonság tervezéséhez, szervezéséhez, irányításához, kockázatokkal arányos megvalósításához, felügyeletéhez, folyamatos fenntartásához és továbbfejlesztéséhez szükséges erőforrások biztosításáért való felelősség.	jegyző
Kockázati vezető	A kockázatok szervezeti szintű áttekintésének és elemzésének, valamint a kockázatmenedzsment szervezeten belüli egységes működésének biztosításáért való felelősség.	jegyző
Kockázatkezelésért felelős személy	A kockázatkezelési tevékenységek szervezeten belüli végrehajtásáért, valamint az információbiztonsági irányítási folyamatoknak a stratégiai, működési és költségvetés-tervezési folyamatokkal történő összehangolásáért való felelősség.	jegyző
EIR-ért felelős személy(ek)	Az EIR rendeltetésszerű és biztonságos használatáért, biztonsági állapotának nyomon követéséért, valamint az EIR-el kapcsolatos engedélyezési eljárás lefolytatásáért való felelősség.	Az EIR nyilvántartásban rögzített felelős személy(ek).
Az elektronikus információs rendszerek biztonságáért felelős személy	Az információbiztonsági tevékenységek tervezéséért, felügyeletéért és ellenőrzéséért való felelősség.	Információbiztonsági felelős (IBF vagy EIRBF)
Üzemeltetésért felelős	Az EIR-ek és rendszerelemeik működtetési, üzemeltetési felelőssége.	IT Üzemeltető

Biztonsági vezető	Fizikai biztonsággal kapcsolatos tevékenységek ellátásáért való felelősség.	jegyző
Humánerőforrás menedzsmentért felelős	Foglalkoztatottak be- és kiléptetéséért, a személyi ügyekhez kapcsolódó tevékenységek koordinálásáért való felelősség. Információbiztonsági képzések lebonyolításáért és adminisztrációjáért való felelősség.	jegyző
Beszerzésekért felelős	Informatikai erőforrások, eszközök és szolgáltatások beszerzésének lebonyolításáért való felelősség.	jegyző

A biztonsági szerepköröket betöltő személyek kinevezése, megbízása, illetve indokolt esetben kinevezésük, megbízásuk visszavonása a jegyző feladata és felelőssége.
A jegyző a felelősségét nem, de az egyes – különösen a döntés előkészítéssel összefüggő – feladatok végrehajtását delegálhatja a jelen Szabályzat keretében, fentiekben meghatározott biztonsági szerepköröket betöltő személyek felé.
Az IBSZ-ben rögzített szabályok és alkalmazásuk megfelelőségét, valamint az előírt tevékenységek és intézkedések végrehajtását az IBF jogosult és köteles feladatellátása, az IBSZ felülvizsgálata, illetve rendszeres biztonsági helyzetértékelése keretében ellenőrizni, s annak eredményéről a jegyzőt indokolt esetben, illetve éves beszámolójában tájékoztatni.

AZ INFORMÁCIÓBIZTONSÁGGAL KAPCSOLATOS ENGEDÉLYEZÉSI ELJÁRÁS

A jegyző jogosult és köteles a Hivatal hatáskörébe tartozó – jelen IBSZ-ben engedélyezéshez kötött – minden információbiztonsággal kapcsolatos tevékenységgel, intézkedéssel kapcsolatban gondoskodni arról, hogy a jóváhagyásuk és az engedélyek kiadása a megfelelő felhatalmazással rendelkező személy(ek) által, a döntéshez szükséges és indokolt információk rendelkezésre állásával, a biztonsági kockázatok és követelmények figyelembe vételével, szabályozott keretek között és minden esetben megvalósuljon, különösen, de nem kizárólagosan az alábbi, engedélyezéshez kötött esetekben:

a) új távoli-, illetve vezeték nélküli hozzáférési megoldás bevezetése, meglévő használatának felfüggesztése, kivezetése, illetve kiváltása;
b) a Hivatal rendelkezésében lévő EIR használatának megszüntetése, kivezetése, illetve kiváltása;
c) új EIR beszerzése, fejlesztése;
d) a fejlesztés elfogadása, átvétele, bevezetésének elrendelése;
e) ügymenet-folytonossági intézkedések végrehajtása (helyettesítő eljárások, illetve helyreállító tevékenységek végrehajtásának elrendelése; kieséssel járó hibajavítás jóváhagyása);
f) információbiztonsági képzési programok lebonyolításának jóváhagyása;
g) szervezeti információk nyilvánosságra hozatala, közzététele;
h) kockázatkezelési intézkedések végrehajtása;
i) cselekvési-, illetve intézkedési tervek végrehajtása;
j) rendszerbiztonsági terv jóváhagyása, védelmi intézkedések végrehajtásának elrendelése;
k) új felhasználói szoftver beszerzése;
l) egyedi azonosítás és hitelesítés alóli kivétel igény;
m) csoportszintű hozzáférés beállítására vonatkozó igény;
n) szervezeti adatot tartalmazó rendszerelem karbantartási célú kiszállítása;
o) együttműködésen alapuló informatikai eszköz használatba vétele;
p) felhasználói fiókok kezelése;
q) a munkavégzéshez szükséges azonosítók kezelése és a hitelesítő eszközök kiosztása;
r) felhasználó általi szoftvertelepítés;
s) szervezeten kívüli, idegen adathordozó csatlakoztatása.

Az a) – j) pontokban felsorolt információbiztonsági engedélyezési jogköreit a jegyző nem ruházhatja át, nem delegálhatja más biztonsági szerepkört betöltő személyre.
A k) – o) pontokban felsorolt, információbiztonsági engedélyezéshez kötött új igény vagy tevékenység esetén a jegyző a jóváhagyási jogkörét delegálhatja az EIR-ért felelős számára.

A p) – s) pontokban foglalt tevékenységek végrehajtását feladatellátása keretében az IT üzemeltető a jegyző erre vonatkozó általános engedélyével végzi, a r) és s) pontokban esetén a szükséges biztonsági ellenőrzés végrehajtását követően.
Minden, a jelen Szabályzat személyi hatálya alá tartozó foglalkoztatott, illetve a Hivatallal bármely más, munkavégzésre irányuló jogviszony alapján kapcsolatba kerülő személy köteles az engedélyezési eljárás lefolytatásában közreműködni, a döntés előkészítéséhez szükséges információkat a jóváhagyásra jogosult rendelkezésére bocsátani.
A jóváhagyásra jogosult felelőssége az információbiztonsággal kapcsolatos engedélyezési eljárásban az IBF bevonásáról gondoskodni. Az IBF feladata a 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.

KOCKÁZATMENEDZSMENT

A Hivatal alapvető érdeke és célja rendeltetésszerű, a mindenkori hatályos, vonatkozó jogszabályi előírásoknak maradéktalanul megfelelő, eredményes és biztonságos működésének folyamatos biztosítása, valamint emiatt és ebből következően a működésére ható, változó kockázatok felismerése és hatékony kezelése.
Ennek érdekében a Hivatal az alaptevékenysége végzéséhez használt EIR-ekkel, az azokban kezelt adatokkal és az EIR-ek által nyújtott vagy azokon keresztül elérhető szolgáltatásokkal összefüggő kiberbiztonsági kockázatok kezelésével kapcsolatban az alábbiakat határozza meg:

- a jegyző feladata és felelőssége gondoskodni a kockázatmenedzsment tevékenységek megszervezéséről és végrehajtásáról, valamint az ahhoz szükséges erőforrások rendelkezésre állásának biztosításáról;
- a jegyző feladata és felelőssége a kockázatkezelés végrehajtásáért felelős biztonsági szerepköröket betöltő személyek kijelölése, akik a kockázatkezelés teljes folyamatában kötelesek egymással munka- illetve feladatkörüknek megfelelően együttműködni, valamint az IBF szakmai támogatásával az alábbi feladatok és tevékenységek elvégzésében közreműködni:
    - a Hivatal által használt EIR-ek beazonosítása, az EIR-ben kezelt adatok és az adott EIR-nek a Szervezet működésében betöltött szerepe és funkciója alapján, a hatályos jogszabályi előírásokban meghatározott hatáselemzési szempontok szerinti biztonsági osztályba sorolása, s mindezeknek az EIR-ek nyilvántartásában történő, dokumentált rögzítése;
    - a Hivatal által használt EIR-eket érintő fenyegetettségek alapján az azokra ható, releváns kockázatok felmérése, azonosítása és értékelése, továbbá a felmerült, illetve feltárt kockázatok kezelésére vonatkozó, a kockázatokkal arányos védelmi intézkedési javaslatok kidolgozása és döntésre előterjesztése;
    - a jóváhagyott kockázatkezelési intézkedések dokumentált végrehajtása;
    - a végrehajtott kockázatkezelési intézkedések hatásosságának és eredményességének, valamint az érintett EIR-ek biztonságára gyakorolt hatásaik, teljesítményük mérése, elemzése és értékelése, rendszeres felülvizsgálata és az azokkal kapcsolatos jelentések elkészítése, a vezetői döntések előkészítése.

A Hivatal az információbiztonsági kockázatok komplex kezelését az alábbi, egymással szorosan összefüggő szinteken valósítja meg:

- rendszerelem szinten: rendszerelem szintű sérülékenység- és frissítés menedzsment alkalmazásával (a Biztonsági riasztások és tájékoztatások kezelése szakaszban foglalt módon);
- rendszer szinten: az EIR jogszabályban meghatározott biztonsági osztályának megfelelő védelmi intézkedések azonosításával és azoknak az EIR rendszerbiztonsági tervében történő dokumentálásával, valamint azok következetes alkalmazásával, ellenőrzésével és nyomon követésével;
- szervezeti szinten: az EIR és az általa feldolgozott adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából értelmezhető fenyegetések azonosításával, a szervezeti vagyonelemekre, személyekre vagy más szervezetekre vonatkozó lehetséges káros hatásaik és azok mértékének, valamint a bekövetkezési valószínűségük alapján a feltárt kockázatok értékelésével,

elemzésével, s annak eredményeként a kockázat kezelésére vonatkozó válaszlépések, intézkedések alkalmazásával.

Kockázatkezelési stratégia

Az információbiztonsági kockázatkezelési stratégia célja, hogy a Hivatal által a rendeltetésszerű működését érintően végzett szervezeti szintű általános kockázatkezelési tevékenységéhez igazodó, egységes módszertan alkalmazásával biztosítsa a Hivatal által használt EIR-ek működésével, használatával, valamint az azokban kezelt adatokkal összefüggésben azonosítható biztonsági kockázatok átfogó, következetes, a változó kiberfenyegetettségi környezetre időben reagáló, korszerű és minél teljesebb körű kezelését.
Az információbiztonsági kockázatok elemzésének és kezelésének rendje, az azzal összefüggő tevékenységek, feladatok és felelősségek részletesen az Információbiztonsági Kockázatkezelési Szabályzatában (a továbbiakban: Kockázatkezelési Szabályzat) kerültek rögzítésre. Az információbiztonsági kockázatkezelési stratégia részeként a Kockázatkezelési Szabályzatban került továbbá meghatározásra:

- a Hivatal által elfogadott és alkalmazott kockázatfelmérési és értékelési módszer, illetve szempontrendszer;
- a Hivatal által elfogadható, felvállalható kockázatok szintje;
- a kockázatok kezelésének szabályai;
- a kockázatkezeléssel kapcsolatos kommunikáció szabályai;
- valamint a kockázatkezelési javaslatok alapján hozott döntések és az azok alapján elrendelt védelmi intézkedések megvalósításának időbeli nyomon követését biztosító eljárás.

A Hivatal az ellátási láncokra vonatkozó kockázatkezelési stratégiát fentiek keretében, az információbiztonsági kockázatkezelési stratégiába integráltan, az ellátási láncokkal összefüggésben azonosított kockázatok súlyozott értékelésére vonatkozó szempontrendszer következetes alkalmazásával és érvényesítésével definiálja és valósítja meg, szintén a Kockázatkezelési Szabályzatban előírt módon.
A kockázatmenedzsmenthez kapcsolódó intézkedések dokumentált felülvizsgálatát az IBF legalább évente köteles biztonsági helyzetértékelése keretében elvégezni, s annak eredményéről a jegyzőt beszámolójában tájékoztatni.
A jegyző feladata és felelőssége gondoskodni arról, hogy a Hivatal kiberbiztonsági állapotának és az alaptevékenysége végzéséhez használt EIR-ek biztonságának megfelelősége, valamint az azzal összefüggő védelmi intézkedések megfelelősége, végrehajtásuk rendszeres ellenőrzése és értékelése megvalósuljon.

ÜGYMENET-FOLYTONOSSÁG

A Hivatal az általa az alaptevékenysége végzéséhez használt EIR-ek rendelkezésre állásának, valamint az EIR-ekben tárolt, illetve kezelt adatok sértetlenségének és rendelkezésre állásának megőrzése érdekében az alábbi intézkedéseket teszi:

- gondoskodik a működéséhez szükséges, a rendelkezésében lévő EIR-ekben általa felügyelt adattároló rendszerelemeken tárolt adatok, információk megfelelő és rendszeres biztonsági mentéséről, valamint a mentési adathordozók biztonságos tárolásáról;
- gondoskodik az informatikai eszközök (rendszerelemek) rendszeres karbantartásáról, szükség szerinti javításáról;
- a kieső informatikai erőforrások (pl.: hardvereszközök) pótlásáról szükség esetén rendkívüli beszerzéssel gondoskodik;
- külső szolgáltató igénybe vétele esetén fentiekről az arra vonatkozó szerződésben történő rögzítésük útján gondoskodik;
- az alaptevékenysége végzéséhez szükséges EIR-eket érintő informatikai erőforrások kiesésére vonatkozóan tervet készít, amely tartalmazza az adott EIR kapcsán a problémakezeléshez szükséges azonnali intézkedéseket, a helyreállítási idő függvényében szükséges helyettesítő eljárásokat, a helyreállításhoz szükséges erőforrásokat, az intézkedések végrehajtásáért felelős szerepköröket, feladataikat, továbbá a normál működési folyamathoz történő visszatérés feltételeit;
- gondoskodik az alaptevékenysége végzéséhez szükséges EIR-eket használó foglalkoztatottaknak a munkaköri feladataiknak és szerepkörüknek megfelelő mértékű, az ügymenet-folytonosság szempontjából indokolt és szükséges ismeretekről, az ezzel kapcsolatos feladataikról és kötelezettségeikről való felkészítéséről;

- jelen Szabályzat keretében szabályozza és meghatározza az ügymenet-folytonossághoz kapcsolódó eljárásrendet.

Az ügymenet-folytonossági terv elkészítésének koordinálása, módszertani támogatása és szakmai tartalmának ellenőrzése az IBF feladata. A terv elkészítésében, végrehajtásában és felülvizsgálatában részt vesznek, illetve közreműködnek munka- illetve feladatkörüknek megfelelő mértékben az alábbi, a jelen Szabályzatban nevesített biztonsági szerepköröket betöltő személyek:

- EIR-ért felelős,
- Üzemeltetésért felelős,
- Kockázatkezelésért felelős.

Az ügymenet-folytonossági tervnek a végrehajtásában érintettekkel történő megismertetése, számukra hozzáférhetőségük biztosítása a jegyző feladata és felelőssége.
Az ügymenet-folytonosságot érintő előírások dokumentált felülvizsgálatát az IBF legalább évente köteles biztonsági helyzetértékelése keretében elvégezni, s annak eredményéről a jegyzőt beszámolójában tájékoztatni.

Ügymenet-folytonosságra vonatkozó eljárásrend

Esemény felismerése, jelzése

Amennyiben olyan esemény következik be, amely a Hivatal alaptevékenysége végzéséhez használt EIR-t, illetve rendszerelemeit, a munkavégzéshez szükséges informatikai eszközöket részben vagy teljesen működésképtelenné teszi, a jegyzőt haladéktalanul értesíteni kell, aki tájékoztatja az ügymenet-folytonossági terv végrehajtásában, valamint az azokról szóló döntések meghozatalában érintetteket.
Az értesítés az eseményt észlelő személy kötelessége.

Döntés az erőforrás kiesés kezelésének módjáról

A Hivatal a bekövetkezett erőforrás kieséses állapot körülményeiről és hatásairól, az erőforrás kiesés megszüntetésére vonatkozó intézkedések végrehajtásának becsült időtartamáról (helyreállítási idő) rendelkezésre álló információk mérlegelését követően az alábbi biztonsági szerepköröknek és rendelkezési szinteknek megfelelően dönt az esemény kezelési módjáról:

- kisebb hatású, az informatikai erőforrások szűk körét érintő vagy várhatóan rövid ideig tartó erőforrás kiesés esetén (pl.: olyan hibajelenség előfordulásakor, amely helyben – esetleg távoli segítségnyújtás igénybe vételével – kezelhető, mint például egy eszköz újraindítása) a szükséges intézkedés megtételéről döntést hozhat a jegyző;
- az informatikai erőforrások széles körét vagy egészét érintő veszélyhelyzet esetén az ügymenet-folytonossági tervben rögzített helyettesítő eljárások, illetve helyreállító tevékenységek végrehajtásának elrendelése a jegyző feladata és felelőssége.

Az erőforrás kieséses állapot körülményeinek és hatásainak értékeléséhez, az indokolt intézkedések mérlegeléséhez az IBF szakmai-, módszertani támogatást biztosít.
Amennyiben a bekövetkezett esemény kapcsán, illetve a probléma kezelése során megállapítható, hogy az veszélyezteti a Hivatal által használt EIR-ekben tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát, úgy a jegyző köteles a jelen Szabályzat Biztonsági események kezelése fejezetében meghatározottak szerint eljárni.

Veszélyhelyzet elhárítása, visszatérés a normál működési folyamathoz

A helyzet kezeléséről hozott döntésnek megfelelően az ügymenet-folytonossági tervben meghatározott, a helyreállításban közreműködő felelős személyek végrehajtják a szükséges intézkedéseket, majd annak eredményéről tájékoztatják a jegyzőt és az IBF-et.
A jegyző az ügymenet-folytonossági tervben foglalt, az erőforrás kiesés sikeres megszüntetésére vonatkozó feltételek fennállása esetén rendelheti el a normál működési folyamathoz történő visszatérést.

BIZTONSÁGI MENTÉSEK

A Hivatal az általa az alaptevékenysége végzéséhez használt, rendelkezésében lévő EIR-ek rendszeres biztonsági mentésével kapcsolatban az alábbi intézkedéseket határozza meg:

- a rendszeres biztonsági mentésekre vonatkozó információkat (mentendő adatok köre, mentési gyakoriság, megőrzési idő, tárolási helyszín, stb.) az adott EIR rendszerbiztonsági tervében rögzíti;
- a biztonsági mentéseknek ki kell terjednie az EIR felhasználói és rendszerszintű információira, valamint minden olyan adatra, amely az ügymenet-folytonossági tervben foglalt helyreállítási, illetve újraindítási feladatok maradéktalan teljesítéséhez szükséges;
- a biztonsági mentések konfigurálása és rendszeres végrehajtása a fentiek szerint dokumentált mentési rend alapján az IT üzemeltető feladata és felelőssége;
- az eseti biztonsági mentések, valamint a helyreállítási, illetve tesztelési célú visszatöltések végrehajtásáról az IT üzemeltető köteles nyilvántartást vezetni;
- amennyiben a Hivatal által használt EIR-eket, rendszerelemeiket érintő hiba vagy biztonsági esemény kezelése biztonsági mentésből történő helyreállítási tevékenységet igényel, annak végrehajtása az IT üzemeltető feladata és felelőssége.

A fentiekben rögzített intézkedések megfelelőségét és végrehajtását az IBF jogosult és köteles feladatellátása, illetve rendszeres biztonsági helyzetértékelése keretében ellenőrizni, s annak eredményéről a jegyzőt indokolt esetben, illetve beszámolójában tájékoztatni.

BIZTONSÁGI ESEMÉNYEK KEZELÉSE

Biztonsági eseménynek minősül minden olyan nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az EIR-ben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az EIR által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.
A Hivatal alapvető érdeke, hogy az alaptevékenysége végzéséhez használt EIR-eket érintő minden biztonsági eseményt a legrövidebb időn belül észleljen és felismerjen, s azokra ügymenet-folytonossága fenntartása, megőrzése érdekében hatékony és gyors válaszintézkedésekkel tudjon reagálni.
A Hivatal annak érdekében, hogy a biztonsági események bekövetkezése által okozható kár minimalizálható legyen, azok tervezett kezelését jelen Szabályzat keretei között az alábbiakban szabályozza, s azzal összefüggésben az itt meghatározott eljárásrendet lépteti életbe.

A biztonsági események jelzése, jelentése

A jelen Szabályzat személyi hatálya alá tartozó foglalkoztatottak kötelesek az általuk használt EIR-ek bármely rendszerelemének, hardver- illetve szoftver komponenseinek rendellenes, zavart vagy hibás működését, hibajelzését, illetve bármely rendellenes eseményt annak észlelését követően közvetlen munkahelyi felettesük vagy az IT üzemeltető számára haladéktalanul jelezni.
A Hivatal gondoskodik arról, hogy a foglalkoztatottak számára a jelzés megtételével kapcsolatos lényeges és naprakész információk (az IT üzemeltető elérhetőségei) folyamatosan rendelkezésre álljanak.
Az IT üzemeltető a jelzés formájától függetlenül köteles gondoskodni a bejelentés adatainak dokumentált rögzítéséről, illetve indokolt esetben a felhasználók által végrehajtandó intézkedések számukra történő visszajelzéséről.
Az IT üzemeltető a számára bejelentett, illetve az üzemeltetett rendszerekből érkező jelzés vagy általa észlelt eseménnyel összefüggésben biztonsági esemény gyanújának felmerülése esetén köteles értesíteni a jegyzőt és az IBF-et.

A biztonsági események kivizsgálása, értékelése és kezelése (biztonsági eseménykezelési terv)

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 IBF támogatja a rendelkezésre álló információk kiértékelését, mely alapján a biztonsági esemény minősítésére vonatkozó javaslat előterjesztésre kerül a jegyző részére.
A biztonsági esemény értékeléséhez, kivizsgálásához, illetve bejelentéséhez esetlegesen szükséges további információk (pl.: naplóbejegyzések) begyűjtésében az IT üzemeltető köteles közreműködni.
Az IBF a biztonsági esemény kivizsgálását követően javaslatot tesz a jegyző számára az esemény kezelési módjára, illetve a bejelentési kötelezettség körébe tartozó biztonsági eseményt jelenti a vonatkozó, hatályos

jogszabályi előírásokban meghatározott eseménykezelő szerv, illetve felügyeleti hatóság felé. Az IBF a bejelentett biztonsági eseményeket figyelemmel kíséri és dokumentálja.
Az informatikai erőforrások kiesésével járó esemény bekövetkezése esetén az ügymenet-folytonosságra vonatkozó eljárásrend, vírustámadás esetén a Kártékony kódok elleni védelem szakaszban meghatározott intézkedések alkalmazandók.
A biztonsági esemény jellegétől és várható hatásaitól függően a bekövetkezett vagy okozható kár, kockázat mérséklése, illetve a fenyegetettség vagy veszélyhelyzet elhárítása, megszüntetése érdekében az IBF által javasolt és szükséges, illetve a jegyző által jóváhagyott és elrendelt intézkedések végrehajtásában minden érintett köteles együttműködni.
Az érintetteknek a biztonsági eseménnyel kapcsolatos információkról történő indokolt tartalmú tájékoztatásáról a jegyző gondoskodik.
A biztonsági esemény kezelésének lezárását követően a rendelkezésre álló információk vizsgálata alapján az IBF jogosult a hasonló események jövőbeni előfordulási kockázatának csökkentése érdekében indokolt új védelmi intézkedések bevezetésére, illetve meglévő intézkedések módosítására javaslatot tenni a jegyző számára.

TUDATOSSÁG ÉS KÉPZÉS

A folyamatosan változó kiberbiztonsági környezetben a kockázatok, illetve a biztonsági események megelőzésének, illetve megfelelő kezelésének előfeltétele azok, valamint a bekövetkezésüket potenciálisan okozó körülményekre utaló jelek, a veszélyes helyzetek és cselekmények, káros tevékenységek felismerése. Az ezzel kapcsolatos készségek és képességek, a biztonságtudatos hozzáállás és munkavégzés kialakítása, támogatása és fenntartása céljából a Hivatal gondoskodik a foglalkoztatottak biztonságtudatossági felkészítése keretében a munkaköri feladataiknak és szerepkörüknek megfelelő ismeretek számukra történő átadásáról, az ezzel kapcsolatos feladataik és kötelezettségeik velük való megismertetéséről, amelynek szabályait jelen Szabályzat keretei között az alábbiakban írja elő, s azzal összefüggésben az itt meghatározott eljárásrendet lépteti életbe.

Biztonságtudatossági képzési eljárásrend

A Hivatal az általa használt EIR-ekhez hozzáféréssel rendelkező foglalkoztatottakat az új munkavállalók kezdeti képzésének részeként a munkavégzésükhöz kapott infokommunikációs eszközök rendeltetésszerű használatára, a munkaköri feladataik ellátása során használandó EIR-ek alapvető biztonsági követelményeire, továbbá az IBSZ előírásain alapuló, az információbiztonsággal kapcsolatos előírások, szabályok betartására, valamint a rendellenes működés, a külső- és belső fenyegetések, a biztonsági események felismerésére és jelzési, jelentési kötelezettségére vonatkozó feladataik és felelősségeik megismertetését célzó felkészítésben részesíti.
A képzés, továbbképzés szakmai tartalmának saját tananyag esetén összeállítása, külső forrásból származó tananyag esetén jóváhagyása, illetve az alkalmazására vonatkozó javaslattétel az IBF feladata.
A Hivatal a munkaköri feladatai ellátása során bármely EIR használatára kötelezett foglalkoztatottja számára biztosítja az adott EIR felhasználására, annak biztonsági követelményeire vonatkozóan rendelkezésre álló, feladat- és szerepkörének megfelelő információk és dokumentációk folyamatos hozzáférhetőségét, illetve – amennyiben elérhető – az EIR vagy rendszerelemének gyártója, fejlesztője, disztribútora vagy szolgáltatója által biztosított, releváns képzésen történő részvételét.
A folyamatos biztonságtudatosítás részeként alkalmazandó, az új biztonsági fenyegetések megjelenésére reagáló figyelemfelhívó kampányok, tájékoztatók, illetve oktatások tematikájának meghatározása, indokolt rendszerességű lebonyolításuk kezdeményezése az IBF feladata.
A képzési programok lebonyolításáról a jegyző dönt, valamint gondoskodik a részvétel feltételeinek biztosításáról.
A képzési program jellegétől és lebonyolítási módjától függő formátumú, az azon való részvételt igazoló dokumentumok megőrzéséről a jegyző köteles gondoskodni.
Minden jelen Szabályzat személyi hatálya alá tartozó köteles részt venni az információbiztonsággal kapcsolatos számára előírt képzéseken.

RENDSZER- ÉS SZOLGÁLTATÁSBESZERZÉS

A Hivatal az általa használt, rendelkezésében lévő, illetve felügyelete alatt álló EIR-ek, illetve rendszerelemeik beszerzésére vonatkozó speciális információbiztonsági szabályokat jelen Szabályzat keretei között az alábbiakban írja elő, s azzal összefüggésben az itt meghatározott eljárásrendet lépteti életbe.
A Hivatal alaptevékenysége végzéséhez használt EIR-ek folyamatos és biztonságos működéséhez, működtetéséhez szükséges erőforrások rendelkezésre állásának biztosításáról a jegyző köteles gondoskodni.
Az adott EIR dokumentációjában, illetve rendszerbiztonsági tervében rögzített működési környezetnek és biztonsági követelményeknek megfelelő erőforrás-, szolgáltatás-, illetve eszközigényre vonatkozó beszerzési javaslatok elkészítése és a jegyző számára történő jelzése az IT üzemeltető feladata és felelőssége. A beszerzésre vonatkozó javaslatnak a döntés előkészítés megfelelő támogatása érdekében tartalmaznia kell:

- a beszerzési igény szakmai indoklását;
- amennyiben releváns, a beszerzési alternatívákat és azok jellemzőit;
- a becsült egyszeri, illetve rendszeres költségeket.

A Hivatal rendelkezésében lévő EIR-ek gyártói támogatással már nem rendelkező, illetve azon rendszerelemei, amelyeknek a támogatása a következő beruházási ciklusban lejár vagy megszűnik, azoknak a cseréjét, kiváltását, gyártói támogatásának meghosszabbítását vagy a gyártótól független további támogatásának biztosítását célzó beszerzési javaslat kellő időben történő elkészítése és jelzése az IT üzemeltető feladata és felelőssége. A nem támogatott rendszerelemmel kapcsolatos beszerzés, minthogy a támogatás hiányában az adott rendszerelem további felhasználása kezelendő kiberbiztonsági kockázatot jelent, minden esetben biztonsággal összefüggő beszerzésnek minősül.
A beruházási tervben a jegyző az EIR-ek biztonságával összefüggő beszerzéseket elkülönítetten köteles kezelni.
A beszerzések lefolytatásáról a jegyző dönt.
A Hivatal a beszerzési dokumentációban meghatározza a beszerzés tárgyával kapcsolatos funkcionális, biztonsági és dokumentációs, külső szolgáltatás esetén a rendelkezésre állásra, szolgáltatási szintre és a támogatásra vonatkozó követelményeket, s azokat szerződéses kötelemként rögzíti. A beszerzési dokumentáció elkészítése a gazdasági vezető feladata és felelőssége, amelyben az IT üzemeltető köteles közreműködni.
Az IBF jogosult minden információbiztonságot érintő beszerzéssel kapcsolatos dokumentáció tartalmának megismerésére és véleményezésére, valamint azzal összefüggésben szakértői javaslatot tenni a jegyző számára.

Fejlesztésre vonatkozó szabályok

A Hivatal a saját rendelkezésében lévő EIR továbbfejlesztésére, illetve új EIR fejlesztésére vonatkozó beszerzés esetén az alábbiakban rögzített biztonságtervezési elveket alkalmazza.
Az EIR-nek a kitűzött és elérendő céloknak maradéktalanul megfelelő funkcionalitással kell rendelkeznie, s teljesítenie kell a fejlesztési specifikációban meghatározott, az EIR biztonsági osztály besorolásának megfelelő, az adott EIR esetében alkalmazható védelmi követelményeket. Ennek érdekében a Hivatal a fejlesztési igény felmerülésétől kezdődően bevonja a folyamatba az IBF-et, aki szakmai támogatást nyújt a biztonságspecifikus kérdésekben, illetve véleményezi a tervezett fejlesztéssel kapcsolatban rendelkezésre álló információkat és dokumentumokat, továbbá indokolt esetben javaslatot tesz azok kiegészítésére, módosítására a jegyző számára.
Új EIR fejlesztése esetén annak a biztonsági osztály besorolásának megfelelő, a Hivatal által meghatározott és a rendszerbiztonsági tervben rögzített, az adott EIR esetében alkalmazható védelmi követelményeket maradéktalanul teljesítenie kell, hiányzó vagy hiányosan megvalósított védelmi intézkedésekkel, illetve funkcionalitással az EIR nem vehető át. A fejlesztést végző köteles a rendszerbiztonsági tervhez szükséges információkat a Hivatal rendelkezésére bocsátani, annak elkészítésében és aktualizálásában közreműködni.
Új EIR fejlesztése esetén a Hivatal követelményként előírja, hogy az újonnan beszerzésre kerülő rendszerelemeinek aktív és folyamatos gyártói támogatással kell rendelkeznie az új EIR bevezetését követő legalább 2 éves időtartamra, támogatás nélküli vagy kivezetés előtt álló rendszerelem nem szerezhető be.
Nyilvános hálózat felől elérhető EIR, illetve rendszerelem esetén a Hivatal sérülékenységi teszt dokumentált végrehajtását írhatja elő, amelynek 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 tesztelési eljárásokat és ellenőrzési listákat;
- a feltárt sérülékenység(ek) lehetséges hatásait;
- egy támadó milyen információkat képes elérni az elektronikus információs rendszerben és annak elhárítására milyen javítások végrehajtása szükséges;
- a sérülékenység teszt eredményét, annak szakmai, módszertani elemzését.

A gazdasági vezető feladata és felelőssége gondoskodni arról, hogy a fejlesztésre vonatkozóan meghatározott biztonsági követelmények teljesítése a megállapodásban garanciális feltételként érvényesítésre kerüljön.
Az IBF a fejlesztési folyamat során, annak előzetesen meghatározott mérföldköveinek elérését követően ellenőrzi a biztonsági követelmények megvalósításának státuszát, amelyben a fejlesztést végző, az IT üzemeltető köteles együttműködni.
Az elkészült fejlesztés biztonsági követelményeknek való megfelelését az IBF és az IT üzemeltető bevonásával vizsgálja és értékeli, s tesz a fejlesztés elfogadására, jóváhagyására, illetve nem megfelelőség esetén kijavítására javaslatot a jegyző számára.
A fejlesztés elfogadásáról, átvételéről és bevezetése elrendeléséről, illetve javításáról a jegyző dönt.

TERVEZÉS

A Hivatal az alaptevékenysége végzéséhez használt EIR-ek és az azokban kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, azok zárt, teljes körű, folytonos és kockázatokkal arányos védelmének megvalósítása és az EIR teljes életciklusán keresztül történő fenntartása érdekében szükséges tervezéssel összefüggő tevékenységek és feladatok végrehajtásának és felügyeletének biztosítása céljából az általa használt EIR-ekre vonatkozó biztonságtervezési eljárásrendet jelen fő fejezetben, az alábbiak szerint határozza meg.
A Hivatal által használt, meglévő EIR-ek rendszerelemeinek, illetve az új EIR-ek fejlesztését, beszerzését érintő, a beszerzés tervezési szakaszában alkalmazandó információbiztonsági szabályokat a Rendszer- és szolgáltatásbeszerzés fejezet tartalmazza.

Rendszerbiztonsági terv

A Hivatal a rendelkezésében lévő EIR-ek esetében rendszerbiztonsági tervben határozza meg és dokumentálja:

- az EIR hatókörét, alapfeladatait (biztosítandó szolgáltatásait), biztonságkritikus elemeit és alapfunkcióit;
- az EIR jogszabály szerinti biztonsági osztály besorolását;
- az EIR működési körülményeit és más EIR-ekkel való kapcsolatait;
- az EIR beállításait és a használatával kapcsolatos feltételeket, szabályokat;
- az EIR biztonsági követelményeit és az azoknak megfelelő, aktuálisan alkalmazott vagy tervezett védelmi intézkedéseket.

A rendszerbiztonsági terv az EIR biztonsági osztály besorolásának megfelelő követelmények teljesítésével összefüggő, megvalósítandó védelmi intézkedésekkel kapcsolatban tartalmazza a végrehajtandó feladatokat, valamint a végrehajtásukhoz rendelt határidőket és felelősségeket.
A rendszerbiztonsági terv elkészítésében az IBF és az IT üzemeltető köteles közreműködni. A rendszerbiztonsági tervet a jegyző hagyja jóvá és rendeli el az abban foglalt, tervezett védelmi intézkedések végrehajtását.
A jegyző gondoskodik arról, hogy a Hivatal által foglalkoztatottak, valamint a Hivatallal munkavégzésre irányuló egyéb szerződéses jogviszonyban lévő személyek a feladatellátásukhoz szükséges mértékben a rendszerbiztonsági terv és a kapcsolódó rendszer-dokumentációk tartalmát megismerjék.
A Hivatal az Információ- és dokumentumvédelem fejezetben leírtak szerint gondoskodik a rendszerbiztonsági terv védelméről, továbbá gondoskodik arról, hogy a rendszerbiztonsági tervben a meghatározott védelmi intézkedések és feladatok végrehajtása megtörténjen.
Az IBF a rendszerbiztonsági tervben a feladatok végrehajtására vonatkozó határidőknek megfelelően ellenőrzi a védelmi intézkedések megvalósítását, amelyben az IT üzemeltető köteles együttműködni.
A rendszerbiztonsági terv felülvizsgálatát az EIR-ben vagy annak működési környezetében történt változások, illetve a tervezett védelmi intézkedések ellenőrzése, értékelése által indokolt esetben kezdeményezheti a jegyző, az IBF és az IT üzemeltető vagy bármely más, a terv végrehajtásában érintett

biztonsági szerepkört betöltő személy. A felülvizsgálat elvégzésében az IBF szakmai támogatásával a fentiekben nevesített biztonsági szerepköröket betöltő személyek kötelesek közreműködni.

Viselkedési szabályok

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 Szervezet a Személybiztonsági feltételek és a Biztonságtudatossági képzési eljárásrend szakaszokban meghatározottak szerint gondoskodik.
A Hivatal az általa foglalkoztatottaktól és a Hivatallal egyéb munkavégzésre irányuló jogviszonyban álló személyektől egyaránt elvárja, hogy vállalt kötelezettségeiknek maradéktalanul eleget tegyenek, s a Szervezet érdekeit sértő vagy azzal ellentétes tevékenységet – különösen szándékosan – ne végezzenek. A Hivatal az erre vonatkozó garanciális elemeket a munkavégzésre irányuló jogviszony alapját képező megállapodásban, illetve külön jognyilatkozatokban (pl.: titoktartási nyilatkozat) rögzíti.
A Hivatal által kezelt adatok, függetlenül azok típusától vagy tartalmától, kivétel nélkül belső használatú, szervezeti adatoknak minősülnek, amelyek bizalmasságát, sértetlenségét és rendelkezésre állását az azokhoz hozzáféréssel rendelkező, azokat megismerő foglalkoztatottak és a Hivatallal egyéb munkavégzésre irányuló jogviszonyban álló személyek kötelesek megvédeni. A belső használatú adatok és információk kizárólag a jegyző erre vonatkozó jóváhagyását követően, s az általa engedélyezett felületeken hozhatók nyilvánosságra.
A szervezeti adatok védelme érdekében tilos:

- a munkahelyi e-mail cím magáncélú használata, azzal történő regisztráció nem a munkavégzéshez kapcsolódó internetes szolgáltatások (pl.: hírlevél, levelező lista feliratkozás; webáruház, stb.) igénybevételéhez;
- a munkahelyen alkalmazott azonosító és hitelesítő adatok (pl.: jelszavak) magáncélú használata;
- belső használatú adatok és információk, illetve azokat tartalmazó fájlok internetes vagy közösségi média felületeken vagy alkalmazásokban történő engedély nélküli megosztása, illegális közzététele, illetve ideiglenes vagy tartós tárolása (pl.: felhő-alapú tárterületen vagy szolgáltatásban);
- a Hivatal által a munkavégzés céljára biztosított számítógépen vagy egyéb infokommunikációs eszközön fájlcserélő szolgáltatás használata, valamint a munkavégzéshez nem kapcsolódó letöltések végrehajtása.

Az engedély nélküli tevékenységet végrehajtó, szabályszegő személy felelősségre vonása a Fegyelmi intézkedések szakaszban meghatározottak szerint történik.

NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG

A Hivatal alapvető érdeke, hogy az általa az alaptevékenysége végzéséhez használt EIR-ek működésével és használatával összefüggő eseményekről, továbbá az azokhoz és azokban kezelt adatokhoz történő hozzáférésekről, s az azokban bekövetkezett vagy eszközölt változásokról olyan hiteles információkkal rendelkezzen, amelyek lehetővé teszik a Szervezet számára fontos események, illetve változások utólag is igazolható módon történő visszakövetését, kivizsgálását, valamint indokolt esetben a felelősség megalapozott megállapítását.
Ennek biztosítása céljából a Hivatal a naplózással és elszámoltathatósággal kapcsolatos szabályokat jelen Szabályzat keretei között az alábbiakban írja elő, s azzal összefüggésben az itt meghatározott naplózási eljárásrendet lépteti életbe.

Naplózási képesség vizsgálata

A Hivatal az általa az alaptevékenysége végzéséhez használt EIR-ekben, illetve rendszerelemeikben történt, illetve végrehajtott változások rögzítésével, a naplózható események körével kapcsolatban az alábbi, általános minimum elvárásokat támasztja:

Eseménycsoport	Naplózható események
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, • engedélyezés, • módosítás, • letiltás, • törlés.
Hálózati forgalommal kapcsolatos események:	• megvalósult kapcsolat, • blokkolt kapcsolat.
Naplózással kapcsolatos események (sikeres és sikertelen):	• elindítás, (újraindítás), • leállítás, • beállítások módosítása, • napló kiürítése, törlése, • naplóvesztés lehetősége (pl.: tárhely kapacitás elfogyása).

Új EIR vagy rendszereleme beszerzése, illetve bevezetése előtt az EIR, illetve rendszerelem adattartalmától és funkciójától függően indokolt és releváns szintű naplózási képességének előzetes vizsgálatát az IT üzemeltető az EIR-ért felelőssel együttműködve, az IBF bevonásával és szakmai támogatásával köteles elvégezni, s annak eredményét, az elvártként meghatározott naplózási funkcionalitást a gazdasági vezető számára továbbítani, aki azt a beszerzési dokumentációban megfelelőségi követelményként rögzíti.
Meglévő EIR és rendszerelemei esetében azok naplózási képességeit a rendszeres kockázatelemzés keretében az IBF az IT üzemeltető és az EIR-ért felelős bevonásával vizsgálja és értékeli. A naplózási funkciók hiányát az adott EIR, illetve rendszerelem kapcsán az EIR rendszerbiztonsági tervében rögzített naplózási követelményeket figyelembe véve kockázatként azonosítja és kezeli.

Naplóbejegyzések tartalma

A Hivatal az esemény vizsgálatához szükséges és elégséges információk rendelkezésre állásának biztosítása érdekében a naplóbejegyzések elvárt, minimális tartalmát az alábbiakban határozza meg:

- 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) tartalmazniuk kell.

A naplózási képesség vizsgálata során feladatellátása keretében a fenti minimális követelmények teljesülését az IT üzemeltető és az IBF értékelési szempontként köteles alkalmazni.

Naplóinformációk megőrzése, védelme

A Hivatal az általa használt EIR-ek és azon rendszerelemeik esetében, amelyeknél a naplóinformációk kezelése a hatáskörébe tartozik az adott EIR, illetve rendszerelem adattartalmát, funkcióját, működését és tulajdonságait figyelembe véve határozza meg a naplóbejegyzésekre vonatkozóan a biztonsági események utólagos kivizsgálásának biztosítása céljából indokolt és szükséges megőrzési időtartamot.
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 és állományokhoz történő hozzáférést, illetve a naplózási beállítások módosítását kiemelt vagy privilegizált hozzáférési jogosultsághoz

köti, a jogosultak körét munka-, illetve feladatkörhöz rendelten a legkisebb jogosultság elve alapján definiálja.
A Hivatal a naplózásukra vonatkozóan meghatározott részletes követelményeket a rendelkezésében lévő EIR-ek esetében az adott EIR rendszerbiztonsági tervében, illetve az általa használt, de nem saját rendelkezésében lévő EIR-ek és azon rendszerelemeik esetében, amelyeknél a naplózási beállítások, illetve a naplóinformációk kezelése a hatáskörébe tartozik, az üzemeltetési leírásban rögzíti.
A naplózási képesség vizsgálata során feladatellátása keretében a naplóinformációk megőrzésére és védelmére vonatkozó funkciókat az IT üzemeltető és az IBF értékelési szempontként köteles alkalmazni.

Naplózás beállítása, kezelése

A Hivatal azon felügyelete alá tartozó EIR-ek, illetve rendszerelemeik esetében, amelyeknél a naplózási beállítások, illetve a naplóinformációk kezelése a hatáskörébe tartozik, az adott EIR-re, illetve rendszerelemeire meghatározott, a naplózandó eseményekre, a naplóbejegyzések tartalmára, megőrzésükre vonatkozó követelmények szerint a naplózás, továbbá a tárolókapacitás és a hozzáférési jogosultságok beállítása az IT üzemeltető feladata és felelőssége.
Annak érdekében, hogy az események hiteles információkon alapuló és pontos időbeli visszakövethetősége biztosítható legyen, az IT üzemeltető feladata minden rendszerórával rendelkező rendszerelem esetében megbízható, azonos központi időforrás alkalmazásának konfigurálása.
az IT üzemeltető feladata és felelőssége gondoskodni a naplózás beállításoknak megfelelő működésének felügyeletéről, a naplózással és az időszinkronnal kapcsolatban felmerülő hibák kezeléséről.

Naplóbejegyzések vizsgálata

Az IT üzemeltető köteles a naplóbejegyzések vizsgálatát, elemzését a nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából az adott EIR-re vonatkozóan meghatározott rendszerességgel elvégezni, s amennyiben problémát tapasztal, akkor a jegyzőt és az IBF-t tájékoztatni.
Amennyiben a naplóbejegyzések vizsgálata, elemzése során megállapítható, hogy az esemény veszélyeztette vagy veszélyeztetheti a Hivatal által használt EIR-ekben tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát, akkor az IT üzemeltető köteles a Biztonsági események kezelése fejezetben meghatározott eljárásrendben foglaltak szerint eljárni.

Naplózás felülvizsgálata

Az IBF jogosult a naplózható események, illetve a naplózásra beállított események körének és a naplózás konfigurációjának felülvizsgálatára, s a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához szükség szerint további események naplózására, a naplóbejegyzések tartalmának, megőrzésének, tárolásának, illetve a naplózással összefüggő bármely követelmény vagy intézkedés módosítására javaslatot tenni.

HOZZÁFÉRÉS-FELÜGYELET

A Hivatal az alaptevékenysége végzéséhez használt EIR-ekhez, valamint az azokban kezelt adatokhoz, az EIR-ek rendszerelemeihez és az EIR-ek által nyújtott vagy azokon keresztül elérhető szolgáltatásokhoz való logikai hozzáférések felügyeletével kapcsolatos szabályokat jelen Szabályzat keretei között az alábbiakban írja elő, s azzal összefüggésben az itt meghatározott hozzáférés-felügyeleti eljárásrendet lépteti életbe.
A fizikai hozzáférésekre vonatkozó szabályokat a Fizikai hozzáférések felügyelete szakasz tartalmazza.
A hozzáférések felügyeletével kapcsolatos szabályok és kötelezettségek megismertetéséről és annak dokumentálásáról a Hivatal a Személybiztonsági feltételek és a Biztonságtudatossági képzési eljárásrend szakaszokban meghatározottak szerint gondoskodik.
Az IBF a jelen fejezetben meghatározott, a logikai hozzáférések felügyeletével kapcsolatos szabályok betartásának ellenőrzését, illetve azok felülvizsgálatát legalább évente köteles biztonsági helyzetértékelése keretében elvégezni, s annak eredményéről a jegyzőt beszámolójában tájékoztatni.

Felhasználói fiókok kezelése

A Hivatal az általa használt, rendelkezésében lévő EIR-ekben engedélyezett, illetve tiltott fióktípusokat, valamint a hozzáférési szinteket és azok jellemzőit, a felhasználói fiókok kezelésére, a jogosultságok

hozzárendelésére vagy megszüntetésére, továbbá a beállításukra, módosításukra, illetve törlésükre jogosult szerepköröket az EIR rendszerbiztonsági tervében határozza meg és dokumentálja.
A felhasználói fiókok kezelésének, létrehozásuk, módosításuk, illetve megszüntetésük, valamint ezek engedélyezésének szabályait az Azonosítás és hitelesítés fejezet, továbbá Az információbiztonsággal kapcsolatos engedélyezési eljárás fejezet és az Eljárás a jogviszony megszűnésekor szakasz tartalmazza.
A hozzáféréssel kapcsolatos biztonságkritikus események (pl.: sikertelen bejelentkezési kísérletek), valamint a hozzáféréseken (fiók, csoport) végzett műveletek naplózását a Hivatal a Naplózás és elszámoltathatóság fejezetben meghatározottak szerint végzi, annak jellemzőit, illetve az azzal összefüggő események kezelésére alkalmazott intézkedéseket a rendszerbiztonsági tervben rögzíti.
A rendszerbiztonsági tervben meghatározott beállítások végrehajtásáról az IT üzemeltető köteles gondoskodni.

Sikertelen bejelentkezési kísérletek

A Hivatal a rendelkezésében lévő EIR rendszerbiztonsági tervében határozza meg és dokumentálja az EIR, illetve az ahhoz hozzáférést biztosító rendszerelemek (pl.: munkaállomások és kiszolgálók) sikertelen bejelentkezéssel kapcsolatos, az adott EIR vagy rendszerelem kapcsán értelmezhető és releváns biztonsági beállításait (fiókzárolási házirend).
A rendszerbiztonsági tervben meghatározott beállítások végrehajtásáról az IT üzemeltető köteles gondoskodni.
Új EIR fejlesztése esetén a Hivatal a sikertelen bejelentkezési kísérletek kezelésével kapcsolatban minimális feltételként az alábbi szabályoknak történő megfelelést követeli meg:

- a felhasználó egymást követő, előzetesen beállított, konfigurálható számú (legfeljebb 10) sikertelen bejelentkezési kísérlete esetén automatikusan zárolja a felhasználói fiókot (fiókzárolási küszöb);
- a fiók zárolását automatikusan, az előzetesen beállított, konfigurálható időtartam (30 perc – 24 óra) elteltével legyen képes feloldani (fiókzárolás időtartama, fiókzárolási számlázó nullázása).

A Hivatal a követelmények teljesítését a Rendszer- és szolgáltatásbeszerzés fejezetben foglaltak szerint eljárva vizsgálja és hagyja jóvá.
Központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR-ek esetében a Hivatal a rendszer tulajdonosa által biztosított konfigurációs lehetőségeket és az azzal összefüggésben meghatározott szabályokat alkalmazza.
Az IBF jogosult a hozzáférések, illetve felhasználói fiókok kezelésével kapcsolatos beállítások és tevékenységek ellenőrzésére. Az ellenőrzés részét képezi az engedélyezett és a ténylegesen beállított hozzáférések és jogosultságok ellenőrzése, felülvizsgálata, amelyben az IT üzemeltető köteles közreműködni, ahhoz információkat nyújtani. Az ellenőrzést az IBF legalább évente köteles biztonsági helyzetértékelése keretében elvégezni, s annak eredményéről a jegyzőt beszámolójában tájékoztatni.

A rendszerhasználat jelzése

A Hivatal a rendelkezésében lévő EIR esetében a rendszerhasználat jelzésével kapcsolatos intézkedéseket a rendszerbiztonsági tervben határozza meg és dokumentálja, s amennyiben technológiai szempontból megvalósítható, akkor a beállítások végrehajtásáról az IT üzemeltető köteles gondoskodni.
A Hivatal nyilvánosan elérhető EIR, illetve ahhoz hozzáférést biztosító rendszerelem (pl.: terminál, vezeték nélküli hálózat) működtetése esetén gondoskodik arról, hogy az

- kijelezze a rendszer használatának feltételeit, mielőtt ahhoz további hozzáférést biztosít;
- kijelezze az adatvédelmi szabályoknak való megfelelőségére vonatkozó információkat, amennyiben a hozzáféréshez adatkezelés, adatrögzítés, illetve arról vagy a rendszer használatáról naplózás történik;
- tájékoztatást biztosítson a rendszer engedélyezett felhasználásáról.

Új EIR fejlesztése esetén a Hivatal követelményként előírja, hogy az legyen képes a rendszerhasználat jelzésére vonatkozó interaktív bejelentkezési üzenet megjelenítésére és a felhasználási feltételek elfogadásával kapcsolatos aktivitás, tevékenység kezelésére, s ezek teljesítését a Rendszer- és szolgáltatásbeszerzés fejezetben foglaltak szerint vizsgálja, illetve hagyja jóvá.

Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

A Hivatal a rendelkezésében lévő EIR-ek rendszerbiztonsági tervében azonosítja és határozza meg, valamint dokumentálja az EIR-ben azonosítás vagy hitelesítés nélkül végrehajtható felhasználói tevékenységeket.

A Hivatal által használt EIR-ekhez hozzáférést biztosító, a Szervezet által felügyelt munkaállomások és kiszolgálók kizárólag azonosítást és hitelesítést követően vehetők igénybe.
A Hivatal a rendelkezésében lévő, a felügyelete, irányítása alatt álló, nyilvánosan elérhető (közzétett) tartalmakat kezelő EIR esetében a tartalom adminisztrálásához, illetve a rendszer üzemeltetéséhez szükséges privilegizált hozzáférések szintén csak azonosításhoz és hitelesítéshez kötötten alkalmazhatók.
Fentiek beállításáról, továbbá az esetükben az azonosítás és hitelesítés nélküli hozzáférést vagy anonim bejelentkezést lehetővé tevő beépített fiókok (pl.: vendég) letiltásáról az IT üzemeltető köteles gondoskodni.

Távoli hozzáférés

A Hivatal a rendelkezésében lévő EIR rendszerbiztonsági tervében határozza meg és dokumentálja az EIR-hez való távoli hozzáférés szabályait, a távoli hozzáférésre jogosult szerepköröket, illetve felhasználói fiókokat, valamint a távoli hozzáférés típusának megfelelő kapcsolódási- és konfigurációs követelményeket.
A rendszerbiztonsági tervben meghatározott beállítások végrehajtásáról az IT üzemeltető köteles gondoskodni.
A Hivatal az általa használt EIR-ekhez történő, illetve az üzemeltetési célú (pl.: távsegítség biztosítása) távoli hozzáférések kapcsán egyaránt minimálisan a titkosított adatátviteli csatorna alkalmazását (pl.: VPN kapcsolaton keresztül megvalósítva) követeli meg.
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 távoli hozzáféréshez használt, illetve tervezett megoldás biztonsági követelményeknek való megfelelőségét az IBF 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 IBF javaslata alapján dönt a használatának engedélyezéséről, illetve ellenkező esetben a követelményeknek megfelelő rendszerrel történő kiváltásának elrendeléséről.

Vezeték nélküli hozzáférés

A Hivatal a rendelkezésében lévő EIR rendszerbiztonsági tervében határozza meg és dokumentálja az EIR-hez való vezeték nélküli hozzáférés szabályait, valamint a vezeték nélküli hozzáférés típusának megfelelő kapcsolódási- és konfigurációs követelményeket.
A rendszerbiztonsági tervben meghatározott beállítások végrehajtásáról az IT üzemeltető köteles gondoskodni.
A Hivatal által munkavégzés céljára biztosított vezeték nélküli hálózat hozzáférés-védelemmel (minimum jelszavas védelemmel) és a csatlakoztatható eszközök azonosításával és szűrésével létesíthető. A munkavégzés céljára biztosított vezeték nélküli hálózathoz kizárólag a Szervezet által biztosított, illetve felügyelt mobil infokommunikációs eszköz csatlakoztatható.
A vezeték nélküli hozzáféréshez alkalmazott, illetve tervezett technológia rendszerelemeinek és beállításainak biztonsági követelményeknek való megfelelőségét az IBF jogosult megvizsgálni, s annak eredményéről a jegyző számára javaslatot tenni, aki dönt a vezeték nélküli hozzáférés engedélyezéséről vagy tiltásáról, a követelményeknek megfelelő technológiával történő kiváltásának elrendeléséről.

Mobil eszközök hozzáférés-ellenőrzése

A Hivatal a rendelkezésében lévő EIR rendszerbiztonsági tervében határozza meg és dokumentálja az EIR-hez mobil eszközökkel történő kapcsolódás szabályait, a kapcsolódási- és konfigurációs követelményeket, valamint a kapcsolódásra engedélyezett mobil eszközök felügyeletével összefüggő biztonsági intézkedéseket.
A rendszerbiztonsági tervben meghatározott, továbbá a Hivatal által munkavégzés céljára biztosított mobil eszközök használatba vétele előtt azok esetében az Adathordozók védelme fejezetben és a Kártékony kódok elleni védelem szakaszban előírt, valamint a biztonságos távoli hozzáféréshez szükséges beállítások végrehajtásáról az IT üzemeltető köteles gondoskodni.

Külső rendszerek használata

A Hivatal a rendelkezésében lévő EIR rendszerbiztonsági tervében azonosítja és dokumentálja az EIR-hez kapcsolódó, illetve ahhoz hozzáférésre engedélyezett külső rendszereket. Külső rendszerből hozzáférést az

EIR-hez, illetve annak használatával a Hivatal által ellenőrzött információk feldolgozását, tárolását vagy továbbítását kizárólag akkor és azon személyek számára engedélyez és hagy 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 rendszert befogadó szervezettel.

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

Nyilvánosan elérhető tartalom

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

- a Szervezet 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) továbbítása korlátozás nélküli megtekintésre, illetve felhasználásra – a jegyző általános engedélyével.

A hatályos jogszabályi előírásokban meghatározott közzétételi kötelezettséggel kapcsolatos szabályokat, feladatokat és felelősségeket a Hivatal tárgyban vonatkozó belső előírása tartalmazza.
A Hivatalnál kizárólag a jegyző által engedélyezett információkat lehet közzétenni. Minden más információ közzététele TILOS!
A jegyző feladata és felelőssége gondoskodni a nyilvánosságra hozásra, illetve közzétételre javasolt tartalom ellenőrzéséről, valamint az azok közzétételre feljogosított foglalkoztatottaknak a közzététel tartalmával (általánosan közzétételre engedélyezett információk köre, nem nyilvános információk köre, stb.) kapcsolatos felkészítéséről.
Minden foglalkoztatott köteles munkahelyi felettese számára jelezni, ha a Hivatal által kezelt vagy bármely egyéb felületen olyan információk megjelenését észleli, amelyek ismeretei szerint nem hozhatók nyilvánosságra (pl.: belső használatú információk vagy szervezeti adatok).
A jegyző jogosult és köteles rendszeresen átvizsgálni a nyilvánosan hozzáférhető és a honlapon közzétett információkat, s amennyiben nem nyilvános tartalmat talál, intézkedni annak eltávolításáról.
A nyilvánosan elérhető tartalmakat kezelő, illetve a közzétételre alkalmazott felületen az információk elhelyezésében, törlésében az adott felület karbantartásával, illetve adminisztrálásával megbízott felelős köteles közreműködni.

AZONOSÍTÁS ÉS HITELESÍTÉS

A Hivatal az alaptevékenysége végzéséhez használt EIR-ekhez a munka, illetve feladatkörüknek megfelelő mértékben hozzáférést biztosít a foglalkoztattak és a Hivatallal bármely egyéb munkavégzésre irányuló jogviszonyban álló személyek számára. A hozzáférésekhez szükséges azonosítók és hitelesítő eszközök kezelésével és felügyeletével kapcsolatos szabályokat a Hivatal jelen Szabályzat keretei között az alábbiakban írja elő, s azzal összefüggésben az itt meghatározott eljárásrendet lépteti életbe.
A Hivatal által az alaptevékenysége végzéséhez használt EIR-ekhez történő felhasználói hozzáférés a felhasználók által végzett tevékenységek nyomon követhetőségének biztosítása érdekében alapértelmezetten kizárólag egyedi azonosítást és hitelesítést követően engedélyezett. Szervezeten kívüli felhasználók esetében az egyedi azonosítás és hitelesítés mellett a hozzáféréssel kapcsolatos kockázatok által indokolt esetben a külső partnert képviselő személyazonosságának igazolása, ellenőrzése céljából a Hivatal további biztonsági feltételeket és eljárásokat is jogosult meghatározni, s azokat megállapodásukban rögzíteni. Csoportszintű hozzáférés csak a munkavégzés folyamatosságának, illetve 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 változtatással járó önálló művelet nem hajtható végre (pl.: egyirányú, passzív kommunikáció: csoportos levelezési cím, terjesztési lista). Ettől eltérni indokolt esetben és Az információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben előírt vezetői jóváhagyást követően az Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek szakaszban foglaltak szerint lehet.
Az EIR-ekhez való hozzáférések típusait, az azonosítás és hitelesítés módját és az azzal összefüggő követelményeket, az alkalmazott, illetve tervezett további védelmi intézkedéseket, valamint a hozzáférésre

engedélyezett szervezeten kívüli felhasználók körét a Hivatal a rendelkezésében lévő EIR rendszerbiztonsági tervében határozza meg és dokumentálja.
Az azonosítók és hitelesítő eszközök kezelésének engedélyezésével összefüggő szabályokat Az információbiztonsággal kapcsolatos engedélyezési eljárás fejezet és az Eljárás a jogviszony megszűnésekor szakasz tartalmazza.
A felhasználói fiókokkal végzett tevékenységek naplózását a Hivatal a Naplózás és elszámoltathatóság fejezetben meghatározottak szerint végzi, annak jellemzőit a rendszerbiztonsági tervben rögzíti.
Új EIR fejlesztése esetén a rendszer azonosítási és hitelesítési megoldásait, az azzal kapcsolatos biztonsági követelmények teljesítését a Hivatal a Rendszer- és szolgáltatásbeszerzés fejezetben foglaltak szerint vizsgálja, illetve hagyja jóvá.
Az IBF a jelen fejezetben meghatározott, az azonosítással és hitelesítéssel kapcsolatos szabályok betartásának ellenőrzését, illetve azok felülvizsgálatát legalább évente köteles biztonsági helyzetértékelése keretében elvégezni, s annak eredményéről a jegyzőt beszámolójában tájékoztatni.

Privilegizált fiókok

Az EIR-kehez, illetve az azokban kezelt adatokhoz magasabb szintű hozzáférési jogosultsággal rendelkező, privilegizált felhasználói fiókok körét, valamint az esetükben bevezetett, illetve tervezett hitelesítési eljárást és gyakorlati megoldást a Hivatal a rendelkezésében lévő EIR rendszerbiztonsági tervében határozza meg és dokumentálja.
Új EIR fejlesztése esetén a Hivatal a privilegizált felhasználói fiókkal való hozzáféréshez visszajátszás elleni védelmet biztosító, többtényezős hitelesítés alkalmazását követeli meg.
A meglévő EIR-ek esetében, amennyiben a rendelkezésében lévő EIR-ben, illetve az ahhoz való hozzáférést biztosító rendszerelemben technológiai szempontból megvalósítható, akkor a Hivatal gondoskodik a többtényezős hitelesítés kialakításáról a privilegizált hálózati hozzáférésekhez.

Azonosító kezelés

A Hivatal a rendelkezésében lévő EIR-ekben, illetve rendszerelemeikben egyedi azonosítás céljára felhasználóneveket alkalmaz, a felhasználói azonosítók kezelése: létrehozása, kiosztása, hozzárendelése Az információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben foglaltak szerint jóváhagyott egyénhez, csoporthoz, szerepkörhöz vagy eszközhöz, valamint nyilvántartásuk az IT üzemeltető feladata és felelőssége.
A korábban kiosztott, már nem használt, illetve az Eljárás a jogviszony megszűnésekor szakaszban foglaltak szerint letiltott egyedi azonosító újbóli felhasználása vagy más egyénhez, csoporthoz, szerepkörhöz vagy eszközhöz történő hozzárendelése felhasználói azonosító esetén a letiltását követő 5 évig, eszköz azonosító esetén az azzal azonosított eszköz használatból történő kivonásáig tilos!

A hitelesítésre szolgáló eszközök kezelése

A hitelesítő eszközök kiosztása Az információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben foglaltak szerint jóváhagyott személyek számára az Azonosító kezelés szakaszban előírtak szerint az azonosítók kezelésére feljogosított szerepkört betöltő feladata és felelőssége.
A Hivatal a rendelkezésében lévő EIR-ek, illetve rendszerelemeik esetében alkalmazott hitelesítő eszközöket és jellemzőiket (pl.: jelszó házirend, a birtoklásalapú hitelesítésre szolgáló eszközök használati ideje, ismételt felhasználhatóságuk feltételei, stb.) az adott EIR-nek a Szervezet működésében betöltött szerepét és funkcióját, az EIR-ben kezelt adatok típusát és mennyiségét, valamint a gyártó, illetve kibocsátó ajánlásait egyaránt figyelembe véve, a rendszerbiztonsági tervben határozza meg és dokumentálja.
A Hivatal a felhasználói jelszavakra vonatkozó minimálisan alkalmazandó általános jelszó követelményeket az alábbiak szerint állapítja meg:

- 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 magasabb védelmi szintet jelentő irányba, felfelé lehet (pl.: erősebb jelszavak vagy a „jelszó helyett jelmondat"-elv alkalmazásával), amennyiben az adott EIR, illetve rendszerelem azt képes kezelni.

Központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR esetében a Hivatal a rendszer tulajdonosa által meghatározott jelszóképzési szabályokat alkalmazza.
A hitelesítő eszköz kiosztásáért felelős az ahhoz kapcsolódó kezdeti jelszó beállítását, illetve az alapértelmezett jelszó megváltoztatását a fenti jelszóképzési szabályoknak megfelelően köteles elvégezni, valamint gondoskodni arról, hogy a jelszónak a hozzárendelt azonosítót birtokló személyhez történő továbbítása biztonságos módon, például illetéktelen hozzáféréstől védett, titkosított csatornán történjen. Ha a kezdeti jelszó kötelező megváltoztatásának kikényszerítése az adott EIR-ben vagy rendszerelemben nem automatikusan történik, akkor gondoskodik arról, hogy az beállításra kerüljön, illetve amennyiben az nem támogatott, akkor felhívja az eszköz birtokosának figyelmét annak megváltoztatására.
Új rendszerelem beszerzése esetén a privilegizált hozzáférések alapértelmezett jelszavait (pl.: hálózati eszköz admin hozzáférésének jelszava) az IT üzemeltető köteles a rendszerelem első konfigurációja, telepítése alkalmával megváltoztatni.
A kiosztott hitelesítő eszköz birtokosának a 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 Biztonsági események kezelése fejezetben meghatározottak szerint jelenteni.
Hitelesítő eszközt érintő biztonsági esemény, illetve a hozzáférésekkel összefüggő további indokolt esetekben (pl.: csoporttagság megváltozása, ideiglenes hozzáférés szükségtelenné válása) a hitelesítő eszköz kiosztásáért felelős köteles gondoskodni a hitelesítő eszköz tartalmának (pl.: a jelszó) módosításáról, illetve visszavonásáról.

Újrahitelesítés

A Hivatal az alaptevékenysége végzéséhez feltétlenül szükséges, rendelkezésében lévő EIR-ekhez, illetve a működése szempontjából kritikus infrastruktúra részének minősülő rendszerelemeikhez történő hozzáférések, különösen, de nem kizárólagosan a privilegizált felhasználói fiókkal, hálózaton keresztül történő, illetve távoli hozzáférések esetében a jogosulatlan hozzáférés kockázatának csökkentése érdekében munkaszakasz zárolást alkalmaz, melynek feloldását újrahitelesítés kikényszerítéséhez köti. A Hivatal a munkaszakasz zárolásban érintett EIR, illetve rendszerelemei körét, valamint az azzal kapcsolatos beállításokat és szabályokat a rendszerbiztonsági tervben határozza meg és dokumentálja.

KONFIGURÁCIÓKEZELÉS

A Hivatal az általa használt EIR-ek és rendszerelemeik konfigurációjának kezelésére vonatkozó szabályokat jelen Szabályzat keretei között az alábbiakban írja elő, s azzal összefüggésben az itt meghatározott konfigurációkezelési eljárásrendet lépteti életbe.
A Hivatal által használt EIR-ek esetében a konfiguráció kezelése általánosan az IT üzemeltető feladata és felelőssége. Ettől eltérő esetben a Hivatal az erre feljogosított szerepkört a rendszerbiztonsági tervben rögzíti.
A konfiguráció megváltozását annak végrehajtója köteles dokumentálni a jelen fejezetben meghatározott, vonatkozó rendszer dokumentációban, illetve nyilvántartásban.
Az IBF a jelen fejezetben meghatározott, a konfigurációk kezelésével kapcsolatos szabályok betartásának ellenőrzését, illetve azok felülvizsgálatát legalább évente köteles biztonsági helyzetértékelése keretében elvégezni, s annak eredményéről a jegyzőt beszámolójában tájékoztatni.

Alapkonfiguráció

A Hivatal a rendelkezésében lévő EIR-ek alapkonfigurációjára vonatkozó információkat, továbbá annak változásait a rendszerbiztonsági tervben dokumentálja és tartja karban.
Az alapkonfiguráció felülvizsgálatát a Hivatal a Rendszerbiztonsági terv szakaszban előírtak szerint hajtja végre.
Központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR 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.

Konfigurációs beállítások

A Hivatal a rendelkezésében lévő EIR-ek rendszerelemeire vonatkozó egységes biztonsági konfigurációs beállításokat a legszűkebb funkcionalitás elvének megfelelően, a működési követelményeknek még

megfelelő, ugyanakkor biztonsági szempontból a lehető leginkább korlátozott módon, az ügymenet szempontjából nem szükséges funkciók, portok, protokollok, szolgáltatások korlátozásával, illetve tiltásával a rendszerbiztonsági tervben 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 konfigurációs beállításokat.
A rendszerelemekre meghatározott konfigurációs beállítások végrehajtása az IT üzemeltető feladata és felelőssége. Amennyiben a konfigurálás során a meghatározott beállításokhoz képest eltérést tapasztal, úgy azt köteles a rendszer dokumentációjában rögzíteni.

Rendszerelem leltár

A Hivatal által használt EIR-ek rendszerelemeiről, a hardver és szoftver komponensekről az IT üzemeltető köteles naprakész és részletes nyilvántartást vezetni, amelynek 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 az IT üzemeltető köteles biztosítani a Hivatal számára a nyilvántartás adataihoz történő folyamatos hozzáférést.

A szoftverhasználat korlátozásai

A Hivatal által használt EIR-ek működési környezetét képező kiszolgálókon és munkaállomásokon, informatikai rendszereiben kizárólag jogtiszta, a Szervezet által megvásárolt kereskedelmi, illetve szabad felhasználású, valamint jogszabályban előírt központi szolgáltató által biztosított szoftver termékek telepítése és használata engedélyezett.
Az IT üzemeltető feladata és felelőssége ellenőrizni a kiszolgálókon és munkaállomásokon telepített szoftver alkalmazásokat, a mennyiségi licencekkel védett szoftverek használatát a rendszerelem leltárban, illetve kereskedelmi szoftver esetén a felhasználásra vonatkozó szerződésben szereplő engedélyezett licence szám alapján, valamint az állomány megosztásokat az esetlegesen szerzői joggal védett szoftverek, illetve tartalmak jogosulatlan terjesztésére, megjelenítésére, előadására vagy sokszorosítására irányuló tevékenységek szűrése céljából. Amennyiben a szoftver felhasználására vonatkozó licence darabszámhoz képest eltérést tapasztal, az IT üzemeltető feladata és felelőssége kezdeményezni a felhasználók számának megfelelően a szükséges többlet licencek beszerzését, illetve a licencek mennyiségének csökkentését.
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 vonása Fegyelmi intézkedések szakaszban meghatározottak szerint történik.

Felhasználó által telepített szoftverek

A Hivatal a foglalkoztatottak számára az informatikai eszközöket és erőforrásokat a munkavégzés céljára biztosítja, azokon kizárólag a munkavégzéshez szükséges szoftverek és alkalmazások használatára jogosultak. A munkaállomásokra az IT üzemeltető jogosult új szoftver telepítésére, a felhasználók nem telepíthetnek programokat, továbbá nem módosíthatják a telepített szoftverek konfigurációját, működését és nem távolíthatják el azokat!
Kivételt fenti korlátozás alól a munkavégzés által indokolt esetben, illetve például a személyes használatra engedélyezett mobil munkaállomás esetén Az információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben foglaltak szerint a jegyző engedélyezhet.
A munkavégzés, az ügymenet, illetve az adott folyamat hatékonyságát javító szoftverek használatára a foglalkoztatottak javaslatot tehetnek munkahelyi felettesük felé, aki Az információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben foglaltaknak megfelelően eljárva kezdeményezheti a szoftver beszerzésének és telepítésének engedélyezését.
A munkaállomásokra telepített szoftvereket az IT üzemeltető feladata és felelőssége a munkaállomás eseti vagy rendszeres karbantartása alkalmával, de legalább évente ellenőrizni.

ÉRTÉKELÉS, ENGEDÉLYEZÉS ÉS MONITOROZÁS

A Hivatal az alaptevékenysége végzéséhez használt EIR-ek és működési környezetük védelmi intézkedéseinek rendszeres értékelésének biztosítása céljából az azzal kapcsolatos szabályokat jelen Szabályzat keretei között az alábbiakban írja elő, s azzal összefüggésben az itt meghatározott biztonságértékelési eljárásrendet lépteti életbe.
A jelen fejezetben rögzített szabályok és alkalmazásuk megfelelőségét az IBF jogosult és köteles feladatellátása keretében, az IBSZ felülvizsgálata során ellenőrizni, s annak eredményéről a jegyzőt beszámolójában tájékoztatni.

Biztonsági értékelések

A Hivatal az alaptevékenysége végzéséhez használt, rendelkezésében lévő EIR-ek és működési környezetük védelmi intézkedéseinek biztonsági értékelését a rendszerek teljes életciklusában az alábbiakban felsorolt, tervezett tevékenységek következetes végrehajtásával valósítja meg.
A Rendszer- és szolgáltatásbeszerzés fejezetben foglaltak szerint új EIR vagy rendszerelem beszerzése, bevezetése vagy fejlesztése során már annak tervezési szakaszában meghatározza az EIR biztonsági osztály besorolásának megfelelő, teljesítendő biztonsági követelményeket, s azok megvalósítását ellenőrzi és értékeli.
A rendszerbiztonsági tervben rögzíti az EIR biztonsági osztály besorolásának megfelelő követelmények teljesítésével összefüggő, megvalósítandó védelmi intézkedéseket, végrehajtandó feladatokat, valamint a végrehajtásukhoz rendelt határidőket és felelősségeket, s a tervben meghatározott határidőknek megfelelően ellenőrzi és értékeli a védelmi intézkedések megvalósítását.
A Kockázatmenedzsment fejezetben foglaltak szerint vizsgálja rendszerelem, rendszer, illetve szervezeti szinten egyaránt a felmerülő kockázatokat, gondoskodik a kockázatelemzés rendszeres végrehajtásáról, a kockázatok kezelésére vonatkozó védelmi intézkedések kiválasztásáról, tervezéséről és végrehajtásáról, s a végrehajtott kockázatkezelési intézkedések hatásosságának és eredményességének, valamint az érintett EIR-ek biztonságára gyakorolt hatásaik, teljesítményük méréséről, elemzéséről és értékeléséről, továbbá mindezek rendszeres felülvizsgálatáról.
Folyamatosan figyelemmel kíséri az általa használt EIR-ek, illetve rendszerelemeikkel kapcsolatos új fenyegetettségekre, sérülékenységekre vonatkozó legfrissebb információkat, s gondoskodik az azokra történő hatékony reagálásról, a szükséges védelmi intézkedések végrehajtásáról.
Az elektronikus információs rendszer monitorozása szakaszban foglaltak szerint folyamatosan figyelemmel kíséri az EIR állapotát, összegyűjti és elemzi az EIR-rel kapcsolatos eseményekre vonatkozó információkat.
A felügyeleti információkat felhasználja A biztonsági események kivizsgálása, értékelése és kezelése (biztonsági eseménykezelési terv) szakaszban foglaltak szerint a biztonsági események értékelése során a hasonló események jövőbeni előfordulási kockázatának csökkentése érdekében indokolt új védelmi intézkedések bevezetésére, illetve meglévő intézkedések módosítására vonatkozó javaslatok készítéséhez.
A Hivatal a megbízott IBF feladatellátása által gondoskodik a megvalósított védelmi intézkedéseknek, valamint a biztonsági követelményeknek történő megfelelése rendszeres értékeléséről, s az értékelés eredményének visszacsatolásáról és beépítéséről a kockázatmenedzsment, illetve a biztonságtervezési folyamatokba.
A Hivatal által használt EIR-ek és működési környezetük védelmi intézkedéseit, a bevezetett intézkedések működőképességét, valamint a tervezettnek, az előírt biztonsági követelményeknek megfelelő működését az IBF felülvizsgálati tevékenysége keretében jogosult és köteles ellenőrizni, illetve értékelni:

- új elektronikus információs rendszer bevezetése;
- a biztonsági osztályba sorolás;
- a rendszerbiztonsági terv elkészítése, illetve felülvizsgálata, az abban meghatározott intézkedések ellenőrzése, értékelése;
- a kockázatelemzés, illetve helyzetfelmérés;
- a kockázatkezelési intézkedések, a cselekvési, illetve intézkedési tervek végrehajtásának ellenőrzése;
- valamint az IBSZ felülvizsgálata során.

Az IBF feladata a biztonságértékelés eredményét összefoglaló jelentés (biztonsági helyzetértékelés) elkészítése és megküldése a jegyző számára. Az értékelés eredményétől függően az IBF a jelentésében javaslatot tehet a jegyző számára a meglévő intézkedések, valamint a tervek módosítására, felülvizsgálatára, illetve új védelmi intézkedések bevezetésére.

Az intézkedési terv és mérföldkövei

A Hivatal az alaptevékenysége végzéséhez használt, rendelkezésében lévő EIR-ek rendszerbiztonsági tervében rögzíti az EIR biztonsági osztály besorolásának megfelelő követelmények teljesítésével összefüggő, megvalósítandó védelmi intézkedéseket, végrehajtandó feladatokat, valamint a végrehajtásukhoz rendelt határidőket és felelősségeket, s a tervben meghatározott határidőknek megfelelően ellenőrzi és értékeli a védelmi intézkedések megvalósítását.
A Hivatal a Kockázatmenedzsment fejezetben foglaltak szerint gondoskodik a kockázatelemzés rendszeres végrehajtásáról, a kockázatok kezelésére vonatkozó védelmi intézkedések kiválasztásáról, tervezéséről és végrehajtásáról, valamint a tervezett védelmi intézkedések meghatározott végrehajtási határidőihez igazodva azok megvalósításának ellenőrzéséről és értékeléséről.

Engedélyezés

Az információbiztonsággal kapcsolatos engedélyezés kiterjed minden, a Hivatal hatókörébe tartozó emberi, fizikai és logikai erőforrásra, eljárási és védelmi szintre, valamint folyamatra. Az engedélyezés részletes szabályait Az információbiztonsággal kapcsolatos engedélyezési eljárás fejezet tartalmazza.

Folyamatos felügyelet

A Hivatal a rendelkezésében EIR-ek folyamatos felügyeletét Az elektronikus információs rendszer monitorozása és a Biztonsági értékelés szakaszban foglaltak szerint látja el és értékeli az alkalmazott védelmi intézkedések hatékonyságát, biztonsági teljesítményüket. Az értékelés során egyaránt figyelembe veszi az adott védelmi intézkedéssel megvalósított kontroll megfelelő működésének megszakadásával, megkerülésével vagy kijátszásával, az EIR-ek rendelkezésre állásával kapcsolatos, illetve annak elvesztésével járó biztonsági események számát, a kiesés időtartamát, továbbá a reagáláshoz, a helyreállításhoz szükséges időt.
A Hivatal a Kockázatmenedzsment fejezetben foglaltak szerint gondoskodik a rendelkezésében EIR-ekkel összefüggő kockázatok kezeléséről, a kockázatok monitorozásáról, változásaik nyomon követéséről, felülvizsgálatukról, továbbá a kockázatkezelési válaszintézkedések hatékonyságának értékeléséről.

RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG

A Hivatal az általa használt EIR-ekre, illetve amennyiben és amelyekre értelmezhető, rendszerelemeikre vonatkozó rendszer- és információsértetlenségi eljárásrendet jelen fő fejezetben, az alábbiak szerint határozza meg.
A Hivatal informatikai infrastruktúrájába, üzemeltetés felügyeleti hatáskörébe tartozó, biztonságkritikus rendszerelemek észlelt, illetve ismertté vált hibáinak javításáról, illetve rendszeres karbantartásáról az IT üzemeltető köteles gondoskodni.
A hibajavítás rendszeres támogatását és felügyeletét, valamint az ismert sérülékenységekből adódó kockázatok csökkentését, illetve kezelését, a Hivatal rendszerelem szintű sérülékenység- és frissítésfigyelés alkalmazásával látja el a Biztonsági riasztások és tájékoztatások kezelése szakaszban foglaltak szerint.

Kártékony kódok elleni védelem

A Hivatal minden interneteléréssel rendelkező munkaállomásán és a Szervezet 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.: e-mail 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, működési feltételei biztosításáról (pl.: szükséges licencek) a Hivatal köteles gondoskodni. Az IBF 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 egyenszilárdságú és kockázatokkal arányos védelmét (pl.: kritikus sérülékenységei válnak ismertté, gyártói támogatása nem biztosítja valamely elvárt funkcionalitást vagy megszűnik, stb.).
Minden foglalkoztatott 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 Biztonsági események kezelése fejezetben meghatározottak szerint eljárni.
Vírusfertőzés tényének fennállása esetén az IT üzemeltető jelzése nyomán a jegyző kihirdeti a vírusriadó állapotot, s gondoskodik a foglalkoztatottak ezzel kapcsolatos tájékoztatásáról.
A vírusriadó időtartama alatt minden foglalkoztatott köteles együttműködni a vírusfertőzés továbbterjedését, valamint a helyreállítási tevékenységeket érintően az IT üzemeltető, illetve az IBF által meghatározott intézkedések (pl.: munkaállomások ideiglenes leállítása, internet használat felfüggesztése, stb.) végrehajtásában.
A helyreállítási tevékenység keretében az IT üzemeltető gondoskodik – szükség szerint a foglalkoztatottak bevonásával, közreműködésével – a fertőzött eszköznek a 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 biztonsági 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.

Az elektronikus információs rendszer monitorozása

A Hivatal az általa használt, rendelkezésében lévő EIR-ek, illetve rendszerelemeik esetében a Naplózás és elszámoltathatóság és a Hozzáférés-felügyelet fejezetekben meghatározott tevékenységekkel biztosítja az EIR állapotának figyelemmel kísérését, az EIR-rel kapcsolatos események összegyűjtését és elemzését.
Fokozott kockázatra utaló jel észlelése esetén a Hivatal az EIR felügyeletét az IBF szakmai javaslata alapján, a feltételezett kockázattól függően a naplózandó események körének kibővítésével, a naplóinformációk tartalmának módosításával, illetve a naplóvizsgálati gyakoriság növelésével erősíti meg, melynek beállítása, illetve végrehajtása az IT üzemeltető feladata és felelőssége.
Az EIR rendellenes működése, jogosulatlan használat, illetve hozzáférés észlelése vagy gyanúja esetén a Hivatal a Biztonsági események kezelése fejezetben előírt eljárásrendet követi.
Az EIR-ek állapotának figyelemmel kísérésével kapcsolatban rendelkezésre álló felügyeleti információkat az IBF számára, annak éves felülvizsgálati tevékenységéhez, illetve eseti jelleggel a biztonsági esemény értékeléséhez, kivizsgálásához, illetve bejelentéséhez az IT üzemeltető köteles biztosítani.

Biztonsági riasztások és tájékoztatások kezelése

Az IT üzemeltető feladata és felelőssége az üzemeltetésében lévő rendszerelemek gyártói által kiadott biztonsági riasztások és tájékoztatások, valamint az esetileg vagy rendszeresen általuk kiadott hibajavító csomagok, biztonsági frissítések figyelemmel kísérése.
Az IBF folyamatosan figyelemmel kíséri a hazai-, illetve nemzetközi kiberbiztonsági szakmai fórumok, továbbá felügyeleti szervek által a széles-körben használt rendszerelemeket érintő fenyegetettségekre, sérülékenységekre vonatkozó legfrissebb információkat és biztonságtudatossági figyelemfelhívó kampányokat, s jelzi az IT üzemeltető, illetve a Hivatal számára a szükséges védelmi intézkedések megtétele, illetve a felhasználók tájékoztatása céljából. A felhasználók tájékoztatásáról a jegyző gondoskodik.
Az IT üzemeltető a riasztás, illetve tájékoztatás alapján ellenőrzi az általa üzemeltetett rendszerelemek esetében azok érintettségét, s amennyiben a szükséges hibajavító csomag vagy biztonsági frissítés hiánya, illetve a sérülékenység fennállásának ténye megállapításra kerül, akkor megszervezi vagy elvégzi azok ütemezett telepítését, s azt a Karbantartás fejezetben meghatározottak szerint dokumentálja.
Ha a sérülékenységről szóló jelzés időpontját megelőzően az annak javítására vonatkozó intézkedések már megtörténtek, akkor az IT üzemeltető erről visszajelzést küld az IBF számára.

Abban az esetben, ha a hibajavítás végrehajtása az EIR(ek) vagy rendszerelemeik működésében, a hozzáférésükben előre láthatóan kiesést okoz, akkor az IT üzemeltető a javítás ütemezését úgy köteles megszervezni, hogy a kiesés időtartama a lehető legkisebb mértékű legyen, valamint előzetesen jelezni ezt a jegyző számára, hogy a tervezett javítási időablakhoz kapcsolódó munkaszervezési és tájékoztatási feladataikról gondoskodni tudjanak. A kieséssel járó tervezett hibajavítás jóváhagyásáról a jegyző dönt.
Az elvégzett hibajavítást követően az IT üzemeltető feladata és felelőssége a sérülékenység fennállásának tesztelése, visszaellenőrzése és a változás dokumentált rögzítése.

RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM

A Hivatal az alaptevékenysége végzéséhez használt, rendelkezésében lévő EIR-ek, valamint az azokban kezelt szervezeti adatok kockázatokkal arányos védelmének megvalósítása és fenntartása érdekében a rendszer- és kommunikációvédelmi szabályokat jelen Szabályzat keretei között az alábbiakban írja elő, s azzal összefüggésben az itt meghatározott eljárásrendet lépteti életbe.
Az IBF a jelen fejezetben meghatározott szabályok betartásának ellenőrzését, illetve azok felülvizsgálatát legalább évente köteles biztonsági helyzetértékelése keretében elvégezni, s annak eredményéről a jegyzőt beszámolójában tájékoztatni.

Szolgáltatásmegtagadással járó támadások elleni védelem

A Hivatal a kockázatkezelési és biztonsági tervezési tevékenységei során rendszeresen vizsgálja és értékeli a hálózati kommunikációval összefüggő, köztük a szolgáltatásmegtagadással járó támadások elleni védelemmel kapcsolatban alkalmazott intézkedései megfelelőségét, s meghatározza és dokumentálja a kockázatokkal arányos, megvalósítandó válaszintézkedéseket.
A Hivatal a szolgáltatásmegtagadással járó támadások elleni védelem érdekében a hálózati-, illetve internet szolgáltatást nyújtó kiválasztása során előnyben részesíti azon szolgáltatókat, amelyek a hálózati túlterheléses támadások kivédésére saját megoldással, illetve megfelelő kapacitásokkal rendelkeznek.
A Hivatal A szoftverhasználat korlátozásai és a Kártékony kódok elleni védelem szakaszokban 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 Biztonsági események kezelése fejezetben foglaltak szerint jár el.

A határok védelme

A Hivatal a belső hálózat védelmének biztosítása érdekében határvédelmi megoldást (tűzfal) alkalmaz a hálózati forgalom felügyeletére, irányítására. A határvédelmi eszköznek utólag visszakereshető módon, szabványos formátumban naplóznia kell 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 Naplózás és elszámoltathatóság fejezet tartalmazza.
A határvédelmi eszköz adminisztrálása a védett, belső hálózatból, illetve távoli hozzáférés esetén csak biztonságos kommunikációs csatornán keresztül engedélyezett.
A határvédelmi eszköz konfigurálásáról az IT üzemeltető köteles gondoskodni.
A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomások és kiszolgálók a belső hálózatból kizárólag a határvédelmi eszközön felügyelt interfészeken keresztül kapcsolódhatnak külső hálózatokhoz vagy külső EIR-ekhez.
A határvédelemmel kapcsolatos biztonsági követelmények, védelmi intézkedések megvalósítását a Hivatal a Kockázatmenedzsment tevékenysége keretében folyamatosan figyelemmel kíséri és értékeli, az azzal összefüggésben meghatározott intézkedéseket a Kockázatkezelési Szabályzatban foglaltak szerint, valamint rendszerbiztonsági tervben dokumentálja.
A Hivatal a nyilvánosan hozzáférhető rendszerelemeket (pl.: web kiszolgáló szervert) a belső 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 és felelőssége

Együttműködésen alapuló informatikai eszközök

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomásokon kizárólag abban az esetben engedélyezett együttműködésen alapuló informatikai eszköz (pl.: kamera, mikrofon) használata, amennyiben a 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 IBF jogosult előzetesen ellenőrizni, használatának engedélyezése Az információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben meghatározottak szerint történik.

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

KARBANTARTÁS

A Hivatal az alaptevékenysége végzéséhez használt EIR-ek folyamatos működésének biztosítása, rendelkezésre állásának megőrzése érdekében a karbantartással kapcsolatos szabályokat jelen Szabályzat keretei között az alábbiakban írja elő, s azzal összefüggésben az itt meghatározott eljárásrendet lépteti életbe.
Az IT üzemeltető feladata az üzemeltetésében lévő rendszerelemek hardver, illetve szoftver komponenseinek rendszeres, illetve eseti karbantartásáról, szükség szerinti javításáról gondoskodni, s az azzal kapcsolatos tevékenységeket és információkat szükségszerűen, az erre rendszeresített dokumentumban rögzíteni (pl.: javítási nyilvántartás, karbantartási napló, stb.).
A karbantartás megszervezéséről, illetve végrehajtásáról az IT üzemeltető az adott rendszerelemre vonatkozó gyártói ajánlásoknak megfelelő módon és rendszerességgel köteles gondoskodni.
A Hivatal a rendelkezésében lévő EIR-ek karbantartására vonatkozó lényeges és naprakész információkat (pl.: karbantartásra jogosult szervezet, szerződéses szolgáltató partner megnevezése, elérhetőségei; karbantartás módja: helyszíni, távoli; távoli hozzáférés esetén a biztonságos hálózati kapcsolatra vonatkozó követelmények: titkosított kommunikációs csatorna, hitelesítés módja; stb.) az adott EIR rendszerbiztonsági tervében rögzíti, s gondoskodik arról, hogy az hozzáférhető legyen az érintett biztonsági szerepköröket betöltő személyek számára.
Helyszíni karbantartás esetén a karbantartásra jogosult szervezet által a feladatellátásra kijelölt személy(ek) munkavégzését az IT üzemeltető felügyeli és ellenőrzi.
A karbantartás elvégzéséhez szükséges és elégséges szintű hozzáférés, illetve jogosultság, távoli karbantartás esetén a biztonságos hálózati kapcsolat ideiglenes beállításáról, valamint a karbantartás befejezését követő visszavonásáról, távoli karbantartás esetén az ahhoz engedélyezett hálózati kapcsolat, illetve munkaszakasz lezárásáról az IT üzemeltető köteles gondoskodni.
Amennyiben a karbantartás, illetve javítás a helyszínen nem végezhető el és emiatt az érintett rendszerelem kiszállítására van szükség, akkor az adathordozót is tartalmazó rendszerelem (eszköz) esetén, ha azon az adatok tárolása titkosítatlan formában történik, az elszállítás előtt az IT üzemeltető feladata az adathordozó kiszereléséről, illetve amennyiben az nem lehetséges, akkor az adathordozón található adatok és információk szükség szerinti eseti biztonsági mentéséről, s az adathordozóról történő visszaállíthatatlan módú törléséről gondoskodni. Amennyiben a karbantartást igénylő rendszerelem esetében egyik adatbiztonsági intézkedés sem megvalósítható ezek közül, akkor az IT üzemeltető ezt a jóváhagyási kérelmében köteles jelezni a kiszállítás engedélyezésére jogosult vezető számára, aki ezen információ, valamint az adathordozón tárolt adatok típusa és a bizalmasságuk, sértetlenségük, illetve rendelkezésre állásuk sérülésével vagy elvesztésével összefüggő kockázatok mérlegelése alapján Az információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben foglaltak szerint dönt a kiszállítás engedélyezéséről vagy tiltásáról, utóbbi esetben a helyszíni

karbantartás vagy a karbantartás tervezett helyszínén a Szervezet által felügyelt munkavégzés feltételeinek biztosításáról.

ADATHORDOZÓK VÉDELME

A Hivatal az általa tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése érdekében az adathordozók, illetve a hordozható adattárolók védelmével kapcsolatos szabályokat jelen Szabályzat keretei között az alábbiakban írja elő, s azzal összefüggésben az itt meghatározott eljárásrendet lépteti életbe.
A Hivatal a digitális 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.

Az adathordozók használati szabályai

A Hivatal által használt EIR-ekhez, illetve rendszerelemeikhez a munka-, illetve feladatkörük ellátásához szükséges mértékben kizárólag a használatukra jogosult személy(ek)/foglalkoztatott(ak) férhetnek hozzá.
A Hivatal az általa használt EIR-ek beépített adathordozót tartalmazó rendszerelemeinek biztonságos elhelyezéséről és felügyeletéről jelen Szabályzat Fizikai és környezeti védelem fejezetében előírt módon gondoskodik.
A munkavégzéshez a Hivatal által biztosított olyan adathordozón vagy beépített adattárolót tartalmazó mobil eszközön, amely a Szervezet által felügyelt, ellenőrzött környezetből, illetve területről bármely okból (otthoni használat, szállítás, adattovábbítás, stb.) esetileg vagy rendszeresen kikerülhet, azon a munkahelyi információkat az adathordozó típusának megfelelően lehetőség szerint fájl- vagy tárolószintű titkosítással ellátva kell tárolni. A mobil eszköz vagy adathordozó 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 foglalkoztatott feladata és felelőssége.
A munkavégzéshez a Hivatal által biztosított adathordozók, beépített adattárolót tartalmazó mobil eszközök (pl.: laptop, tablet, okostelefon) és hordozható adattároló eszközök (pl.: memóriakártya, külső háttértároló eszköz vagy merevlemez, optikai adathordozó lemez, stb.) jogosulatlan hozzáférés elleni, fizikai védelméről, biztonságos tárolásáról és kezeléséről a használatára jogosult foglalkoztatott köteles gondoskodni. Használaton kívül az adathordozót el kell zárni, illetve illetéktelenek számára hozzáférhető helyen folyamatos felügyelet nélkül, őrizetlenül hagyni (pl.: közterületen parkoló zárt gépjárműben is) TILOS!
Amennyiben az adathordozó használata már nem szükséges, akkor a használatra átvevő foglalkoztatott köteles visszaszolgáltatni a jegyző számára, aki gondoskodik a használatból kivont adathordozó biztonságos tárolásáról, illetve a jelen fejezet Az adathordozók törlése szakaszában meghatározottak szerint intézkedik annak további felhasználásáról.
Az adathordozó vagy mobil eszköz elvesztése, ellopása biztonsági eseménynek minősül, melyet minden foglalkoztatott az észlelést követően haladéktalanul köteles jelenteni munkahelyi felettese számára, aki a Biztonsági események kezelése fejezetben meghatározottak szerint köteles eljárni ilyen esetben.
A Hivatal által használt EIR-ekhez, illetve rendszerelemeihez kizárólag a Hivatal által biztosított és/vagy ellenőrzött adathordozó csatlakoztatása engedélyezett. Eltérni ettől indokolt esetben, a jegyző jóváhagyását és az adathordozó biztonsági ellenőrzésének az IT üzemeltető által történő elvégzését követően lehet. A nem a Hivatal tulajdonát képező, idegen adathordozó csatlakoztatását megelőzően az IT üzemeltető feladata az adathordozó megbízhatóságának ellenőrzése (pl.: vírusellenőrzés).
A Hivatal a rendelkezésében lévő EIR-ekhez, illetve rendszerelemeikhez, amelyek működése, használata vagy üzemeltetése során adatexport vagy feltöltés indokolt és szükséges a munkavégzés céljából, az azokhoz csatlakoztatásra engedélyezett adathordozók típusát, forrását, illetve további jellemzőit az adott EIR rendszerbiztonsági tervében rögzíti.
Olyan idegen adathordozót, amelynek a tulajdonosa (származása) nem ismert, nem beazonosítható, a Hivatal bármely rendszereleméhez vagy eszközéhez csatlakoztatni TILOS!
Adathordozó vagy mobil eszköz engedély nélküli csatlakoztatása biztonsági eseménynek minősül, amely a Biztonsági események kezelése fejezetben, illetve a Fegyelmi intézkedések szakaszban meghatározott eljárást, illetve következményeket vonja maga után.

Az adathordozók törlése

A jegyző, illetve munkavégzéshez kiadott beépített adathordozót tartalmazó mobil eszköz vagy hordozható adattároló esetén a foglalkoztatott közvetlen felettese az eszközön tárolt adatok típusa, továbbá a bizalmasságuk, sértetlenségük, illetve rendelkezésre állásuk sérülésével vagy elvesztésével összefüggő kockázatok mérlegelése alapján kezdeményezheti az eredeti felhasználási célja alól bármely okból kivonásra kerülő adathordozó tartalmának törlését.
Az IT üzemeltető feladata az adathordozó típusának megfelelő, helyreállíthatatlanságot biztosító törlési technikát (pl.: többszörös felülírás, roncsolás, stb.) alkalmazva gondoskodni az adathordozón tárolt adatok törléséről azok leselejtezése, megsemmisítése vagy újrafelhasználásra való kibocsátása előtt.

FIZIKAI ÉS KÖRNYEZETI VÉDELEM

A Hivatal az általa használt EIR-ek, illetve rendszerelemeik elhelyezését biztosító, saját rendelkezésében, illetve felügyelete alatt álló létesítményekre, épületekre és helyiségekre vonatkozó fizikai védelmi eljárásrendet jelen fő fejezetben, az alábbiak szerint határozza meg.

Belépési engedélyek

A Hivatal saját rendelkezésében, illetve felügyelete alatt álló létesítményekbe és épületekbe a foglalkoztatottak számára állandó belépési jogosultságot biztosít. A Hivatallal bármely más munkavégzésre irányuló szerződéses jogviszonyban álló további személyek számára feladatellátásuk által indokolt mértékben az állandó belépést a jegyző engedélyezheti.
A foglalkoztatottak nyilvántartásáról a jegyző köteles gondoskodni, a további, állandó belépési engedéllyel rendelkező személyek nyilvántartásának elkészítéséről és kezeléséről, valamint naprakész állapotban tartásáról, eseti-, illetve rendszeres felülvizsgálatáról a jegyző, illetve az általa e feladat ellátásával megbízott munkatárs feladata és felelőssége gondoskodni. A jegyző által jóváhagyott nyilvántartás írásos belépési engedélynek minősül.

Belépések ellenőrzése

A Hivatal által használt EIR-ek, illetve rendszerelemeik elhelyezését biztosító, saját rendelkezésében, illetve felügyelete alatt álló épületek látogatók számára biztosított bejáratain és számukra nyitott területein kívül minden más be- és kilépésre alkalmas nyílászárót használaton kívül zárt állapotban kell tartani. A zárható helyiségeket azok elhagyását követően az utolsó kilépő személy köteles zárt állapotba helyezni. 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.
Minden foglalkoztatott köteles ellenőrizni munkavégzési helyén a felügyelete alatt álló helyiség nyílászáróinak megfelelő működését, zárhatóságát. Rendellenesen működő, nem zárható nyílászáró észlelése esetén a hibát észlelő foglalkoztatott haladéktalanul köteles jelezni azt közvetlen felettese számára.
Az állandó belépésre nem jogosult személyek (pl.: látogatók, munkavégzésre irányuló szerződéses jogviszonyban álló karbantartók, stb.) belépésének adatait az őket fogadó és/vagy kíséretüket, felügyeletüket ellátó foglalkoztatott köteles a belépésekről vezetett nyilvántartásban (belépési napló) rögzíteni.
Az informatikai erőforrásokat koncentráltan tartalmazó, illetve az EIR-ek központi rendszerelemeinek helyt adó helyiségekbe (pl.: szerver szoba) történő belépések adatainak dokumentált rögzítéséről az IT üzemeltető köteles gondoskodni.

Fizikai hozzáférések felügyelete

A Hivatal az általa használt EIR-ek rendszerelemeinek helyt adó, saját rendelkezésében, illetve felügyelete alatt álló helyiségek védelméről elektronikus vagyonvédelmi rendszer (behatolásjelző-, illetve riasztórendszer) alkalmazásával gondoskodik.
A Hivatal által használt EIR-ek rendszerelemeinek helyt adó helyiségekben ideiglenes belépési engedéllyel rendelkező személyek (pl.: látogatók, munkavégzésre irányuló szerződéses jogviszonyban álló karbantartók, stb.) kizárólag felügyelet mellett tartózkodhatnak, illetve végezhetnek munkát. A felügyelet biztosítása az ideiglenes belépési engedéllyel rendelkező személyt fogadó és/vagy kíséretét ellátó foglalkoztatott, az

informatikai erőforrásokat koncentráltan tartalmazó, illetve az EIR-ek központi rendszerelemeinek helyt adó helyiség (pl.: szerver szoba) esetében az IT üzemeltető feladata.
A Hivatal saját rendelkezésében, illetve felügyelete alatt álló, látogatók számára folyamatosan vagy ideiglenesen – pl.: átszervezés, költözés, átépítés miatt – nyitott, felügyelet nélkül hozzáférhető területein, helyiségeiben a hálózathoz való csatlakozásra alkalmas, szabad hálózati végpontok letiltásáról, illetve fizikai csatlakozásuk hálózati elosztón történő megszüntetéséről az IT üzemeltető köteles gondoskodni.
Fizikai hozzáféréssel kapcsolatos biztonsági esemény gyanújának felmerülése, bekövetkezése, illetve észlelése esetén a Biztonsági események kezelése fejezetben foglaltak szerint az azt észlelő haladéktalanul köteles jelezni közvetlen felettese számára.

Rendszerelemek be- és kiszállítása

A Hivatal által használt EIR-ek központi rendszerelemeinek a Szervezet által ellenőrzött, felügyelt területről történő kiszállítását, illetve azokhoz új központi rendszerelem beszállítását a jegyző engedélyezheti, s az IT üzemeltető gondoskodik annak szakmai felügyeletéről, valamint az eszközmozgás indokának megfelelő dokumentálásáról.

Környezeti károk elleni védelem

A Hivatal az informatikai erőforrásokat koncentráltan tartalmazó, illetve az EIR-ek központi rendszerelemeinek helyt adó (pl.: szerver szoba) helyiség 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 az általa használt EIR-ek rendszerelemeit képező informatikai eszközök elhelyezése során 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 a Szabályzatban rögzített biztonsági szerepkört betöltő személyek számára ismert legyen, továbbá arról, hogy az állagmegóvási, illetve karbantartási feladatok ellátása keretében működőképességük ellenőrzése rendszeresen megtörténjen és biztosítva legyen.
A Hivatal az informatikai erőforrásokat koncentráltan tartalmazó, illetve az EIR-ek központi rendszerelemeinek helyt adó helyiségben 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 figyelembevételével a Hivatal az érintett, rendelkezésében lévő EIR rendszerbiztonsági tervében rögzíti.
A légkondicionáló berendezés vagy egyéb telepített felügyeleti mérőeszköz helyi riasztásjelzésének észlelése esetén minden foglalkoztatott köteles a közvetlen felettesét, illetve az IT üzemeltetőt arról haladéktalanul értesíteni.

SZEMÉLYI BIZTONSÁG

A Hivatal elemi érdeke, hogy az alaptevékenysége végzéséhez használt EIR-ekhez, valamint az azokban kezelt adatokhoz, az EIR-ek rendszerelemeihez és az EIR-ek által nyújtott vagy azokon keresztül elérhető szolgáltatásokhoz munkavégzésük során a feladatellátásuk által indokolt mértékben hozzáférő foglalkoztatottak, illetve a Hivatallal bármely más munkavégzésre irányuló szerződéses jogviszonyban álló további személyek tevékenységüket biztonságosan, szakszerűen és felelősséggel, a Hivatal érdekeinek és az általa meghatározott szabályoknak megfelelően, kötelezettségeik és felelősségük tudatában végezzék, s erre vonatkozóan a Szervezet számára a szükséges jogi garanciák biztosítottak legyenek.
A Hivatal fentiek érdekében a személyi biztonsággal kapcsolatos szabályokat jelen Szabályzat keretei között az alábbiakban írja elő, s azzal összefüggésben az itt meghatározott eljárásrendet lépteti életbe.

Személybiztonsági feltételek

A munkaköri alkalmasság jogszabályban meghatározott vizsgálata, illetve az ezzel kapcsolatos feladatok elvégzése, úgymint az adott munkakör betöltéséhez szükséges iskolai végzettség, szakképzettség,

szakképesítés, illetve gyakorlati idő meglétének, valamint – amennyiben indokolt – egészségi és pszichikai alkalmasságra vonatkozó vizsgálatról szóló igazolások ellenőrzése a jegyző feladata és felelőssége.
A Hivatal által használt EIR-ekhez hozzáféréssel rendelkező foglalkoztatottak személybiztonsági szempontból azonos követelményeknek kell, hogy megfeleljenek. Esetükben a munkaköri alkalmassági követelményeknek történő megfelelés, a munkavégzésükre vonatkozó előírások, szabályozók, illetve eljárásrendek megismerése és maradéktalan betartása, valamint a titoktartási nyilatkozatban vállalt felelősségük képezik a személybiztonsági besorolásuknak megfelelő kötelezettségek alapját, az ezzel kapcsolatos garanciális feltételeket. Ennek megfelelően kötelesek a tevékenységüket érintő biztonsági előírások, szabályozók, illetve eljárásrendek megismerésével és betartásával kapcsolatos felelősségükről, valamint titoktartási kötelezettségükről nyilatkozatot tenni.
A Hivatallal egyéb munkavégzésre irányuló jogviszonyban álló személyek (pl.: üzemeltetési, karbantartási feladatokat ellátók) esetében a jegyző feladata és felelőssége a tevékenység alapját képező jogviszonyt megalapozó megállapodásban a szükséges garanciális feltételeket rögzíteni.
Az IBF jogosult minden információbiztonságot érintő szerződés tartalmának megismerésére és véleményezésére, valamint szükség esetén további biztonsági tárgyú szerződéses feltételekre, garanciális elemekre vonatkozó javaslatot tenni a jegyző számára.

Kiemelt kockázatú munkakörök

A Hivatal rendeltetésszerű működésének folyamatos biztosítására, fenntartására az engedélyezési és döntési folyamatokban, a döntések előkészítésében, végrehajtásában és ellenőrzésében betöltött szerepük miatt a jelen Szabályzatban rögzített biztonsági szerepköröket betöltő személyek, valamint az EIR-ekhez, illetve az abban kezelt adatokhoz magasabb hozzáférési jogosultsággal rendelkező további foglalkoztatottak (pl.: kulcsfelhasználók) feladatellátása és rendelkezésre állása jelentős hatással bír, emiatt információbiztonsági szempontból az általuk betöltött munka- illetve feladatköröket a Hivatal kiemelten kockázatosként kezeli.
A Hivatal a kiemelten kockázatos munka- illetve feladatkörökkel összefüggő kockázatokat kockázatmenedzsment tevékenysége során felméri és értékeli.
A jegyző feladata és felelőssége a kiemelten kockázatos munka- illetve feladatköröket betöltő személyek megfelelő helyettesítésének megszervezéséről tartós távollétük vagy akadályoztatásuk esetén gondoskodni.

Eljárás a jogviszony megszűnésekor

A Hivatal által használt EIR-ekhez hozzáféréssel rendelkező foglalkoztatottak munkaviszonyának megszűnése esetén a jegyző feladata kezdeményezni a számukra kiadott fizikai és logikai hozzáférési jogosultságok visszavonását (felfüggesztését), valamint gondoskodni a kiadott, a Szervezet tulajdonát képező minden eszköz (pl.: infokommunikációs eszközök, kulcsok, hozzáférési kódok, stb.) dokumentált visszavételéről legkésőbb munkavégzés alóli felmentésük időpontjában. A Hivatallal bármely más munkavégzésre irányuló jogviszonyban álló további személyek (külső szerződő fél) esetén ez a határidő a szerződéses jogviszony megszűnésének időpontja.
A jogviszony megszűnésének záró időpontját követően a távozó munkatárs felhasználói fiókjának, egyedi azonosítójának letiltását, valamint a munkavégzés céljából számára biztosított eszközök és erőforrások (pl.: elektronikus levelezési postafiókja) adattartalmának végleges törlését a jegyző feladata és felelőssége kezdeményezni, amennyiben az ahhoz kapcsolódó információkra sem a Hivatal alaptevékenysége megfelelő elvégzésének folytatása, sem jogszabályi kötelezettségek teljesítése, sem pedig bármely folyamatban lévő hatósági vizsgálat vagy eljárás, illetve biztonsági események kivizsgálása céljából nem lehet szükség.
A foglalkoztatott 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 feladatait, tevékenységeit és munkaadatait; valamint gondoskodik a dokumentált munkakör, illetve feladat átadás-átvételi eljárás lefolytatásáról a foglalkoztatott 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, illetve kezelt EIR-ekhez és szervezeti információkhoz való hozzáférés folyamatosságának biztosításáról;
- továbbá amelynek során tájékoztatja a kilépőt a reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről.

A Hivatal a szerződésben meghatározott módon tájékoztatja a jogviszony megszűnéséről azon szerződéses partnereit, amelyek esetében a kilépő foglalkoztatott munkaköri feladatai a Hivatallal fennálló szerződésük 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, 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).

Az áthelyezések, átirányítások és kirendelések kezelése

A Hivatal foglalkoztatottja munkakörének vagy feladatainak megváltozása, illetve áthelyezése, átirányítása esetében az Eljárás a jogviszony megszűnésekor szakaszban 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 és felelőssége kezdeményezni, hogy a foglalkoztatott számára az új munka-, illetve feladatköre által indokolt EIR-ek használatához szükséges jogosultságok, hozzáférések beállítása megtörténjen;
- a munkavégzéséhez szükséges eszközök a megfelelő beállításokkal a rendelkezésére álljanak;
- továbbá az ezek biztonságos és rendeltetésszerű használatához szükséges ismeretek a számára átadásra kerüljenek.

Fegyelmi intézkedések

A biztonsági szabályok szándékos megsértőivel szemben a Hivatal fegyelmi eljárást indít. Ha felmerül a lehetősége annak, hogy a biztonsági eseményt kiváltó ok bűncselekmény elkövetéséhez kötődik, abban az esetben a jegyző jogosult és köteles büntetőjogi feljelentést is tenni.
Amennyiben a biztonsági szabályokat nem a Hivatal személyi állományába tartozó személy sérti meg, akkor a jegyző a Szervezet jogi képviselőjének bevonásával megvizsgálja a jogi lépések megtételének indokoltságát és megteszi a szükséges intézkedéseket. A Hivatallal munkavégzésre irányuló egyéb jogviszonyban álló személy esetén a jegyző érvényesíti a vonatkozó szerződésben, megállapodásban meghatározott következményeket.
A Hivatal saját rendelkezésében lévő, illetve felügyelete alatt álló EIR-ekkel, rendszerelemeikkel összefüggő biztonsági esemény esetén a fegyelmi, illetve hatósági eljárásban felhasználni kívánt evidenciák begyűjtéséhez az IBF szakmai iránymutatást, támogatást biztosít, s az IT üzemeltető köteles közreműködni.
A biztonsági szabályok megsértése esetén alkalmazott eljárás, illetve intézkedések során figyelembe kell venni a Biztonsági események kezelése fejezetben foglalt előírásokat is.

ZÁRÓ RENDELKEZÉSEK

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 Információbiztonsági Szabályzat hatályba lépésével egyidejűleg a 2023.04.01. napján kiadott Informatikai Biztonsági Szabályzat hatályát veszíti.

INFORMÁCIÓBIZTONSÁGI KOCKÁZATKEZELÉSI SZABÁLYZAT

Bodrogkeresztúri Közös Önkormányzati Hivatal

Jóváhagyta / Kiadta: 2025-11-15

Dávid Zoltán
jegyző

Verziókövetés			
Kiadás / Hatályba lépés dátuma	**Szerző(k) / Véleményező(k) / Jóváhagyó(k)**	**Verzió**	**Leírás**
2025.11.10.	Bihari Emil, IBF (HANGANOV Kft.)	1.0	Első változat.
2025.11.15.	Dávid Zoltán, jegyző	1.1	Jóváhagyott, kiadott változat.

TARTALOM

1 A SZABÁLYZAT CÉLJA 3

2 A SZABÁLYZAT HATÁLYA 3

2.1 A SZABÁLYZAT SZEMÉLYI HATÁLYA 3
2.2 A SZABÁLYZAT TÁRGYI HATÁLYA 3
2.3 A SZABÁLYZAT IDŐBELI HATÁLYA 3

3 A SZABÁLYZAT KIADÁSA, KEZELÉSE, FELÜLVIZSGÁLATA 3

4 A KOCKÁZATKEZELÉSBEN ÉRINTETT SZEREPKÖRÖK 4

5 KOCKÁZATKEZELÉSI ELJÁRÁSREND 4

5.1 KOCKÁZATELEMZÉS 4
5.1.1 Kockázatok azonosítása 5
5.1.2 Hatáselemzés 5
5.1.3 Bekövetkezési valószínűség megállapítása 6
5.1.4 Kockázatok értékelése 7
5.2 KOCKÁZATKEZELÉS 7
5.2.1 A kockázat elkerülése 7
5.2.2 A kockázat csökkentése 8
5.2.3 A kockázat áthárítása, megosztása 8
5.2.4 A kockázat felvállalása 8
5.2.5 A kockázatkezelési javaslat és végrehajtása 9
5.3 KOCKÁZATMENEDZSMENT KOMMUNIKÁCIÓ 9
5.4 KOCKÁZATOK KEZELÉSÉNEK NYOMON KÖVETÉSE 9

6 ZÁRÓ RENDELKEZÉSEK 9

1. SZÁMÚ MELLÉKLET – FENYEGETÉSEK KATALÓGUSA 10

2. SZÁMÚ MELLÉKLET – KOCKÁZATKEZELÉSI JELENTÉS MINTA 12

1 A SZABÁLYZAT CÉLJA

A Bodrogkeresztúri Közös Önkormányzati Hivatal (a továbbiakban: Hivatal vagy Szervezet) Információbiztonsági Kockázatkezelési Szabályzatának (a továbbiakban: Szabályzat) célja a Szervezet rendeltetésszerű, eredményes és biztonságos működésének folyamatos fenntartását támogató, a Szervezet által használt elektronikus információs rendszerekre (a továbbiakban: EIR) ható információbiztonsági kockázatok, továbbá az EIR-ek, rendszerelemek és rendszerszolgáltatások fejlesztésével, beszerzésével, karbantartásával, üzemeltetésével és selejtezésével összefüggően felmerülő ellátási lánccal kapcsolatos kockázatok azonosításával, értékelésével, kezelésével és felügyeletével összefüggő tevékenységek, feladatok és felelősségek meghatározása.

Célja továbbá fentiek rögzítésével biztosítani, hogy a Szervezetnél az információbiztonsági kockázatok kezelése a vonatkozó, mindenkori hatályos jogszabályi előírásokban meghatározott követelményeknek megfelelően történjen.

2 A SZABÁLYZAT HATÁLYA

2.1 A Szabályzat személyi hatálya

A Szabályzat személyi hatálya kiterjed a Hivatal által foglalkoztatott, továbbá mindazon a Szervezettel munkavégzésre irányuló bármely szerződéses jogviszonyban lévő személyekre, akik munka-, illetve feladatkörükből adódóan vagy a Szervezetnél betöltött, a Hivatal Információbiztonsági Szabályzatában (a továbbiakban: IBSZ) rögzített biztonsági szerepkörük alapján a Szervezet által használt és rendelkezésében lévő EIR-ek, illetve egyéb támogató rendszerek kezelésében (üzemeltetésében, karbantartásában, javításában, fejlesztésében, illetve felügyeletében) részt vesznek.

2.2 A Szabályzat tárgyi hatálya

A Szabályzat tárgyi hatálya kiterjed a Hivatal által használt és rendelkezésében lévő EIR-ek, illetve egyéb támogató rendszerek részét képező minden rendszerelemre, eszközre (pl.: környezeti infrastruktúra, hardver, szoftver, hálózat és adathordozók), valamint az ezekben keletkezett, feldolgozott, tárolt vagy bármely más módon kezelt adatokra.

2.3 A Szabályzat időbeli hatálya

A Szabályzat a kiadása napján lép hatályba és visszavonásáig hatályos.

3 A SZABÁLYZAT KIADÁSA, KEZELÉSE, FELÜLVIZSGÁLATA

A Szabályzat előkészítése, szakmai tartalmának az IBSZ-ben rögzített biztonsági szerepkört betöltő személyekkel együttműködve történő kidolgozása, valamint a vonatkozó, hatályos jogszabályi előírásokban foglalt követelményekhez és a Szervezet működéséhez egyaránt igazodó kialakításának koordinálása az IBF feladata.

A Szabályzat jóváhagyása és kiadása a jegyző feladata és felelőssége. A Szabályzat kihirdetéséről és a személyi hatálya alá tartozókkal történő megismertetéséről a jegyző köteles gondoskodni.

A Szabályzat felülvizsgálatát és frissítését a következő gyakorisággal kell elvégezni:

- a Szervezet kockázatmenedzsment folyamataiban, az alkalmazott módszertanban, illetve a vonatkozó, hatályos jogszabályi előírásokban bekövetkező, vagy
- a Hivatal szervezetében, illetve a biztonsági szerepkörökben történő olyan jelentős változás esetén, amely a Szabályzat értelmezését és megfelelő alkalmazását, következetes végrehajtását akadályozza vagy gátolja;
- amikor jelentős változások történnek az érintett ellátási láncban, vagy amikor a rendszer, a működési környezet vagy más körülmények változása esetén szükségessé válhat az ellátási lánc megváltoztatása;
- fentiek hiányában annak érdekében, hogy a változó kiberfenyegetettségi környezetben a Szabályzat relevanciája és hatékonysága biztosítható legyen, legalább 2 évenkénti rendszerességgel.

A Szabályzat indokolt eseti felülvizsgálatára javaslatot tehet, illetve azt kezdeményezheti bármely a Szabályzat személyi hatálya alá tartozó, a Szervezet IBSZ-ében rögzített biztonsági szerepkört betöltő személy. A rendszeres felülvizsgálat kezdeményezése a jegyző feladata és felelőssége. A Szabályzat felülvizsgálatáról a jegyző dönt.

4 A KOCKÁZATKEZELÉSBEN ÉRINTETT SZEREPKÖRÖK

A jegyző feladata és felelőssége gondoskodni a kockázatmenedzsment tevékenységek megszervezéséről és végrehajtásáról, valamint az ahhoz szükséges erőforrások rendelkezésre állásának biztosításáról.

A Szabályzat személyi hatálya alá tartozó, a Szervezet IBSZ-ében rögzített biztonsági szerepkört betöltő személyek feladata és felelőssége a jegyző irányításával és az IBF szakmai támogatásával a Szervezet által használt EIR-eket érintő kockázatok elemzése, valamint a kockázatok kezelésére vonatkozó, a kockázatokkal arányos védelmi intézkedési javaslatok kidolgozása és döntésre előterjesztése.

A jegyző dönt a javasolt kockázatkezelési válaszlépések végrehajtásának elrendeléséről, a végrehajtásukért felelős(ök) és határidő kijelölésével.

A jóváhagyott kockázatkezelési intézkedések dokumentált végrehajtása az arra kijelölt felelős(ök) kötelessége, végrehajtásukat az IBF jogosult feladatellátása keretében ellenőrizni.

A Szabályzat személyi hatálya alá tartozó, az IBSZ-ben rögzített biztonsági szerepkört betöltő személyek feladata és felelőssége a végrehajtott kockázatkezelési intézkedések hatásosságának és eredményességének, valamint az érintett EIR-ek biztonságára gyakorolt hatásaik, teljesítményük mérésében, elemzésben és értékelésében, rendszeres felülvizsgálatában és az azokkal kapcsolatos jelentések elkészítésében, a vezetői döntések előkészítésében munka- illetve feladatkörüknek megfelelő mértékben az IBF szakmai útmutatásai alapján és a jegyző irányításával közreműködni.

A Szabályzat személyi hatálya alá tartozók munka- illetve feladatkörüknek megfelelő mértékben kötelesek a Szabályzat tartalmát, a benne foglalt előírásokat, különösen a számukra meghatározott feladatokat és felelősségeket megismerni, a kockázatkezelés teljes folyamatában egymással együttműködni.

5 KOCKÁZATKEZELÉSI ELJÁRÁSREND

A Hivatal által használt EIR-ek esetében a kockázatkezelés folyamataihoz kapcsolódó feladatok végrehajtását az alábbiakban rögzített eljárásrend, illetve módszertan szerint kell elvégezni.

5.1 Kockázatelemzés

A kockázatelemzést, illetve annak aktualizálását az IBF az alábbi esetekben kezdeményezi, s a Szervezet által használt és rendelkezésében lévő EIR-ek, illetve egyéb támogató rendszerek kezelésében (üzemeltetésében, karbantartásában, javításában, fejlesztésében, illetve felügyeletében) részt vevő, az IBSZ-ben rögzített biztonsági szerepköröket betöltő személyek közreműködésével, illetve bevonásával hajtja végre:

- új EIR bevezetése;
- meglévő EIR-ek esetén, amennyiben a változás (beleértve az új fenyegetések és sebezhetőségek megjelenését, valamint az időközben végrehajtott védelmi intézkedéseket is), a megváltozott körülmény vagy a tervezett változtatás az EIR-ben, illetve működési környezetében olyan nagy mértékű eltéréssel vagy módosítással jár, amely jelentősen befolyásolja az EIR biztonsági állapotát és az alkalmazott védelmi intézkedéseket.

A kockázatok felmérésének és elemzésének folyamata az alábbi főbb lépéseket foglalja magában:

- a kockázatok azonosítása,
- hatásaik elemzése,
- bekövetkezési valószínűségük becslése,
- a kockázatok értékelése.

5.1.1 Kockázatok azonosítása

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

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 a fenyegetettség kihasználásának bekövetkezése esetén az milyen adatokat érinthet és milyen mennyiségben.

A Szervezet fentiek alapján az általa használt EIR-ekkel kapcsolatban értelmezhető fenyegetéseket a jelen Szabályzat 1. számú mellékletében rögzített fenyegetések katalógusában felsorolt szempontrendszer alapján határozza meg.

Amennyiben a Szervezet működésének körülményei, az általa használt EIR-ek jellemzői, a korábbi kockázatelemzések tapasztalatai vagy az új fenyegetések megjelenése miatt indokolt, az IBF, illetve az IBSZ-ben rögzített biztonsági szerepköröket betöltő további személyek jogosultak javaslatot tenni a fenyegetés katalógus kibővítésére vagy módosítására, új fenyegetések felvételére, illetve a meglévők módosítására, amelyről a jegyző dönt, s gondoskodik arról, hogy a jóváhagyott módosítások a Szabályzat felülvizsgálata alkalmával érvényesítésre kerüljenek.

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 Szervezet, illetve az általa használt EIR-ek biztonsági osztály besorolásának megfelelően jogszabályban meghatározott védelmi intézkedések megvalósításának státuszát, működésének, hatékonyságának megfelelőségét is figyelembe kell venni.

5.1.2 Hatáselemzés

A fenyegetettség kihasználásának hatásait, az azonosított kockázatok bekövetkezése esetén a lehetséges következményeket, azok kiterjedését, a várható kár mértékét a Szervezet az alábbi, a vonatkozó, hatályos jogszabályi előírásban[1] rögzített szempontrendszer, s az azokhoz kapcsolódóan meghatározott kockázati besorolási értékek alkalmazásával elemzi, illetve értékeli:

Hatás (kár) értéke	Következmények
1	Az „alap" biztonsági osztály esetében legfeljebb csekély káresemény következhet be, mivel: • az elektronikus információs rendszerben jogszabály által nem védett adat vagy legfeljebb kis mennyiségű személyes adat sérülhet; • a Szervezet üzleti vagy ügymenete szempontjából csekély értékű, vagy csak belső (Szervezeti) szabályzóval védett adat vagy rendszer sérülhet; • a lehetséges társadalmi-politikai hatás a Szervezeten belül kezelhető; • a közvetlen és közvetett anyagi kár a Szervezet éves költségvetésének vagy nettó árbevételének 1%-át nem haladja meg.
2	A „jelentős" biztonsági osztály esetében közepes káresemény következhet be, mivel: • nagy mennyiségű személyes adat, illetve különleges személyes adat sérülhet; • személyi sérülések esélye megnőhet (ideértve például a káresemény

[1] 7/2024. (VI. 24.) MK rendelet
a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

Hatás (kár) értéke	Következmények
	miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket); • a Szervezet üzleti vagy ügymenete szempontjából érzékeny folyamatokat kezelő rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat sérülhet; • a káresemény lehetséges társadalmi-politikai hatásai a Szervezettel szemben bizalomvesztést eredményezhetnek, a jogszabályok betartása, vagy végrehajtása elmaradhat, vagy a Szervezet vezetésében személyi felelősségre vonást kell alkalmazni; • a közvetlen és közvetett anyagi kár meghaladja a Szervezet éves költségvetésének vagy nettó árbevételének 1%-át, de nem haladja meg annak 10%-át.
3	A „magas" biztonsági osztály esetében nagy káresemény következhet be, mivel: • különleges személyes adat nagy mennyiségben sérülhet; • emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be; • nemzeti adatvagyon helyreállíthatatlanul megsérülhet; • az ország, a társadalom működőképességének fenntartását biztosító kritikus infrastruktúra rendelkezésre állása nem biztosított; • a Szervezet üzleti vagy ügymenete szempontjából nagy értékű, üzleti titkot vagy különösen érzékeny folyamatokat kezelő rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet; • súlyos bizalomvesztés állhat elő a Szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok is sérülhetnek; • a közvetlen és közvetett anyagi kár meghaladja a Szervezet éves költségvetésének vagy nettó árbevételének 10%-át.

A hatáselemzés során figyelembe kell venni, hogy az egyes rendszerelemek több EIR részeként egyaránt funkcionálhatnak, emiatt az azokra ható kockázatok bekövetkezése esetén hatásaik további EIR-ekre is kiterjedhetnek.

5.1.3 Bekövetkezési valószínűség megállapítása

Az azonosított kockázatok bekövetkezésének reális valószínűségét, s ezek alapján a kockázati besorolási értéküket a Szervezet az alábbiak szerint határozza meg.

A bekövetkezési valószínűség megállapítása az iparági tapasztalatok, a fenyegetésekre, azok kihasználásának gyakoriságára vonatkozó nyílt forrásokból hozzáférhető kutatások, statisztikák, illetve trendek, valamint a korábbi biztonsági incidensek tapasztalatai alapján történik, az informatikai infrastruktúra esetében a rendszerelem típusának megfelelő, feltárt és jellemző sérülékenységek figyelembevételével, mindezek ismeretének segítségével, szakértői tapasztalatokon alapuló, az előfordulási gyakoriságra és a támadási potenciálra vonatkozó becslés útján.

A támadási potenciál a sikeres támadás esélyét fejezi ki és függ a támadási cél értékétől, a támadáshoz szükséges szakértelemtől, eszközöktől és időtől, valamint a védelem erősségétől is.

A bekövetkezési valószínűség lehetséges besorolási értékei ezek alapján az alábbiak lehetnek:

Besorolás	Bekövetkezési valószínűség
alacsony	Bekövetkezhet, de nem valószínű.
közepes	Elképzelhető, hogy bekövetkezik a jövőben (előfordulhat visszaélés vagy károkozás).
magas	Várhatóan bekövetkezik a közeljövőben (bárki által kihasználható, ismert sérülékenység).

5.1.4 Kockázatok értékelése

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

Besorolás	Értéke
alacsony	1
közepes	2
magas	3

A következmények várható hatása (kár mértéke), valamint a bekövetkezési valószínűség értékeinek szorzata képezi a kockázati értéket, ami az alábbiak szerint jeleníthető meg (kockázatértékelési mátrix):

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

A kockázati kritériumrendszer (mátrix) alapján a becsült kockázat értéke (eredő kockázat) szolgál a kockázatok besorolásának, kategorizálásának, majd a kockázatkezelési intézkedésekre vonatkozó javaslat, illetve döntés alapjául.

A Szervezetnél alkalmazott kockázati kategóriák eszerint:

Kockázat értéke	Kockázati kategória
1 – 2	alacsony szintű kockázat
3 – 5	közepes szintű kockázat
6 – 8	magas szintű kockázat
9	

A kockázatértékelés eredményét az IBF a „Kockázatkezelési jelentés minta" (jelen Szabályzat 2. számú melléklete) szerinti tartalommal dokumentáltan rögzíti.

5.2 Kockázatkezelés

A kockázatelemzés alapján a feltárt kockázatok kezelésének módját, a kockázat megszüntetésére vagy elfogadható szintre való csökkentésére irányuló válaszlépéseket a kockázat értéke, illetve az intézkedések alkalmazhatósága, megvalósításuk költsége és várható hatásai alapján kell meghatározni.

A Szervezetnél alkalmazott, lehetséges kockázatkezelési válaszlépések:

- kockázat elkerülése,
- kockázat csökkentése,
- kockázat áthárítása, megosztása,
- kockázat felvállalása.

5.2.1 A kockázat elkerülése

Amennyiben a kockázat költségarányos kezelésére vagy csökkentésére nincs reális lehetőség, akkor a kockázat előfordulásának elkerülését biztosítandó javasolható a fenyegetés vagy sebezhetőség forrásának megszüntetése (pl.: egy adott folyamat vagy tevékenység átszervezésével, helyettesítésével vagy megszüntetésével), a kockázatos tevékenység, az érintett EIR vagy rendszerelem használatának, illetve funkciójának megszüntetése, amennyiben az hatékonyan, a Szervezet alaptevékenységének ellátását nem veszélyeztető módon kivitelezhető.

A kockázat elkerülése bármely szintű kockázati kategória besorolás esetén alkalmazható kockázatkezelési válaszlépés a Szervezetnél.

A kockázat elkerüléséről a kockázatkezelési javaslat alapján a jegyző dönt.

5.2.2 A kockázat csökkentése

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

A javasolt kockázatcsökkentő védelmi intézkedés lehet már meglévő intézkedés módosítása vagy új kontroll, illetve intézkedés 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 csökkentése bármely szintű kockázati kategória besorolás esetén alkalmazható és preferált kockázatkezelési válaszlépés a Szervezetnél.

A kockázat csökkentéséről a kockázatkezelési javaslat alapján a jegyző dönt.

5.2.3 A kockázat áthárítása, megosztása

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

A kockázat áthárítása bármely szintű kockázati kategória besorolás esetén alkalmazható kockázatkezelési válaszlépés, kivéve, ha az azonosított magas vagy kritikus szintű kockázat olyan, a Szervezet alaptevékenysége végzéséhez feltétlenül szükséges, működése szempontjából kritikus infrastruktúrát és kulcsfontosságú erőforrást vagy EIR-t érint, amelynek a megfelelő működése az ellátási lánctól (pl.: beszállítótól, külső, harmadik fél szolgáltatótól, stb.) függ vagy ha a kockázat forrása közvetlenül az ellátási lánchoz tartozó szereplő, akkor a Szervezet a kockázat áthárításának alkalmazását kizárja, s helyette a kockázat tényleges megszüntetését vagy mérséklését célzó válaszlépésként a kockázat csökkentését vagy elkerülését fogadja kizárólag el.

A kockázat áthárításáról a kockázatkezelési javaslat alapján a jegyző dönt.

5.2.4 A kockázat felvállalása

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

- a megállapított kockázati kategória besorolás: alacsony vagy közepes;
- nem történik külső vagy belső normatíva (jogszabály, szabályozó) megsértése;
- a közvetlen, illetve közvetett kár értéke nem haladja meg a Szervezet költségvetésének vagy éves nettó árbevételének 1%-át;
- a társadalmi-politikai hatás a Szervezeten belül kezelhető, nem sérül a Szervezet 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.

Az alacsony szintű kockázati kategória besorolású kockázat indoklás nélkül felvállalható.

A közepes szintű kockázati besorolású kockázat elfogadása, felvállalása kizárólag részletes indoklással, a jegyző dokumentált jóváhagyásával történhet meg.

Kritikus vagy magas kockázati kategória besorolású kockázat nem vállalható fel!

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

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

5.2.5 A kockázatkezelési javaslat és végrehajtása

A kockázatelemzés eredménye alapján a kockázatkezelési javaslat elkészítését az IBF a kockázatok kezelésére kijelölt biztonsági szerepköröket betöltő személyek közreműködésével végzi el. A javaslat tartalmazza a lehetséges válaszintézkedéseket és a megvalósításukra vonatkozó részletes előírásokat, feladatokat, a javasolt határidőket és a végrehajtásukért felelős szerepköröket.

A kockázat kezelésére vonatkozó javaslatot minimálisan a „Kockázatkezelési jelentés minta" (jelen Szabályzat 2. számú melléklete) szerinti tartalommal kell dokumentáltan rögzíteni.

A kockázatkezelési javaslatban foglalt válaszintézkedés elfogadásáról – több alternatív válaszintézkedés esetén a kiválasztásáról – és végrehajtásának elrendeléséről a jegyző dönt. Az intézkedések végrehajtásának elrendelése a jegyző feladata és felelőssége, amelyet írásos formában a „Kockázatkezelési jelentés minta" (jelen Szabályzat 2. számú melléklete) szerinti tartalommal kell dokumentáltan az adott intézkedés, feladat végrehajtásáért felelős és határidő megjelölésével rögzíteni.

Az intézkedések végrehajtásában köteles minden, a jelen Szabályzat személyi hatálya alá tartozó személy munka-, illetve feladatkörének megfelelő mértékben közreműködni.

5.3 Kockázatmenedzsment kommunikáció

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

- az érintettek információt kapnak a Szervezet 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 a „Kockázatkezelési jelentés minta" (jelen Szabályzat 2. számú melléklete) szerinti tartalommal elkészített kockázatelemzési jelentés megőrzéséről, valamint tartalmának a kockázatkezelésben érintettekkel történő megismertetéséről a jegyző köteles gondoskodni.

5.4 Kockázatok kezelésének nyomon követése

A Kockázatkezelési jelentésben elrendelt intézkedések végrehajtását, az elvégzésükre meghatározott határidő leteltét követően az IBF – indokolt esetben a Szabályzat személyi hatálya alá tartozó további biztonsági szerepkört betöltő személy(ek) bevonásával – ellenőrzi, s annak eredményét a jelentésben az adott kockázatnál dokumentáltan rögzíti.

A kockázatkezelési intézkedések végrehajtásának következményeként új kockázati tényezők jelenhetnek meg, illetve meglévő kockázatok módosulhatnak. Az új kockázatokat be kell vonni a kockázatmenedzsment folyamatba, a módosult kockázatokat azok felülvizsgálatakor ismételten elemezni és kezelni szükséges.

A kockázatkezeléshez kapcsolódó intézkedések dokumentált felülvizsgálatát az IBF legalább évente köteles biztonsági helyzetértékelése keretében elvégezni, s ennek eredményéről a jegyzőt beszámolójában tájékoztatni.

6 ZÁRÓ RENDELKEZÉSEK

A Szabályzat rendelkezéseit minden, a személyi hatálya alá tartozó köteles betartani. A Szabályzatban foglaltak be nem tartása esetén a Hivatal jogosult hátrányos jogkövetkezményeket alkalmazni.
Jelen Szabályzat hatályba lépésével egyidejűleg a 2023.04.01. napján kiadott Kockázatelemzési és Kockázatkezelési Eljárásrendhatályát veszti.
Jelen Szabályzat az aláírás napján lép hatályba.

1. SZÁMÚ MELLÉKLET – FENYEGETÉSEK KATALÓGUSA

A 7/2024. (VI. 24.) MK rendelet 3. számú melléklete alapján.

1.	**Fenyegetés**	**Érintett információbiztonsági alapelvek**
2.	Tűz	R
3.	Kedvezőtlen környezeti feltételek	S, R
4.	Víz	S, R
5.	Szennyeződés, por, korrózió	S, R
6.	Természeti katasztrófák	R
7.	Katasztrófák a környezetben	R
8.	Jelentős környezeti események	B, S, R
9.	Áramellátás megszakadása, vagy hibája	S, R
10.	Kommunikációs hálózatok megszakadása, vagy zavara	S, R
11.	Beszállítói láncok megszakadása, vagy zavara	R
12.	Külső szolgáltatók hibája, vagy működési zavara	B, S, R
13.	Elektromágneses interferencia	S, R
14.	Kompromittáló elektromágneses kisugárzás	B
15.	Kémkedés	B
16.	Lehallgatás	B
17.	Eszközök, adathordozók, dokumentumok eltulajdonítása	B, R
18.	Eszközök, adathordozók, dokumentumok elvesztése	B, R
19.	Rossz tervezés vagy az alkalmazkodás hiánya	B, S, R
20.	Védett információ nyilvánosságra kerülése	B
21.	Nem megbízható forrásból származó információk	B, S, R
22.	Hardver vagy szoftver hamisítása (manipulációja)	B, S, R
23.	Információmanipuláció	S
24.	Elektronikus információs rendszerbe történő illetéktelen belépés	B, S
25.	Eszközök vagy adathordozók megsemmisülése	R
26.	Eszközök vagy az elektronikus információs rendszer működésének megszakadása	R
27.	Eszközök vagy az elektronikus információs rendszer hibás működése	B, S, R
28.	Erőforrások hiánya	R
29.	Szoftverek sérülékenységei vagy hibái	B, S, R
30.	Jogszabályok vagy szerződések megszegése	B, S, R
31.	Eszközök vagy az elektronikus információs rendszer engedély nélküli kezelése vagy használata	B, S, R
32.	Eszközök vagy az elektronikus információs rendszer hibás kezelése vagy használata	B, S, R

33.	Engedélyekkel való visszaélés	B, S, R
34.	Személyi állomány elvesztése	R
35.	Támadás	B, S, R
36.	Kényszerítés, zsarolás vagy korrupció	B, S, R
37.	Eltulajdonított személyazonossággal történő visszaélés	B, S, R
38.	Cselekmények letagadása	B, S
39.	Személyes adatokkal történő visszaélés	B
40.	Rosszindulatú szoftverek (malware)	B, S, R
41.	Szolgáltatásmegtagadással járó támadás (DOS)	R
42.	Szabotázs	R
43.	Pszichológiai manipuláció (social engineering)	B, S
44.	Manipulált hálózati adatforgalom	B, S
45.	Helyiségekbe történő engedély nélküli behatolás	B, S, R
46.	Adatvesztés	R
47.	Védendő információk sértetlenségének elvesztése	S
48.	Kártékony mellékhatások	B, S, R

Alkalmazási útmutató

A táblázat a fenyegetések megnevezését és az adott fenyegetések által potenciálisan érintett információbiztonsági alapelvek betűjeleit tartalmazza, az alábbiak szerint:

- Bizalmasság: B
- Sértetlenség: S
- Rendelkezésre állás: R

2. SZÁMÚ MELLÉKLET – KOCKÁZATKEZELÉSI JELENTÉS MINTA

Kockázatkezelési jelentés

Bodrogkeresztúri Közös Önkormányzati Hivatal

Verziókövetés			
Dátum:	**Készítette / Jóváhagyta / Kiadta:**	**Verzió**	**Leírás**
2025.	NÉV, beosztás, (képviselt szervezet)	1.0	Első változat – jóváhagyásra előkészítve
2025.	NÉV, beosztás, (képviselt szervezet)	1.1	Jóváhagyott, kiadott változat.

Sorszám	
Kockázat megnevezése, leírása: (az azonosított kockázattal kapcsolatos minden rendelkezésre álló információ leírása: pl.: a fenyegetés által érintett EIR-ek vagy rendszerelemek megnevezése; a veszélyeztetett adatok típusa, mennyisége; a kockázat kihasználása vagy az esemény bekövetkezése által okozható károk, következmények; stb.)	
Fenyegetés típusa: (az azonosított kockázat az EIR-ben kezelt adatok mely tulajdonságát – vagy többet is – fenyegeti: B: bizalmasság, S: sértetlenség, R: rendelkezésre állás)	B / S / R
Hatás (kár) megállapított értéke: (1 – 3)	1 / 2 / 3
Bekövetkezés valószínűségének értéke: (A: alacsony / 1, K: közepes / 2, M: magas / 3)	A / K / M
Kockázati kategória besorolás: (A kockázat értékelésének eredménye: A: alacsony / 1-2; K: közepes / 3-5; M: magas / 6-8; KR: kritikus /9)	alacsony / közepes / magas / kritikus
Kockázatkezelési javaslat: (A kockázat kezelésére javasolt válaszintézkedés, amely lehet: • a kockázat elkerülése,	A kockázat elkerülése / csökkentése / áthárítása / felvállalása Válaszintézkedés leírása:

• a kockázat csökkentése, • a kockázat áthárítása, • a kockázat felvállalása. Ha van, illetve lehetséges, akkor több, különböző válaszintézkedés felsorolása, s annak részletes kifejtése, pl.: új védelmi intézkedés bevezetése, az adott EIR vagy rendszerelem kivezetése, cseréje, stb. – a szükséges intézkedések várható hatásaival)	
A kockázat kezelésével kapcsolatos döntés (és annak indoklása): (A kockázatkezelési javaslatok közül a jóváhagyott intézkedésre vonatkozó vezetői döntés megjelölése és indoklása – közepes szintű kockázat felvállalását kötelező indoklással is ellátni!)	A kockázat elkerülése / csökkentése / áthárítása / felvállalása
Az intézkedés végrehajtásáért felelős: (a végrehajtásért felelős személy vagy szerepkör megnevezése: név, beosztás, képviselt szervezet neve – külső szolgáltató esetén)	
A végrehajtás határideje:	20__._____.____
A kockázatkezelés eredménye: (A kockázatkezelési döntésnek megfelelő intézkedések végrehajtásának és hatásosságának utólagos nyomon követése, visszaellenőrzése alapján az eredményének leírása, mint például a kockázat megszüntetésre, lezárásra került / már nem áll fenn, további javasolt intézkedés, stb.)	
Visszaellenőrzés dátuma:	20__._____.____
Ellenőrzést végezte (név, beosztás):	

A jelentésben rögzített, jóváhagyott válaszintézkedések végrehajtását elrendelem.

Kelt:

_____

Dávid Zoltán
jegyző