Vértesszőlősi Polgármesteri Hivatal

INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

KIBERVÉDELMI ELŐÍRÁSOK, SZABÁLYOK ÉS ELJÁRÁSRENDEK GYŰJTEMÉNYE

Érvényes: 2026.06.23.

Jóváhagyta: .....

dr. Kadocsa Izabella
Jegyző

Vértesszőlős Község Jegyzője 2.

Verziótörténet

Verzió	Dátum	Készítette / módosította	Módosítás
v1.0	2026.04.17.	ITSCHecurity Kft.	Compliance szabályzat

TARTALOMJEGYZÉK

1. BEVEZETÉS ÉS KÖVETELMÉNYEK

1.1. A SZABÁLYZAT CÉLJA

Az IBSZ (Informatikai Biztonsági Szabályzat, vagy Kibervédelmi Szabályzat) alapvető célja, hogy szabályozza a **Vértesszőlősi Polgármesteri Hivatal** (továbbiakban: Hivatal), valamint annak Elektronikus Információs Rendszerét (továbbiakban: EIR) használók, a vele informatikai rendszerüzemeltetési szerződéses kapcsolatban lévő egyéb szervezetek EIR-ében kezelt adatok bizalmasságát, sértetlenségét és rendelkezésre állását, illetve a rendszerek funkcionalitását fenyegető veszélyforrások elleni védelmi intézkedéseket, ezáltal biztosítsa a Hivatal célkitűzéseinek és feladatainak teljesítését.

Az IBSZ további célja, hogy biztosítsa a hatályos jogszabályoknak való megfelelőséget, különös tekintettel azokra az előírásokra, amelyek alapján az informatikai rendszerek biztonsági besorolása szerint kell gondoskodni.

Az IBSZ célja továbbá, hogy a Hivatal külső informatikai üzemeltetője, a Forel Computer Kft. (továbbiakban: Rendszergazda) valamint a felhasználók – és az informatikai rendszerüzemeltetési szolgáltatás esetleges ügyfelei – számára meghatározza az EIR üzemeltetésére, illetve használatára vonatkozó szabályokat, eljárásokat.

A dokumentumnak az alábbi részletes céljai vannak:

a) Határozza meg az IT biztonság szervezeti kereteit, az IT biztonsági feladatokat ellátó szerepköröket, azoknak a feladatát, felelősségét és hatáskörét,
b) Határozza meg az IT biztonsági intézkedések működtetésével összefüggő feladatokat, amelyeket a mindennapi működés során végre kell hajtani, alkalmazni kell,
c) Határozza meg az IT biztonsági intézkedés végrehajtásának felelősét, akin számonkérhető a biztonsági intézkedések működtetése, alkalmazása.
d) Határozza meg az IT biztonsági intézkedés végrehajtásában, alkalmazásában közreműködő egyéb szereplőket, érintettjeit és azok feladatait.

Az IBSZ-ben meghatározott biztonsági intézkedések részletes végrehajtási utasításait, eljárásait kapcsolódó dokumentumok, mint például üzemeltetési kézikönyvek, felhasználói kézikönyvek tartalmazzák.

1.2. HATÁLYA

A szabályzat hatálya a következőkre terjed ki:

1.2.1. SZERVEZETI-SZEMÉLYI HATÁLY

A szabályzat szervezeti hatálya a Hivatal valamennyi olyan szervezeti egységére kiterjed, amely a Hivatal EIR-eit használja, üzemelteti, fejleszti, továbbá ilyen tevékenységeket irányít és ellenőriz.

A szabályzat személyi hatálya kiterjed a Hivatallal munkavégzésre irányuló bármely jogviszonyban álló természetes és jogi személyre, tehát azokra, akik kapcsolatba kerülnek a Hivatal EIR-eivel (azt használják, üzemeltetik, fejlesztik, telepítik, javítják stb.), így

a) a munkaviszony alapján foglalkoztatott alkalmazottakra;
b) a Hivatallal szerződéses kapcsolatban álló természetes és jogi személyekre;
c) más szervezetek képviseletében a Hivatal munkahelyein vagy ezek környezetében tartózkodó személyekre;
d) a rendszer bármely részén karbantartást végző támogató személyzetre.

1.2.2. TÁRGYI HATÁLY

A szabályzat tárgyi hatálya kiterjed az Szervezet EIR-eire, így az EIR-t alkotó

a) környezeti infrastruktúra elemeire;
b) hardver eszközökre, készülékekre, berendezésekre;
c) szoftverekre;
d) adathordozókra;
e) dokumentációkra.

A tárgyi hatály kiterjed továbbá az EIR-ben rögzített, tárolt, feldolgozott vagy továbbított adatokra.

1.2.3. TERÜLETI HATÁLY

Alkalmazandó a Hivatal központi telephelyére (2837 Vértesszőlős, Templom utca 57.) továbbá mindazon területekre, ahol a Hivatal informatika használatával a tevékenységét kifejti, függetlenül annak geográfiai elhelyezkedésétől.

1.2.4. IDŐBELI HATÁLY

Az IBSZ, úgyis mint információbiztonsági szabályzatok gyűjteménye, a kiadásának napján lép hatályba. Jelen szabályzat kiadásával a korábban érvényben lévő informatikai szabályzatok, kézikönyvek, házirendek hatályukat veszítik.

1.3. A SZABÁLYZAT FELÜLVIZSGÁLATA (A5.36)

Az IBSZ eseti módosítására van szükség, ha a benne szereplő adatok megváltoztak, illetve az EIR működésében, vagy az EIR működését meghatározó jogszabályi környezetben, szabványokban jelentős változások következnek be.

A szabályzatot és a benne foglalt eljárásrendeket legalább évente egy alkalommal felül kell vizsgálni.

A szabályzat eseti módosításának, felülvizsgálatának kezdeményezése és a felülvizsgálat, valamint a módosítás elvégzése az informatikai rendszerek biztonságáért felelős személy (továbbiakban: IBF) feladata. A módosítások engedélyezése és az újabb változat jóváhagyása a Hivatal vezetőjének hatásköre.

Felelős: IBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

1.4. HATÁSKÖRI ÉS ILLETÉKESSÉGI SZABÁLYOK

Az IBSZ belső használatú dokumentum, amelynek kivonatolt változatát (Kiberbiztonsági Kézikönyv, vagy Házirend), az EIR felhasználói, illetve egyéb érintettek (a Hivatallal szerződéses kapcsolatban álló természetes és jogi személyek, más szervezetek képviseletében a Hivatal munkahelyein tartózkodó személyek) megismerhetik és birtokolhatják, de illetéktelenek nem adhatják tovább.

A Hivatal informatikáért felelős vezetőjének (továbbiakban: IT vezető) feladata gondoskodni arról, hogy a szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható.

1.5. ÁLTALÁNOS RENDELKEZÉSEK

1.5.1. A VEZETŐSÉG ELKÖTELEZETTSÉGE

A vezetőség elkötelezett a kibervédelmi intézkedések rendszerének kialakítására, bevezetésére, működtetésére, figyelemmel kísérésére, átvizsgálására, fenntartására és fejlesztésére, melyet a következőkkel biztosít:

- jelen szabályzatgyűjtemény kialakításával;
- a kiber- és információvédelmi célok és tervek kialakításának biztosításával;
- az információvédelemért viselt feladat- és felelősségi körök kialakításával;
- az információvédelmi célok teljesítése és a kibervédelmi szabályozásoknak való megfelelés fontosságának, a jogszabályok szerinti felelősségek, valamint a folyamatos fejlesztési szükségességének kinyilvánításával a Hivatal felé;
- elegendő erőforrás biztosításával az kibervédelmi intézkedések rendszerének létrehozásához, bevezetéséhez, működtetéséhez és fenntartásához;
- az elfogadható kockázati és kockázati szintű ismérvekről való döntéssel;
- belső kiberbiztonsági auditok elvégzésének biztosításával;
- az kibervédelmi intézkedések rendszerének vezetőségi átvizsgálásával;

1.5.2. AZ ERŐFORRÁSOK

A Hivatal meghatározta és rendelkezésre bocsátja azokat az erőforrásokat, amelyek szükségesek:

- Az kibervédelmi intézkedések rendszerének működtetéséhez, figyelemmel kíséréséhez, átvizsgálásához, fenntartásához és fejlesztéséhez;
- Annak biztosításához, hogy az információbiztonsági eljárások támogatják a működési követelményeket;
- A jogi és szabályozási követelmények, valamint a szerződéses biztonsági kötelezettségek azonosításához és intézéséhez;
- A megfelelő biztonság megőrzéséhez az összes, hatályba léptetett intézkedés helyes alkalmazásával;
- Az átvizsgálások szükség szerinti végrehajtásához, és az átvizsgálások eredményeire való megfelelő válaszadáshoz;
- A védelmi intézkedések eredményességének javításához, ahol szükséges;

1.6. KAPCSOLÓDÓ DOKUMENTUMOK

Az IBSZ-hez a következő dokumentumok kapcsolódnak:

1.6.1. JOGSZABÁLYOK (A5.31)

- 2012. évi I. törvény a munka törvénykönyvéről;
- 2012. évi C. törvény a Büntető Törvénykönyvről;
- 2013. évi V. törvény a Polgári Törvénykönyvről;
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Infotv.);
- 1999. évi LXXVI. törvény a szerzői jogról (továbbiakban: Szjt.);
- Az Európai Parlament és Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (továbbiakban: GDPR);
- 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól;
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról;
- 418/2024. (XII.23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról (a továbbiakban: Korm. rendelet);

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

1.6.2. SZABVÁNYOK, AJÁNLÁSOK, EGYÉB KÖVETELMÉNYEK

- Az EP és ET 2022. december 14-i (EU) 2022/2555 irányelve (továbbiakban EU NIS2);
- MSZ ISO/IEC 27001:2023 Informatika. Biztonságtechnika. Az információbiztonság-irányítási rendszerek. Követelmények;
- NIST 800-53 Rev5. Security and Privacy Controls for Information Systems and Organizations

1.7. SZEREP- ÉS FELELŐSSÉGI KÖRÖK AZ INFORMÁCIÓBIZTONSÁGBAN (A5.2 – A5.3)

A munkavállalók információbiztonsági szerepkörének a munkavállalók munkaköri leírásában is meg kell jelennie. Erről a munkahelyi vezetők kötelesek gondoskodni.

Az informatikai biztonsági szereplők jelen pontban nem említett további feladatait, felelősségét a munkaköri leírásuk tartalmazza.

1.7.1. ÁLTALÁNOS SZEREPKÖRÖK

Ezek a szerepkörök alapvetők a Hivatal életében.

1.7.1.1. JEGYZŐ

A Hivatal első számú vezetője.

Feladatai:

- Kinevezi, illetve megbízza az információbiztonsági felelőst (továbbiakban: IBF)
- Meghatározza az informatikai rendszerek védelmének felelőseire, feladataira, az ehhez szükséges hatáskörökre és a felhasználókra vonatkozó szabályokat, illetve kiadja az IBSZ-t.
- Biztosítja az IBSZ-ben megfogalmazott informatikai biztonsági szereplők részére a munkavégzésükhöz szükséges hatáskört és erőforrásokat.
- Biztosítja a Hivatal minden felhasználója számára a munkavégzéshez szükséges informatikai eszközöket és szoftvereket.
- Felelős a Hivatal informatikai rendszereinek kialakításáért, a fejlesztési feladatok meghatározásáért, valamint a rendszerek információbiztonságáért.
- Az IBF-fel rendszeresen ellenőrizteti, hogy a Hivatalnál megfelelően alkalmazzák-e az IBSZ előírásait.
- Az informatika fejlesztési koncepciójának meghatározása az ő hatásköre.
- Egyszemélyi felelősségének megtartása mellett az egyes funkciók irányítását átadhatja más szervezeteknek és személyeknek.

Elkötelezett az információbiztonsági intézkedések végrehajtása iránt, amelynek keretében biztosítja a megvalósításhoz szükséges erőforrásokat, valamint támogatja a biztonsági célok teljesülését és a szabályzatban foglaltak következetes betartását.

1.7.1.2. IT VEZETŐ

A Hivatal informatikai üzemeltetésének felügyeletéért felelős személy. A feladatkört külső szolgáltatóként a Forel Computer Kft. megbízott munkatársa látja el.

Feladatai:

- Gondoskodik az informatikai biztonságra vonatkozó jogszabályok és az IBSZ végrehajtásáról és betartásáról.
- Fokozott figyelmet fordít az informatikai rendszerek bevezetése és továbbfejlesztése során az IBSZ-ben rögzített információbiztonsági előírások teljesülésére.
- Az IBF-fel történő folyamatos kooperáció
- Engedélyezi az információbiztonsággal kapcsolatos eljárási és védelmi követelményszinteket és folyamatokat.
- Felelős az informatikai rendszerek üzemeltetéséhez szükséges erőforrások biztosításáért és a rendszerek folyamatos működéséért. Gondoskodik a folyamatos munkát biztosító koordinációról és a zökkenőmentes végrehajtást akadályozó tényezők megszüntetéséről.
- Meghatározza az informatikai feladatok prioritását, végrehajtási sorrendjét.
- Felügyeli az alap informatikai szolgáltatásokat megvalósító alaprendszerek (pl. központi címtár, fájl szerver szolgáltatások, levelező rendszer stb.) és rendszerszoftverek (pl.: operációs rendszerek, adatbáziskezelő szoftverek, tűzfal szoftverek stb.), a szerver és felhasználói oldali informatikai eszközök, illetve hálózati eszközök üzemeltetését.
- Biztosítja a Hivatal informatikai eszközeinek minél kisebb kieséssel történő üzemeltetését. Felügyeli az informatikai eszközök műszaki karbantartását, javítását a leggazdaságosabb megoldásokat helyezve előtérbe.
- Irányítja az új rendszerszoftverek, alaprendszerek bevezetését. Törekszik arra, hogy az üzleti célkitűzéseket támogató és a folyamatok hatékony működését biztosító, korszerű informatikai rendszerek kerüljenek kialakítása.

Ezen szerepkör összeférhetetlen az IBF-fel: az IT vezető főként a Hivatal üzleti igényeit és technológiai fejlesztéseit helyezi előtérbe, míg az IBF elsősorban a biztonsági szempontokra koncentrál, emiatt ellentétes érdekeket képviselnek.

1.7.1.3. ADATVÉDELMI TISZTVISELŐ (DPO)

Az Infotv. előírásainak és a Hivatal hatályos adatvédelmi szabályzatának szervezeten belüli betartásáért felelős személy.

Felelőssége nemcsak az EIR-ben kezelt adatokra vonatkozik, hanem minden adatkezelésre, függetlenül annak megjelenési formájától (pl.: papír alapú nyilvántartásokra, szerződésekre, dokumentumokra stb.).

Feladatai:

- Szorosan együttműködik a Rendszergazdával, segíti annak munkáját és iránymutatást nyújt adatkezeléssel összefüggő kérdésekben.
- Ellenőrzi az adatvédelmi előírások betartását.
- Egyéb adatvédelmi feladatait az Adatvédelmi és Adatbiztonsági elvárás(ok) határozza meg.

1.7.1.4. ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGÁÉRT FELELŐS SZEMÉLY (IBF)

A Hivatalnál az elektronikus információs rendszerek biztonságáért felelős személy (továbbiakban: IBF) a Hivatal informatikai biztonsági vezetője. Ezt a munkakört a szolgáltató megbízási szerződése rögzíti.

Feladatai:

- Felelős a Hivatalnál előforduló valamennyi, az EIR védelméhez kapcsolódó feladat felügyeletéért.

- Gondoskodik a Hivatal EIR biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról. Irányítja ezen tevékenységek tervezését, szervezését, koordinálását és ellenőrzését.
- Előkészíti és rendszeresen felülvizsgálja a Hivatal Informatikai Biztonsági Szabályzatát.
- Információbiztonsági szempontból véleményezi a Hivatal szabályzatait és szerződéseit, biztosítja a biztonsági követelmények érvényre juttatását.
- Összeállítja az információbiztonsági ismeretek és előírások oktatási anyagát, megszervezi az információbiztonsági képzések lebonyolítását.
- Részt vesz az EIR bevezetése és továbbfejlesztése során a biztonsági rendszer tervezésében, kialakításában, a védelmi eszközök alkalmazására vonatkozó döntés előkészítésben, a biztonságot növelő intézkedések kialakításában.
- Kockázatelemzés végzésével követi az EIR-t fenyegető veszélyforrások változásait, és kezdeményezi a szükséges védelmi intézkedéseket. Javaslatot tesz új védelmi eszközök és technológiák beszerzésére, illetve bevezetésére.
- Bejelentés alapján kivizsgálja a biztonsági eseményeket, és javaslatot tesz további intézkedésekre.
- Kapcsolatot tart a hatósággal és a kijelölt nemzeti kiberbiztonsági incidenskezelő központtal, amelynek feladatait a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézetének egy biztonsági eseményekkel foglalkozó akciócsoportja látja el (a továbbiakban: Kiberbiztonsági incidenskezelő központ).
- Írásban jelent a Hivatal vezetőjének minden olyan vitás kérdést, melyet az érintett területekkel együttműködve nem tud rendezni, illetve a biztonsági előírások teljesülésének veszélyeztetését észleli és közvetlen intézkedése eredménytelen maradt.
- Az IBSZ súlyos megszegését jelenti a Hivatal vezetőjének, aki az előírások ellen vétőkkel szemben fegyelmi felelősségre vonási eljárást kezdeményezhet.

Jogai:

- Jogosult az IBSZ előírásainak betartását bármely érintett szervezeti egységnél ellenőrizni.
- Ellenőrzési tevékenysége során betekintést nyerhet az EIR működésébe és a kapcsolatos dokumentumokba.
- Közvetlenül jogosult bármely érintett szervezeti egység vezetőjének, beosztott munkatársának olyan utasítást adni, mely az IBSZ-ben foglaltak betartását, annak végrehajtását célozza.
- Feladata ellátása során a Hivatal vezetőjének közvetlenül adhat tájékoztatást, jelentést.

Ezen szerepkör összeférhetetlen az IT vezetővel (érdekek ütközése), illetve a Rendszergazdával (felügyeleti ellenőrzés), azaz el kell kerülni, hogy ugyanazon személy legyen a végrehajtási, illetve az ellenőrzési oldalon.

Az ellenőrzés hatékonysága lecsökken, valamint rendkívül kockázatossá válik, ha ugyanaz a személy, vagy csoport felügyeli és ellenőrzi saját tevékenységét (önellenőrzés).

1.7.1.5. RENDSZERGAZDA

Az EIR felett a Forel Computer Kft. részéről felügyeletet gyakorló személy.

Feladatai:

- Felelős a rábízott informatikai rendszerek üzemszerű, folyamatos működéséért. Rendszeresen ellenőrzi a rendszerek és elemeiknek helyes működését.
- Felügyeli az informatikai rendszerek (és környezetének) biztonsági állapotát. Folyamatosan ellenőrzi az informatikai rendszer védelmi eszközeinek megfelelő működését.

- Felelős a biztonsági kockázatok minimalizálásáért, az üzemeltetési feladatokat veszélyeztető és akadályozó tényezők felismeréséért és jelentéséért.
- Felelős az informatikai rendszerek biztonsági mentéseinek készítéséért, ellenőrzéséért, tárolásáért és a kapcsolódó nyilvántartások vezetéséért.
- Átvizsgálja az EIR és kapcsolódó környezetük (alkalmazói szoftverek, szerverek, hálózati eszközök, határvédelmi eszközök és egyéb biztonsági eszközök) eseménynaplóit.
- Gondoskodik az informatikai rendszerek katasztrófahelyzetben történő újraindíthatóságáról, illetve az ehhez szükséges beállítások, paraméterek rendelkezésre állásáról.
- Az informatikai rendszerekre vonatkozóan feltölti és naprakészen tartja az Informatikai rendszerek nyilvántartását (EIR nyilvántartás), a rendszer Alapkonfigurációját és az Rendszerelem leltárt
- Elvégzi az informatikai rendszerek hibáinak felderítését, az ebből adódó szoftvertelepítési, frissítési feladatokat, valamint koordinálja a külső partnerek által végzett javításokat.
- Az informatikai rendszerek kialakítása és üzemeltetése során biztosítja az információbiztonsági és adatvédelmi előírások feltételeit és figyelemmel kíséri az előírások betartását. Mindezek tekintetében együttműködik az IBF-fel és az adatvédelmi felelőssel.
- Indokolt esetben az IT vezető tájékoztatásával és jóváhagyásával dokumentáltan engedélyezi az előírt üzemeltetéstől eltérő eljárások, konfigurációk alkalmazását.
- Nyomon követi az informatikai rendszer változásait, és ennek megfelelően módosítási javaslatokat dolgoz ki.
- Véleményezi az esetleges fejlesztési igények megvalósíthatóságát, az új védelmi megoldások beépíthetőségét a működő rendszerbe.
- Fokozott figyelmet fordít arra, hogy a szervereket/egyéb eszközöket kiemelt jogosultságokkal bejelentkezett állapotban ne hagyja felügyelet nélkül magára, a feladata elvégzése után kijelentkezik a rendszerből.
- Biztosítja a felhasználó oldali informatikai eszközök (számítógépek és tartozékok) működőképességét, fenntartja a folyamatos munkavégzéshez szükséges állapotot.
- Elvégzi az új eszközök IBSZ-ben rögzített információbiztonsági előírásoknak megfelelő biztonsági beállítását, és folyamatosan biztosítja a biztonsági beállítások helyességét és sértetlenségét.
- Az elhasználódott eszközök, adathordozók selejtezése, illetve újra felhasználásra kiadása esetén biztosítja a szükséges adatok mentését és az adathordozók biztonságos törlését, illetve megsemmisítését.
- Fogadja sürgős esetben a telefonon érkező felhasználói bejelentéseket és az egységes kezelés érdekében utólagosan rögzíti e-mailben.
- Koordinálja a megoldandó e-mailben vagy telefonon bejelentett hibajegyek kiosztását az EIR-hez kijelölt, felelős munkatársak számára, figyelembe véve a terheltségüket és a szabadság, betegség stb. miatti helyettesítésüket.
- A szolgáltatási szintek biztosítása érdekében figyelemmel kíséri a kiosztott hibajegyek gyors, prioritásuknak megfelelő megoldását, és szükség esetén módosítja a hibajegyek kiosztását.
- Az e-mailben bejelentett biztonsági eseményekről az esemény kivizsgálása céljából értesíti az IBF-t.

Ezen szerepkör összeférhetetlen az IBF-fel, mert a Rendszergazdák hozzáférést és ellenőrzést gyakorolhatnak az információbiztonsági rendszerek felett, ami a biztonságos működés és az ellenőrzés hiányát eredményezheti.

1.7.1.6. ADATGAZDA

Annak a szervezeti egységnek (adatgazdai területnek) a vezetője, amelyik szervezeti egységhez az EIR-ben tárolt adatok kezelése rendelhető, illetve ahol az adat keletkezik.

Feladatai:

- Meghatározza az adatok kezelésének célját, és meghozza az adatkezelésre vonatkozó döntéseket (beleértve a felhasznált eszközök megválasztását).
- Új EIR-t integrálása esetén meg kell vizsgálnia, hogy továbbra is fennállnak-e, illetve értelmezhetőek a Hivatal által előírt biztonsági követelmények.
- A biztonsági követelmények teljesülése esetén elfogadja és engedélyezi a rendszer működését.

1.7.1.7. KULCSFELHASZNÁLÓ (ADMIN)

Az EIR-hez az adatgazdai terület vezetője által kijelölt, a rendszerben tárolt adatok védelméért, a rendszer funkcionális működéséért felelős Felhasználó.

Feladatai:

- Folyamatosan figyelemmel kíséri a felügyelete alá rendelt EIR megfelelő működését. Ha hibás működést tapasztal, erről e-mailben vagy sürgős esetben telefonon értesíti a Rendszergazdát.
- Közreműködik a Hivatal Készenléti tervének elkészítésében, elvégzi a terv rendszeres tesztelését.
- Az EIR hibás működése esetén - ha úgy ítéli meg, - Készenléti terv alapján eljárva kezdeményezi a rendszer használatának felfüggesztését, és írásban rögzíti a felfüggesztés okát, a tapasztalt jelenséget. Ezzel egyidejűleg erről értesíti a Rendszergazdát és szükség szerint az intézkedésre jogosult vezetőt. Továbbá intézkedik arról, hogy a munkafolyamatok rögzítése a rendszer helyreállításáig papír alapú bizonylatokon történjen.
- Engedélyezi a külső és belső felhasználók különböző szintű hozzáférését az EIR-hez.
- Felügyeli, karbantartja az EIR kódrendszerét. Más rendszerekkel közös, kiemelt kódok esetén egyeztet a Kulcsfelhasználóval.
- Gondoskodik a felügyelete alá tartozó EIR-rel dolgozó felhasználók betanításáról, a kezelési és információbiztonsági szabályok megismertetéséről. Ehhez szükség szerint segítséget kérhet a Rendszergazdatól és az IBF-től.
- Gondoskodik az információbiztonsági és adatvédelmi előírások maradéktalan betartatásáról az adatfeldolgozás során, ebben együttműködik az IBF-fel és az Adatvédelmi felelőssel.
- Összefogja és koordinálja az EIR-rel kapcsolatban felmerülő fejlesztési, módosítási, javítási igényeket, ezeket képviseli a Rendszergazda felé, illetve a rendszer külső fejlesztői felé. Kapcsolatot tart a Rendszergazdával.
- Vezeti az új vagy módosított EIR tesztelését. Felelős azért, hogy a tesztelés úgy történjen, hogy abból legyen tapasztalat minden üzemszerű működtetési körülményre, és lehetőség szerint nem üzemszerű működtetésre is.

1.7.1.8. MUNKAHELYI VEZETŐ

A Hivatal szakterületi vezetői és a további vezetők.

Feladatai:

- Felelős a saját területén a jelen eljárás betartásáért és betartatásáért.
- Köteles az IBSZ-ben foglaltakat megismerni és azt a munkaterületük beosztott munkatársaival megértetni, a rájuk bízott feladatokat határidőre elvégeztetni, és a végrehajtást folyamatosan ellenőrizni.

1.7.1.9. FELHASZNÁLÓ

Az EIR-rel kapcsolatba kerülő, azt használó munkatársak.

Feladatai:

- Minden Felhasználó köteles megismerni és betartani az IBSZ-ben leírtakat.
- Jelenti a jogszabályokban, szabályzatokban megfogalmazott előírások bárki által történő megszegését a munkahelyi vezetőjének, továbbá az IBSZ megszegését az IBF-nek.
- Köteles jelenteni, ha biztonsági problémát okozó jelenséget tapasztal (biztonsági eseményt).
- Figyelemmel kíséri az EIR működését. Ha hibás működést tapasztal, erről azonnal értesíti a Kulcsfelhasználót és sürgős esetben telefonon keresztül közvetlenül a Rendszergazdát. Rendellenes működés esetén az adatfeldolgozást felfüggeszti.
- Együttműködik az információbiztonságért és informatikai üzemeltetésért felelős személyekkel.
- Nem hagyja bejelentkezett állapotban felügyelet nélkül a számítógépét. Ha távozik a számítógéptől vagy befejezi a munkát, kilép az alkalmazói rendszerekből és zárolja, illetve kikapcsolja számítógépet. Ha utolsóként távozik a helyiségből, akkor a Hivatal előírásainak megfelelően zárja a helyisége.
- Karbantartás előtt szükség esetén segítséget nyújt az üzemeltető munkatársnak a számítógépen tárolt adatok mentéséhez. A karbantartásokat, javításokat helyben végző külső partnerek szakembereit még átmeneti időre sem hagyhatja felügyelet nélkül.
- Köteles meghatározott időközönként információbiztonsági képzésen részt venni. Csak a képzés eredményes megtörténtét követően dolgozhat az EIR-ben.
- Szakszerűen kezeli a munkavégzéséhez biztosított informatikai eszközöket (a számítógépet és a hozzá kapcsolt tartozékokat).
- Gondoskodik az informatikai eszközök állagmegóvásáról, a rárakódott szennyeződések eltávolításáról. Óvja nedvességtől, víztől, mágneses és elektromos erőtértől, mechanikai behatásoktól. Szintén óvja a hálózat elemeit.
- Az informatikai eszközök sérülését azonnal jelenti e-mailben a Rendszergazdának.
- Gondoskodik a nevére szólóan kiosztott belépőkártya, és egyéb belépést biztosító eszköz megfelelő kezeléséről és őrzéséről.
- Köteles az EIR-hez hozzáférést biztosító jelszavát titokban tartani. A Felhasználó viseli a felelősséget minden olyan műveletért, amely neki felróható mulasztás miatt az adott felhasználóhoz tartozó azonosítóval kerül.

Jogai:

- A felhasználók jogosultak a rájuk vonatkozó jogszabályok, szabályzatok és a munkájukhoz szükséges információbiztonsági előírások megismeréséhez.
- Jogosultak az EIR-ek technikai problémáiról, tervezett karbantartásokról vagy rendkívüli eseményekről tájékoztatást kapni.
- Jogosultak megtagadni a számítógépes munkát, ha az súlyos törvénysértéshez, vagy bűncselekményhez vezetne.
- Jogosultak a számítógépes munkavégzéssel kapcsolatos sérelmeik jogorvoslati kezelésére. Jogorvoslati kérdésekben az IT vezető, magasabb szinten a Hivatal vezetője áll rendelkezésre.
- Jogosultak a számítógépes tevékenységük során felmerült problémák, akadályok elhárításához támogatást kapni a Rendszergazdától. A segítségnyújtáshoz az igényt e-mailben, sürgős esetben telefonon kell bejelenteni. A telefonos bejelentésről 24 órán belül írásos (e-mail) feljegyzést kell készíteni.

1.7.2. KOCKÁZATI SZEREPKÖRÖK

A fellépő kockázatok - legyen az informatikai, technológiai, vagy ellátási lánc kockázata – azonosításával, értékelésével és kezelésével foglalkozó munkatársak.

- A kockázatkezelési hatáskörök és felelősségek szükség szerint a munkaköri leírásokban, esetleg egyéb szabályozásokban rögzítendők.

1.7.2.1. KOCKÁZATKEZELÉSI VEZETŐ (KOCKÁZATMENEDZSER)

A kockázatkezelési stratégiákért, politikákért, folyamatokért felelős személy. A Hivatalnál ezt a szerepkört a Jegyző látja el.

Feladatai:

- Felelős az olyan kockázatkezelési politikák és folyamatok kialakításáért és végrehajtásáért, amelyek segítik a Hivatalt a kockázatok hatékony kezelésében és csökkentésében.
- Azonosítania és értékelnie kell a jelentkező külső, vagy belső kockázatokat, melyek kezelésére javaslatokat kell előkészítenie.
- Együtt kell működnie és kommunikálnia kell a kockázatkezelésben érintett felekkel.
- Kockázatértékelési jelentést kell készítenie a kockázatokról, a kockázatkezelési tevékenységekről a Hivatal vezetőjének (illetve más érintett fél számára).

1.7.2.2. KOCKÁZATFELELŐS (KOCKÁZATGAZDA)

A kockázatkezelési intézkedések végrehajtásáért és a nyomon követésért felelős.

Feladatai:

- Felelős a kockázatkezelési intézkedések végrehajtásáért és felügyeletéért. Ez magában foglalja a megelőző intézkedések, ellenőrzések és eljárások bevezetését, valamint a kockázatokat csökkentő, lehetőleg elfogadható szintre csökkentő intézkedések végrehajtását.
- Tájékoztatja a vezetőséget és az érintett feleket a kockázatok állapotáról, a kockázatkezelési intézkedésekről és az esetleges kockázatokkal kapcsolatos fejleményekről.
- Folyamatosan monitorozza a kockázatok állapotát, a kockázatkezelés hatékonyságát, valamint az elfogadható kockázati szinteket a Hivatalban. Figyelemmel kíséri a teljesítménymutatókat és rendszeresen felülvizsgálja és javítja a kockázatkezelési folyamatoka.

1.7.2.3. KOCKÁZATKEZELÉSI TANÁCSADÓ

Külső- vagy belső tanácsadó, aki szakértelmet és tanácsadást nyújt a kockázatkezelési stratégiák, folyamatok és eszközök kialakításához és végrehajtásához.

Feladatai:

- Támogatja a Kockázatkezelési vezetőt abban, hogy azonosítsa és értékelje a különböző kockázatokat, amelyek befolyásolhatják a Hivatal tevékenységeit.
- Segít a Hivatalnak stratégiákat kidolgozni a kockázatok kezelésére és csökkentésére. (pl: új technológiák alkalmazása, diverzifikáció vagy egyéb stratégiai lépések).

1.7.3. VÉSZHELYZETI SZEREPKÖRÖK (KÉSZENLÉTI TERV AKTIVÁLÓDÁSA ESETÉN)

Vészhelyzet esetén az elhárításban, illetve helyreállításban érintettek.

1.7.3.1. VÉSZHELYZETI VEZETŐ

Felelős a vészhelyzet alatt az irányításáért és koordinálásáért. A Hivatalnál ezt a szerepkört az IT vezető látja el.

Feladatai:

- Ki kell értékelnie a helyzetet. Ennek során figyelembe veszi a kialakult vészhelyzet természetét, kiterjedését és hatásait.

- Megfelelő döntéseket kell hoznia a kár csökkentése, vagy a vészhelyzet elhárítása érdekében. Ezek a döntések magukban foglalhatják a biztonsági intézkedések aktiválását, a szükséges erőforrások mozgósítását és a kommunikációs lépéseket.
- Koordinálnia kell az összes vészhelyzetben érintett személyt, vagy csoportot. Jelentenie kell az elvégzett feladatokat és a helyzet alakulását a Hivatal vezetőjének.
- Előkészíti és beépíti a megelőző intézkedéseket a Készenléti tervbe annak érdekében, hogy minimalizálja a vészhelyzet kialakulásának vagy hatásainak kockázatát a jövőben.

1.7.3.2. VÉSZHELYZETI CSOPORT (INCIDENSKEZELŐ CSOPORT)

A rendszer, infrastruktúra vagy üzleti folyamatok helyreállításáért és újraindításáért felelősek csoportja

Feladata:

- A Vészhelyzeti vezető irányításával végrehajtják a Készenléti tervezet.
- Felelősök a kritikus rendszerek és adatok visszaállításában.
- Tesztelniük kell és ki kell értékelniük a helyreállított rendszerek működőképességét.
- Együtt kell működniük más érintett felekkel (pl. szolgáltatók, beszállítók).
- Az elvégzett feladatokról folyamatosan tájékoztatniuk kell a Vészhelyzeti vezetőt.
- Dokumentálniuk kell a végrehajtott lépéseket, úgymint a helyreállítási folyamatokat és elért eredményeket.

1.8. ALAPVETŐ INFORMÁCIÓBIZTONSÁGI FELADATOK

1.8.1. JOGSZABÁLYKÖVETÉS

Az informatikai biztonságot érintő jogszabályok változásának követése az IBF feladata. A jogszabályok megváltozása esetén az IBF feladata, hogy szükség esetén javaslatot tegyen intézkedésekre, folyamatok, eljárások módosítására. Amennyiben szerződés keretében keletkezik új, informatikai biztonságra vonatkozó követelmény, a projektvezető feladata a követelmény jelzése az IBF-nek, illetve az IT vezetőnek.

1.8.2. JOGTISZTASÁG

A szoftverek jogtisztaságának betartása érdekében a szoftverek használatához szükséges licencekről nyilvántartást kell vezetni. A licenc nyilvántartás kérdése hozzákapcsolódik más IT eszközök nyilvántartásához. A licencek nyilvántartása a Rendszergazda, a nyilvántartás értékelése az IT vezető feladata. Amennyiben megalapozott licenc-igény következik be, úgy a beszerzést kezdeményezi.

1.8.3. TÖRVÉNYI MEGFELELÉS

Az törvénynek való megfelelés érdekében el kell készíteni és folyamatosan naprakészen kell tartani a törvény által előírt adatvédelmi nyilvántartásokat. A nyilvántartások elkészítése és karbantartása az Adatvédelmi felelős felelőssége. A nyilvántartás elkészítéséhez az Adatgazdáknak információt kell nyújtaniuk számára.

1.8.4. VEZETŐSÉGI ÁTVIZSGÁLÁS

1.8.4.1. ÁLTALÁNOS KÖVETELMÉNYEK

A vezetőség tervezett időszakonként átvizsgálja a Hivatal kibervédelmi intézkedéseinek rendszerét, hogy biztosítsa annak folyamatos alkalmasságát, megfelelőségét és eredményességét. Ezen átvizsgálás tartalmazza a fejlesztési lehetőségeket és a rendszerbeli változások szükségességének értékelését, beleértve a biztonsági szabályozásokat és a biztonsági célokat is. Az átvizsgálások eredményeit dokumentálni kell és a feljegyzéseket meg kell őrizni.

1.8.4.2. AZ ÁTVIZSGÁLÁS BEMENŐ ADATAI

A vezetőségi átvizsgálás bemenő adatainak tartalmaznia kell:

- Az kibervédelmi intézkedések rendszere auditjának és átvizsgálásának eredményeit,
- Az érdekelt felek visszajelzéseit,
- A technikákat, termékeket vagy eljárásokat, amelyeket a Hivatal felhasználhat a rendszer teljesítményének és hatásosságának fejlesztésére,
- A megelőző és helyesbítő tevékenységek helyzetét,
- Azokat a sebezhető pontokat vagy fenyegetettségeket, amelyeket nem kezeltek megfelelően a korábbi kockázatfelméréskor,
- A hatékonysági mérések eredményét,
- A korábbi vezetőségi átvizsgálások utóintézkedéseit,
- Bármilyen változást, amely hatással lehet az kibervédelmi intézkedések rendszerére,
- A fejlesztésre vonatkozó javaslatokat.

1.8.4.3. AZ ÁTVIZSGÁLÁS KIMENŐ ADATAI

A vezetőségi átvizsgálás kimenő adatai döntéseket és beavatkozásokat tartalmaznak a következőkkel kapcsolatban:

- A kibervédelmi intézkedések rendszerének megerősítése és hatékony alkalmazása
- A kockázatfelmérési és kockázatjavítási terv frissítése.
- Az információbiztonságot befolyásoló eljárások és intézkedések szükség szerinti módosítása, hogy összhangban legyenek azokkal a belső vagy külső eseményekkel, amelyek hatással lehetnek a kibervédelmi rendszerre, beleértve a változásokat:
  - A működési követelményekben,
  - A biztonsági követelményekben,
  - A meglévő működési követelményeket befolyásoló működési folyamatokban,
  - A jogi vagy szabályozási követelményekben,
  - A szerződési kötelezettségekben,
  - A kockázati és/vagy a kockázatelfogadási szintek kritériumaiban.
- Az erőforrás szükségletek.
- Az intézkedések hatékonysága mérésének fejlesztése.

1.8.5. INTÉZKEDÉSI TERV ÉS MÉRFÖLDKÖVEI

A Hivatal az információbiztonság és az ellátási lánc kockázatkezelése terén, valamint az EIR intézkedési terveinek kidolgozása és karbantartása érdekében egy dokumentált folyamatot vezet be, hogy megfelelő választ tudjon adni az eszközök, valamint a személyek és más szervezetek által jelentett kockázatokra. A folyamat részeként biztosítottak az intézkedések rendszeres felülvizsgálata és frissítése, hogy azok hatékonyan reagáljanak a változó környezeti kockázatokra és a szervezeti igényekre.

A Hivatal évente legalább egyszer, valamint jelentős változás esetén (új rendszer, beszállító, technológia) áttekinti az EIR-ekhez kapcsolódó kockázatokat.

A feltárt kockázatok alapján minden EIR-re vonatkozóan intézkedési terv készül, amely tartalmazza:

- a kockázatok leírását,
- a szükséges intézkedéseket,
- a felelőst, határidőt,
- a végrehajtás státuszát.

A dokumentum folyamatosan karbantartandó: minden végrehajtott vagy módosított intézkedés után frissíteni kell.

Jelen intézkedési tervet a Kockázatmenedzsment.xls tartalmazza.

1.8.6. EIR NYILVÁNTARTÁSA

Az EIR nyilvántartása külön dokumentumban, az *[EIR-nyilvántartás]* -ban szerepel.

1.8.7. INFORMÁCIÓK OSZTÁLYOZÁSA (A5.12 – A5.13)

Az információkat a megfelelő védelem kialakítása érdekében osztályozni kell. Az információnak különböző érzékenységi foka lehet, egyes tételek kiegészítő védettségi szintet, illetve különleges kezelést igényelhetnek. A következőkben leírtaknak megfelelően jelöljük és kezeljük ezeket:

1.8.7.1. BIZALMAS / MINŐSÍTETT

Ezen besorolású információk különösen nagy értéket képviselnek a Hivatal számára, jogi következményei is lehetnek, ha ezen információkat nyilvánosságra hozzák. Ezen besorolású információkat a Hivatalon kívül általában nem ismerik, ezért ez a kategória gazdasági szempontból is értékes lehet másoknak. Ezen információk elvesztése, vagy nyilvánosságra hozatala ügyfelek, vagy piacok elvesztését, presztízsveszteséget, versenyelőny elvesztését, illetve jogszabályok, törvények megsértését vonhatják maguk után.

Ilyen típusú információk lehetnek:

- személyes adatok,
- hang- és videofelvételek,
- üzleti titkok,
- vállalati pénzügyi adatok,
- alkalmazotti adatok (egészségügyi, pénzügyi adatok)
- vállalati döntések szabályai, üzleti modellek
- szabadalom előtt álló munkák, szoftverfejlesztéssel kapcsolatos információk
- hozzáférés-korlátozás alá eső (pl: projekt, vagy feladatvégrehajtás érdekében bizalmas) rendszerek

Az ebbe a kategóriába sorolt információkhoz való hozzáférés szükségességi alapon történik, az információ tulajdonosának jóváhagyásával. Ezen információt hordozó tárolókon fel kell tüntetni, hogy bizalmas információt tartalmaz, nem hozható nyilvánosságra (pl: papírra, borítékra ráírni, hogy bizalmas, vagy az adathordozót „bizalmas" címkével ellátni)

A Hivatalon kívüli személyek ezen információkat nem hozhatják nyilvánosságra eltérő megállapodás és az információ tulajdonosának, illetve a Hivatal vezetőjének jóváhagyása nélkül.

A Bizalmas kategóriájú információkat tilos továbbítani a nem védett külső hálózatokon, vagy útvonalakon. Ez általában a fájlok és e-mailek titkosítását, jelszavas védelmét, esetleg a papírmásolatok biztonságos csomagolását jelenti. Titkosítás nélkül továbbítható, ha úgy módosítják, hogy a kategóriája alacsonyabb szintre csökkenjen. Például, ha minden azonosító információt eltávolítanak egy tranzakciós fájlból, így annak elvesztése nem jelentene veszélyt a vállalatra, akkor az információkat titkosítás nélkül továbbíthatják nyílt hálózatokon keresztül. Az ilyen tevékenységet minden esetben a DPO-nak kell jóváhagynia.

1.8.7.2. KORLÁTOZOTT / FOKOZOTT

A besorolás olyan információkra vonatkozik, amelyek a cégen belül nem mindenki számára elérhetők, de nem tartalmaznak olyan információt, ami a bizalmas minősítést indokolják:

- Osztályok saját dokumentumai

- Nem személyes ügyféladatok
- Gyártási és üzemeltetési dokumentációk
- Forráskódok
- Számlák

1.8.7.3. BELSŐ HASZNÁLATÚ/ALAP

Ezen besorolás azon információkra vonatkozik, amelyek kisebb értéket képviselnek, mint a Bizalmas információk, de a Hivatal még mindig nem kívánja nyilvánosságra hozni, vagy szélesebb körben terjeszteni. Ez az alapértelmezett: ha az információ mellé más besorolás nincs hozzárendelve, akkor minden információ belső használatúnak minősül

- Vállalati telefonkönyvek a személyzetről, munkakörökről, elérhetőségekről
- Belső e-mailek (kivéve azok, amelyek Bizalmas szintű információkat tartalmaznak)
- Találkozók, megbeszélések jegyzetei, kivéve a Bizalmas témákkal kapcsolatosakat

Ezen kategóriába sorolt információk rendszerint hozzáférhetőek az alkalmazottak számára, de kilépő alkalmazottak esetében a Hivatal megkövetelheti nyilvánosságra hozatali, vagy külön titoktartási nyilatkozat aláírását.

Csak az információ kezelőjének engedélyével lehet ezen kategóriájú információkhoz jutni. Bizonyos típusú munkavégzés automatikus hozzáférést ad az ebbe az besorolásba tartozó adatokhoz.

Ezen információkat tartalmazó papírtermékeket és adathordozókat biztonságos módon kell tárolni és kezelni.:

- Ezen kategóriába sorolt információkat csak biztonságos nyomtatóra nyomtathatja
- A biztonsági mentési adathordozókat titkosítja
- Az információk papírmásolatait elzártan kezeli

A Hivatalon kívüli személyek ezen információkat nem hozhatják nyilvánosságra eltérő megállapodás és az információ tulajdonosának jóváhagyása nélkül.

A belső használatra vonatkozó információkat megfelelő felügyelet nélkül tilos továbbítani a nem védett külső hálózatokon, vagy útvonalakon. Ez általában a fájlok és e-mailek titkosítását, esetleg a papírmásolatok biztonságos csomagolását jelenti. Titkosítás nélkül továbbítható, ha maszkolják, vagy módosítják, annak érdekében, hogy a kategóriája a belső használatból alacsonyabb szintre csökkenjen. Például, ha minden azonosító információt eltávolítanak egy tranzakciós fájlból, így annak elvesztése nem jelentene veszélyt a Hivatalra, akkor az információkat titkosítás nélkül továbbíthatják nyílt hálózatokon keresztül. Az ilyen tevékenységet a DPO-nak kell jóváhagynia.

1.8.7.4. NYILVÁNOS/NYÍLT

Ez a kategória tájékoztatásra szolgál, amelyet a Hivatal a nagyközönség számára hozzáférhetővé tesz, ideértve a következőket:

- Információk a weboldalon
- Sajtóközlemények
- Termék- vagy szolgáltatási brosúrák
- Reklámok
- Állásajánlatok

Ezen kategóriába sorolt információkról feltételezhető, hogy széles körben férhetnek hozzá, de figyelni kell ezen információk pontosságára (ne lehessen módosítani, „elferdíteni"). Nem igényel külön jelölést vagy speciális tárolást, csak a rendelkezésre állásának biztosítását. Óvni kell az illetéktelen módosításoktól.

Minden EIR-t minősíteni kell a rendszer által kezelt adatok osztályba sorolása alapján. Amennyiben egy EIR több kategóriába tartozó adatot kezel, a legmagasabb kategóriát kell a rendszer minősítésének tekinteni. Az információkezelő rendszerek védelme érdekében alkalmazott biztonsági intézkedéseket alapvetően a rendszerek biztonsági osztálya szerint kell meghozni.

1.8.8. BIZTONSÁGI TELJESÍTMÉNY MÉRÉSE

Az információbiztonsági teljesítmény mérésének célja az, hogy az irányítók átfogó képet kapjanak az információbiztonsági helyzetről, és fel tudják mérni a kibervédelmi intézkedések rendszerének hatékonyságát. A mutatókat össze kell vetni az előző év hasonló mutatóival, így képet lehet kapni arról, hogy milyen mértékben növekedett (vagy csökkent) a biztonsági teljesítmény. Az információbiztonsági teljesítmény mérésére az alábbi mutatókat, eszközöket és módszereket kell használni:

1.8.8.1. KOCKÁZATELEMZÉS

A kockázatelemzés segít azonosítani az információbiztonsági fenyegetéseket, a kockázatokat, valamint a lehetséges hatásokat. A kockázatelemzés alapján a Hivatal képes felmérni az információbiztonsági teljesítményét, illetve mérni a biztonsági rendszer hatékonyságát.

1.8.8.2. TELJESÍTMÉNYMUTATÓK

Az információbiztonsági teljesítménymutatók segítségével mérhetők az információbiztonsági folyamatok hatékonysága. Az ilyen mutatók a hálózati átviteli sebesség, az adatbiztonság szintje, az incidenskezelési idő, a hibajavítási idő vagy a biztonsági ellenőrzések gyakorisága.

1.8.8.3. TELJESÍTMÉNYMÉRÉSI MÓDSZEREK

Az információbiztonsági teljesítmény mérésére használhatóak az oktatás-felmérési kérdőívek, a biztonsági átvilágítások, illetve az auditok.

1.8.8.4. ELLENŐRZÉSEK

Az információbiztonsági ellenőrzések során meg kell vizsgálni, hogy a munkavállalók betartják-e az információbiztonsági szabályokat, a belső irányelveket, valamint az érvényben lévő jogszabályokat. Az ellenőrzések eredményei alapján is mérhető az információbiztonsági rendszer hatékonysága.

1.8.9. SZERVEZETI ARCHITEKTÚRA

A szervezeti struktúra kialakításának és működtetésének olyan módon kell történnie, hogy Szervezet a működési és kiberbiztonsági kockázatokat rendszeresen azonosítani tudja, a feladat- és felelősségi körök egyértelműen meghatározottak és visszakövethetők legyenek (lásd. 1.7. Szerep- és felelősségi körök az információbiztonságban), továbbá a döntéshozatal és a kontrolltevékenységek szabályozottan, előre rögzített eljárások mentén haladjanak, nem eseti jelleggel.

1.8.10. KRITIKUS INFRASTRUKTÚRA BIZTONSÁGI TERVE

A kritikus infrastruktúra biztonsági terve elérhető a Rendszerbiztonsági tervekben és a Készenléti tervekben.

1.8.11. KOCKÁZATMENEDZSMENT-STRATÉGIA

A kockázatmenedzsment-stratégia célja, hogy az elektronikus információs rendszerek (EIR-ek) működéséhez és használatához, a szervezeti vagyonhoz, munkavállalókhoz, partnerekhez, valamint a személyes adatok kezeléséhez kapcsolódó biztonsági kockázatokat azonosítsa, értékelje, kezelje és folyamatosan felülvizsgálja.

Ezen stratégia a Hivatal minden szervezeti egységére és munkavállalójára kiterjed.

1.8.11.1. KOCKÁZATOK AZONOSÍTÁSA

A következő kockázati területek kerülnek feltérképezésre:

1.8.11.1.1. EIR-EKKEL KAPCSOLATOS KOCKÁZATOK

- Az informatikai rendszerek meghibásodása vagy kiesése, amely akadályozhatja a Hivatal működését.
- Adatvesztés vagy adatok sérülése.
- Kiberbiztonsági fenyegetések, például vírusok, zsarolóprogramok, illetéktelen hozzáférések.
- A rendszerekhez hozzáférő személyek nem megfelelő jogosultságkezelése.
- Tesztelési hiányosságok, kompatibilitási problémák

1.8.11.1.2. RENDSZER- ÉS VAGYONELEMEKHEZ KAPCSOLÓDÓ KOCKÁZATOK

- Informatikai eszközök eltulajdonítása vagy megrongálása.
- Szoftverlicenc- és adatvagyon-kezelés hiányosságai.
- Az üzleti folyamatokat támogató rendszerek nem megfelelő működése.

1.8.11.1.3. SZEMÉLYEKHEZ KAPCSOLÓDÓ KOCKÁZATOK

- Véletlen, vagy szándékos felhasználói hibák.
- Jogosultságkezelés hiányosságai.

1.8.11.1.4. MÁS SZERVEZETEKHEZ KAPCSOLÓDÓ KOCKÁZATOK

- Megbízhatatlan, nem minősített vagy túlzottan centralizált beszállítók.
- Szerződéses kötelezettségek nem teljesítése.
- Harmadik fél által okozott adat- vagy rendszerbiztonsági incidensek.
- Késedelmes vagy hibás szállítás.

1.8.11.1.5. SZEMÉLYES ADATOK KEZELÉSÉVEL KAPCSOLATOS KOCKÁZATOK

- Jogszabályoknak (GDPR) való nem megfelelés;
- Személyes adatokhoz való illetéktelen hozzáférés;
- Adatvesztés vagy adatmanipuláció.

1.8.11.2. KOCKÁZATKEZELÉS-ÉS CSÖKKENTÉS MÓDSZEREI

1.8.11.2.1. MEGELŐZŐ INTÉZKEDÉSEK

- Informatikai biztonsági szabályzatok alkalmazása.
- Jogosultságok szabályozása, naplózás bevezetése.
- Biztonságtudatossági képzések, rendszeres oktatás.
- Beszállítói minősítési rendszer alkalmazása.
- Szerződéses biztonsági követelmények érvényesítése.

1.8.11.2.2. ÉSZLELŐ INTÉZKEDÉSEK

- Rendszeres audit elvégzése, naplóelemzések.
- Felügyeleti rendszerek, behatolásérzékelők használata

1.8.11.2.3. REAGÁLÓ ÉS HELYREÁLLÍTÓ INTÉZKEDÉSEK

- Incidenskezelési eljárások tervezése, használata.
- Adatmentés és helyreállítás - tervek és folyamatok kidolgozása.
- Incidenskezelési tervek az ellátási láncra is

1.8.11.3. A STRATÉGIA HIVATALON BELÜLI ALKALMAZÁSA

Jelen IT kockázatmenedzsment-stratégia alkalmazása a Hivatal minden szintjén kötelező. Ennek érdekében minden szervezeti egységnek azonos elvek szerint kell eljárnia a kockázatok kezelésében. A kockázatok értékelését és dokumentálását egységes módszertan szerint kell végezni. A Hivatalon belül kijelölésre kerülnek a kockázatkezelésért felelős személyek (Lásd: IBSZ 1.6 Szerep- és felelősségi körök).

1.8.11.4. FELÜLVIZSGÁLAT ÉS AKTUALIZÁLÁS

A stratégiát legalább évente egy alkalommal felül kell vizsgálni, hogy alkalmazkodni tudjon a szervezeti változásokhoz, a technológiai és szabályozási környezet változásaihoz, valamint az újonnan felmerülő kockázatokhoz.

Az eseti módosításának, felülvizsgálatának kezdeményezése és a felülvizsgálat, valamint a módosítás elvégzése az informatikai rendszerek biztonságáért felelős személy (továbbiakban: IBF) feladata.

1.8.12. ENGEDÉLYEZÉSI FOLYAMATOK MEGHATÁROZÁSA

Új EIR bevezetése, meglévő módosítása vagy kivezetése csak az IT vezető előzetes jóváhagyásával történhet. A cél, hogy minden ilyen döntés előtt átgondolják a lehetséges biztonsági kockázatokat, és azok kezelése biztosított legyen. A kockázatok kezelésével konkrét felelősökét kell meghatározni.

1.8.13. SZERVEZETI MŰKÖDÉS ÉS ÜZLETI FOLYAMATOK MEGHATÁROZÁSA

Meg kell határozni a szervezeti célokat és az üzleti folyamatokat, figyelembe véve az információbiztonságot, valamint a szervezeti működésre, eszközökre, személyekre, más szervezetekre gyakorolt kockázatokat.

1.8.14. BIZTONSÁGI SZEMÉLYZET KÉPZÉSE

A biztonsági személyzet képzését és fejlesztését az oktatási tematika részévé kell tenni.

1.8.15. TESZTELÉS, KÉPZÉS ÉS FELÜGYELET

Éves szinten, dokumentáltan el kell végezni az EIR-hez kapcsolódó biztonsági teszteléseket, képzéseket és felügyeleti tevékenységeket.

1.8.16. SZAKMAI CSOPORTOKKAL ÉS KÖZÖSSÉGEKKEL VALÓ KAPCSOLATTARTÁS (A5.5 – A5.6)

Az IBF feladata a Nemzeti Kiberbiztonsági Intézettel (NKI), illetve a Szabályozott Tevékenységek Felügyeleti Hatóságával (SZTFH) történő kapcsolattartás. Amennyiben valamely esemény kapcsán szükséges, úgy a következő szervezetekkel történő kapcsolattartás is szükséges lehet:

1. Nemzeti Média- és Hírközlési Hatóság (NMHH)
   Kapcsolat az elektronikus kommunikáció biztonsága és az adatvédelem terén.
2. Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)
   A DPO mellett az adatvédelmi előírások betartása és az adatvédelmi incidensek kezelése érdekében.
3. Nemzeti Bűnüldözési Ügynökség (NBU)
   A kibertérben elkövetett bűncselekmények elleni küzdelem és az információbiztonsági incidensek nyomozása és kezelése érdekében.

A Hivatal a jogszabályban meghatározottak szerint bejelentette a Nemzeti Kiberbiztonsági Intézet részére az IBF azonosító adatait, ezzel megteremtette kapcsolattartás feltételeit az információbiztonság felügyeletével megbízott kormányzati szervekkel is.

Az IBF-nek folyamatosan figyelemmel kell kísérnie a fenti szervezetek által kiadott riasztásokat és gondoskodnia kell az EIR-re vonatkozó megfelelő ellenintézkedésekről és válaszlépésekről.

Amennyiben a riasztás érinti a Hivatal felhasználóit, akkor az IBF elektronikus levélben és a Hivatal intranetén keresztül értesíti a felhasználókat a riasztásban foglaltakról, a megtett védelmi intézkedésekről, valamint felhívja a felhasználók figyelmét a felhasználói oldalról követendő magatartásra.

1.8.17. FENYEGETETTSÉG TUDATOSÍTÓ PROGRAM (A5.7)

A Hivatal felismerte a növekvő információbiztonsági fenyegetésekre való tudatosítás fontosságát, ezért bevezeti a Fenyegetettség tudatosító programot a Hivatalon belül. A program célja:

a) Fenyegetések Felderítése
   A program a legújabb információbiztonsági fenyegetéseket és támadási módszereket követi, és folyamatosan frissíti a kapcsolódó fenyegetési információkat.
b) Információmegosztás Szervezeten belül
   Az informatikai üzemeltetés és a felhasználók között létrehoz egy hatékony információmegosztási rendszert, amely lehetővé teszi biztonsági szakemberek és a felhasználók számára a legújabb fenyegetésekről szóló információk cseréjét.
c) Tudatosság növelése
   A munkatársak és a vezetőség részére tart tréningeket és tudatosságnövelő programokat, hogy felismerjék a legfrissebb fenyegetéseket, és megfelelően tudjanak rájuk reagálni.
d) Kapcsolat a Szakmai szervezetekkel
   Folyamatos kell legyen a kapcsolat a Kibervédelemmel foglalkozó közösséggel, beleértve a szakmai szervezeteket (ISACA) és a kormányzati szerveket (NBSZ-NKI), hogy időben meg tudják osztani egymással az információkat az aktuális fenyegetésekről.

Ezen program bevezetése révén a Hivatal aktívan részt vesz az információbiztonság iránti tudatosság növelésében, és hatékonyan reagál a folyamatosan változó információbiztonsági kihívásokra.

1.8.18. KOCKÁZATKEZELÉSI KERETRENDSZER, KOCKÁZATKEZELÉSÉRT FELELŐS SZEREPKÖRÖK

A kockázatkezelési keretrendszer a 15. Kockázatkezelés fejezetben, a kockázatkezelésért felelős szerepkörök pedig az *1.7.2 Kockázati szerepkörök* pontban kaptak helyet.

1.8.19. ELLÁTÁSI LÁNC KOCKÁZATKEZELÉSI STRATÉGIÁJA

Rangsorolni és értékelni kell azokat a beszállítókat, amelyek kritikus technológiákat, termékeket és szolgáltatásokat szállítanak a Hivatal alapvető feladatainak ellátásához. Ez a stratégia összhangban van az üzletmenet-folytonossági tervvel (BCP), a kockázatkezelési irányelvekkel, valamint az ellátási lánc biztonságára vonatkozó megfelelőségi követelményekkel.

Ellátási lánc kockázatkezelési folyamata:

1.8.19.1. AZONOSÍTÁS

A Hivatal azonosítja azokat a külső partnereket, szolgáltatókat és rendszerelemeket, amelyek működés szempontjából kritikus szolgáltatást biztosítanak.

1.8.19.2. ÉRTÉKELÉS

A beszállítók értékelését el kell végezni. Szempontkét figyelembe kell venni a következőket:

- általuk kezelt, vagy elérhető információk
- szolgáltatás elérhetősége
- technológiai kitettség

- esetleges korábbi incidensek

1.8.19.3. KEZELÉS

Magas kockázatú partnerek esetében biztonsági követelményeket kell előírni. Különösen a hozzáférés-felügyelet, a naplózás és a titkosítás a prioritás.

Szerződésben kell rögzíteni az incidens-jelentési és együttműködési kötelezettségeket. Ezen partnerek esetében rendszereres beszállítói értékelést kell végezni.

Szükség esetén helyettesítő szolgáltatót kell kijelölni

1.8.19.4. MONITORING

Legalább éves szinten felül kell vizsgálni az ellátási lánccal kapcsolatos kockázatokat. Ezen felülvizsgálat szempontjai között kell, hogy szerepeljenek a következők:

- szolgáltatásokban felmerülő változások
- bekövetkezett incidensek, vagy SLA-sértések
- jogszabályi környezet változásai, vagy szervezeti környezet változása

1.8.19.5. DOKUMENTÁLÁS

- A tevékenységek kapcsán dokumentálni, illetve vezetni kell
- a beszállítói nyilvántartást
- értékelési táblázatot
- elfogadott kockázatokat, illetve megtett intézkedéseket

1.8.20. FOLYAMATOS FELÜGYELETI STRATÉGIA (A5.7)

A stratégia célja, hogy a Hivatal az információs rendszerek, hálózatok és szolgáltatások működését folyamatosan figyelje, észlelje a biztonsági eseményeket és szabálytalanságokat, valamint időben reagáljon azokra a Hivatal információvagyonának védelme érdekében.

Folyamatos felügyeleti folyamat

1.8.20.1. MEGFIGYELÉS ÉS ADATGYŰJTÉS

A Hivatal központi napló- és eseménygyűjtő rendszert alkalmaz, amely:

- rögzíti a kritikus eseményeket (sikeres/sikertelen bejelentkezés, konfiguráció-módosítás, hálózati anomália, jogosulatlan hozzáférési kísérlet),
- naplózza a rendszerek üzemállapotát, szolgáltatás-elérhetőségét és teljesítményét,
- biztosítja a naplók időbélyeggel, hitelesen és megőrzési rend szerint történő tárolását.

1.8.20.2. ÉSZLELÉS ÉS RIASZTÁS

- Automatikus riasztási mechanizmusok (e-mail, SMS, dashboard) segítik a gyors reagálást.
- A rendellenességek, túlterhelések és biztonsági események valós idejű megjelenítése biztosított.
- A naplóadatok elemzése során alkalmazható szabályok a potenciális támadások azonosítására.

1.8.20.3. ÉRTÉKELÉS ÉS REAGÁLÁS

- Az azonosított eseményeket a Biztonsági események kezelése eljárásrend szerint osztályozzák, értékelik és kezelik.
- Súlyos események esetén az IBF értesítése és a vészhelyzeti csoport aktiválása történik.

- A reagálás eredményeit minden esetben dokumentálni kell.

1.8.20.4. JELENTÉS ÉS FELÜLVIZSGÁLAT

- Rendszeres biztonsági jelentések készülnek a naplózott eseményekről.
- Évente legalább egyszer felülvizsgálatra kerül a felügyeleti rendszer hatékonysága és lefedettsége.
- A tapasztalatok alapján a Hivatal módosíthatja a naplózási és monitorozási szabályzatokat.

1.9. EGYÉB ELŐÍRÁSOK

1.9.1. ESZKÖZÖK ÁTADÁSA MUNKAVISZONY LÉTESÍTÉSEKOR

Az eszközök átadásának folyamatát minden esetben dokumentálni kell.

1.9.2. JELSZÓHASZNÁLAT, -BIZTONSÁG

A munkaállomások és 8 karakter, tartalmaznia kell min. 1 db kis betűt, 1 db nagybetűt és 1 db számot is. (lásd 8.21. A hitelesítésre szolgáló eszközök kezelése pont)

A jelszavakat legfeljebb 180 naponta kötelező megváltoztatni. (lásd 8.21. A hitelesítésre szolgáló eszközök kezelése pont)

A rendszergazdai jogosultsággal rendelkező felhasználók felhasználó nevüket és jelszavukat zárt borítékban kötelesek elhelyezni a Hivatal páncélszekrényében.

1.9.3. ADATBIZTONSÁG

Az archivált adatokat, és a biztonsági mentéseket, azonos biztonsági szinten kell kezelni, mint a használatban lévő adatokat, nyilvántartásokat.

A mentésekhez használt berendezéseket, eszközöket, informatikai „ürességi" vizsgálat nélkül, selejtezni, értékesíteni tilos.

1.9.4. MUNKAÁLLOMÁSOK VÉDELME

A munkaállomásokon egyedi vírusvédelmi szoftvereket kell futtatni. A szoftver beállítása és frissítése egyedileg történik. (lásd: 18.8. Kártékony kódok elleni védelem pont)

A munkaállomásokat jelszóval kell védeni.

A képernyővédőt jelszóval kell védeni. A képernyővédőt automatikusan aktiválni kell 10 perc inaktivitás után.

A munkaállomások merevlemezei csak a rajta található adatok végleges és biztonságos megsemmisítését követően selejtezhetők. Az adatok megsemmisítéséről jegyzőkönyvet kell felvenni. (lásd: 11.8. Adathordozók törlése pont)

1.9.5. HORDOZHATÓ ESZKÖZÖK VÉDELME

A felhasználók számára kiadott hordozható eszközök (notebook, mobiltelefon, hordozható adattároló) biztonságos tárolásáért, lopás és elvesztés elleni védelméért a felhasználó felel.

A hordozható eszközökre érzékeny, személyes, titkos adatot másolni tilos a meghajtó teljes titkosítása nélkül!

Hordozható eszközök csak a rajta található adatok végleges és biztonságos megsemmisítését követően selejtezhetők. Az adatok megsemmisítéséről jegyzőkönyvet kell felvenni. (lásd: *11.8. Adathordozók törlése* pont)

2. HOZZÁFÉRÉS-FELÜGYELET (A5.15; A5.18)

2.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Ezen eljárásrendnek a középpontjában azok a meghatározott célok állnak, amelyeket el kell érni a hozzáférés-felügyelet terén, például az adatbiztonság növelése vagy a jogosultságok megfelelő kezelése. Továbbá szabályozza, hogy a hozzáférés-felügyeleti eljárások mely területekre és rendszerekre vonatkoznak, valamint meghatározza az egyes szereplők, mint például a Felhasználók vagy a Rendszergazdák, felelősségi körét és jogosultságait ezen a területen. Biztosítja, hogy a szabályzat és az eljárásrendek megfeleljenek a vonatkozó jogszabályoknak, irányelveknek és szabályozásoknak.

Felelős: IBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

2.2. FIÓKKEZELÉS (A5.16)

A Hivatal az Elektronikus Információs Rendszerek (EIR) biztonsága érdekében az alábbi fióktípusokat és kezelési elveket alkalmazza:

FIÓKTÍPUSOK ÉS HASZNÁLATI SZABÁLYOK

Fióktípus	Felhasználói kör	Jogosultság szintje	Főbb szabályok
Normál fiók	Minden munkatárs	Feladatkörre korlátozott	Egyedi, névre szóló azonosítás kötelező.
Névre szóló rendszergazdai fiók	Informatikai üzemeltetők	Kiemelt	Kizárólag rendszerfelügyeletre; napi munkához normál fiók használata kötelező.
Beépített rendszergazdai fiók	Rendszerelemek (root, admin)	Teljes körű	Használatuk tilos; kizárólag vészhelyzeti tartalékként funkcionálnak.
Technikai fiók	Szoftverek, eszközök (pl. nyomtató)	Funkcióspecifikus	Személyek nem használhatják (kivéve tesztelés). Névre szóló fiók nem válthatja ki.

JOGOSULTSÁGKEZELÉSI ALAPELVEK

Szerepkör alapú hozzáférés beállítása. A jogosultságokat tilos közvetlenül a felhasználókhoz rendelni. Ehelyett jogosultsági csoportokat kell létrehozni, amelyek megfelelnek az adott munkakörnek (pl. "pénztáros", "beszerző").

Előnye az áttekinthetőbb struktúra, gyorsabb auditálhatóság és egyszerűbb jogosultság-visszavonás. Ez az elv akkor is kötelező, ha a csoportnak csak egy tagja van.

Minden jogosultsági csoportról leírást kell készíteni, amely tartalmazza a csoport célját és tartalmát. Ezt a listát a felhasználók számára is elérhetővé kell tenni az igénylési folyamat megkönnyítésére.

A személyes tárhely, azaz a felhasználók saját („home") mappája kivételt képeznek a csoportosítási szabály alól.

ENGEDÉLYEZÉSI ÉS KEZELÉSI REND

A fiókok életciklusáért (létrehozás, módosítás, törlés) a kijelölt rendszergazda felel.

A névre szóló és a beépített rendszergazdai fiókok bármilyen módosításához az IT vezető előzetes engedélye szükséges.

Tilos névre szóló fiókot technikai fiókként használni (pl. automatizált riportküldéshez), mert a munkavállaló távozásakor a szolgáltatás leállhat.

A Hivatal EIR-hez kizárólag olyan személy kaphat hozzáférést, akinek a munkájához szükséges az EIR használata, és aki megismerte és dokumentáltan elfogadta a rendszerre vonatkozó hozzáférési szabályokat, valamint:

a. a Hivatal alkalmazottja (rögzítésre került a Hivatal munkaügyi rendszerében), vagy;
b. informatikai rendszerüzemeltetési szerződéssel rendelkező cég alkalmazottja (ideértve a Rendszergazda külsős munkatársait), vagy;
c. a Hivatallal megbízási vagy vállalkozási szerződéses kapcsolatban álló magánszemély, egyéni vállalkozó vagy cég alkalmazottja, vagy;
d. a Hivatalnál munkát vagy más tevékenységet folytató, érvényes szerződéssel rendelkező hallgató, illetve gyakornok.

Azok a felhasználók, akik nem a Hivatal alkalmazottjai csak az IT vezető tudtával és jóváhagyásával kaphatnak hozzáférést. Csak valós, aktív munka- vagy szerződéses viszonyban álló személyeket lehet regisztrálni a rendszerben.

A jogosultságok kezelésekor alapelvként kell érvényesíteni, hogy csak a felhasználók feladatellátásához szükséges és elégséges mértékű jogosultságok biztosíthatók.

A munkahelyi vezetők feladata, hogy a beosztott munkatársaikra vonatkozóan megkérjék azokat a hozzáférési jogosultságokat, amelyek az EIR használatához kapcsolódóan a munkatársak feladatellátásához szükségesek.

A beosztott munkatársak feladatkörében vagy az EIR-ben bekövetkező változások esetén a munkahelyi vezetőknek felül kell vizsgálniuk a munkatársak hozzáférési jogosultságait és kezdeményezniük kell a szükségtelen jogosultságok visszavonását, illetve új jogosultságok kiadását.

A Hivataltól kilépő alkalmazottak hozzáférési jogosultságának megszüntetését a Személyügyi ügyintéző kezdeményezi.

A Kulcsfelhasználónak 3 havonta felül kell vizsgálnia a felhasználói fiókokat, és ellenőriznie kell, hogy minden kilépő alkalmazott hozzáférési jogosultsága megszüntetésre került-e.

A felhasználói fiókok felülvizsgálata céljából a Személyügyi ügyintéző a Rendszergazda kérésére annak rendelkezésére bocsájtja a Hivatalnál aktuálisan dolgozó alkalmazottak listáját, illetve az elmúlt 3 hónapban kilépettek listáját.

A munkahelyi vezetők felelőssége, hogy azonnal értesítsék a Kulcsfelhasználót a következő esetekben:

a) ha az adott Felhasználó hozzáférése a rendszerhez a továbbiakban szükségtelen;
b) ha az adott Felhasználó jogviszonya megszűnik;
c) ha a rendszerhasználathoz szükséges ismeretek megváltoznak.

Csak a következő esetekben engedélyezett a rendszer használata:

a) érvényes hozzáférési engedély birtokában;
b) tervezett rendszerhasználat esetén.

A kilépő alkalmazottakról a Személyügyi ügyintéző írásban értesíti a Rendszergazdát és a Kulcsfelhasználót, akik megszüntetik az alkalmazottak jogosultságait.

A hozzáférési jogosultságok megszüntetésével egyidejűleg az elektronikus belépőkártyák jogosultságát is meg kell szüntetni, függetlenül attól, hogy a belépőkártya visszaadásra került-e, vagy sem.

A jogosultságok megszüntetéséért a Rendszergazda és a Kulcsfelhasználó a felelős.

2.15. HOZZÁFÉRÉS-ELLENŐRZÉS ÉRVÉNYESÍTÉSE (A8.3)

A Hivatalnál csak olyan EIR használható, amely képes a kiadott hozzáférési jogosultságokat érvényesíteni, azaz az EIR-ben kezelt adatokhoz, a rendszerelemekhez csak a megfelelő jogosultsággal rendelkezők férhetnek hozzá.

2.71. SIKERTELEN BEJELENTKEZÉSI KÍSÉRLETEK

A felhasználói azonosító ismeretében a támadók gyakran kísérlik meg a jelszót próbálkozással kitalálni (sokszor nyers erő felhasználásával, azaz egy szótár szavainak vagy az összes lehetőség végig próbálásával).

Ennek a támadásnak kell csökkenteni a hatékonyságát azzal, hogy ha túl sok sikertelen bejelentkezési kísérlet történik egy megadott időn belül, akkor a rendszer egy rövid ideig zárolja a felhasználói fiókot, vagyis nem engedi a bejelentkezést.

Az EIR-nek a következő fiókzárolási házirendet kell alkalmaznia sikertelen bejelentkezési kísérletek esetén:

Szabály megnevezése	**Beállított érték**	**Magyarázat**
Fiókzárolás alsó értéke	5 sikertelen próbálkozás	A rendszer ennyi hibás jelszó megadása után zárolja a felhasználói fiókot és tagadja meg a rendszerbe történő bejelentkezést.
Fiókzárolás időtartama	fiók feloldásig	Ennyi ideig kerül zárolásra a felhasználói fiók.
Fiókzárolási számláló nullázása	-	Ha ennyi percig nem történt sikertelen bejelentkezési kísérlet, a rendszer nullázza a sikertelen bejelentkezések számát.

2.75. A RENDSZERHASZNÁLAT JELZÉSE

Az EIR elindításakor – még a bejelentkezés előtt – tájékoztatni kell a felhasználókat a következőkről:

a) a Felhasználó a Hivatal EIR-ét használja;
b) a rendszer használatot a Hivatal figyelheti, rögzítheti, naplózhatja;
c) a rendszer jogosulatlan használata tilos, és büntetőjogi vagy polgárjogi felelősségre vonással jár;
d) a rendszer használatával a Felhasználó elfogadja és tudomásul veszi a fentieket.

A figyelmeztető üzenetet mindaddig a képernyőn kell tartani, amíg a Felhasználó közvetlen műveletet nem végez az EIR-be való bejelentkezéshez vagy további rendszer hozzáféréshez.

2.88. AZONOSÍTÁS VAGY HITELESÍTÉS NÉLKÜL ENGEDÉLYEZETT TEVÉKENYSÉGEK

A Hivatal EIR-ében azonosítás és hitelesítés nélkül semmilyen felhasználói tevékenység nem engedélyezett.

A jelszavas (vagy más) hitelesítésnek ki kell terjednie a szerverekre, valamint minden hálózaton üzemelő és hálózattól független, egyedi munkaállomásra.

A fentiek alól kivételt képez a Hivatal Internetes honlapja, amelyen bárki számára hitelesítés nélkül elérhető, publikus információkat helyez el.

2.100. TÁVOLI HOZZÁFÉRÉS

Távoli hozzáférésnek minősül minden olyan hozzáférés a Hivatal EIR-hez, amelyben a kommunikáció egy külső, nem a Hivatal által ellenőrzött hálózaton (pl. Interneten) zajlik.

Az EIR-hez történő távoli hozzáférés alapesetben az alábbi felhasználók számára biztosítható:

- a Hivatal azon alkalmazottai számára, akik a lassú adatkapcsolattal (pl.: Internet, mikrohullámú kapcsolat) rendelkező telephelyen dolgoznak, vagy munkájuk megköveteli, hogy azt sokféle helyszínen, mobil eszközökkel végezzék;
- infrastruktúra szolgáltatás esetén
- A Hivatal által üzemeltetett szoftverek és rendszerek külsős fejlesztői és rendszertámogatást ellátó partnerek számára

Távoli hozzáférés esetében minimálisan elvárt biztonsági követelmény, hogy a hitelesítés során használt jelszó a hálózaton titkosított formában kerüljön továbbításra, és amennyiben lehetséges a teljes adatforgalmat titkosítani kell.

A távoli hozzáférést alapesetben az általános jogosultságigényléshez leírtak szerint kell igényelni.

A felhasználói körre és hozzáférés igénylésére vonatkozóan az alapesettől való eltéréseket az egyes hozzáférés típusok szabályozása tartalmazza.

A Hivatal távoli hozzáférésre az Internetet használja (a telefonos kapcsolatfelvétel nem támogatott) és az alábbi hozzáférés típusokat alkalmazhatja:

Virtuális magánhálózat (VPN)

A virtuális magánhálózat (VPN) egy nyilvános hálózat (pl. Internet) egyes végpontjai között kiépített logikai hálózat, amelyen keresztülmenő adatok nem láthatók az eredeti hálózaton, mivel titkosított adatcsomagokba vannak csomagolva.

A Hivatal VPN hozzáférést biztosít az alapesetben engedélyezett felhasználók mellett:

- a Rendszergazda munkatársai számára távoli asztal hozzáféréssel kombinálva a többtényezős hitelesítés megvalósításához;
- közvetlen (optikai) adatkapcsolattal nem rendelkező telephelyek és a központi telephely Interneten keresztüli összekötésére (site-to-site VPN);
- indokolt esetben – az IT vezető engedélyével – az EIR-hez támogatást nyújtó külső partnerek számára távoli asztal hozzáféréssel kombinálva;
- nagyon indokolt esetben az otthoni munkavégzés támogatására.

A VPN kapcsolat titkosított, így az adatok bizalmasságára nézve biztonságos, de a Hivatal hálózatához távolról kapcsolódó számítógép részévé válik a hálózatnak, és ezzel fenyegetést jelenthet a hálózatra nézve (pl. vírusfertőzést okozhat). A kockázatok csökkentése érdekében az alábbiakról kell gondoskodni:

- A VPN hozzáférést úgy kell létrehozni, hogy csak a szükséges rendszerelemek legyenek elérhetők a távolról kapcsolódó számítógépekről.
- A távoli hozzáférés esetében is ugyanazokat a munkaállomásokra vonatkozó biztonsági előírásokat kell betartani, mint a belső hálózatban használt számítógépek esetén (pl.: naprakész vírusvédelmi szoftverrel, telepített biztonsági frissítésekkel, bekapcsolt tűzfallal kell a számítógépnek rendelkeznie).

A telephelyek közötti VPN kapcsolatok a telephely minden felhasználójára érvényesek, a hozzáférést nem kell külön igényelni.

A VPN szerver központi felügyeleti rendszerén a Rendszergazda napi szinten megvizsgálja a regisztrált sikeres vagy sikertelen belépéseket, a szokásostól eltérő aktivitásokról tájékoztatja az IT vezetőt, aki megteszi a szükséges intézkedéseket

Távoli asztal (RDP)

A Hivatal távoli asztal hozzáférést biztosít az alapesetben engedélyezett felhasználók mellett:

- a Rendszergazda munkatársai számára rendszerüzemeltetés céljából;
- indokolt esetben – az IT vezető engedélyével – az EIR-hez támogatást nyújtó külső partnerek számára;
- nagyon indokolt esetben az otthoni munkavégzés támogatására.

A hozzáférés titkosított kapcsolaton keresztül kell, hogy megvalósuljon.

Saját számítógép távoli elérése VPN kapcsolattal, távoli asztallal

Indokolt esetben – az IT vezető engedélyével – a felhasználók saját számítógépükbe távolról bejelentkezhetnek.

Távoli hozzáférést (távtámogatást) biztosító szoftver (VnC)

Távoli hozzáférést biztosító szoftver lehetővé teszi egy számítógép, vagy eszköz távoli irányítását egy másik eszközről. A gyártó honlapján regisztrálni kell egy fiókot (a Hivatal által biztosított kapcsolattartási adatokkal – e-mail, a Központi felügyelethez. A kliens(ek)re és az irányító eszközre is telepíteni szükséges a Távoli hozzáférést biztosító szoftvert. A Felhasználó gyakorlatilag azt érzékeli, mintha közvetlenül a távvezérelt eszköz előtt dolgozna.

A Hivatal ilyen módon Távoli hozzáférést biztosít:

- a Rendszergazda Rendszergazda szerepkörben dolgozó munkatársai számára rendszerüzemeltetés céljából;
- indokolt esetben az otthoni munkavégzéssel, vagy távmunkával dolgozó, engedélyezett felhasználók számára;
- különösen indokolt esetben – az IT vezető engedélyével – az EIR-hez támogatást nyújtó külső partnerek számára.

A hozzáférés minden esetben titkosított kapcsolaton keresztül valósul meg, ezen kapcsolat létrehozása a Távoli hozzáférést biztosító szoftver feladata.

Elvárás, hogy a távoli bejelentkezésnél biztosított legyen, hogy a Felhasználó tudomással bírjon a távoli hozzáférés megtörténtéről, maga engedélyezze.

2.108. VEZETÉK NÉLKÜLI HOZZÁFÉRÉS

A Hivatal a következőkben leírtak szerint elkülönített vezeték nélküli hozzáférést biztosíthat az alkalmazottai és a vendégek számára a Hivatal telephelyeire vonatkozóan.

Az alkalmazottak és vendégek WiFi hozzáférésére vonatkozó védelmi intézkedések beállítása a Rendszergazda feladata. Amennyiben egy WiFi hozzáférésre a továbbiakban nincs szükség, annak letiltása a Rendszergazda feladata.

Alkalmazottak

Kizárólag az alkalmazottak számára a Hivatal a belső hálózatra történő kapcsolódáshoz legalább IEEE 802.11n szabványnak megfelelő (WiFi) vezeték nélküli hozzáférést biztosít a Hivatal tulajdonában levő mobil eszközökön.

A vezeték nélküli hozzáférésnél az alábbi módon kell gondoskodni az illetéktelen használat megelőzéséről:

- A vezeték nélküli WiFi eszközön (hozzáférési ponton/routeren) WPA2/WPA3 protokollt kell alkalmazni (a sok esetben alapértelmezett, bizonyítottan könnyen feltörhető WEP protokoll használata kifejezetten tilos).
- A vezeték nélküli hozzáféréshez legalább 9 karakter hosszú, a felhasználói jelszó kiválasztására vonatkozó szabályoknak megfelelő, véletlenszerűen generált hozzáférési kulcsot kell beállítani.
- A hozzáférési kulcsokat a rendszergazdának 365 naponta meg kell változtatnia, és ezt dokumentálnia.
- A hozzáférési kulcsokat a Rendszergazda beépített adminisztrátori jelszavakkal megegyező módon tárolja.
- A kulcsok kezelésére a fenti eltéréssekkel a felhasználói jelszavakra vonatkozó előírások és biztonsági intézkedések vonatkoznak.
- A WiFi eszközön le kell tiltani a WiFi Protected Setup (WPS) használatát, amely a hozzáférési kulcs ismerete nélkül is lehetővé tenné az eszközökhöz való kapcsolódást.
- A WiFi eszköz web-es adminisztrálási felületének eléréséhez tikosított (HTTPS) kapcsolatot kell alkalmazni az alapértelmezett menedzsment-port megváltoztatásával.
- A rendszerbe csak olyan céges eszköz csatlakozhat be, amelynek csatlakozását az IT vezető előzetesen engedélyezte és a hálózaton regisztrálva lett (MAC azonosítóval). A becsatlakozott eszközök felügyelete a Rendszergazda feladata.
- A Wifi hozzáférés AD authentikációval is megvalósítható.

A belső hálózathoz való vezeték nélküli hozzáférés mobil eszközön történő beállítását a Rendszergazdától e-mailben kell igényelni. A beállítás csak az IT vezető írásos jóváhagyásával történhet.

Vendégek

A Hivatal a vendégei számára nem biztosít vezeték nélküli hozzáférést.

2.113. MOBIL ESZKÖZÖK HOZZÁFÉRÉS-ELLENŐRZÉSE

A Hivatal EIR-hez mobil eszközről történő hozzáférésnél a telephelyen belüli vezeték nélküli hozzáférés esetén a Vezeték nélküli hozzáférés pont, az Interneten keresztüli távoli hozzáférés esetén a Távoli hozzáférés pont rendelkezései szerint kell eljárni.

Mobil eszközökkel történő hozzáférés csak a Hivatal tulajdonában lévő mobil eszközökről engedélyezett. Ezen eszközöket ESET Mobile Device Management (MDM) teszi biztonságossá, központilag felügyelhetővé.

A mobil eszközök esetén nagyobb valószínűséggel fordulhat elő az eszköz elvesztése vagy eltulajdonítása. A kockázatok csökkentése érdekében az alábbiakról kell gondoskodni:

- A hordozható számítógépeket felhasználói azonosítás nélkül használni tilos;
- A hordozható számítógépek háttértárolóját titkosítani kell (pl. Windows operációs rendszer esetén a beépített BitLocker funkció használatával). A számítógép üzembe helyezési folyamatának részét kell képeznie a titkosítás beállításának.
- A mobiltelefonokhoz táblagépekhez való hozzáférést képernyő mintával PIN kóddal (amely nem azonos a SIM kártya feloldásához alkalmazott PIN kóddal), vagy biometrikus azonosítással kell védeni. Ennek beállítása az eszköz használójának a feladata, de e-mailben bejelentve segítség kérhető a Rendszergazdától.
- A mobiltelefonok, táblagépek elvesztése vagy eltulajdonítása esetén gondoskodni kell az eszköz tartalmának távolról történő törléséről.
- A mobil eszközök elvesztését vagy eltulajdonítását a Munkahelyi vezetőnek jelenteni kell.

2.115. KÜLSŐ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK HASZNÁLATA

A Hivatal a külső EIR-ek használatát csak akkor engedélyezi, ha azokban is érvényesülnek az IBSZ-ben megfogalmazott biztonsági elvárások, illetve, ha az adatgazda engedélyezte.

A Hivatal felhasználóinak a hozzáférését külső rendszerekhez, a külső EIR adatgazdája engedélyezheti, ha a munkavégzéshez szükséges.

Ha a Hivatal adatfeldolgozói tevékenységet végez külső rendszerekben, annak részleteit és biztonsági követelményeit szerződésben kell rögzíteni (Adatfeldolgozói szerződés)

az engedélyezett és szabályozott külső rendszerek (pl. szerződéses SaaS, AI-eszközök)

Minden egyéb külső rendszer használata tilos!

A fentiek előírások alól kivételnek tekinthető olyan külső rendszer használata, amire jogszabály kötelezi a Hivatalt.

2.124. NYILVÁNOSAN ELÉRHETŐ TARTALOM

A Hivatal az Internetes honlapján, illetve a hivatalos, szociális média oldalán bárki számára elérhető, publikus információkat tesz közzé.

Az információk közzétételéről minden esetben a Hivatal vezetője dönt. Az ő engedélye nélkül semmilyen információ nem tehető közzé.

Az Adatvédelmi felelős áttekinti a közzétenni kívánt tartalmat annak érdekében, hogy ellenőrizze, nem tartalmaznak nem nyilvános információkat.

Az adatvédelmi felelős további feladata, hogy 30 naponta áttekintse a publikált tartalmakat, és amennyiben nem nyilvános információt talál, úgy azt eltávolítja.

A Hivatal hivatalos honlapja: https://vertesszolos.hu .

3. TUDATOSSÁG ÉS KÉPZÉS (A6.3)

3.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend meghatározza a tudatosság és képzés területén elérni kívánt célokat és feladatokat. Ez magában foglalja az információbiztonsági szabályok betartásának növelését és az adatvédelem iránti tudatosság fejlesztését.

Kiemelten kezeli a vezetők szerepét és elkötelezettségét ezen a területen. Fontos, hogy összhangban legyen a vonatkozó jogszabályokkal és szabványokkal. Emellett rögzíti, hogy milyen szankciók vagy intézkedések léphetnek érvénybe a szabályok megsértése esetén. A szabályzat folyamatos frissítése és könnyű elérhetősége minden alkalmazott számára biztosítja a hatékony és megfelelő tudatosság és képzés fenntartását.

Felelős: IBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel ismertetni kell.

3.2. BIZTONSÁGTUDATOSSÁGI KÉPZÉS

A képzések célja

Az Információ biztonsági képzések alapvető célja a munkatársak, és a szabályzat hatálya alá tartozók ismereteinek bővítése, frissítése. A képzési és tudatossági tananyagot éves szinten frissíteni szükséges. A belső és külső biztonsági eseményekből levont tanulságot is be kell építeni a képzésekbe.

A képzésekkel szembeni elvárások, képzések fajtái:

a) Betanító képzés:
   Célja az új vagy áthelyezett Felhasználó megismertetése a rendszerrel, és az informatikai szabályokkal. A kezdeti képzések keretében kell megtartani egyénileg, vagy csoportosan.
b) Szinten tartó képzés:
   Célja az ismeretek felfrissítése, a jogszabályváltozások követése, a technikai változások megismerése, amennyiben a rendszert érintő változások megkövetelik. A képzés anyaga épülhet a Hivatalban tapasztalt események elemzésére is.
c) Fejlesztő képzések:
   Az információbiztonság témakörére épített tréning jellegű képzés, az elvárt magatartások begyakorlása, és a várható események kezelése, az oktatási anyag része. A képzés irányulhat a technikai változások beillesztésére való felkészülésre, a logikai változások tanulmányozására.

A képzés témakörei:

A képzésen a következő témaköröket kell minimálisan érinteni:

a) Információbiztonsági alapfogalmak;
b) Támadási formák;
c) számítógépes kártevők fajtái;
d) ember által elkövetett támadások fajtái;
e) Vonatkozó jogszabályok, szabályzatok;
f) Felhasználók feladatai, felelőssége és jogai;
g) Biztonsági események felismerése és jelentése;
h) Az Internet és az elektronikus levelezés biztonsága;

i) Vírusok és egyéb kártevők elleni védelmi intézkedések;
j) A hibák, üzemzavarok bejelentések menete;
k) Jogosultsági rendszer, jogosultság igénylés folyamata;

Az EIR-hez való hozzáférés engedélyezésére, vagy kijelölt feladat végrehajtására csak a képzésen való részvételt követően kerülhet sor.

3.4. BIZTONSÁGTUDATOSSÁGI KÉPZÉS – BELSŐ FENYEGETÉS

A Fejlesztő képzéseknek ki kell térniük a belső fenyegetések potenciális jeleinek felismerésére és jelentésére is.

3.9. SZEREPKÖR ALAPÚ BIZTONSÁGI KÉPZÉS

Kiemelt fontosságú, hogy a speciális szerepkörökben, vagy speciális feladatot végző munkavállalók ne csak általános, hanem szerepkör alapú biztonsági képzést kapjanak.

Ilyen kiemelt szerepkörök:

a) Felsővezetők;
b) Adatgazdák;
c) Rendszergazdák/Rendszerüzemeltetők

Számukra az általános képzésen túl szerepkörre, vagy feladatkörre irányuló képzést szükséges tartani!

Az EIR-hez való hozzáférés engedélyezésére, vagy kijelölt feladat végrehajtására csak a képzésen való részvételt követően kerülhet sor.

A biztonsági személyzetnek az EIR-ben bekövetkezett változások esetén minden esetben haladéktalanul képzésben kell részesülnie.

3.13. A BIZTONSÁGI KÉPZÉSRE VONATKOZÓ DOKUMENTÁCIÓK

A Hivatalnak a többi képzéssel együtt dokumentálnia kell biztonságtudatosságra vonatkozó alap-, és szerepkör alapú biztonsági képzéseket. A dokumentumoknak tartalmazniuk kell:

a) Az oktatás tematikáját
b) Az oktatás anyagait
c) Az oktatás helyét és idejét
d) A résztvevők felsorolását és aláírását
e) Az oktató megnevezését, és aláírását.

A Hivatal a képzésen résztvevőkkel a képzés megtörténtét elismerteti, és a dokumentumokat megőrzi legalább 5 évig.

4. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG (A8.15)

4.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend feladata a Hivatal belső folyamatainak és tevékenységeinek rögzítése, nyomon követése és ellenőrzése. Ennek révén biztosítja az átláthatóságot, az események követését, valamint az esetleges hibák vagy visszaélések azonosítását és kezelését. Emellett segíti a jogszabályoknak való megfelelést és a biztonságot. A szabályzat további célja, hogy elősegítse az elszámoltathatóságot, azaz az egyének és csoportok felelősségének és számadási képességének biztosítását a tevékenységeikért és döntéseikért.

A naplózás során az EIR automatikusan rögzíti az eseménynaplóban a rendszerben bekövetkező eseményeket, hibákat, felhasználói tevékenységeket és ezek időpontját.

A naplózás lehetővé teszi a változások észlelését, a felhasználók számon kérhetőségét, és elengedhetetlen a biztonsági események kezeléséhez.

Felelős: IBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

4.2. NAPLÓZHATÓ ESEMÉNYEK

A naplózásnak az EIR kapcsolódó környezetére is ki kell terjednie, vagyis az alkalmazói szoftverek mellett a szerverek, hálózati eszközök, határvédelmi eszközök és egyéb biztonsági eszközök esetén is engedélyezni kell a naplózást.

Biztosítani kell, hogy az EIR és kapcsolódó környezetük naplózni tudják a következő eseményeket:

a) a felhasználók be- és kijelentkezését a rendszerbe (beleértve mind a sikeres, mind a sikertelen belépési kísérleteket);
b) a Rendszergazdák a rendszer bármely rétegébe történő be-és kijelentkezését;
c) a Rendszergazdák tevékenységét a rendszer bármely rétegében;
d) a felhasználói fiókok és jogosultságok módosítását;
e) a konfigurációs beállítások módosítását;
f) az alkalmazói szoftverekben az adatállományok (adatbázisok) módosítását;
g) a rendszer eseményeket (pl. a rendszer leállását és újra indulását);
h) a rendszerben fellépő hibákat.

Amennyiben valamely rendszer nem képes minden előírt eseményt naplózni, annál törekedni kell, hogy a későbbi fejlesztések során alkalmas legyen, illetve a leghatékonyabb megoldást kell megvalósítani.

A naplózási beállításokat az IBF a rendszer bevezetésekor és évente felülvizsgálja annak érdekében, hogy elegendőek-e a biztonsági események kivizsgálásához.

4.3. NAPLÓBEJEGYZÉSEK TARTALMA

Az EIR naplóbejegyzéseinek a következőket kell tartalmazniuk:

a) az esemény típusát;
b) az esemény időpontját;
c) az esemény helyét (mely lokáció, rendszerelem vagy rendszer);
d) az esemény forrását (miből származott az esemény);

e) az esemény leírását (mi lett a kimenetel);
f) a Felhasználó azonosítóját;

4.5. NAPLÓZÁS TÁRKAPACITÁSA

A naplók tárkapacitását az EIR fejlesztőjének a bevonásával az előzetes kapacitástervezési folyamat során kell kialakítani.

Az operációs rendszer naplóit tároló köteten a szabad kapacitás nem csökkenhet 10% alá.

Az informatikai rendszer naplóit tartalmazó köteten a szabad kapacitás nem csökkenhet 15% alá.

A naplók tárkapacitásának figyelését az EIR felügyeleti tevékenységébe kell beépíteni.

4.7. NAPLÓZÁSI HIBA KEZELÉSE

Az EIR naplóinak a figyelését oly módon kell kialakítani, hogy naplózási hiba esetén a rendszer küldjön riasztást a rendszergazdának.

Amennyiben kivitelezhető, naplóhiba esetén függessze fel a további feldolgozást a hiba elhárításáig.

A rendszergazda felelőssége, hogy a lehető leghamarabb, de maximum 1 órán belül reagáljon és kezdje meg a hiba elhárítását.

4.13. NAPLÓBEJEGYZÉSEK FELÜLVIZSGÁLATA, ELEMZÉSE ÉS JELENTÉSTÉTEL

Az EIR és kapcsolódó környezetük (alkalmazói szoftverek, szerverek, hálózati eszközök, határvédelmi eszközök és egyéb biztonsági eszközök) eseménynaplóit az üzemeltetési feladatok részeként a rendszergazdának legalább havonta át kell vizsgálnia.

Nem megfelelő, vagy szokatlan működésre utaló jelek esetén értesíteni kell az IT vezetőt, aki dönt az esetleges további lépésekről. Incidens gyanúja esetén az IBF is haladéktalanul értesítendő.

Incidens gyanúja esetén az adott naplóbejegyzések szélesebb körű vizsgálata szükséges, a naplóvizsgálatot a Rendszergazda végzi és az IBF koordinálja.

4.24. IDŐBÉLYEGEK (A8.17)

Az EIR-nek valamennyi naplóbejegyzését időbélyeggel (időbejegyzéssel) kell ellátnia, melyhez a rendszerórát kell alapul venniük. Az EIR elemeinek rendszeróráját hálózati idő protokoll (Network Time Protocol, NTP) segítségével az egyezményes koordinált világidőhöz kell szinkronizálni.

A rendszerekben engedélyezett időeltérés 1 másodperc.

4.25. NAPLÓINFORMÁCIÓK VÉDELME

Gondoskodni kell arról, hogy az EIR naplóinformációi védettek legyenek a jogosulatlan hozzáféréssel, módosítással és törléssel szemben. A naplóinformációk védelmét a Hivatal a hozzáférési jogosultságok megfelelő beállításával éri el.

Jogosulatlan hozzáférés, módosítás vagy a naplóinformáció törlésének észlelésekor a Rendszergazda értesíti az IT vezetőt, illetve az IBF-t.

4.38. A NAPLÓBEJEGYZÉSEK MEGŐRZÉSE

A naplóinformációk mentését be kell vonni a Társaság mentési rendszerébe. A mentéseket tárkapacitással összhangban úgy kell kialakítani, hogy a naplóbejegyzések ne vesszenek el. A naplóinformációkat biztonsági események utólagos kivizsgálása érdekében:

a) a határvédelmi eszközök és az arra alkalmas hálózati eszközökre vonatkozóan legalább 1 év;
b) a kliens oldali operációs rendszerek naplóira vonatkozóan legalább 1 hónap;
c) a szerver oldali operációs rendszerek naplóira vonatkozóan legalább 1 év;
d) az alkalmazás szoftverek naplóira vonatkozóan 1 évig;
e) konzisztens adatbázisok naplóira vonatkozóan (tranzakció log) 1 év;

A megőrzési idők biztosítása érdekében az alkalmazói szoftverek naplóinak mentését, az archív mentését, az egyéb környezeti naplók mentését a havi mentésekkel együtt kell végezni.

4.40. NAPLÓBEJEGYZÉSEK LÉTREHOZÁSA

A Hivatalnál csak olyan EIR használható, amely megfelel a következő követelményeknek:

a) Tegye lehetővé a Rendszergazdáknak a naplózható események kiválasztását.
b) Biztosítsa a naplóbejegyzések előállítási lehetőségét a 4.2 Naplózható események pontban meghatározott naplózható eseményekre.

5. ÉRTÉKELÉS, ENGEDÉLYEZÉS ÉS MONITOROZÁS (A8.16)

5.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend fő feladata a biztonságértékelési folyamatok és eljárások meghatározása, dokumentálása és megvalósítása a Hivatalban. Ennek révén biztosítja a Hivatal belső biztonsági intézkedéseinek összhangját a vonatkozó jogszabályokkal és irányelvekkel, valamint elősegíti az átláthatóságot és hatékonyságot a biztonsági intézkedések felügyeletében és követésében.

Az eljárásrend célja továbbá, hogy biztosítsa a folyamatos megfelelést és hatékonyságot a biztonsági területen, valamint a rendszeres felülvizsgálatok révén lehetőséget teremtsen a frissítésekre és az esetleges fejlesztésekre.

Felelős: IBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

5.2. BIZTONSÁGI ÉRTÉKELÉSEK

BIZTONSÁGÉRTÉKELÉSI TERV CÉLJA

A biztonsági elemzés során a rendszer vagy hálózat biztonsági kockázatait lehet azonosítani, ami lehetővé teszi a problémák orvoslását. A Hivatal továbbá képes lesz arra, hogy előre felismerje a potenciális biztonsági problémákat és meghozza a szükséges intézkedéseket a kockázatok minimalizálása érdekében. Emellett azonosítani tudja a biztonsági eszközök hiányosságait, illetve fel tudja mérni ezen eszközök hatékonyságát. Ezen tevékenységeket évente, vagy a rendszerben történő nagyobb változtatásokkor el kell végezni.

ÉRTÉKELŐ CSOPORT TAGJAI

BELSŐ ÉRTÉKELŐCSAPAT

- IBF / információbiztonsági vezető (módszertan, kontrollok, jelentés összefogása)
- IT üzemeltetés (AD, hálózat, szerverek, mentés, végpontvédelem – bizonyítékok, beállítások)
- Alkalmazásgazdák / fejlesztés (alkalmazás- és konfigurációkontrollok)
- OT/SCADA felelőse
- Belső ellenőrzés / compliance / kockázatkezelés
- Adatvédelem/DPO (ha a kontrollok érintenek személyes adatkezelést)

FÜGGETLEN ÉRTÉKELŐK

- Információbiztonsági tanácsadó cég (kontroll-értékelés, gap analysis, technikai és szervezeti megfelelés)
- Külső sérülékenységvizsgáló / pentest szolgáltató (különösen technikai tesztekhez)
- Kiberbiztonsági auditor (SZTFH, vagy NKI)

FORRÁSOK AZONOSÍTÁSA

a) Napló fájlok
   A rendszer vagy hálózat működéséről készített log fájlok segíthetnek azonosítani a biztonsági problémákat, például a sikertelen bejelentkezéseket vagy a támadásokat. A naplófájlok kezelésének, mentésének és elemzésének részletszabályait az IBSZ Naplózás és elszámoltathatóság fejezete tartalmazza.
b) Sérülékenységi vizsgálatok

A vizsgálat célja az, hogy teszteljék a rendszer vagy hálózat biztonságát, és felismerjék a biztonsági problémákat. Külső- és belső sérülékenységi vizsgálatokkal mérhető fel a rendszerek jelenlegi biztonsági állapota és javítások eszközölhetők a biztonság fokozása érdekében.

c) Biztonsági értesítések
A biztonsági értesítések és figyelmeztetések számos forrásból érkezhetnek, például a szoftvergyártóktól, biztonsági szakemberektől, vagy IT biztonsági közösségi fórumokról. Heti szinten több alkalommal (naponta) figyelni kell ezen riasztásokat. https://nki.gov.hu/figyelmeztetesek/riasztas/

d) Felhasználói tevékenységek
A felhasználói tevékenységek elemzése segíthet azonosítani a biztonsági problémákat, például a rosszindulatú felhasználókat vagy a belső fenyegetéseket.

ADATGYŰJTÉS, ADATELEMZÉS

Az adatok gyűjtését a Hivatal számos eszközzel végzi:

a) Hálózati monitorozó eszköz (Zabbix)
A Hivatal által használt hálózati monitorozó eszköz lehetővé teszi a hálózatforgalom elemzését, az adatok áramlásának figyelését, a hálózati kapcsolatok nyomon követését. Ezen felül azonnali riasztást küld, ha az adott hálózati eszköz „eltűnik" (pl: meghibásodás, áramszünet stb. miatt) a rendszerből.

b) Pentest és vulnerability scanner (Heimdal Security)
A sérülékenységi vizsgálatot végző eszközök segítségével a Rendszergazda különböző teszteket végezhet az adott rendszerek biztonsági réseinek felismerésére és a sebezhetőségek kihasználására. A sérülékenységfelmérő eszközök elősegítik az esetleges sebezhetőségek, illetve a támadók által kihasználható rések azonosítását.

BIZTONSÁGI PROBLÉMÁK AZONOSÍTÁSA

Az információbiztonsági problémák azonosítása kulcsfontosságú a biztonság fenntartása érdekében. Az alábbiakban lépések segítenek az információbiztonsági problémák azonosításában:

a) Kockázatértékelés
A kockázatelemzés során ki kell értékelni a különböző biztonsági kockázatokat, például a hálózati támadásokat, a malware fertőzéseket, a fizikai lopásokat stb. Ezen elemzés és értékelés az IBSZ 15. Kockázatkezelés fejezetében foglaltak szerint történik.

b) Sebezhetőségek azonosítása
Az információbiztonsági sebezhetőségek azonosítók a rendszerek és szoftverek rendszeres ellenőrzése, a sérülékenységfelmérések, a sérülékenységi vizsgálatok és a vulnerability scanner eszközök használatával.

c) Jogosulatlan hozzáférések ellenőrzése
Rendszeresen kell ellenőrizni és kontroll alatt tartani a hozzáféréseket, ez segít megakadályozni a jogosulatlan adathozzáféréseket és az illetéktelen tevékenységeket.

d) Rendszeres ellenőrzések
Az előírások szerint rendszeresen ellenőrizni szükséges az EIR-t és szoftvereket, hogy azonosítani lehessen a lehetséges problémákat és hibákat. Az ellenőrzések magukban kell foglalják a biztonsági naplók ellenőrzését, a rendszerek konfigurációinak ellenőrzését és a biztonsági mentések ellenőrzését.

e) Tanulás a múltbéli incidensekből
A múltbeli biztonsági incidensek felhasználhatók a jövőbeli biztonsági problémák elkerüléséhez. Meg kell vizsgálni a korábbi biztonsági incidenseket, hogy azonosítani lehessen azok okait, és megfelelő intézkedéseket lehessen alkalmazni a hasonló események megelőzésére.

TELJESÍTMÉNYMUTATÓK

Az információbiztonsági teljesítménymutatók segítségével mérhetők az információbiztonsági folyamatok hatékonysága.

a) Incidensek száma időszakonként (kategorizálás súlyosság szerint)
b) Hibák száma időszakonként (hibák átlagos javítási ideje)
c) Jogosultságok felülvizsgálatából fakadó mérőszámok
d) Biztonsági ellenőrzések rendszeressége és eredményei
e) Frissítések időzítése és végrehajtása

Az értékelés alapján összefoglaló jelentést kell készíteni az értékelés eredményéről. A jelentés készítése a megadott paraméterek alapján a Rendszergazda feladata. A jelentést kapja az IT vezető és az IBF.

5.4. BIZTONSÁGI ÉRTÉKELÉSEK – KIBERBIZTONSÁGI AUDIT

Legalább kétévente kiberbiztonsági auditot kell végrehajtani az EIR-ek biztonsági intézkedéseinek értékelésére. Az auditot külső személy vagy független szervezet végezhet.

5.7. INFORMÁCIÓCSERE (A5.14)

Az IT vezető jóváhagyja és szabályozza az információcserét az EIR és más külső rendszerek között. A Hivatalnak kapcsolódási pontokra vonatkozó biztonsági megállapodásokat kell kötnie a külső partnerekkel és szolgáltatókkal.

Amikor Szervezet új információcsere-megállapodást köt egy külső rendszerrel kapcsolatban, akkor dokumentálni kell az egyes rendszerek interfészeinek jellemzőit. A felek rögzítik a biztonsági követelményeket, védelmi intézkedéseket és felelősségi köröket is. Emellett fel kell jegyezni a megosztott információk hatásának szintjét, figyelembe véve a szolgáltatási szintre (SLA), a felhasználókra, a titoktartásra és a Hivatal által meghatározott egyéb megállapodásokra vonatkozó előírásokat is.

Ezen megállapodásokat éves szinten felül kell vizsgálni, illetve változás esetén frissíteni.

5.10. AZ INTÉZKEDÉSI TERV ÉS MÉRFÖLDKÖVEI

Az EIR gyengeségeinek vagy hiányosságainak kijavítására a Hivatalnak Intézkedési tervet kell kidolgoznia. Ezen tervben meg kell határozni az intézkedések céljait, a célok eléréséhez szükséges mérföldköveket.

Az intézkedési tervet a szükséges intézkedések végrehajtásáért felelős személyek és a vonatkozó határidők megjelölésével kell elkészíteni vonatkozó eljárási szabályok, felelősök, határidők megjelölésével, figyelembe véve a védelmi intézkedések értékeléseit, a független auditokat és felülvizsgálatokat, valamint a folyamatos felügyeleti tevékenységek eredményeit.

Az Intézkedési tervben rögzíteni kell az alábbiakat:

a) a megvalósítandó intézkedéseket;
b) amennyiben a feladat jellege egy éven túl mutat, akkor részfeladatokat (mérföldköveket), illetve részhatáridőket kell meghatározni, abban az esetben, ahol ez értelmezhető;
c) a feladatok végrehajtásának becsült munkaidő ráfordítását (és az esetleges költségeket);
d) a feladatok mellé rendelt felelőst;
e) a feladatok végrehajtásának határidejét.

A tervet az IBF javaslatainak figyelembevételével az IT vezető irányításával és a Rendszergazda közreműködésével kell kidolgozni, melyet a Hivatal vezetője hagy jóvá.

Az intézkedési terv elkészítéséért, végrehajtásáért, felülvizsgálatáért és a megtett intézkedésekről a Hivatal vezetőjének történő beszámolásért az IBF a felelős.

A hiányosságokat a kockázat mértéke szerint kell rangsorolni. A magas kockázatú elemeket (pl. vírusvédelem hiánya) soron kívül, a dokumentációs jellegű hibákat hosszabb határidővel kell kezelni.

5.12. ENGEDÉLYEZÉS

A Jegyző feladata kijelölni az EIR Adatgazdáit.

Abban az esetben, ha a Hivatal új EIR-t integrál más rendszerekkel, az Adatgazdának és az IBF-nek meg kell vizsgálnia, hogy továbbra is fennállnak-e, illetve értelmezhetőek a Hivatal által előírt biztonsági követelmények (pl. jelszókövetelmények, legkisebb jogosultság elve, naplózási követelmények). Amennyiben a követelmények fennállnak, úgy az Adatgazda elfogadja és engedélyezi a rendszer működését.

Emellett rendszeresen egyeztetnie kell a különböző rendszerek üzemeltetőivel, valamint részt kell vennie a biztonsági kérdésekkel kapcsolatos döntéshozatali folyamatokban a Hivatal belső irányelvei és szabályzatai alapján.

5.15. FOLYAMATOS FELÜGYELET (A8.6)

A folyamatos felügyeleti stratégia célja az EIR, hálózatok és adatok biztonságának fenntartása, az esetleges kockázatok korai észlelése és kezelése. A rendszer teljesítményének, hatékonyságának követésében a következő metrikák segítenek:

a) Elérhetőség (Availability): A rendszer vagy alkalmazás mennyi időn keresztül volt elérhető a tervezett működési időszakban. Az elérhetőségi metrikák segítenek azonosítani a hálózati hibákat.
b) Teljesítmény (Performance): Átlagos válaszidő, illetve átviteli sebesség.
c) Skálázhatóság (Scalability): A rendszer képessége, hogy rugalmasan növelje a terhelését, és hatékonyan kezelje a megnövekedett terhelést.
d) Rendszerkihasználtság (System Utilization): CPU- és memória kihasználtsága.
e) Biztonság (Security): A rendszerre irányuló támadási kísérletek vagy sikeres támadások száma, illetve a rendszerben talált hibák és sebezhetőségek száma.
f) Jogosultság-kezelés (Access Control): Sikeres és sikertelen bejelentkezések száma.
g) Teljesítményproblémák (Troubleshooting): A rendszerből származó hibaüzenetek és naplóbejegyzések elemzése a hibák és problémák azonosításához.

Az elemzések alapján válaszintézkedésekre lehet szükség, melyet az IT vezető jóváhagyásával a Rendszergazdának kell foganatosítania. A rendszer biztonsági állapotáról rendszeresen jelentést kell kapnia az IT vezetőnek és az IBF-nek.

5.16. FOLYAMATOS FELÜGYELET – FÜGGETLEN ÉRTÉKELÉS

A Hivatal külső, független értékelőket (auditorok) alkalmaz az EIR-ek biztonsági állapotának ellenőrzésére.

Ez magában foglalja a biztonsági protokollok, eljárások és infrastruktúra átfogó értékelését, annak érdekében, hogy azok megfeleljenek a jelenlegi biztonsági fenyegetésekkel és kihívásokkal szembeni elvárásoknak.

Az értékelők vagy értékelőcsoportok feladatai közé tartozik:

- A védelmi intézkedések hatékonyságának értékelése, beleértve a fizikai és logikai biztonsági mechanizmusokat.
- A biztonsági politikák, eljárások és gyakorlatok aktualitásának és relevanciájának felülvizsgálata.

- A biztonsági incidensek kezelésére és válaszadásra vonatkozó eljárások hatékonyságának értékelése.
- A rendszer sebezhetőségeinek és a potenciális biztonsági réseknek az azonosítása.
- Javaslatok megfogalmazása a biztonsági intézkedések javítására és a felmerült kockázatok kezelésére.

A Hivatal biztosítja, hogy az értékelések eredményei alapján megtegye a szükséges lépéseket a rendszer biztonságának folyamatos javítása és a biztonsági kockázatok csökkentése érdekében.

Az értékelők függetlenségét a teljes folyamat során biztosítani kell.

5.18. FOLYAMATOS FELÜGYELET – KOCKÁZATMONITOROZÁS

A folyamatos felügyeleti stratégiának része kell legyen:

a) a hatékonyság ellenőrzése;
b) a megfelelés ellenőrzése;
c) a változások nyomon követése;

5.25. BELSŐ RENDSZERKAPCSOLATOK

Az EIR összekapcsolása csak akkor lehetséges a belső rendszerek esetében, ha annak kockázatait a rendszer Rendszergazdája, a Hivatal mindenkori Szervezeti és Működési Szabályzatában meghatározott - legfelsőbb vezetője, illetve az IBF mérlegeli, majd az IT vezető jóváhagyja.

Jóváhagyás esetén dokumentálni kell az interfész jellemzőit, követelményeit.

A kapcsolatot meg kell szüntetni, ha használat okafogyottá válik. A kapcsolat megszüntetését az IT vezető hagyja jóvá.

A Rendszergazda feladata, hogy évente, vagy nagyobb változtatásokkor felülvizsgálja a kapcsolat további szükségességét.

6. KONFIGURÁCIÓKEZELÉS (A8.9)

6.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

A konfigurációkezelés célja, hogy az EIR elvárt biztonsági osztályának megfelelően biztosítsa azok megbízható működését a rendszerösszetevők telepítésének, konfigurálásának, megváltoztatásának, tesztelésének és nyilvántartásának szabályozott körülmények közötti végrehajtásával. Segíti a változások nyomon követését és dokumentálását, ideértve az új bevezetéseket, módosításokat és törléseket is. Emellett segít az azonosított hibák kezelésében és a rendszerek visszaállításában a hibás konfigurációból a stabil állapotba.

Felelős: IT vezető

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

6.2. ALAPKONFIGURÁCIÓ

Az EIR-hez rendszerenként dokumentált formában el kell készíteni egy-egy Alapkonfigurációt és ezt biztonságos helyen kell tárolni.

Az Alapkonfiguráció dokumentációjának célja, hogy új rendszerelemek esetén rögzítse, hogyan kell az elemet telepíteni és konfigurálni, illetve meghibásodás esetén a rendszerelemeket hogyan kell újra telepíteni.

A dokumentáció az egyes eszköztípusokra (pl.: szerver, munkaállomás, tűzfal, router stb.) vonatkozóan meghatározza az adott feladat ellátásához szükséges hardver és szoftver környezetet.

Az Alapkonfigurációnak minimálisan a következőket kell magában foglalnia:

a) a feladat ellátásához szükséges minimális és ajánlott hardver elemek listáját;
b) a szükséges szoftverek listáját;
c) a szoftverek konfigurációs beállításait, paramétereit;
d) ha a rendszer biztonsági osztálya előírja, a dokumentációnak tartalmaznia kell az engedélyezett szolgáltatások, portok és protokollok listáját a „szükséges minimum" elv alapján

A dokumentáció részeként egy logikai és fizikai hálózati topológia rajzot is készíteni kell, amelyen követhető a rendszerelemek elhelyezkedése a rendszer architektúrájában.

Felelős: Az EIR Alapkonfigurációját a Szerverüzemeltető készíti el, 6 havonta felülvizsgálja, és a módosításokat átvezeti. A dokumentációt az IT vezető felügyeli.

6.7. A KONFIGURÁCIÓVÁLTOZÁSOK FELÜGYELETE (VÁLTOZÁSKEZELÉS) (A8.19, A8.32)

A Hivatal a következő eljárást követi a változáskezelési folyamat során:

- Azonosítja és rögzíti azokat a rendszerváltozásokat, amelyek a változáskezelési felügyelet szabályozási keretébe tartoznak.
- Elemzi, és biztonsági szempontok figyelembevételével elfogadja vagy elveti a rendszerkonfiguráció jelentős módosításaira irányuló javaslatokat.
- Végrehajtja az elfogadott módosításokat az EIR-en belül.
- Folyamatosan nyilvántartja, és hozzáférhető módon őrzi az EIR-en végrehajtott változtatásokkal kapcsolatos dokumentációt.
- Felülvizsgálja és ellenőrzi azokat a tevékenységeket, amelyek a változások bevezetésével összefüggésben állnak.

A Rendszerüzemeltető koordinálja és felügyeli a konfigurációs változtatásokat, - amelyeket adott gyakorisággal, vagy amikor a változások bevezetésének feltételei fennállnak, - alkalmaznak.

Változáskezelés hatálya alá tartozó tevékenységek:

- jelentős változással járó verzióváltások, új fejlesztések;
- rendszerelemek cseréje (hardver/szoftver);
- a rendszer működésének jelentős módosítása, jelentős beavatkozást igénylő hangolások.

A változáskezeléssel kapcsolatosan az alábbi előírásokat kell figyelembe venni:

a) A rendszer bármely funkciójának jelentős megváltoztatásához az IT vezető és adatgazdai terület vezetőjének engedélye szükséges.
b) A változtatást az kezdeményezi, akinél az igényként felmerül.
c) A változtatásokra vonatkozó igénybejelentést, véleményezést, döntést, a változtatás kivitelezését dokumentálni kell.
d) A tervezett jelentős változtatást véleményezés céljából az IBF-nek is meg kell küldeni, aki kockázatelemzéssel megállapítja a változtatás rendszerre gyakorolt hatását.
e) A fejlesztők az éles rendszerben csak az IT vezető felügyelete mellett végezhetnek változtatást.
f) A fejlesztők nem rendelkezhetnek hozzáférési jogokkal az éles informatikai rendszerhez, ezért közvetlenül változtatást sem végezhetnek a rendszeren. A változtatást a rendszer üzemeltetőjének kell elvégezni.
g) A változtatást az éles üzembe való állítás előtt az erre a célra létrehozott tesztkörnyezetben tesztelni kell.
h) Az éles üzembe állítást csak a változással érintett rendszerek, adatok teljes mentését követően lehet elvégezni.
i) A változtatást munkaidőn kívül kell elvégezni, csak rendkívüli esetben végezhető munkaidőben.
j) Amennyiben a változtatáshoz a rendszer leállítása szükséges, akkor arról a Rendszergazda legalább 1 munkanappal korábban köteles tájékoztatni a felhasználókat.

6.15. BIZTONSÁGI HATÁSVIZSGÁLATOK

A változtatás megkezdése előtt az IBF-nek az előzetes kockázatelemzéssel és a biztonsági funkciók tesztelésével kell biztosítania a változtatás éles környezetre ható biztonsági kockázatainak minimalizálását.

6.18. A VÁLTOZTATÁSOKRA VONATKOZÓ HOZZÁFÉRÉS KORLÁTOZÁSOK

A változtatásokat csak a Rendszergazda munkatársai, vagy az aktuális és szükséges jogosultságokkal rendelkező külsős személyek végezhetik el az IT vezető jóváhagyásával. Minden változtatást automatikusan naplózni kell.

6.23. KONFIGURÁCIÓS BEÁLLÍTÁSOK

Az EIR működtetése során csak az Alapkonfigurációjában szereplő, jóváhagyott hardver és szoftver elemek, konfigurációs beállítások használhatók. Ettől eltérni nem lehet.

A kötelező konfigurációs beállítások érvényesítését az IBF az éves ellenőrzési tervében foglaltak szerint az 6.2 Alapkonfiguráció pont alapján ellenőrzi.

6.26. LEGSZŰKEBB FUNKCIONALITÁS

Az EIR-t a „szükséges minimum" elv alapján úgy kell konfigurálni, hogy csak azok a szolgáltatások, portok, protokollok legyenek engedélyezve, amelyek az ügy- és üzletmenet szempontjából létfontosságú szolgáltatások nyújtásához szükségesek.

Az engedélyezett szolgáltatások, portok és protokollok listáját a rendszer Alapkonfigurációjában kell rögzíteni.

Az engedélyezett szolgáltatások, portok és protokollok kizárólagos használatát az IBF az éves ellenőrzési tervében foglaltak szerint ellenőrzi.

6.36. RENDSZERELEM LELTÁR (A5.9)

A Hivatalnak leltárt kell vezetnie az EIR valamennyi hardver/szoftver eleméről és gondoskodnia kell a leltár teljességéről és naprakészségéről.

A leltárnak tartalmaznia kell:

- a rendszerben használt hardver és szoftverek elemek listáját, az azonosításukhoz szükséges adatokat és a hardver/szoftver elemek összerendelését;
- az egyes elemek használóját, felelősét;
- a szoftver elemekhez rendelt szoftverlicenceket.

A leltár gyakorlati megvalósítása a következő módon történik:

A munkaállomások és szerverek (mind fizikai, mind virtuális környezetben) leltározása a Hivatalnál alkalmazott Heimdal Security rendszer segítségével történik. Ennek érdekében minden érintett eszközön telepítésre kerül a Heimdal Security kliens, amely egy központi adatbázisban naprakészen gyűjti és tárolja a leltározott eszközök részletes hardverjellemzőit, valamint a telepített szoftverek adatait.

A szervereket, munkaállomásokat, hálózati eszközöket, a meghatározott nagyobb értékű számítógép tartozékokat (pl.: monitor, nyomtató, szkenner, szünetmentes tápegység, szalagos egység stb.) a Hardver nyilvántartásban kell nyilvántartani. Az egységes kezelés érdekében a virtuális szervereket is tartalmaznia kell a nyilvántartásnak. A kis értékű számítógép tartozékokat (pl.: billentyűzet, egér, hangszóró stb.) és a kábeleket nem kell nyilvántartani, ezeket a Hivatal anyagként kezelni.

A vásárolt, bérelt vagy fejlesztett szoftverek (továbbiakban: licencköteles szoftverek) licenceit a Szoftver nyilvántartásban kell vezetni. A szabad felhasználású szoftverek esetében külön nyilvántartás vezetése nem kötelező, azonban azok telepített példányait a Heimdal Security rendszer által végzett automatikus leltár tartalmazza.

Az EIR Alapkonfigurációjának részeként hálózati topológia rajzot kell készíteni, amelyeken követhető a Rendszerelem leltárban szereplő rendszerelemek elhelyezkedése a rendszer architektúrájában.

Változások (pl.: új informatikai eszközök/szoftverek üzembe helyezése vagy selejtezése; informatikai eszközök áthelyezése; szoftverek telepítése/eltávolítása; stb.) esetén folyamatosan karban kell tartani a nyilvántartásokat. A változások átvezetése a Rendszergazda azon munkatársának felelőssége, aki a változással kapcsolatos műveletet végrehajtotta.

A Rendszerelem leltárt, valamint a Hardver- és Szoftver nyilvántartások adott rendszerhez kapcsolódó rendszerelemeit a rendszergazdának hathavonta felül kell vizsgálnia, a feltárt eltéréseket javítania kell.

Hardver nyilvántartás

A Hardver nyilvántartásnak az alábbi adatokat kell az informatikai eszközökre vonatkozóan minimálisan tartalmaznia:

- az eszköz csoportját (pl.: fizikai szerver, virtuális szerver, asztali számítógép, laptop, switch, router, monitor, nyomtató, szünetmentes tápegység stb.);
- az eszköz informatikai azonosítóját;

- az eszköz rövid megnevezését (szerverek esetén a szerver funkciójának rövid leírását; munkaállomások esetén a Felhasználó nevét);
- az eszköz gyártóját és típusát;
- a fő jellemzőket (számítógépek esetén a processzor típusát, a memória és háttértár méretét, hálózati eszközök esetén a portok számát stb.);
- számítógépek estén az operációs rendszer típusát;
- az eszközért felelős személy nevét (ez munkaállomások esetén a felhasználó, szerver oldali eszközök esetén a Rendszergazda nevét);

A nyilvántartáshoz kapcsolódóan – az informatikai eszközök üzemeltetésének támogatására – a Rendszergazdának visszakereshető formában meg kell őriznie az eszköz számlájának szkennelt másolatát, a garancia jegyet, telepítő adathordozót és az egyéb gyártói dokumentációt (pl.: kezelési és karbantartási útmutató, műszaki leírás stb.). A megőrzési idő az eszközök selejtezéséig tart.

Szoftver nyilvántartás

A Szoftver nyilvántartásban az alábbi adatokat kell minimálisan vezetni:

- a szoftver nevét és verziószámát;
- a szoftver funkciójának rövid megnevezését;
- a beszerzett licencek darabszámát;

A nyilvántartáshoz kapcsolódóan – a szoftverlicencek igazolása céljából – a Rendszergazdanak visszakereshető formában meg kell őriznie a szoftverek számlájának szkennelt másolatát és a szoftverlicencet igazoló egyéb dokumentumokat (pl.: licencszerződés, licencengedély, licence kulcs stb.).

6.47. A SZOFTVERHASZNÁLAT KORLÁTOZÁSAI (A5.10, A5.32, A8.18)

A Hivatal minden Felhasználó számára biztosítja a munkavégzéshez szükséges szoftvereket, ezért a Hivatal számítógépein csak legális, a Hivatal által rendelkezésre bocsátott szoftverek használhatók a licencszerződésben foglaltak szerint.

Ebből következően tilos telepíteni a Felhasználó vagy külső partnerek tulajdonában lévő szoftvereket, valamint tilos a szoftvereket a licenc által megengedett darabszámot meghaladó számban használni!

Az előfizetéses licenccel rendelkező szoftverekről (pl. Windows, Office, ESET Antivirus) nyilvántartást kell vezetni. Ezen szoftverek használatát szúrópróba-szerűen ellenőrizni kell. A nyilvántartást évente felül kell vizsgálni. A központi adminisztrációs felülettel rendelkező rendszereknél a felhasználók listáját ill. a felhasználás mennyiségét évente felül kell vizsgálni.

Az egyéb telepítési licenctköteles szoftverekről (pl. Total Commander, PicPic, XNView stb.) nyilvántartást kell vezetni, amelyet telepítés vagy eltávolítás esetén aktualizálni kell.

A Hivatal számos külső partnertől vásárolja meg a szoftverek licencengedélyét. A Hivatal a licencszerződéssel nem válik a szoftverek tulajdonosává, azok telepítő adathordozóit és dokumentációját a szoftver fejlesztőjének külön engedélye nélkül nem áll jogában másolni.

Az IT vezető felelőssége, hogy csak a Hivatal által vásárolt/bérelt, illetve a Hivatal számára belső vagy külső fejlesztéssel készült jogtiszta szoftverek, valamint az engedélyezési eljáráson átesett szabad szoftverek kerüljenek üzembe helyezésre.

A legális szoftverhasználat biztosítása és az EIR biztonsága érdekében az alábbi előírásokat kell betartani:

- Licencköteles szoftvereket csak a Rendszergazda munkatársai, illetve az IT vezető által ezzel megbízott külső partnerek alkalmazottai telepíthetnek.
- A licencköteles szoftverek telepítő adathordozóit és licenckulcsait a másolatok ellenőrzése érdekében a rendszergazdának elzárva kell tárolnia és ellenőriznie kell a hozzáféréseket.
- A rendszergazdának ellenőrzés alatt kell tartania a hálózati megosztások jogosultság beállítását és tartalmát, és gondoskodnia kell arról, hogy a megosztások ne tegyék lehetővé a szerzői jogokkal védett szoftverek illegális használatát, illetve a szoftverek telepítőkészletének vagy licenckulcsának illetéktelen másolását, terjesztését.
- Szoftver telepítőkészleteket kizárólag a Rendszergazda helyezhet el hálózaton megosztott mappákban az általa végzett szoftvertelepítések végrehajtása céljából. A licencköteles szoftverek telepítőkészletéhez csak a Rendszergazda munkatársai rendelkezhetnek hozzáférési jogosultsággal, az engedélyezett szabad szoftverek telepítőkészletéhez a felhasználók is hozzáférhetnek az automatizált telepítési folyamatok működése érdekében.
- Kiemelt jogosultságú segédprogramok használata csak az IT vezető jóváhagyásával és kizárólag a Rendszergazda számára engedélyezett. Ezen programok használata közben nagy körültekintéssel kell eljárniuk
- A szoftvereket kizárólag a licencszerződés előírásainak megfelelően lehet használni. A hálózati megosztásra, vagy több felhasználó által használt szerverekre (terminál szerverekre) történő szoftvertelepítést megelőzően ellenőrizni kell, hogy a licencszerződés milyen feltételekkel teszi lehetővé az ilyen használatot.
- Amennyiben a Hivatal munkatársainak tudomására jut, hogy szoftvereket illegálisan, érvényes licencengedély nélkül vagy nem a licencszerződésnek megfelelően használnak, akkor ezt kötelesek a munkahelyi vezetőjüknek és az IBF-nek jelenteni.
- A Hivatal elítéli az illegális szoftverhasználatot, szándékos károkozásnak tekinti az illegális szoftverek telepítését, és az előírás megsértőivel szemben fegyelmi felelősségre vonásra kerülhet sor.
- Azon munkatársak, akik illegális szoftvermásolatot készítenek, szereznek be, telepítenek vagy használnak, a szerzői jogi törvény (továbbiakban: Szjt.) szerint szankcionálhatók és kártérítésre kötelezhetők. Ezért a Hivatal semmilyen felelősséget nem vállal.

6.49. FELHASZNÁLÓ ÁLTAL TELEPÍTETT SZOFTVER (A5.10)

A felhasználók nem telepíthetnek, vagy távolíthatnak el szoftvereket – kivéve amennyiben kialakításra került a felhasználók számára az általuk önállóan telepíthető termékpaletta.

A korlátozást az operációs rendszer segítségével kell kikényszeríteni, azaz a felhasználók csak korlátozott felhasználói fiókot használnak, amelynek nincs jogosultsága a telepítésre.

A szabályok betartását az IBF az éves ellenőrzési tervében foglaltak szerint, személyes megtekintéssel ellenőrzi.

Telepítés nélkül futtatható szoftverek

A telepítés korlátozása a telepítés nélkül futtatható (ún. portable) szoftverek segítségével megkerülhető.

Léteznek olyan telepítés nélkül használható szoftverek, melyeket szerzői jogok védelme alatt álló szoftverek feltörésével, illegális módon hoztak létre. Az ilyen szerzői jogot sértő szoftverek birtoklása és használata illegális szoftverhasználatnak minősül.

A telepítés nélkül futtatható szoftverek nehezen felügyelhetők, használatuk biztonsági és licenc problémákat vet fel, ezért általános esetben a Hivatal számítógépein a telepítés nélkül futtatható szoftverek elindítása vagy a számítógépen történő tárolása tilos!

A telepítés nélkül futtatható szoftverek használatát a Rendszergazda indokolt esetben engedélyezheti. Az ilyen szoftverek engedélyezése során ugyanúgy kell eljárni, mintha a szoftver telepítésre kerülne az adott számítógépre (a licenckötelés szoftverekhez érvényes licenccel kell rendelkezni, a szabad szoftvereknek át kellett esniük az engedélyezési eljáráson).

Automatizáltan települő szoftverek

Az engedélyezett szabad szoftverek és az összes munkaállomáshoz licenccel rendelkező szoftverek telepítése vagy a szoftverek verziófrissítése céljából a Rendszergazda alkalmazhat automatizált telepítési módszereket, amelyek pl. a hálózati bejelentkezés folyamán, egy szoftver indításának részeként, vagy a Felhasználó opcionális döntése alapján indulnak el.

Ezeket az automatizált telepítéseket a Rendszergazda által végzett telepítésnek kell tekinteni, akkor is, ha egy felhasználói művelet hatására aktivizálódnak.

Az automatizált telepítésekkel szembeni követelmény, hogy a telepítéseket naplózni kell és a rendszergazdának a naplók vizsgálatával felügyeletet kell gyakorolnia a telepítési folyamat felett.

7. KÉSZENLÉTI TERVEZÉS (A5.29, A5.30, A8.14)

7.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

A jelen eljárásrend célja az üzletmenet-folytonosság biztosítása és a Hivatal működésének fenntartása kritikus helyzetekben. Ennek érdekében különféle intézkedéseket és terveket foglal magában.

Készenléti terv létrehozása és fenntartása elsődleges fontosságú a Hivatal számára. Cél a kritikus üzleti funkciók gyors helyreállítása mellett, a személyzet folyamatos működésre való felkészítése, hogy azok képesek legyenek hatékonyan kezelni az esetleges kritikus helyzeteket.

Az EIR mentései és helyreállítása kritikus a Hivatal adatintegritásának megőrzése és a szolgáltatások folytonossága szempontjából. Ez magában foglalja a rendszeres mentéseket, azok megbízhatóságának és sértetlenségének tesztelését, valamint a rendszer helyreállítását és tranzakcióinak visszaállítását kritikus időkben.

A Hivatal az alábbi intézkedéseket hajtja végre az üzletmenet-folytonosság biztosítása érdekében:

- Előkészíti, írásba foglalja, közzéteszi, és ismerteti az érintett személyekkel - szerepkörüknek megfelelően - a Készenléti tervet,
- Meghatározza a szervezeti, folyamatbeli és rendszerszintű követelményeket,
- Meghatározza a célokat, hatáskört, szerepköröket, felelősségeket, a vezetőség elkötelezettségét, a Hivatalon belüli együttműködés kereteit, valamint a megfelelőségi kritériumokat,
- Kidolgozza az üzletmenet-folytonossági eljárásokat, és a hozzá kapcsolódó ellenőrzéseknek a végrehajtását.
- Rendszeresen felülvizsgálja és frissíti az üzletmenetfolytonossági eljárásokat a Hivatal által meghatározott időközönként, valamint a Hivatal által meghatározott események bekövetkezte után.
- Az EIR Készenléti tervét világosan megfogalmazza, dokumentálja, és kihirdeti a kulcsfontosságú személyek és szervezeti egységek számára, valamint tájékoztatja a kulcsfontosságú személyeket és szervezeti egységeket a Készenléti terv változásairól.
- Szinkronizálja a folyamatos működés tervezését a biztonsági incidensek kezelésével.
- Rendszeres időközönként felülvizsgálja az EIR Készenléti tervét.
- Az EIR vagy működési környezet változásai, a terv megvalósításának, végrehajtásának vagy tesztelésének során felmerülő problémák alapján frissíti a Készenléti tervet.
- A Készenléti terv teszteléséből, gyakorlatából vagy tényleges alkalmazásából származó tapasztalatokat integrálja a tesztelési és gyakorlati folyamatokba.
- Megvédi a Készenléti tervet a jogosulatlan megismeréstől és módosítástól.
-

Felelős: IT vezető, Adatgazda, IBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, a Rendszergazdával, valamint a Vészhelyzeti szereplőkkel (1.7.3.) minden esetben ismertetni kell.

7.2. ÜZLETMENET-FOLYTONOSSÁGI TERV

A Hivatal az alábbi intézkedésekkel biztosítja az EIR üzletmenet-folytonosságát.

Kialakítja az EIR üzletmenet-folytonossági tervét, amely:

- Meghatározza az alapszolgáltatásokat és -funkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket.
- Meghatározza a helyreállítási célokat, prioritásokat és metrikákat.
- Kijelöli a vészhelyzeti szerepköröket, felelősségeket, kapcsolattartókat és elérhetőségeiket.
- Meghatározza az EIR zavarai esetén is fenntartandó szolgáltatásokat.
- Tartalmazza az EIR teljes körű helyreállításának részletes tervét, amely biztosítja a védelmi intézkedések integritását a helyreállítás után.
- Összhangban áll a Hivatalt érintő érvényes jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.
- Tartalmazza az üzletmenet-folytonossági információk megosztásának szabályait.
- Magába foglalja a Hivatal meghatározott személyei vagy szerepkörei által történő felülvizsgálatot és jóváhagyást.

7.10. A FOLYAMATOS MŰKÖDÉSRE FELKÉSZÍTŐ KÉPZÉS

A Hivatal az EIR folyamatos működésére felkészítő képzést tart a felhasználóknak, illetve az érintett szerepkörüknek és felelősségüknek megfelelően.

Az üzletmenet-folytonosság megfelelő szinten tartása, valamint a nem várt események esetén alkalmazandó Készenléti terv megfelelő hatékonysággal történő végrehajtása érdekében a tervek végrehajtásában érintett szereplők részére a szerepkörbe kerülésüket vagy a tervek változását követően felkészítő és évente ismétlő képzéseket kell tartani.

A képzéseken a következő területeket kell legalább érinteni:

- az EIR-re ható főbb fenyegetéseket;
- a fenyegetések minimalizálása érdekében megtett kockázatkezelő intézkedéseket;
- a konfigurációkezelési és változáskezelési eljárások megfelelő használatát;
- a mentési eljárásokat;
- a katasztrófa esetén szükséges lépéseket.

A képzés tartalmának összeállítása és a képzés lebonyolítása az IBF feladata.

A képzéseket a Hivatal évente szervezi, vagy amikor az EIR változásai ezt szükségessé teszik.

Nagyobb változások esetén, vagy ha az IBF úgy látja, akkor felül kell vizsgálnia és frissíteni kell a képzés anyagát.

7.35. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER MENTÉSEI (A8.13)

A biztonsági mentés módszerei, gyakorisága, illetve a helyreállítás lehetőségei a Mentési Rend dokumentumban kaptak helyet.

7.43. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER HELYREÁLLÍTÁSA ÉS ÚJRAINDÍTÁSA

A biztonsági mentésből történő helyreállítás lehetőségei a Mentési Rend dokumentumban kaptak helyet. A rendszerek karbantartáskor, vagy vészhelyzet esetén történő leállításának sorrendjét az EIR nyilvántartásban szereplő prioritások szerinti ütemezés szerint kell megvalósítani. Az újraindítás ugyanezen analógiára történik – de a sorrend megfordul.

8. AZONOSÍTÁS ÉS HITELESÍTÉS (A5.17)

8.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend célja a biztonságos és megbízható azonosítás és hitelesítés biztosítása a Hivatal tevékenységeihez. Feladatai közé tartozik a szabályok, irányelvek és eljárások kidolgozása, dokumentálása és megismertetése a Hivatalon belül.

Emellett a rendszeres felülvizsgálatok és frissítések biztosítják a megfelelőséget és a hatékonyságot az azonosítási és hitelesítési folyamatokban.

Felelős: IT vezető

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

8.2. AZONOSÍTÁS ÉS HITELESÍTÉS (A8.5)

Az EIR-ben egyedileg kell azonosítani és hitelesíteni a Hivatal valamennyi belső felhasználóját, ami lehetővé teszi, hogy egyénileg nyomon lehessen követni a felhasználók által végzett tevékenységeket.

Ennek érdekében a Hivatalnál alkalmazott névkonvenció alapján a felhasználóknak egyedi, névre szóló felhasználói azonosítókat kell képezni. Ez fokozottan vonatkozik a kiemelt jogosultságokkal rendelkező, rendszergazda felhasználók fiókjaira.

8.3. AZONOSÍTÁS ÉS HITELESÍTÉS (FELHASZNÁLÓK) – PRIVILEGIZÁLT FIÓKOK TÖBBTÉNYEZŐS HITELESÍTÉSE (A8.2)

A kiemelt jogosultságokkal rendelkező, ún. privilegizált felhasználók (rendszergazdák) hálózati bejelentkezésére többtényezős hitelesítést kell alkalmazni.

A többtényezős hitelesítés két különböző módszerrel kell, hogy történjen. A hagyományos jelszavas hitelesítés mellett a második tényező lehet pl. egy titkosító kulcs birtoklása (tárolhatja szoftver vagy hardver token); egy biometrikus azonosító (pl.: ujjlenyomat, írisz, érminta); vagy egy mobiltelefonra SMS-ben, vagy Push üzenetben küldött egyszer használatos jelszó.

8.7. AZONOSÍTÁS ÉS HITELESÍTÉS (FELHASZNÁLÓK) – HOZZÁFÉRÉS A FIÓKOKHOZ – VISSZAJÁTSZÁS ELLENI VÉDELEM

Olyan hitelesítési mechanizmusokat kell használni, amelyek biztosítják a visszajátszás elleni védelmet (pl: OTP kódok, időbélyegek, időzítők, jogosultság időkorlát)

8.14. AZONOSÍTÓ KEZELÉS

A felhasználói azonosítókat a Rendszergazda kezeli, kiosztásukat a munkahelyi vezetőnek kell engedélyeznie.

Az azonosítókat úgy kell létrehozni, hogy azok egyértelműen hozzárendelhetők legyenek a kívánt személyhez (vagy szoftverek/hardver eszközök által használt technikai felhasználói fiókok esetén a kívánt rendszerelemhez).

Az azonosítók ismételt felhasználása tilos. Azonos nevű felhasználók esetén a felhasználói azonosítókat sorszám kiegészítéssel kell megkülönböztetni, abban az esetben is, ha az egyik felhasználói fiók már inaktív.

Az EIR-ben, a 3 hónapnyi inaktivitás után a fiókokat felül kell vizsgálni. Ezekről a Rendszergazdának, a felhasználók munkahelyi vezetőjével egyeztetnie kell, szükség esetén a fiókot fel kell függeszteni.

Az inaktivitás következtében vagy más okból letiltott felhasználói fiókokat csak a munkahelyi vezetőtől a Rendszergazdának e-mailben írt kérelem alapján lehet feloldani a hozzáférési jogosultságok igénylésének folyamata szerint.

8.21. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE

Az illetéktelen hozzáférés megakadályozása érdekében a Felhasználó, vagy Eszköz identitását ellenőrizni kell.

A Rendszergazda első alkalommal egy a jelszókomplexitás követelményeinek megfelelő, véletlenszerű jelszót generál kezdeti jelszónak.

A jelszó minél komplexebb, annál kisebb a valószínűsége, hogy a Felhasználó nevében visszaélést követnek el. Ennek érdekében az alábbi szabályokat kell a jelszó kiválasztásakor betartani:

a) a jelszó legyen legalább 8 karakter hosszú és tartalmazzon kisbetűt, nagybetűt, számot és speciális karaktert is;
b) legyen könnyen megjegyezhető és nehezen kitalálható;
c) ne legyen a felhasználói névre vagy a Hivatal nevére utaló;
d) semmi olyasmi felhasználóhoz kötődő adaton ne alapuljon, amely alapján valaki kitalálhatja (ilyenek a nevek, telefonszámok, születési dátumok, lakcímek stb.);
e) ne tartalmazzon azonos, vagy ismert logika szerint egymást követő karaktereket (pl.: 123456, qwerty, asdfgh stb.).

Lehetőséget kell teremteni a bonyolult jelszavak automatikus létrehozására (jelszógenerátor).

A kezdeti jelszó létrehozása után biztosítani kell, hogy a kezdeti jelszavak biztonságos körülmények között kerüljenek a felhasználóknak átadásra.

A felhasználónak a kezdeti jelszavukat az első belépés során meg kell változtatniuk.

Minden Felhasználó felelőssége, hogy a jelszavak használata során betartsa a következő jelszavak védelmére vonatkozó szabályokat.

A felhasználói azonosító létrehozásakor, fiókvisszaállítás esetén, vagy a jelszó elfelejtése miatt beállított jelszót az első bejelentkezéskor azonnal meg kell változtatni.

A jelszó kiválasztásakor be kell tartani a jelszavak képzésére vonatkozó szabályokat és a jelszavakat meghatározott időnként meg kell változtatni.

A Felhasználó a jelszavát köteles titokban tartani, a jelszót tilos leírni, tilos nyilvános helyen kiírva (pl. monitorra ragasztva) tartani vagy másnak továbbadni.

A jelszót a Rendszergazdának sem szabad elárulni. Ha a munkaállomás karbantartásához szükség van a Felhasználó jelszavára, a karbantartást végző munkatárs csak a jelszó Felhasználó általi beírását kérheti.

A Hivatal gondoskodik a felhasználói jelszavak legfeljebb 180 naponta történő cseréjéről.

Ha bármilyen jel mutat arra, hogy a jelszó illetéktelen kézbe jutott vagy feltételezhető a megismerése, azonnal meg kell változtatni a jelszót, és az esetet jelenteni kell a Biztonsági események kezelése pontban leírtak szerint;

A jelszó nem tehető egy automatikus bejelentkezési folyamat részévé (pl. makróra, vagy funkcióbillentyűre).

A Hivatalnál használt jelszavak Szervezeten kívüli rendszerekben nem használhatók.

A jelszószabályok betartása minden felhasználónak jól felfogott érdeke. A Felhasználó felelőssége, ha jelszavának, neki felróható mulasztása miatti megismerése révén valaki a nevében visszaélést követ el az EIR-ben.

Csoportos használatú fiók esetén amennyiben a tagok közül valaki eltávolításra kerül, a fiókjelszót azonnal módosítani kell!

8.22. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE – JELSZÓ ALAPÚ HITELESÍTÉS

A Rendszergazda feladata, hogy a gyakran használt, könnyen kitalálható, vagy kompromittált jelszavakról nyilvántartást vezessen.

A felhasználók által létrehozni, vagy módosítani kívánt jelszavakat ellenőrizni kell, hogy szerepelnek-e a gyakran használt, vagy kompromittált jelszavak listáján. Amennyiben igen, az adott jelszó nem használható.

A jelszavak továbbítása csak titkosított csatornán keresztül történhet, tárolásuk pedig jóváhagyott, sózott kulcsszármaztatási funkcióval, lehetőleg egykulcsos hash-t használva történhet.

8.36. HITELESÍTÉSI INFORMÁCIÓK VISSZAJELZÉSÉNEK ELREJTÉSE

A Hivatalnál csak olyan EIR használható, amely a hitelesítési folyamat során hibás azonosító vagy jelszó megadása esetén csak olyan hibaüzenetet ad vissza, amelyből nem szerezhető további információ sem az azonosítóra, sem a jelszóra vonatkozóan (pl.: nem derülhet ki az üzenetből, hogy a próbált azonosító érvényes, csak a jelszó hibás; vagy nem tartalmazhatja az üzenet a jelszó hosszára vagy bonyolultságára vonatkozó előírásokat).

8.37. HITELESÍTÉS KRIPTOGRÁFIAI MODUL ESETÉN

Amennyiben a hitelesítés egy kriptográfiai modul (titkosítást végző hardver eszköz) felhasználásával történik (ilyen lehet pl. a rendszergazdai fiókok többtényezős hitelesítése), a modul használata során be kell tartani a hitelesítés szolgáltató által rendelkezésre bocsájtott hitelesítési útmutatóban foglaltakat.

8.38. AZONOSÍTÁS ÉS HITELESÍTÉS (SZERVEZETEN KÍVÜLI FELHASZNÁLÓK)

A Hivatalon kívüli felhasználók (külső felhasználók) EIR-hez történő hozzáférése során egyénre szóló, de partnercégre utaló felhasználói azonosítókat kell létrehozni.

Ebben az esetben a felhasználói azonosító létrehozását a külső felhasználó munkáját elrendelő adatgazdai terület vezetője vagy a Kulcsfelhasználó kezdeményezheti.

A külső felhasználóknak kiosztott felhasználói azonosítókkal történő tevékenységeket minden esetben naplózni kell, és ezen tevékenységekre a Rendszergazdának kiemelt figyelmet kell fordítania.

Amennyiben a Hivatalon kívüli felhasználók hitelesítése nyilvános kulcsú titkosítási eljárással történik, a nyilvános kulcsot tartalmazó tanúsítványok csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványok lehetnek.

8.39. AZONOSÍTÁS ÉS HITELESÍTÉS (SZERVEZETEN KÍVÜLI FELHASZNÁLÓK) – MEGHATÁROZOTT AZONOSÍTÁSI PROFILOK HASZNÁLATA

Külső felhasználók esetén egyedi, számukra létrehozott profilokat kell alkalmazni.

8.43. ÚJRAHITELESÍTÉS

Kötelező a felhasználók újra hitelesítése a következő esetekben:

a) lejárt jelszó;
b) hosszabb idejű inaktivitás, vagy hálózati kapcsolat megszakadása;
c) új eszköz használata esetén.

9. BIZTONSÁGI ESEMÉNYEK KEZELÉSE (A5.24)

9.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend fő feladata az informatikai biztonsági események hatékony kezelése és reagálásuk szabályozása a Hivatalban. Célja az események gyors azonosítása, értékelése és megfelelő intézkedések meghozatala az esetleges biztonsági fenyegetések vagy incidensek kezelése érdekében.

Az eljárásrend tartalmazza az események nyomon követésére, dokumentálására és jelentésére vonatkozó irányelveket, valamint meghatározza az eseménykezelésért felelős személyek és csapatok szerepkörét és feladatait. Emellett a rendszeres felülvizsgálatok és frissítések biztosítják az eljárásrend hatékonyságát és megfelelőségét.

Felelős: IBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, a Rendszergazdával, valamint a Vészhelyzeti szereplőkkel (1.7.3.) minden esetben ismertetni kell.

9.2. KÉPZÉS A BIZTONSÁGI ESEMÉNYEK KEZELÉSÉRE

A felhasználókat képezni kell, hogy felismerjék a biztonsági fenyegetéseket, ismerjék fel a gyanús tevékenységeket, és tudjanak helyesen és azonnal reagálni a lehetséges incidensekre. Ezért a Hivatal éves szinten - vagy ha a körülmények megkívánják, akkor gyakrabban – képzést tart a biztonsági események kezelése témában. A képzés anyagának tartalmaznia kell a lehető legtöbb, nagy valószínűséggel elforduló biztonsági eseményt, illetve az ezekhez kapcsolódó teendőket.

9.9. BIZTONSÁGI ESEMÉNYEK KEZELÉSE

A Felhasználó köteles az általa tapasztalt rendellenes eseményeket a Rendszergazdával azonnal közölni, szóbeli közlés esetén legkésőbb a következő munkanapon e-mailben is megerősíteni. A Felhasználó a rendellenes eseményről szóló tájékoztatása során köteles az esemény valamennyi körülményének részletes feltárására.

Ha a felhasználónak gyanúja támad arra, hogy a jelszavát más személy is megismerte vagy személyazonosító eszközét más megszerezte vagy lemásolta, úgy köteles azonnal jelezni ezt a Rendszergazda felé, továbbá amennyiben a lehetőségei adottak, köteles a jelszavát azonnal megváltoztatni, személyazonosító eszközét letíltatni a megfelelő szolgáltatónál.

Amennyiben a rendszerhibát vélhetően külső, illetéktelen beavatkozás, vagy vírustámadás okozta, az érintett eszközt le kell választani a hálózatról, illetve szükség esetén ki kell kapcsolni. Ez a Rendszergazda feladata.

Vírustámadás esetén fokozottan figyelni kell a cserélhető adathordozókra is. A fertőzött számítógépben használt adathordozók kizárólag a vírusellenőrzést követően használhatók más számítógépeken.

A Rendszergazda gondoskodik arról, hogy a többféle módon (e-mailben vagy telefonon) bejelentett biztonsági események a nyilvántartásban minden esetben a „Biztonsági esemény" kategóriába kerüljenek. Rendszergazda ezen kívül telefonon vagy személyesen is jelenti az eseményt az IT vezetőnek és az IBF-nek.

9.25. A BIZTONSÁGI ESEMÉNYEK NYOMONKÖVETÉSE

A biztonsági események bekövetkeztét az események súlyosságától függően és a Biztonsági eseménykezelési tervnek megfelelően dokumentálni kell.

A Rendszergazda feladata a szükséges intézkedések meghozatala, a teljes elhárítási folyamat dokumentálása. Az EIR védelmét ellátó biztonsági eszközök naplóállományainak elemzésével, valamint a kialakított hibakezelési eljárások hatékony működtetésével a Hivatalnak folyamatosan figyelemmel kell kísérnie az EIR-ekben bekövetkező információbiztonsági eseményeket.

Az incidensekről készült feljegyzéseket az IBF rendszeresen áttekinti, szükség esetén további helyesbítő, megelőző intézkedésekre tesz javaslatot.

9.27. A BIZTONSÁGI ESEMÉNYEK JELENTÉSE (A6.8)

Minden munkatárs feladata, hogy az információbiztonsági incidenseket, észlelt gyengeségeket jelentse közvetlen felettesének, eredménytelenség esetén az IT vezetőnek.

Biztonsági eseménynek nevezzük az EIR működésében beállt olyan kedvezőtlen változást, amelynek hatására az EIR vagy a benne kezelt adatok bizalmassága, sértetlensége, rendelkezésre állása sérült vagy sérülhet.

A jellemző biztonsági események a következők:

- szoftver vagy hardver hibás működése;
- nem ellenőrzött rendszerbeli változások;
- a bizalmasság és/vagy sértetlenség sérülése;
- informatikai eszközök elvesztése;
- vírusok és egyéb kártevők általi fertőzés;
- túlterheléses támadások (szolgáltatás megtagadó, DoS támadások);
- az EIR-rel való visszaélés;
- a szabályzatoknak vagy irányelveknek való nem megfelelés;
- a fizikai biztonsági rendelkezések megsértése;
- a hozzáférési előírások megsértése;
- emberi hibák.

A biztonsági esemény bekövetkeztét fajtájuktól és súlyuktól függően jelenteni kell az illetékes hatóságoknak is:

a) Rendőrség: ha a biztonsági esemény bűncselekmény, adatsértés vagy más jogszabálysértés eredménye. A Hivatal vezetője jelenti.
b) NAIH: ha az esemény kapcsolódik személyes adatok kiszivárgásához vagy illetéktelen hozzáféréshez. A DPO jelenti.
c) Kiberbiztonsági incidenskezelő központ (NBSZ-NKI): minden jelentős biztonsági eseményt.

9.31. SEGÍTSÉGNYÚJTÁS A BIZTONSÁGI ESEMÉNYEK KEZELÉSÉHEZ

Az IBF feladata, hogy tájékoztatást és segítséget nyújtson az EIR felhasználóinak a biztonsági események észlelése, kezelése és jelentése érdekében.

9.34. BIZTONSÁGI ESEMÉNYKEZELÉSI TERV (IRP) (A5.26)

Ezen terv meghatározza azokat az eljárásokat és intézkedéseket, amelyeket a Hivatal végrehajt a biztonsági incidensek kezelése során. A terv célja, hogy leírja azokat az eljárásokat és lépéseket, amelyeket a Hivatal alkalmaz az incidensek felismerése, kezelése kapcsán. A terv a károk minimalizálására törekszik a biztonsági incidensek során és lehetővé teszi a gyors és hatékony reakciót azokra.

Felelős: IT vezető, IBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

KÖTELEZŐ ÉRTESÍTÉSI INTÉZKEDÉSEK

A Hivatal minden olyan kiberbiztonsági incidensről értesíti a szolgáltatásait igénybe vevőket, amely hátrányosan érintheti a szolgáltatásnyújtásukat, és amelynek kezelése a szolgáltatásokat igénybe vevők részéről intézkedést igényel.

A Hivatal haladéktalanul, vagy amint az információ rendelkezésre áll tájékoztatja a jelentős kiberfenyegetés által potenciálisan érintett szolgáltatásait igénybe vevőket az intézkedésekről, illetve fenyegetést orvosló lehetőségekről, amelyeket a szolgáltatások igénybe vevői maguk megtehetnek vagy amelyekkel élhetnek

INCIDENS BEJELENTÉSE, ÉSZLELÉSE A HIVATALON BELÜL (A5.25)

A bejelentés, illetve észlelés kétféleképpen történhet:

- A 9.27 A biztonsági események jelentése pont szerint rögzített módon.
- Automatizált jelentés a biztonsági eseményben érintett rendszertől (pl: Naplótárhely-elfogyásról jelzés a Rendszergazdának).

A BEJELENTÉS FOLYAMATA A KIBERBIZTONSÁGI INCIDENSKEZELŐ KÖZPONT IRÁNYÁBA

ELSŐ BEJELENTÉS

- A jelentős biztonsági incidens tudomásszerzésétől számított 24 órán belül benyújtandó.
- A bejelentés tartalmát a Korm. rendelet 77. § 1. pontja határozza meg.

ESEMÉNYBEJELENTÉS

- Az első bejelentést követően 72 órán belül benyújtandó.
- Frissített, aktualizált információkat és az incidens első értékelését kell tartalmaznia.

ZÁRÓJELENTÉS

- Legkésőbb az Eseménybejelentést követő egy hónapon belül benyújtandó.
- A jelentés tartalmazza az incidens részletes leírását, a kiváltó fenyegetést vagy okokat, és az alkalmazott, vagy folyamatban lévő mérséklési lépéseket. Amennyiben a benyújtásának időpontjában még folyamatban van a kiberbiztonsági incidens, akkor az addig elért eredményekről szóló jelentést.

ADATSZOLGÁLTATÁS

A fertőzöttségi mutatókat haladéktalanul meg kell adni, amint elérhetővé válnak.

KÖZBENSŐ HELYZETJELENTÉS

A Kiberbiztonsági incidenskezelő központ kérésére közbenső helyzetjelentést kell benyújtani.

AUTOMATIZÁLT ESEMÉNYEK KEZELÉSE

Az automatizmus által kezelhető incidensek bejelentése nem kötelező, kivéve az ismétlődő eseteket.

EGYÜTTMŰKÖDÉSI KÖTELEZETTSÉGEK

Az incidens kezelése és kivizsgálása során a Hivatalnak együtt kell működnie a Kiberbiztonsági incidenskezelő központtal, amelynek során köteles az bejelentéssel kapcsolatos információk és az incidensben érintettek, az incidensért felelősök azonosításához szükséges technikai adatok, valamint a vizsgálat lefolytatásához szükséges adatok átadására, a vonatkozó dokumentumok és eszközök biztosítására, az incidensben érintett infrastruktúra speciális, ágazati sajátosságainak megosztására.

A Hivatalnak biztosítania kell a hozzáférést az incidenssel érintett infrastruktúrához, és tájékoztatnia kell a Kiberbiztonsági incidenskezelő központ szakembereit az incidens kezelése során tett intézkedésekről, illetve az infrastruktúrával kapcsolatos beállításokról.

A Hivatal köteles továbbá előzetes egyeztetést követően telepíteni a Kiberbiztonsági incidenskezelő központ által szükségesnek ítélt korai figyelmeztető vagy csapdarendszereket, szenzorokat, abban az esetben, ha azok telepítése nem akadályozza vagy veszélyezteti a Hivatal működését.

INCIDENS AZONOSÍTÁSA, KATEGORIZÁLÁSA:

A biztonsági incidensek fajtájuktól függően lehetnek alacsony, közepes és jelentős szintűek.

ALACSONY

Minden olyan esemény, amely kisebb üzemzavart okozhat, de házon belül gyorsan elhárítható.

Ezek lehetnek kisebb problémák, például, ha egy munkaállomás lassabban működik vagy ha kívülről térképezik fel a hálózatot, ezek általában nem befolyásolják a szolgáltatásokat.

Lehetnek olyan helyzetek is, amikor több felhasználó tapasztal zavarokat, például egy funkció nem működik megfelelően vagy megszűnik egy szolgáltatás tartalékrendszere, ami már fokozottabb figyelmet igényel.

KÖZEPES

Összességében közepesnek minősül minden olyan esemény, amely az Alacsony kategóriánál jóval nagyobb hatással van a Hivatalra, de még nem éri el a bejelentésköteles Jelentős incidens mértékét.

Komolyabb esetekben a hibák közvetlenül akadályozzák a rendszerek használatát, például, ha ismert sérülékenységet kihasználnak, megszakad a kommunikáció vagy egy fontos rendszer elérhetetlenné válik.

A legsúlyosabb esetekben akár a teljes hálózati infrastruktúra veszélybe kerülhet, hosszabb ideig nem működnek alapvető szolgáltatások, vagy érzékeny adatok kerülnek illetéktelen kezekbe.

JELENTŐS

Jelentős biztonsági eseménynek minősül minden olyan esemény, amely

a) a Hivatal által nyújtott szolgáltatás legalább 5%-os kiesésével jár, vagy fenyeget;
b) a Hivatal éves árbevételének legalább 5%-os kiesésével jár, vagy fenyeget;
c) Súlyos működési zavart okoz vagy képes okozni a szolgáltatásokban, vagy pénzügyi vagy reputációs veszteséget okoz vagy képes okozni a kiberbiztonsági incidens által érintett szervezetnek vagy személynek;
d) Személyi sérüléssel, vagy halállal jár, fenyeget;
e) Visszatérő – ugyanazon esemény 6 hónapon belül többször is előfordul.

AZ INCIDENS ELHÁRÍTÁSA (A5.26)

A Hivatal haladéktalanul kidolgozza és végrehajtja az incidens felszámolásához szükséges intézkedéseket.

TERVEZÉS ÉS ELŐKÉSZÍTÉS

A biztonsági esemény és incidens kezelés tervezési és előkészítési szakaszának lépései, melynek felelőse az IT vezető

a) Vészhelyzeti Csoport (Incidenskezelő csoport) összehívása, amely biztonsági incidens esetén gyorsan és szakszerűen jár el.
b) Biztonsági esemény és incidens pontos meghatározása (milyen eseményeket tekintünk biztonsági incidensnek) az IBF bevonásával.
c) Incidensek kategorizálási rendszerének kidolgozása.
d) Az incidens kategóriájától és a biztonsági eseménytől függő együttműködés a következő szervezetekkel:
   - Rendszergazda
   - Üzemeltető, fejlesztő és technológia szállító partnerek.

ÉSZLELÉS ÉS JELENTÉS

A kapcsolódó fő feladatok az alábbiak szerint kerültek meghatározásra:

a) Az automatikus eseményfigyelő és feldolgozó rendszerek riasztásainak figyelése és szükség esetén a védelemi intézkedések megerősítése a fenyegetések függvényében.
b) Külső riasztások monitorozása (pl. EIR felügyeletét ellátó szervek riasztásai és értesítései) és szükség esetén a védelemi intézkedések megerősítése a fenyegetések függvényében.
c) A Hivatal határvédelemi és belső biztonságvédelemi rendszereinek és az információ tartalom folyamatos monitorozása.
d) Biztonsági incidensek detektálása:
   - automatikus valós időben, illetve
   - manuálisan.
e) A biztonsági eseményhez kapcsolódó információ gyűjtése és tárolása.
f) Felhasználói bejelentések rögzítése a gyanús eseményekről.
g) Üzemeltetői bejelentések rögzítése a gyanús eseményekről.

VIZSGÁLAT ÉS DÖNTÉS

A Vészhelyzeti vezető koordinálásával a Vészhelyzeti Csoport (Incidenskezelő csoport) elvégzi a kezdeti felmérést. Azt kell eldönteni, hogy az esemény valóban biztonsági incidens-e. Ha az esemény valóban biztonsági incidens, akkor meg kell határozni a várható hatását a bizalmasságra, sértetlenségre és rendelkezésre állásra vonatkozóan, valamint az érintett rendszerekre az incidens besorolási szabályok alapján kategorizálni kell a biztonsági eseményt, amennyiben az jelentősnek minősül, vagy visszatérő akkor pedig meg kell tenni az Első bejelentést a Kiberbiztonsági incidenskezelő központ részére. Ebben a fázisban a Vészhelyzeti vezetőnek, vagy az általa kijelölt kompetens személynek (pl.: Rendszergazdának, továbbiakban Incidens menedzser) kell a vizsgálatot elvégeznie és a döntést meghoznia.

A Kiberbiztonsági incidenskezelő központ a bejelentésre haladéktalanul és – ha lehetséges – az Első bejelentés kézhezvételétől számított 24 órán belül választ ad. Ennek keretében visszajelzést küld az incidensről a bejelentő szervezetnek, valamint – a Hivatal kérésére – útmutatást vagy operatív tanácsokat nyújt a lehetséges mérséklési intézkedések végrehajtásáról.

A Kiberbiztonsági incidenskezelő központ technikai támogatást nyújt, ha az érintett szervezet ezt kéri.

A 4 lehetséges kimenet:

- nem incidens (pl. hibás értesítés);
- alacsony szintű (házon belül kezelhető), vagy;
- közepes szintű (akár külső erőforrás bevonása is szükséges lehet), vagy;
- jelentős szintű (bejelentésköteles).

Amennyiben a normál működés visszaállítása feltételezhetően meg fogja közelíteni a kiesett erőforrás által támogatott alapfeladatok, folyamatok maximálisan megengedhető kiesési idejét (Maximum Tolerable Downtime - MTD), a Vészhelyzeti vezető az állapotot vészhelyzetként kezeli és értesíti az Szervezet legfelső vezetőjét és az IBF-t.

Az incidens kategóriájától függően el kell végezni:

a) A hozzárendelt vezetők (személyek vagy szerepkörök) értesítését;
b) Az incidens típushoz hozzárendelt, nem állandó Vészhelyzeti Csoport (Incidenskezelő csoport) értesítését és a vezetők és szakértők bevonását az incidens elhárításába;
c) A megadott kapcsolattartókon keresztül a külső partnerek értesítését és a szükséges információ megosztását;
d) Felelős hozzárendelését;
e) Információgyűjtés, illetve szükség esetén bizonyítékok gyűjtésének megkezdését;
f) Az incidens elhárítását.

ELHÁRÍTÁS

Az incidens elhárításának fázisa akkor kezdődik, amikor az Vészhelyzeti vezető elvégezte a biztonsági incidens beazonosítását és kategorizálását. A biztonsági incidensre adott válasznak 3 részfolyamata van:

ELSZIGETELÉS ÉS VIZSGÁLAT

Az első lépésben az incidens kategóriájától függően az IT vezető, vagy amennyiben szükséges (Magas és Kritikus kategóriájú incidens esetén) a Vészhelyzeti Csoport (Incidenskezelő csoport) dönt, hogy az incidensben érintett rendszereket, rendszerelemeket el kell-e szigetelni, hogy a támadás vagy fertőzés ne tudjon tovább terjedni. Szokásos megoldás a rendszer leválasztása a hálózatról, vagy a rendszer leállítása. A leválasztott rendszeren lehetőség nyílik az incidens részletes vizsgálatára, a bizonyítékok összegyűjtésére és a megszüntetés módjának eldöntésére, kidolgozására.

A vizsgálat során:

- meg kell határozni, hogy a biztonsági incidens milyen károkat okozott,
- meg kell határozni az azonnali javító intézkedéseket,
- meg kell határozni a biztonsági esemény elhárításának végső megoldását és határidejét,
- meg kell határozni, hogy milyen átmeneti biztonsági intézkedések mellett lehet újraindítani az incidens által érintett rendszert, illetve szolgáltatást, amelyek megakadályozzák az incidens újbóli előfordulását,
- meg kell határozni a megfelelő, a lehetséges kockázatokkal arányos végleges intézkedést, amely megakadályozza a biztonsági incidens újbóli előfordulását,
- a vizsgálatok eredményét és a döntéseket dokumentálni kell.

MEGSZÜNTETÉS

Az elhárítás következő lépése az incidens következtében korrumpálódott vagy gyanús rendszerkomponensek eltávolítása majd „tiszta" változat újra telepítése, vagy a feltört felhasználói fiók deaktiválása. A megszüntetés előtt minden technikai és jogi bizonyítékot össze kell gyűjteni és el kell menteni módosíthatatlan formában. Gondoskodni kell a bizonyítékok megfelelő tárolásáról.

HELYREÁLLÍTÁS

Az incidens okának és hatásainak megszüntetése után az incidens elhárításának utolsó lépése a normál működés visszaállítása.

A helyreállítás történhet:

- Azonnali átmeneti javító intézkedések után egy meghatározott időtartamra, ameddig a végleges javító intézkedések elvégzésre kerülnek;
- Végleges javító intézkedések mellett;
- A helyreállításnak részét kell, hogy képezze a biztonsági rések és folyamathibák kiküszöbölése, annak érdekében, hogy az incidens újból ne következhessen be. A biztonsági rések javítása esetében is megengedett kockázatarányos átmeneti megoldással történő újraindítás, fokozott védelmi készültség mellett. Ezt a döntést a Rendszergazdának kell meghoznia.

INCIDENS ELHÁRÍTÁS UTÁNI FELADATOK (A5.27 – A5.28)

- Az incidens részletes dokumentálása;
- A sérülékenységi pontokon a védelmi intézkedések továbbfejlesztése, szükség esetén fejlettebb eszközök alkalmazása;
- Szabályozások, eljárásrendek, munkautasítások aktualizálása és továbbfejlesztése;
- Incidenskezelési eljárások továbbfejlesztése;
- Bizonyítékok mentése;
- Ha szükséges igazságügyi vizsgálat lefolytatása;
- Ha szükséges fegyelmi eljárás indítása.

Jelentős szintű biztonsági esemény esetén a Hivatal tájékoztatja az illetékes hatóságot a feltárt hiányosságok megszüntetésére készített incidenskezelési tervről.

Az incidens felszámolását követően a Hivatal felülvizsgálja elektronikus információs rendszereinek kockázatelemzését és kockázatkezelését, és végrehajtja a szükséges módosításokat.

10. KARBANTARTÁS (A7.13)

10.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend fő célja, hogy biztosítsa a Hivatal informatikai eszközei és rendszerei megbízható és hatékony működését. Ennek érdekében számos intézkedést és gyakorlatot foglal magában: a szabályozott karbantartásra összpontosít, amely meghatározza és standardizálja a karbantartási folyamatokat a hatékonyság és az egységesítés érdekében. A távoli karbantartás lehetősége is fontos elem, ami lehetővé teszi a távoli hozzáférést a karbantartási munkákhoz, ami hatékonyabb és gyorsabb reakciót tesz lehetővé a problémákra. Végül meghatározza a karbantartást végző személyek felelősségét és kötelességeit is, biztosítva ezzel a megfelelő szakértelmet és felelősséget a karbantartási tevékenységekhez.

Felelős: IT vezető

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

10.2. SZABÁLYOZOTT KARBANTARTÁS

Rendszeres karbantartás

A folyamatos működés biztosítása érdekében az EIR elemeit megadott rendszeres időközönként karban kell tartani.

A hardver eszközök karbantartásának célja, hogy megelőzze az eszközök véletlenszerűen bekövetkező meghibásodását. Ilyen karbantartás lehet például:

a) az eszközök belső portalanítása;
b) az elhasználódó alkatrészek cseréje;
c) a nyomtatók mozgó és szennyeződő alkatrészeinek tisztítása;
d) a szünetmentes tápegységek akkumulátorának öntészttel történő ellenőrzése.

A szoftver elemek karbantartása során kell elvégezni azokat a szerver oldali rendszeres szoftverfrissítéseket, amelyek EIR vagy alapszolgáltatások leállításával járnak.

A karbantartásokat a gyártói ajánlások és a szoftverfrissítésekre vonatkozó előírások figyelembevételével kell végezni.

Karbantartások ütemezése

A karbantartandó eszközök körét és a karbantartás rendszerességét az IT vezető határozza meg, az eszközök alkalmazási körülményeit is figyelembe véve.

Az adott rendszer rendszergazdájának Éves karbantartási tervet kell készítenie, amelyben meg kell tervezni a karbantartások ütemezését.

A karbantartás csak akkor kezdődhet meg, ha azt az IT vezető jóváhagyja

A Hivatal létesítményeiből a rendszerelemek elszállítása karbantartás vagy csere céljából csak az IT vezető jóváhagyásával lehetséges.

Karbantartások folyamata

A tervezett karbantartásokat (és az eseti javításokat) az IT vezetőnek dokumentált formában engedélyeznie kell.

Amennyiben a karbantartás valamely EIR-nek vagy szolgáltatásának a leállításával jár, akkor az érintett felhasználókat a karbantartás megkezdése előtt legalább 1 munkanappal korábban értesíteni kell.

Eszközök kiszállítása (A7.9)

Amennyiben a karbantartáshoz kapcsolódóan adatot tartalmazó adathordozó kiszállítása válik szükségessé, akkor a 11.8 Adathordozók törlése pontban leírtak szerint kell eljárni. Ez alól jellegénél fogva kivételt képez a Rendszergazda informatikai rendszerüzemeltetési szolgáltatásának ügyfelei esetén az eszközök a Rendszergazdához történő visszaszállítása.

A kiszállítást az IT vezető engedélyezi.

Karbantartások ellenőrzése

Az elvégzett karbantartás után az eszköz fajtájától függően funkcionális és biztonsági tesztet kell végezni, melynek eredményét a Karbantartási naplóban kell rögzíteni.

Sikertelen teszt esetén az eszköz nem helyezhető újra éles üzembe. Az eseményt jelenteni kell az IT vezetőnek, aki dönt a további intézkedésekről.

Karbantartások dokumentálása

A karbantartás elvégzését a Karbantartási naplóban kell dokumentálni, amely egyben az elvégzett karbantartások nyilvántartására is szolgál.

A Naplóban a következő adatokat kell rögzíteni:

a) az érintett EIR (-ek) nevét;
b) a karbantartás tárgyát (az érintett hardver/szoftver rendszerelemeket);
c) a karbantartás rövid megnevezését;
d) a karbantartás dátumát és idejét;
e) a karbantartás végzőjét;
f) a karbantartás engedélyezőjét;
g) az elvégzett karbantartás leírását;
h) a karbantartást követő teszt leírását és eredményét.

A Karbantartási naplókat a Rendszergazdának visszakereshető formában kell tárolnia. A megőrzési idő 5 év.

10.11. TÁVOLI KARBANTARTÁS

A távoli karbantartási és diagnosztikai tevékenységeket akkor lehet végezni, ha az jóváhagyásra kerül az IT vezető által.

A karbantartási eszközöknek teljes mértékben meg kell felelniük a Hivatal által előírt biztonsági követelményeknek, mint a kriptográfiai követelmények teljesítését, valamint az eszközökön elérhető biztonsági funkciók alkalmazását.

Csak erős hitelesítési eljárás után kezdődhet meg a tevékenység (MFA).

A távoli karbantartás egy kötelezően naplózandó tevékenység!

A távoli karbantartás befejeztével automatikusan le kell zárni a hálózati kapcsolatokat, kapcsolódó szolgáltatásokat, minimalizálva a biztonsági kockázatokat.

10.18. KARBANTARTÓ SZEMÉLYEK (A7.6)

Belső karbantartók

A karbantartásokat és javítási munkákat csak arra felhatalmazott, kompetens személy végezheti:

a) A hardver hibák felderítését és a speciális szakismeretet, szerszámokat és anyagokat nem igénylő hardver karbantartásokat, javításokat a Rendszergazda munkatársai végzik.
b) A speciális szakismeretet, szerszámokat vagy anyagokat igénylő karbantartások és javítások (és a jótállási időn belüli garanciális javítások) elvégzésére az IT vezető megbízhat külső partnereket.

A külső partnerrel történő karbantartások/javíttatások ügyintézését a Rendszergazda adott eszközért felelős munkatársai végzik.

Külső karbantartó partnerek igénybevétele esetén a Külső karbantartók pontban leírtakat kell alkalmazni.

Külső karbantartók

Abban az esetben, ha az EIR karbantartását a Rendszergazda nem tudja elvégezni, vagy egyéb kötelezettségek miatt nem végezheti el, akkor az IT vezető kezdeményezi a külső partner megbízását.

Karbantartási tevékenységet csak olyan külső partner végezhet, aki érvényes szerződéssel rendelkezik, a titoktartási nyilatkozatot aláírta és dokumentált formában megismerte a Hivatalra vonatkozó információbiztonsági előírásokat.

A karbantartást végző, hozzáféréssel rendelkező külső partnerekről nyilvántartást kell vezetni (Külső karbantartók nyilvántartása), melynek minimálisan a következőket kell tartalmaznia:

a) a karbantartó szervezet/személy megnevezését, címét;
b) a szerződés/megrendelés tárgyát (mely rendszerelemekre terjed ki);
c) a szerződés/megrendelés időtartamát;

Külső partner munkavégzése esetén az IT vezetőnek ki kell jelölnie azokat a munkatársakat, akiknek folyamatos felügyeletet kell biztosítani a karbantartás során.

A külső partnerrel kötött szerződésbe bele kell foglalni, hogy a karbantartást felügyelő munkatársak jogosultak kérni a karbantartást végzők személyazonosságának igazolását, illetve, hogy a karbantartást végző személynek kötelessége a felszólításra a szükséges iratokat bemutatni.

Ha a karbantartás során a Hivatal EIR-hez fizikailag, vagy logikailag hozzá kell férni, a Rendszergazda kötelessége és felelőssége a hozzáférés során folyamatos felügyelet alatt tartani karbantartást végző személyeket.

11. ADATHORDOZÓK VÉDELME (A7.10)

11.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Ezen eljárásrend célja a szervezeti- folyamat- és rendszer szintű követelményeket tartalmazó adathordozók biztonságának fokozott és strukturált biztosítása és védelme a Hivatalban.

Felelős: IT vezető, IBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

11.2. HOZZÁFÉRÉS AZ ADATHORDOZÓKHOZ

Az EIR-ben csak a Hivatal tulajdonában lévő, regisztrált adathordozót lehet használni. Nem a Hivatal tulajdonában lévő adathordozókat csatlakoztatni a Hivatal EIR-hez kizárólag az IT vezető tudtával és engedélyével lehet.

A Hivatalon belül jelenleg engedélyezett adathordozó típusokat, az adathordozókhoz hozzáférő szerepköröket, a hozzáférés módját és célját az alábbi táblázat tartalmazza:

Adathordozó típus	**Szerepkör**	**Hozzáférés / jogosítvány**
EIR szerver oldali háttértárai (HDD, SSD)	Rendszergazda	Fizikai, logikai / karbantartás, mentés, visszaállítás
	Felhasználó	Logikai / szerepkörének megfelelően
Szerver oldali, központi mentések adathordozói	Rendszergazda	Fizikai, logikai / tárolás, mentés, visszaállítás
Munkaállomások háttértárai (HDD/SSD, mobiltelefon, fényképezőgép, kártyaolvasó	Rendszergazda	Fizikai, logikai / karbantartás, mentés, visszaállítás
	Felhasználó	Logikai / szerepkörének megfelelően
Munkaállomás mentések adathordozói (pendrive, külső HDD)	Rendszergazda	Fizikai, logikai / karbantartás, mentés, visszaállítás
	Felhasználó	Fizikai, logikai / tárolás, mentés, visszaállítás
Rendszerelemek telepítő adathordozói (pendrive, DVD)	Rendszergazda	Fizikai, logikai / tárolás, telepítés
Készenléti terveket (Készenléti tervet) és vészhelyzeti adatokat tároló adathordozók (DVD, pendrive, szalag)	A Készenléti tervekben megadott szereplők	Fizikai, logikai / a Készenléti tervekben leírt műveletek elvégzése és a tervek karbantartása
Analóg adathordozók (iratok, fénymásolatok, jegyzetek, rajzok, térképek, fotók	Felhasználó	Fizikai / munkakörének/szerepkörének megfelelően

11.8. ADATHORDOZÓK TÖRLÉSE (A7.14, A8.10)

Az adathordozók vagy adathordozót tartalmazó informatikai eszközök újrahasznosítása, mások rendelkezésre bocsátása vagy selejtezése előtt minden esetben gondoskodni kell arról, hogy az adathordozón tárolt adatok visszaállíthatatlanul eltávolításra kerüljenek.

Ennek érdekében helyreállíthatatlanságot biztosító törlési technikákkal törölni kell az adatokat (olyan szoftvert alkalmazásával, amely többszörösen felülírva törli az adatokat), vagy az adathordozót roncsolással fizikailag kell használhatatlanná tenni, megsemmisíteni.

Használható törlési algoritmusok:

- DoD 5220.22-M
- AR380-19
- GOST P50739-95
- RCMP TSSIT OPS-II

A törlést vagy megsemmisítést az adathordozón lévő adatok gazdájának előzőleg jóvá kell hagynia.

Garanciális eszközök esetén, ha az eszköz hibája miatt nincs mód az adatok törlésére, az IT vezető dönt az adathordozó cserére történő kiadhatóságáról vagy megsemmisítéséről.

Az adatok eltávolítását a Rendszergazda végzi.

Az adatok eltávolításának tényét és módszerét az eltávolítást végző munkatársnak jegyzőkönyveznie kell.

11.14. ADATHORDOZÓK HASZNÁLATA

Az EIR-hez kapcsolódó munkaállomásokon a felhasználók számára általában tilos a külső adathordozók (pl.: DVD, pendrive, külső merevlemez) használata. Ezeken a munkaállomásokon külső adathordozókat csak a Rendszergazda használhat a munkaállomás karbantartása (pl.: vírusirtás, telepítés, mentés vagy visszaállítás) céljából.

Egyes felhasználók– amennyiben munkakörükhöz kapcsolódik, vagy az adott munkafolyamat megkívánja – munkahelyi vezetői engedéllyel használhatnak külső adathordozókat. Ezen adathordozókat minden használat előtt a vírusvédelemnek ellenőrizni kell.

Otthoni munkavégzés és bármilyen más célból bármilyen adatot DVD-n, pendrive-on, külső merevlemezen, elektronikus levélben, Interneten vagy bármilyen más módon az EIR-ből kijuttatni csak az Adatgazda írásos engedélyével szabad.

Az eszközhasználatot az EIR-hez történő csatlakoztatása után, az érintett szervezet minden előzetes értesítés nélkül figyelheti, ellenőrizheti.

A Hivatal az adathordozók használatát információbiztonsági megfontolásból hardver, illetve szoftver úton korlátozhatja.

Olyan adathordozó használata, amelynek nincs azonosítható tulajdonosa, szigorúan tilos!

12. FIZIKAI ÉS KÖRNYEZETI VÉDELEM

12.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK (A7.1)

Jelen eljárásrend célja az EIR-t koncentráltan tartalmazó épületek védelme, biztosítva a fizikai belépési engedélyeket, ellenőrizve a belépést, a fizikai hozzáféréseket és felügyelve az adatátviteli eszközök, kimeneti eszközök hozzáférését. Az eljárásrend magában foglalja az áramellátó berendezések biztosítását, vészhelyzeti tápellátást, valamint tűzvédelmi és környezeti védelmi intézkedéseket.

Felelős: IT vezető

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

12.2. A FIZIKAI BELÉPÉSI ENGEDÉLYEK (A7.2)

A Hivatal központi irodaépületében Ügyfélszolgálatos fogadja a belépőket, ennek megfelelően csak belépési engedéllyel, illetve előre leadott névjegyzék alapján lehet be- és kilépni. Kivételt képez ez alól az ügyfelek ügyfélszolgálati időben történő be- és kilépése.

A Hivatal vezetője összeállítja, jóváhagyja, és kezeli az EIR-eknek helyt adó létesítményekbe belépésre jogosultak listáját. A Hivatallal jogviszonyban vagy munkaviszonyban álló valamennyi személynek rendelkeznie kell belépésre jogosító engedéllyel.

A Személyügyi ügyintéző évente felülvizsgálja a belépésre jogosultak listáját.

Új jogviszony létesítése esetén a Személyügyi ügyintéző, a Jegyző jóváhagyásával rögzíti az új munkatársat. Az új munkatárs beléptető kártyájának vagy kulcsának kiadásáról szintén ő gondoskodik a rögzítést követő első munkanapon.

Az engedély kiadásának alapjául szolgáló jogviszony megszűnése esetén az utolsó munkában töltött napon a munkavállaló engedélye visszavonásra kerül.

12.6. A FIZIKAI BELÉPÉS ELLENŐRZÉSE (A7.3)

A Hivatal épületeibe csak a hivatalos ki- és belépési pontokon engedélyezett a ki- és belépés. A ki- és beléptetés rendszerét és módját a Jegyző határozza meg.

Az informatikai helyiségekbe való belépésre csak abban az esetben adható felhatalmazás, ha az adott személynek arra:

- munkaköri kötelességének, feladatának ellátásához,
- külső személy esetén a Hivatallal szembeni szerződéses kötelezettség teljesítéséhez szüksége van (Ebben az esetben csak a helyiségbe belépésre felhatalmazott munkavállaló kíséretével léphet be ezekre a területekre).

Az informatikai helyiségekbe való belépés – az első bekezdésben foglaltak alkalmazása mellett – állandó jelleggel csak az IT vezető, a Rendszergazda, valamint az IBF számára engedélyezhető. Az engedély kiadása, nyilvántartása, felülvizsgálata, valamint a fizikai belépéseket ellenőrző eszközök nyilvántartásának vezetése az IT vezető felelőssége.

A külső partnerek belépését az informatikai helyiségekbe az IT vezető engedélyéhez kell kötni. Külső partnertől igénybe vett IT szolgáltatás esetén azon géptermekbe, ahol a Hivatal szerverei kerülnek elhelyezésre, a szolgáltató vezetője engedélyezheti a belépést.

A Hivatal a kijelölt pontokon való átjutást felügyeli fizikai belépést ellenőrző rendszerrel vagy eszközzel.

A fizikai hozzáférési kódok és kulcsok kompromittálódása esetén a kódok és kulcsok cseréje szükséges. Abban az esetben is cserélni kell a kódokat és kulcsokat, ha az azokkal rendelkező személy elveszíti a belépési jogosultságát.

12.17. A FIZIKAI HOZZÁFÉRÉSEK FELÜGYELETE (A7.4)

A Hivatal ellenőrzi az EIR-nek helyt adó létesítményekbe, és az irodai térben történt fizikai hozzáféréseket annak érdekében, hogy észlelje a fizikai biztonsági eseményt és reagáljon arra. A Rendszergazda rendszeresen átvizsgálja a fizikai hozzáférésekről készült naplókat, sértetlenség, bizalmasság és rendelkezésre állás szempontjából.

Ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak, megkezdi az esemény kivizsgálását a belső ellenőrzés, az Adatvédelmi felelős bevonásával. A vizsgálatot megelőzően gondoskodik a naplóállományok zárolásáról.

A belső ellenőrzés összehangolja a biztonsági események kezelését, valamint a napló átvizsgálások eredményét.

12.22. LÁTOGATÓI HOZZÁFÉRÉSI NAPLÓK

A látogatói belépésekről szóló digitális nyilvántartást a Hivatal 1 évig megőrzi. A nyilvántartást incidens gyanúja esetén át kell vizsgálni, és az észlelt rendellenességekről tájékoztatni kell az IT vezetőt, szükség esetén az IBF-t.

12.31. VÉSZVILÁGÍTÁS

A Hivatal automatikus vészvilágítási rendszert alkalmaz és tart karban, amely áramszünet esetén aktiválódik, és amely biztosítja a vészkijáratokat és a menekülési útvonalakat.

12.33. TŰZVÉDELEM (A7.5)

A Hivatal az EIR-ek védelme érdekében független energiaforrással rendelkező tűzérzékelő berendezéseket alkalmaz, amelyekkel biztosítja a működést egy esetleges áramkimaradás esetén is. A rendszerek telepítése, működtetése, karbantartása, tesztelése és ellenőrzése megfelel a vonatkozó jogszabályi előírásoknak. A tűzérzékelő rendszerek kiegészítéseként kézi tűzoltókészülékek is kihelyezésre kerültek az érintett területeken.

A rendszerek alkalmazására, kezelésére és felülvizsgálatára vonatkozó szabályokat a Hivatal Tűzvédelmi szabályzata tartalmazza.

12.37. KÖRNYEZETI VÉDELMI INTÉZKEDÉSEK (A7.5)

A szerverszoba üzemi hőmérsékletének szabályozásának érdekében az alábbi szempontok figyelembevétele szükséges:

- A szerverszobában klíma-berendezéseket kell üzemeltetni, a megfelelő üzemi hőmérséklet szabályozására.
- A klíma berendezések darabszámát, és teljesítményét úgy kell tervezni, hogy a szerverszobában nem csak a jelenleg elhelyezett eszközök, hanem a jövőbeli, maximális kihasználtság esetén is (az eszközök hődisszipációs mutatóit figyelembe véve), még egy klímaberendezés meghibásodása esetén is biztosítani tudják a megfelelő szabályozást.

- A klíma-berendezések automatikus újra indítását biztosítani kell az esetleges áramszünet megszűnése esetén.

A szerverszoba hőmérsékletét folyamatosan monitorozni kell. Az optimális hőmérséklet +10 Celsius és +25 Celsius fok közötti, illetve a páratartalom nem haladhatja meg a 70%-ot. Amennyiben ezen értékek eltérnek az optimálistól, a rendszernek riasztást kell kiküldeni elsődlegesen a Rendszergazdának.

12.40. VÍZ-, ÉS MÁS, CSŐVEZETÉKEN SZÁLLÍTOTT ANYAG OKOZTA KÁR ELLENI VÉDELEM (A7.5)

A Hivatalnak védenie kell az EIR-eket a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzáró szelepek hozzáférhetőek, és megfelelően működnek, valamint a kulcsszemélyek számára ismertek.

12.42. BE- ÉS KISZÁLLÍTÁS

A Hivatal vezetője, illetve az IT vezető engedélyezheti, továbbá ellenőrizheti a létesítményeibe bevitt, illetve onnan kivitt információs rendszerelemeket. A behozott és kivitt rendszerelemekről a Rendszergazda nyilvántartást vezet.

13. TERVEZÉS

13.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Az eljárásrend célja az információbiztonság biztosítása, a működés szabályozása és a felhasználói felelősség egyértelmű meghatározása a Hivatalon belül.

További célja a rendszerbiztonsági terv kidolgozása és végrehajtása, amely biztosítja a megfelelő védelmet az EIR számára.

Emellett meghatározza és rögzíti a viselkedési szabályokat, ideértve a közösségi média és külső webhelyek, alkalmazások használatára vonatkozó korlátozásokat is.

Felelős: IT vezető

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

BIZTONSÁGI TERVEZÉSI ELVEK

Biztonsági tervezésnél a következő elveket kell alkalmazni:

a) Rendszer integritás
A rendszernek ellenállónak kell lennie a rosszindulatú támadásokkal és a belső hibákkal szemben. A rendszerek és szolgáltatások integritását folyamatosan ellenőrizni kell, és biztosítani kell az adatok, rendszerek és hálózatok védelmét az illetéktelen módosítással szemben.

b) Védelem rétegezése
A biztonságot több rétegben kell beépíteni a rendszerbe, hogy a hibák és támadások egy rétegből a másikba való átterjedése ne legyen könnyen kivitelezhető. A rétegezésnek magában kell foglalnia a hálózati, rendszer- és alkalmazási szintű védelmi intézkedéseket.

c) Legkisebb jogosultság elve
A felhasználóknak csak azokat a jogosultságokat kell kapniuk, amelyek feltétlenül szükségesek a munkavégzéshez. A rendszereknek szigorú hozzáférési ellenőrzési mechanizmusokkal kell rendelkezniük, és a jogokat rendszeresen felül kell vizsgálni.

d) Biztonsági teljesítmény mérése
A rendszernek meg kell felelnie az alkalmazandó biztonsági előírásoknak és szabványoknak. A biztonsági intézkedések hatékonyságát rendszeresen ellenőrizni kell, és a szabványokkal való összhangot dokumentálni kell. Lásd 5. Értékelés, engedélyezés, monitorozás.

e) Rendszeres felülvizsgálat
A rendszer biztonsági intézkedéseinek hatékonyságát időről időre ellenőrizni kell, és szükség esetén módosítani kell őket. Az incidensek és sérülékenységek elemzésére rendszeres vizsgálatokat kell végezni, és az eredményeket dokumentálni szükséges. A dokumentálás a felülvizsgálatot végzők feladata.

BIZTONSÁGI KÖVETELMÉNYEK

A biztonság tervezésekor a következő követelményeknek kell megfelelni:

a) Azonosítás és hitelesítés

Biztosítani kell, hogy csak engedélyezett felhasználók férhessenek hozzá a rendszerhez, és azonosításuk és hitelesítésük megfelelő módon történjen. Kötelező az erős jelszavak használata, és lehetőség szerint többtényezős azonosítást kell használni.

b) Adatvédelem
A bizalmas és személyes adatokat megfelelő módon kell kezelni és védeni a jogellenes hozzáférés, megváltoztatás vagy elvesztés ellen. Szabályozni kell az adatok gyűjtését, tárolását, feldolgozását és megosztását, és megfelelő titkosítási és hozzáférési irányelveket kell követni a Hivatal belső irányelvei és szabályzatai alapján.

c) Hálózatbiztonság
A hálózati kommunikáció biztonságának meg kell felelnie a legfrissebb biztonsági szabványoknak és meg kell védenie a külső támadásoktól. Tűzfalakat, hálózati szegmentálást, IDS (intrusion detection) és IPS (intrusion prevention) rendszereket kell bevezetni, valamint szigorú hálózati forgalomellenőrzést szükséges alkalmazni.

d) Rendszerszintű biztonság
A rendszernek megfelelő védelemmel kell rendelkeznie a rosszindulatú szoftverek, a tűzfal áttörési kísérletek, a DDOS és bruteforce támadások, illetve más fenyegetések ellen. A rendszerfrissítéseket és javításokat rendszeresen kell végrehajtani, és telepíteni, és alkalmazni a legfrissebb biztonsági patcheket.

e) Rendszerfigyelés
Rendszeresen ellenőrizni kell a rendszer állapotát, hogy figyelmeztetéseket kaphasson a Hivatal a biztonsági incidensekről vagy rendszerhibákról. A logokat és az incidensek nyomon követését megfelelően dokumentálni szükséges, lehetőleg automatizált eszközöket kell használni a rendszerfigyelésre és a biztonsági incidensek időben történő azonosítására.

f) Vészleállítás
Biztosítani kell, hogy a rendszer vészhelyzet esetén gyorsan helyreállítható, az adatok elvesztése minimális legyen. Rendszer biztonsági tervet kell készíteni, amely tartalmazza a rendszeres adatmentést, a redundáns rendszerarchitektúra leírását és a vészleállítási teszteket.

BIZTONSÁGI TESZTELÉS

Rendszeresen kell biztonsági teszteket végezni a tervezési és fejlesztési folyamat során. Ezek magukban foglalhatják a sebezhetőségvizsgálatokat, sérülékenységi vizsgálatokat és biztonsági elemzéseket.

Évente, vagy gyakrabban kell sérülékenységi vizsgálatot végezni, hogy azonosítsuk a biztonsági sebezhetőségeket és az esetleges gyengeségeket a rendszerben. Ez lehetővé teszi a problémák korai azonosítását és a szükséges javítások végrehajtását a rendszerbiztonság javítása érdekében.

Ha lehetőség van rá, ellenőrizni kell a forráskódot is, hogy kizárjuk a biztonsági hibákat és sebezhetőségeket. A kódellenőrzési folyamat magában foglalhatja a statikus kódvizsgálatot, a manuális kódellenőrzést és az automatizált sebezhetőségi szkennereket.

DOKUMENTÁCIÓ ÉS KÉPZÉS

Rendszeresen dokumentálni kell a biztonsági tervezési és fejlesztési folyamatokat. Ez magában foglalhatja a rendszerterveket, biztonsági irányelveket, incidenskezelési eljárásokat és egyéb kapcsolódó dokumentációkat. Az aktuális dokumentációt mindig elérhetővé kell tenni az érintett felek számára úgy, hogy illetéktelenek viszont ne férhessenek hozzá.

Megfelelő képzést kell biztosítani az alkalmazottaknak a biztonsági politikák és eljárások megismerése érdekében. Az új alkalmazottaknak biztonsági oktatást kell kapniuk, és rendszeresen kell frissítő tréningeket tartani a biztonsági tudatosság növelése érdekében.

13.2. RENDSZERBIZTONSÁGI TERV

Az EIR-ekhez Rendszerbiztonsági tervet kell készíteni, amely tartalmazza az EIR

a) rendszerelemeit,
b) alapfeladatát
c) szolgáltatásait.

A tervnek a továbbiakban meg kell határoznia a kapcsolódó szerep- és felelősségi köröket, illetve az EIR által feldolgozott, tárolt és továbbított információk típusát. Ezek mellett tartalmaznia kell - megfelelően alátámasztott módon – a biztonsági osztályát és az EIR-t érintő fenyegetéseket.

Dokumentálni kell a következőket:

a) vonatkozó biztonsági követelmények (alap-, illetve, ha kell, akkor kiegészítő intézkedések)
b) vonatkozó biztonsági intézkedéseket és azok indoklását
c) biztonsági intézkedések végrehajtásának felelőseit, végrehajtóit.

Gondoskodni kell arról, hogy a tervet a felelősök tekintsék át és hagyják jóvá, valamint ismertessék meg mindazokkal, akik az EIR üzemeltetésében, vagy az esetleges vészhelyzeti koordinációban részt vesznek.

A Rendszerbiztonsági terveket a felelősöknek évente felül kell vizsgálni, és frissíteni, ha az EIR-ben, vagy annak üzemeltetési környezetében, változások történnek.

13.3. VISELKEDÉSI SZABÁLYOK

A Hivatal alkalmazottai munkájukból kifolyólag hozzáférést kapnak a Hivatal belső hálózatához. Az Intranet használatának kizárólagos célja a munkavégzés, a Felhasználó nem jogosult magáncélra használni a belső hálózatot.

A hálózat nem használható az alábbi módon, illetve az alábbi tevékenységekre:

- A hatályos magyar törvényekbe ütköző cselekmények.
- A hálózathoz kapcsolódó más - hazai vagy nemzetközi - hálózatok szabályaiba ütköző tevékenységek.
- A hálózat, illetve erőforrásai normális működését megzavaró, veszélyeztető tevékenység (idegen jelszó kiderítése saját és idegen hálózatban, idegen felhasználói név használata az illető tudomása nélkül).
- A hálózatot, illetve erőforrásait indokolatlanul vagy szándékosan túlzott mértékben, pazarló módon igénybe vevő tevékenység (pl. levélbombák, elektronikus játékok, online rádió).
- A hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, módosítása, törlése.
- A hálózat biztonságát veszélyeztető információk, programok terjesztése.
- Mások személyiségi jogait, vallási, etnikai, politikai vagy más jellegű érzékenységét sértő, másokat zaklató tevékenység (pl. pornográf anyagok közzététele).
- Mások munkájának indokolatlan és túlzott mértékű zavarása vagy akadályozása (pl. kéretlen levelek).
- Tilos az Interneten keresztül belső használatú, bizalmas vagy titkos dokumentumokat, adatokat a Hivatalból engedély nélkül kijuttatni, illetéktelen személyek részére hozzáférhetővé tenni.

A tiltott magatartási formák előkészítése, illetve kísérlete is szankcionálható.

TILTOTT TEVÉKENYSÉGEK

a) Tilos olyan tevékenységet végezni, amely célja mások adatainak jogosulatlan megszerzése, megváltoztatása, letörlése.
b) Tilos más felhasználók nevében tevékenykedni.

c) A Felhasználó nem teheti lehetővé mások számára, hogy a nevében tevékenykedjenek. Ezért – többek között – mindent meg kell tennie a jelszavai titkosságának megőrzése érdekében azért, hogy a személyazonosító eszközeit (például, de nem kizárólag: VPN kulcs, azonosító kártya, mobil telefon) más ne használhassa.
d) A Felhasználó köteles törekedni arra, hogy az általa pillanatnyilag használatba vett rendszerekben más személy az ő nevében ne fejthessen ki aktivitást.
e) Tilos más munkavégzését korlátozó tevékenységet végezni nem munka céljából kifejtett aktivitással.
f) Tilos a rendszer bármely elemének eredeti felhasználási céljától eltérő használata vagy az erre irányuló próbálkozás.
g) Tilos a Felhasználók számára a hálózati forgalom figyelése, erre alkalmas szoftver telepítése.
h) Tilos a Hivatal rendszergazdájától kapott IP címtől eltérő más IP cím jogosulatlan használata.
i) Tilos olyan anyag továbbítása, letöltése vagy közzététele az interneten, amely a Magyar- és az Európai Uniós törvényeket sérti.
j) Tilos a Hivatal belső EIR-én kívüli helyszínről elérni vagy megpróbálni elérni a rendszert, kivéve, ha erre az IT vezető engedélyt ad.
k) Tilos külső személy számára információt adni a rendszer valamely hibájáról, sebezhető pontjáról.
l) Tilos a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele.

13.4. VISELKEDÉSI SZABÁLYOK – KÖZÖSSÉGI MÉDIA ÉS KÜLSŐ WEBHELYEK, ALKALMAZÁSOK HASZNÁLATÁRA VONATKOZÓ KORLÁTOZÁSOK

A Hivatal alkalmazottai munkájukból kifolyólag hozzáférést kapnak az Internethez. Az Internet használatának kizárólagos célja a munkavégzés. A Felhasználó munkaidőben nem jogosult magáncélra használni a web elérését.

Az Internet nem használható az alábbi módon, az alábbi tevékenységekre:

- A Hivatal által nem jóváhagyott eszközökről és hálózatokról internetelérést igénybe venni. Tilos az engedély nélküli eszközök vagy személyes hálózatok használata.
- A hatályos magyar törvényekbe ütköző cselekmények, ideértve, de nem korlátozva azokra: mások személyiségi jogainak megsértése; tiltott haszonszerzésre irányuló tevékenység (pl. piramis-, pilótajáték); a szerzői jogok megsértése; szoftver szándékos és tudatos illegális terjesztése.
- A hálózathoz kapcsolódó más - hazai vagy nemzetközi - hálózatok szabályaiba ütköző tevékenységek, amennyiben ezek a tevékenységek ezen hálózatokat érintik.
- Profitszerzést célzó direkt üzleti célú tevékenység (pl. bérletöltés), reklámok terjesztése.
- A hálózat biztonságát veszélyeztető információk, programok terjesztése.
- Mások személyiségi jogait, vallási, etnikai, politikai vagy más jellegű érzékenységét sértő, másokat zaklató tevékenység (pl. pornográf anyagok közzététele).
- Tilos az üzleti titoknak minősülő vagy más érzékeny információk interneten történő megosztása. Az ilyen információkat csak a Hivatali rendszeren belül szabad tárolni és kezelni.

A közösségi hálózatokon való részvétel során kötelező tiszteletteljes és etikus viselkedést tanúsítani. Az online platformokon tilos olyan tartalmak közzététele, amelyek sértik vagy ártanak a Hivatal jó hírnevének. Vigyázzanak arra, hogy az online jelenlétük pozitív és támogató legyen a szervezeti értékeknek és szabványoknak megfelelően.

13.10. BIZTONSÁGI KÖVETELMÉNYEK KIVÁLASZTÁSA

Az EIR alapvető, minden rendszerre érvényes követelményei a következők:

HOZZÁFÉRÉSI ELLENŐRZÉS

Azonosítsa és hitelesítse az egyes felhasználókat vagy rendszerelemeket, és biztosítsa, hogy csak a jogosultak férjenek hozzá az adott erőforrásokhoz vagy funkciókhoz.

ERŐS HITELESÍTÉS

Követelje meg erős jelszavak használatát, és alkalmazzon kétlépcsős azonosítást az arra alkalmas rendszereknél.

TITKOSÍTÁS

Védje az érzékeny adatokat megfelelő titkosítási módszerekkel, hogy megakadályozza az illetéktelen hozzáférést.

RENDSZERFRISSÍTÉSEK

Rendelkeznie kell az alkalmazások, az operációs rendszer és egyéb szoftverek a legújabb biztonsági hibajavításaival és frissítéseivel.

NAPLÓZÁS ÉS NAPLÓVIZSGÁLAT:

Naplóznia kell a rendszereseményeket, beleértve a hozzáférési próbálkozásokat, hogy azonosítsa a potenciális fenyegetéseket vagy jogosulatlan tevékenységeket.

13.11. BIZTONSÁGI KÖVETELMÉNYEK TESTRE SZABÁSA

Ezen követelményeket minden EIR esetén egyedileg kell meghatározni.

14. SZEMÉLYI BIZTONSÁG

14.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed a Hivatal teljes személyi állományára, valamint minden olyan természetes személyre, aki a Hivatal EIR-rel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az EIR-rel tényleges vagy feltételezhető kapcsolatba kerülő személy nem a Hivatal alkalmazottja, a jelen fejezet szerinti elvárásokat a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).

A Hivatal minden alkalmazottjának titoktartási nyilatkozatot kell aláírnia, melyben nyilatkozik arról, hogy a munkája, tevékenysége során tudomására jutott, a Hivatal számára értéket jelentő információt sem jogviszonya fennállása idején, sem annak megszűnése után nem hozza harmadik fél tudomására.

A titoktartási nyilatkozat a munkaszerződés részét kell, hogy képezze, amelyről a Személyügyi ügyintézőnek kell gondoskodnia.

Felelős: Személyügyi ügyintéző, IBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, a Rendszergazdával, valamint a Személyügyi ügyintézővel minden esetben ismertetni kell.

14.2. MUNKAKÖRÖK BIZTONSÁGI SZEMPONTÚ BESOROLÁSA

A Hivatal minden munkakört, kapcsolódó feladatot biztonsági szempontból besorol, a besorolás 4 szintre tagozódik, melyek szorosan kapcsolódnak a szervezeti ábrához.

- Felhasználó (Alacsony biztonsági elvárások)
- Középvezető (Közepes biztonsági elvárások)
- Felső vezető (Magas biztonsági elvárások)
- Rendszergazda (Kiemelt biztonsági elvárások)

Az **alacsony biztonsági elvárásokkal** rendelkező felhasználók kizárólag a munkakörük ellátásához szükséges, minimális jogosultságokkal férhetnek hozzá az EIR-ekhez. Számukra elegendő az egyszerű hitelesítés, azonban érzékenyebb rendszerek esetén ajánlott a többtényezős azonosítás bevezetése. A tudatosság fenntartása érdekében évente kötelező részt venniük információbiztonsági képzésen, és nem rendelkeznek rendszerszintű jogosultságokkal vagy konfigurációs hozzáféréssel.

A **közepes biztonsági elvárások** szintjén lévő középvezetők számára már bővebb hozzáférés engedélyezett a vezetői döntésekhez és az irányított folyamatokhoz kapcsolódóan, de ez kizárólag a szükséges adatkörökre terjedhet ki. Emellett ők kötelesek betartani és betartatni az információbiztonsági előírásokat a beosztott munkavállalókkal is.

A **magas biztonsági elvárások szintjéhez tartozó** felső vezetők kiemelt stratégiai pozíciót töltenek be, ezért hozzáférésük általában széles körű, de elsősorban döntéshozatali és jelentésértékelési célokra korlátozódik. Esetükben a kétlépcsős azonosítás alkalmazása kiemelten javasolt, továbbá elengedhetetlen a rendszerhasználatuk folyamatos felügyelete, valamint a speciálisan számukra kialakított információbiztonsági képzések elvégzése, amelyek a kockázatok kezelésére, a jogszabályi megfelelésre és az irányítási kötelezettségekre fókuszálnak. Amennyiben biztonsági esemény merül fel, a felső vezetők kulcsszerepet kapnak az azonnali döntések meghozatalában és az incidensek megfelelő szintű kezelésében.

A **rendszergazdák** munkája különösen érzékeny biztonsági területnek számít, mivel tevékenységük során közvetlen hozzáféréssel rendelkeznek a Hivatal rendszereinek mélyebb rétegeihez, beleértve az operációs rendszereket, konfigurációs beállításokat és forráskódokat. Mivel ezek a szerepkörök jelentős kockázatot hordoznak, ezért kiemelten szigorú kontrollokat kell alkalmazni velük szemben. A munkavégzésük megkezdése előtt nélkülözhetetlen az előzetes megbízhatósági vizsgálat lefolytatása, amelynek célja annak ellenőrzése, hogy a személy megbízhatóan láthat-e el ilyen típusú munkakört. Minden rendszerszintű hozzáférésüket részletesen naplózni kell, kizárólag titkosított kommunikációs csatornák használata engedélyezett, és ahol lehetséges, ott minden hozzáféréshez többtényezős hitelesítés) alkalmazása kötelező annak érdekében, hogy illetéktelen hozzáférés ne történhessen.

A Hivatalnál az egyes pozíciók részletes biztonsági szempontú besorolása és dokumentálása a Személyügy feladata.

A Hivatal bármely munkaviszony keletkeztetésekor felméri a nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat.

A Hivatal évente felülvizsgálja és frissíti a munkakörök és feladatok biztonság szempontú besorolását.

14.3. SZEMÉLYEK HÁTTÉRELLENŐRZÉSE (A6.1)

ELŐZETES ELLENŐRZÉS

A munkaerő felvétel részét képezi, hogy a Hivatal a személyi állományba jelentkezőn háttérellenőrzés végez. Ezen ellenőrzésnek a részét képezik a következők:

- Személyazonosság-ellenőrzés
- Végzettség és képesítések ellenőrzése
- Munkatapasztalat-ellenőrzés.
- A megadott referenciák felkeresése és véleményük kikérése a jelölt munkavégzéséről és megbízhatóságáról.
- A jelölt közösségi média profiljainak ellenőrzése a nyilvánosan elérhető információk alapján.

ELLENŐRZÉS HOZZÁFÉRÉSI JOGOSULTSÁGOK MEGADÁSA ELŐTT

A Hivatal az EIR-hez való hozzáférési jogosultság megadása előtt ellenőrzi, hogy az érintett személy a besorolásnak megfelelő feltételekkel rendelkezik-e. Ezen feltételek ismételt vizsgálata szükséges, amennyiben a személy jogosultsági szintje, munkaköre változik.

A Hivatal tevékenysége, a kezelt adatok és rendszerek jellege alapján nem indokolt az előzetes háttérellenőrzést követően a személyek ismételt háttérellenőrzése.

14.5. SZEMÉLYEK MUNKAVISZONYÁNAK MEGSZŰNÉSE (A6.5)

A jogviszony megszüntetésekor a következő feladatok végrehajtása szükséges.

HOZZÁFÉRÉSEK MEGSZÜNTETÉSE

A jogosultságok megszüntetésének normál folyamata, hogy a kilépő alkalmazottakról a Személyügy írásban értesíti a Rendszergazdát, amely megszünteti a kilépő alkalmazottak jogosultságait.

A hozzáférési jogosultságok megszüntetésével egyidejűleg az elektronikus belépőkártyák jogosultságát is meg kell szüntetni, függetlenül attól, hogy a belépőkártya visszaadásra került-e, vagy sem.

A jogosultságok megszüntetéséért a hálózati szinten a Rendszergazda, rendszereken belül a kulcsfelhasználó a felelős.

HOZZÁFÉRÉSI JOGOK VISSZAVONÁSA FELADATKÖR VAGY MUNKAKÖR VÁLTOZÁS ESETÉN:

A munkavállaló feladatkörének vagy munkakörének változás esetén a munkahelyi vezetőnek haladéktalanul intézkednie kell a már nem szükséges jogosultságok visszavonása iránt. Ez esetben is - az új jogosultság igényléséhez kell folyamodni. A jogosultság igénylésben jelölni kell, hogy mely jogosultságokat kell megszüntetni. A jogosultságok részleges visszavonásának eljárásrendje egyéb tekintetben megegyezik az új jogosultsági igény eljárásendjével.

A munkahelyi vezetőnek haladéktalanul intézkednie kell a már nem szükséges jogosultságok visszavonása iránt.

HOZZÁFÉRÉSI JOGOK VISSZAVONÁSA RENDES FELMONDÁS ESETÉN:

Ha a Hivatal alkalmazottjának munkaviszonya rendes felmondás keretein belül megszűnik, erről a tényről a közvetlen felettesének, illetve a Személyügynek haladéktalanul tájékoztatást kell nyújtania az IT vezetőnek. A Rendszergazda a jelzett időponttal gondoskodik a Felhasználó összes rendszerhozzáférésének adott időpontban történő megszüntetéséről vagy letiltásáról, illetve ezek kezdeményezéséről. A munkaviszonyt lezáró dokumentumok között szerepeltetni kell a jogosultságok megszűnéséről szóló tájékoztatást, ebben integráltan egy figyelmeztetést a jogosulatlan belépés, vagy annak kísérletének jogi következményeiről.

HOZZÁFÉRÉSI JOGOK VISSZAVONÁSA RENDKÍVÜLI FELMONDÁS ESETÉN:

Amennyiben a munkavállaló munkaviszonya rendkívüli felmondással kerül megszüntetésre, akkor jogosultságainak megszüntetéséről haladéktalanul gondoskodni kell.

Ennek érdekében a felmondást aláíró vezetőnek haladéktalanul tájékoztatnia kell az IT vezetőt. az IT vezető tájékoztatásáért egyetemlegesen felel a felmondást szignáló személy és a Személyügy. A Rendszergazdának haladéktalanul gondoskodnia kell az illetéktelen hozzáférés megakadályozásáról. A munkavállalónak azonnal írásos tájékoztatást kell kapnia jogosultságai megszűnéséről, és a belépési kísérletek következményeiről.

HITELESÍTŐ ESZKÖZÖK ÉRVÉNYTELENÍTÉSE

A Hivatal a munkaviszony, vagy a szerződéses jogviszony megszűnésekor érvényteleníti vagy visszaveszi a személy egyéni hitelesítő eszközeit. A visszavétel tényét a munkaviszonyt lezáró dokumentumok között szerepeltetni kell.

TÁJÉKOZTATÁS

A Hivatal tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről (Titoktartás stb.)

ESZKÖZÖK VISSZAVÉTELE (A5.11)

A Hivatal visszaveszi az EIR-rel kapcsolatos, tulajdonát képező összes eszközt. A visszavétel tényét a munkaviszonyt lezáró dokumentumok között szerepeltetni kell.

A vagyontárgyakkal el kell számolni. A munkahelyi vezetőnek e-mailben kell igényelnie a leadott informatikai eszközök ellenőrzését és az eszközön lévő felhasználói adatok, email fiókok tartalmának mentését.

A bejelentés alapján a Rendszergazdának ellenőriznie kell, hogy az eredeti, rögzített hardver és szoftver specifikációval adják-e vissza az informatikai eszközöket.

FELADATOK ÁTADÁSA

A kilépő alkalmazott munkahelyi vezetőjének feladata, hogy az alkalmazott EIR-rel, vagy azok biztonságával kapcsolatos esetleges feladatainak ellátásáról a munkaviszony megszűnését megelőzően gondoskodjon.

ÉRTESÍTÉS

A Hivatal az általa meghatározott módon a jogviszony megszűnéséről értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket.

TITOKTARTÁS (A6.6)

A Hivatal a jogviszonyt megszüntető személy EIR-rel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik.

Tájékoztatni kell a munkavállalót, hogy a Hivatal EIR-nek használata során a tudomására jutott minden információ bizalmas adatnak minősül, azok illetéktelen, harmadik fél részére történő továbbadása büntetőjogi, illetve polgári jogi következményeket von maga után és a munkavállaló titoktartási kötelezettsége a munkaviszonya megszűnése után is fennáll.

A munkavállaló tájékoztatásáért a Személyügy a felelős.

JOGSÉRTÉSEK MEGELŐZÉSE

A Hivatal a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges EIR-t, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását minden eszközzel megelőzi.

14.8. AZ ÁTHELYEZÉSEK, ÁTIRÁNYÍTÁSOK ÉS KIRENDELÉSEK KEZELÉSE

A Hivatal az EIR-hez való hozzáférési jogosultság megadása előtt ellenőrzi, hogy az érintett személy besorolásnak megfelelő feltételekkel rendelkezik-e.

Amennyiben igen, úgy logikai és fizikai hozzáférést engedélyez az újonnan használni kívánt EIR-hez, figyelembe véve a szükségesség elvét. Szükség szerint módosítani kell a hozzáférési jogosultságot, hogy az megfeleljen az áthelyezés vagy átirányítás miatt bekövetkező változásoknak.

Végül a Szervezeti és Működési Szabályzatban meghatározott módon a jogviszony változásáról értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket.

14.9. HOZZÁFÉRÉSI MEGÁLLAPODÁSOK

A Hivatal EIR-hez kizárólag olyan munkatárs kaphat hozzáférést, akinek a munkájához szükséges az EIR használata, és aki megismerte és dokumentáltan elfogadta a rendszerre vonatkozó hozzáférési szabályokat, valamint aki eleget tesz a szabályzat 2.2 pont a-d feltételeinek. Azon felhasználók, akik nem a Hivatal alkalmazottjai csak az IT vezető tudtával és jóváhagyásával kaphatnak hozzáférést. Csak valós, aktív munka- vagy szerződéses viszonyban álló személyeket lehet regisztrálni a rendszerben.

A jogosultságok kezelésekor alapelvként kell érvényesíteni, hogy csak a felhasználók feladatellátásához szükséges és elégséges mértékű jogosultságok biztosíthatók.

A Hivatal nem vizsgálja felül a hozzáférési megállapodásokat, mert az információk, adatok, EIR-ek kritikussága ezt nem teszi szükségessé.

14.11. KÜLSŐ SZEMÉLYEKHEZ KAPCSOLÓDÓ BIZTONSÁGI KÖVETELMÉNYEK

A Hivatal a külső szolgáltatókkal, egyéb szervezetekkel kötött megállapodásban, szerződésben megköveteli, hogy a külső szervezet határozza meg az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is.

A külső partnerek képviselőivel a mindenkor hatályos IBSZ vonatkozó részeit a feladatnak megfelelő mértékben ismertetni kell. A betekintés mélységének meghatározása az Adatgazda felelőssége. A szerződéskötés és az együttműködés során biztosítani kell, hogy a külső partner (fejlesztő cég) az általa telepített, fejlesztett EIR-t úgy konfigurálja, hogy annak minden eleme és egésze eleget tegyen az IBSZ-ben előírtaknak.

A Hivatal előírja, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik a Hivatal EIR-éhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor azonnal küldjön értesítést az IT vezetőnek, aki megteszi a szükséges intézkedéseket (jogosultságok visszavétele).

A Hivatal folyamatosan ellenőrzi a szerződő féltől megköveteli a személybiztonsági követelményeknek való megfelelését.

14.12. FEGYELMI INTÉZKEDÉSEK (A6.4)

Az IBSZ bárki által történő megszegését az észlelő haladéktalanul köteles jelenteni az IBF-nek.

A Hivatal a felhasználók részéről szándékos károkozásnak tekinti az alábbi tevékenységeket:

- behatolást az EIR környezetébe;
- illetéktelen hozzáférést az adatokhoz, eszközökhöz;
- adatok, eszközök eltulajdonítását, visszaélésszerű felhasználását;
- megtévesztő adatok bevitelét és képzését;
- eszközök, adathordozók megrongálását, működésük, használhatóságuk korlátozását;
- feldolgozások és munkafolyamatok zavarását, késleltetését;
- vírusfertőzött adathordozó szándékos behozatalát, vírusfertőzés előidézését;
- illegális szoftverek telepítését;
- a törvények és szabályok tudatos vagy szándékos megsértését.

A Hivatal gondatlan károkozásnak tekinti az alábbiakat:

- figyelmetlenséget, az ellenőrzés elmulasztását;
- szakmai hozzá nem értést, a kötelezően elvárható gondosság és előrelátás hiányát, elmulasztását;
- megváltozott működési körülményeknek figyelmen kívül hagyását;
- biztonsági követelmények és gyári előírások be nem tartását;
- adathordozók megrongálódását az előírásoktól eltérő tárolás és kezelés miatt;
- karbantartási műveletek elmulasztását;
- biztonsági-, jelző- és riasztóberendezések karbantartásának elhanyagolását;
- eszköz és eljárásbeli biztosítékok EIR-be történő beépítésének elhanyagolását.

Az IBF a tudomására jutott események súlyosságát mérlegeli, és szándékos, illetve gondatlan károkozás esetén jelenti az IT vezetőnek.

Az információbiztonsági előírások megsértőivel szemben fegyelmi felelősségre vonásra kerülhet sor. Az eljárást a jogszabályok és a Hivatal belső szabályzatai szerint kell lefolytatni.

A Hivatal belső eljárási rendje szerint fegyelmi eljárást kezdeményez az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben.

Ha az elektronikus információbiztonsági szabályokat nem a Hivatal személyi állományába tartozó személy sérti meg, érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések fennállásának lehetőségét, szükség szerint bevezeti ezeket az eljárásokat.

14.13. MUNKAKÖRI LEÍRÁSOK

A Személyügy gondoskodik arról, hogy a biztonsági szerepköröknek és felelősségek bele legyenek foglalva a munkaköri leírásokba.

15. KOCKÁZATKEZELÉS

15.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend célja a biztonsági osztályba sorolás meghatározása majd a kockázatértékelés végrehajtása, beleértve az ellátási lánc kockázatainak elemzését is. Emellett biztosítja a sérülékenységmonitorozást és -szkennelést, beleértve a privilegizált hozzáférés is. Az eljárásrend része a kockázatokra adott válasz kidolgozása és a rendszerelemek kritikusságának elemzése, hogy a Hivatal hatékonyan reagálhasson a felmerülő biztonsági fenyegetésekre.

Felelős: IBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, a Rendszergazdával, valamint a Kockázati szereplőkkel (1.7.2.) minden esetben ismertetni kell.

15.2. BIZTONSÁGI OSZTÁLYBA SOROLÁS

A Hivatal a jogszabályban meghatározott szempontok alapján megvizsgálja EIR-eit, és a EIR nyilvántartás alapján meghatározza, hogy azok melyik biztonsági osztályba sorolandók.

A Hivatal vezetője kizárólagosan hagyja jóvá a biztonsági osztályba sorolást.

15.4. KOCKÁZATÉRTÉKELÉS

KEZDETI HELYZETFELMÉRÉS

Az EIR kockázatelemzésének elvégzéséhez fel kell mérni, meg kell ismerni az EIR-t és a jelenlegi információbiztonsági állapotát.

A rendszer funkciójának és – esetleg szenzitív – adattartalmának megismerésén túl – a következő területeket kell a dokumentációk bekérésével, illetve szakmai interjúk lefolytatásával megismerni:

ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

- a Hivatalra vonatkozó jogszabályok, szabályzatok;
- az EIR-re vonatkozó szabályzatok;
- üzemeltetési eljárások;
- ellátási lánc, szerződések, külső partnerek kezelése;
- biztonsági események kezelése;

FIZIKAI VÉDELMI INTÉZKEDÉSEK

- beléptetés;
- az épületben történő közlekedés;
- a szerverterem kialakítása;
- az irodák kialakítása;
- a tiszta asztal, üres képernyő politika alkalmazása.

LOGIKAI VÉDELMI INTÉZKEDÉSEK

- szoftverfejlesztés, változáskezelés;

- a szervizelés, eszközcsere, selejtezés folyamata;
- mentési megoldások;
- a jogosultsági rendszer, a jogosultságigénylés folyamata;
- vírusok és egyéb kártevők elleni védekezés;
- biztonsági frissítések telepítése;
- naplózás, biztonsági rendszerek;
- a hálózat felépítése;
- kriptográfiai (titkosítási) megoldások.

KOCKÁZATOK AZONOSÍTÁSA

GYENGE PONTOK MEGHATÁROZÁSA, KOCKÁZAT MEGNEVEZÉSE

A helyzetfelmérés alapján megszerzett információk birtokában azonosítani kell a kockázat által érintett EIR-t, vagy kontrollt [*VPH_Kockázat-menedzsment*] elnevezésű táblázat (a továbbiakban: *Táblázat) „B" oszlop*, majd röviden le kell írni az adott kockázatot, vagy gyenge pontot (*Táblázat „C" oszlop*).

A gyenge pontok meghatározásánál figyelembe kell venni

a) a jogosulatlan hozzáférés, használat, közzététel, zavarás, módosítás vagy a rendszer megsemmisítésének valószínűségét és káros hatásait az általa feldolgozott, tárolt vagy továbbított információkra és minden kapcsolódó információra vonatkozóan;

b) a személyes adatok feldolgozásából eredő, egyénekre vetített kedvezőtlen hatások valószínűségét és mértékét;

c) az ellátási lánc zavarával, vagy megszakadásával kapcsolatos kockázatokat az adott rendszer szolgáltatásai és rendszerelemei vonatkozásában;

d) a biztonsági értékelések, ellenőrzések és vizsgálatok megállapításait.

FENYEGETŐ TÉNYEZŐK ELEMZÉSE

Meg kell vizsgálni, hogy a fellelt gyenge pontot mely fenyegető tényezők használhatják ki, illetve az adott kockázatot mely fenyegető tényezők okozzák, és azokat a *Táblázat „Fenyegetés" („E") oszlopából* ki kell választani. Ezzel automatikusan kiválasztható az is, hogy az adott Fenyegetés mely információbiztonsági alapelvet érinti (Bizalmasság, Sértetlenség, Rendelkezésre állás, *Táblázat „G" oszlop, Érintett alapelvek*).

BEKÖVETKEZÉS VALÓSZÍNŰSÉGÉNEK MEGHATÁROZÁSA

A bekövetkezés valószínűségét több tényező is meghatározhatja, ezeket meg kell becsülni. Minden esetben figyelembe kell venni a fenyegető tényező kategóriáját (Emberi, Üzleti, Informatikai, Környezeti, Fizikai), mert lehetnek az adott geológiai lokáción jellemzőbb fenyegetések (pl.: vízkár egy árterületen), illetve

kevésbé jellemző fenyegetések (pl.: adatvesztés egy többszörösen biztosított adatmentési rendszerrel ellátott szervezet esetén, ahol másodlagos feldolgozási helyszín és alternatív tárolási helyszín is van).

A felmérésbe bele kell kalkulálni a következő szempontokat:

a) a motiváció (a lehetséges támadók erőforrásai, az informatikai rendszer vagyontárgyainak a lehetséges támadók által érzékelhető vonzereje, sebezhetősége)

b) az értékelendő földrajzi tényezők (pl. vegyi- és üzemanyag gyárak közelsége, szélsőséges időjárási viszonyok valószínűsége, és olyan tényezők, amelyek befolyással lehetnek az emberi tévedésekre és a berendezések hibás működésére, a véletlenszerű fenyegetési források tekintetében)

c) az emberi tényező, mint az egyik legnagyobb probléma kiváltó ok a fenyegetések bekövetkezésének valószínűségében

Továbbá figyelembe kell venni az évek tapasztalatából az eddigi előfordulásokat is, így a következő kategóriákat lehet használni a bekövetkezés valószínűségének meghatározására:

0. N/A – a Hivatalnál az adott kockázat (már) nem tudja kifejteni a hatását
1. nem valószínű – négy évnél ritkábban, esetileg, kis számban és/vagy esetleges valószínűséggel becsülhető az esemény bekövetkezése
2. ritka – háromévente számottevő gyakorisággal és/vagy valószínűséggel fordul elő az adott esemény
3. közepesen valószínű – kétévente számottevő gyakorisággal és/vagy valószínűséggel fordul elő az adott esemény
4. valószínű – egy éven belül többször és/vagy nagy valószínűséggel becsülhető az esemény bekövetkezése
5. majdnem biztos – félévente, vagy akár havi szinten is problémát jelenthet

KOCKÁZAT ÉRTÉKELÉSE

LEHETSÉGES KÖVETKEZMÉNY

Fel kell mérnünk, hogy milyen következményekkel jár az adott kockázat a Hivatalra nézve. Első lépésben leíró módszerrel röviden ki kell fejteni a lehetséges következményt (*Táblázat „H" oszlop*).

KÁRÉRTÉK SZINTEK MEGHATÁROZÁSA

A bekövetkezett káresemény súlyosságának, mértékének jellemzésére a következő kárérték szintek kerültek kialakításra:

1. Elenyésző;
2. Kicsi;
3. Közepes;
4. Nagy;
5. Extrém;

A kárérték szintek meghatározása során azt kell figyelembe venni, hogy

a) milyen tényleges vagy erkölcsi kárt jelentene a rendszerben tárolt adatok bizalmasságának sérülése;
b) milyen következményekkel járna a rendszer ideiglenes elérhetetlensége vagy az adatok sérülése, elvesztése;
c) mennyibe kerülne a meghibásodott eszközök javítása, cseréje;
d) mennyi munkaidő ráfordítással járna a helyreállítás.

KOCKÁZATOK MEGHATÁROZÁSA

Az információbiztonsági kockázatokat a fenyegetés bekövetkezésének a valószínűsége és az okozott kárt jellemző kárérték szint *szorzata* fogja megadni.

A kockázatok nagyságának, értékének meghatározásához a következő kockázati mátrixot kell használni:

Kárérték	Alacsony	Közép-alacsony	Közepes	Közép-magas	Magas
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

Bekövetkezés valószínűsége

A táblázatban a kockázatok jelentése a következő:

a) 1 – 2 Alacsony;
b) 3 – 5 Közép-alacsony;
c) 6 – 11 Közepes;
d) 12 – 16 Közép-magas;
e) 17 – 25 Magas;

NEM TOLERÁLHATÓ KOCKÁZATOK MEGHATÁROZÁSA

A Hivatal azt a döntést hozta, hogy minden Közép-alacsonynál magasabb kockázatot kezelni kíván.

Ennek megfelelően a toleranciamátrix a következő:

Kárérték	Alacsony	Közép-alacsony	Közepes	Közép-magas	Magas
5	T	T	NTH	NT	NT
4	T	T	NTH	NTH	NT
3	T	T	T	NTH	NTH
2	T	T	T	T	T
1	T	T	T	T	T
	1	2	3	4	5

Bekövetkezés valószínűsége

A táblázatban alkalmazott jelölések értelmezése a következő:

a) T – Tolerálható;
b) NTH – Nem tolerálható, hosszú távon kockázatkezelést igényel;
c) NT – Nem tolerálható, azonnali kockázatkezelést igényel.

PRIORITÁS MEGHATÁROZÁSA

A Hivatalnak lehetősége van arra, hogy önállóan is meghatározza egy-egy kockázat Szervezetre gyakorolt hatását, így priorizálva a megoldandó kockázatokat. Minél magasabb a prioritás, annál hamarabb szükséges foglalkozni egy adott kockázattal.

A prioritások a következők lehetnek:

a) **Alacsony** - *Nem szükséges azonnal* foglalkozni vele

b) **Közepes** – A *közeljövőben* megoldást kell találni
c) **Magas** - *Azonnali* válaszlépéseket igényel (most kell vele foglalkozni)

15.5. KOCKÁZATÉRTÉKELÉS – ELLÁTÁSI LÁNC

A Hivatal rendszeresen felméri az ellátási lánc kockázatait is, különös tekintettel a meghatározott EIR-ekre, rendszerelemekre és rendszerszolgáltatásokra.

A Hivatal az ellátási lánc kockázatelemzését felülvizsgálja és frissíti az alábbi esetekben:

- meghatározott időközönként;
- ha jelentős változások következnek be az érintett ellátási láncban;

vagy ha a rendszer, a működési környezet, illetve más körülmények változása indokolttá teheti az ellátási lánc módosítását.

Az ellátási láncban részt vevő szolgáltatók, fejlesztők, beszállítók évente legalább egyszer értékelésre kerülnek. Az értékelés során vizsgálni kell:

- kritikusság a Hivatal szempontjából
- biztonsági tanúsítványokat (pl. ISO 27001, SOC 2),
- szolgáltatási szintet (SLA),
- adatkezelési és hozzáférési feltételeket,
- incidenskezelési képességeket.

A beszállítók kockázati besorolása lehet

- Kiemelkedő: tanúsított, megbízható, stabil partner, bizonyított információbiztonsági megfeleléssel.
- Megfelelő: stabil, megbízható partner, tanúsítvány nélkül, de elfogadható biztonsági gyakorlatokkal és pozitív együttműködési tapasztalattal.
- Feltételes: működése stabil, de biztonsági dokumentáltsága hiányos vagy részben igazolt; további ellenőrzés, kockázatcsökkentő intézkedés szükséges.
- Kockázatos: alacsony bizalmi szintű, korlátozott átláthatóságú partner, kritikus rendszerhez vagy adathoz hozzáféréssel, megfelelő szerződéses biztosíték nélkül.
- Veszélyes: kritikus rendszerhez vagy adathoz hozzáférő partner, aki nem rendelkezik igazolt információbiztonsági megfeleléssel; együttműködés kizárólag kockázatkezelési terv mellett engedhető.

15.9. SÉRÜLÉKENYSÉGEK ELLENŐRZÉSE

A Rendszergazdának rendszeres időközönként, vagy eseti jelleggel amikor ezen sérülékenységekről tudomást szerez, ellenőriznie és javítania kell az EIR-ek sérülékenységeit.

Kritikus/magas kategória: Az elvárt javítási idő 30 napon belül, utóvizsgálat kötelező.

Közepes/alacsony kategória: kockázatalapú ütemezési terv készítése szükséges. Ezt dokumentálni kell a Kockázatmenedzsment táblázatban.

15.18. SÉRÜLÉKENYSÉGMENEDZSMENT – SÉRÜLÉKENYSÉGI INFORMÁCIÓK FOGADÁSA

Ki kell alakítani egy dedikált kommunikációs csatornát (pl: e-mail), amely lehetővé teszi a szervezeti EIR-ekben és rendszerelemekben észlelt sérülékenységekről szóló jelentések fogadását.

15.20. KOCKÁZATOKRA ADOTT VÁLASZ

A Hivatal a kockázatokra többféle válaszlépést adhat. Ezen válaszlépések a következők lehetnek:

Elfogadás

A Hivatal úgy döntött, hogy nem tud azonosítani megfelelő válasz-stratégiát, vagy az aránytalanul költséges lenne. A kockázati fenyegetések esetében nem minden esetben szükséges a csökkentés vagy átruházás, különösen azoknál, amelyeknek alacsony a súlya. A Hivatalnak kell megítélni, hogy szigorúbb (és potenciálisan költségesebb) válaszstratégiát alkalmaz-e.

Megosztás

A Hivatal megosztja a kockázatot részben, vagy akár teljes egészében egy másik féllel, aki azt a legjobban képes kezelni.

Mérséklés

Cél a kockázat valószínűségének és/vagy hatásának csökkentése egy elfogadható küszöb alá. Ennek fajtái lehetnek:

- Megelőző jellegű intézkedések (preventív kontrollok):

A hibák, sérülékenységek, gyenge pontok, illetve ezek kihasználására való lehetőségek kiküszöbölése.

- Korlátozó vagy javító intézkedések (korrektív kontrollok):

A veszélyek hatását csökkentő, enyhítő óvintézkedések, további tevékenységek szükségessége nélkül.

- Észlelő és reagáló intézkedések (detektív kontrollok):

A sérülékenységek, gyenge pontok támadásának észlelése, ártalmas kihatások enyhítésére, illetve válaszreakciók kidolgozása.

Átruházás

A Hivatal átruházza a fenyegetést egy másik félre, aki a legjobban képes minimalizálni a kockázat hatását és/vagy valószínűségét. (pl.: biztosítás kötése, vagy tevékenység kiszervezése, megfelelő beszállítói szerződések megkötése)

Elkerülés

A Szervezt úgy módosítja a jelenlegi tényezőket, hogy megszüntesse a kockázatot vagy megvédje magát annak hatásaitól (pl.: érintett tevékenység megszüntetése)

SZÜKSÉGES INTÉZKEDÉSEK LEÍRÁSA

Ha a Hivatal már felmérte a kockázatokat és úgy döntött, hogy kezelni fogja, akkor meg kell határozni, hogy milyen intézkedések szükségesek a kockázatok kezeléséhez. Ezen intézkedéseket szöveges formában fel kell jegyezni a Táblázat „M" oszlopában a „Szükséges intézkedések leírása" -nál.

A KOCKÁZATFELELŐS

Minden azonosított kockázathoz, amellyel a Hivatalnak foglalkozni kell, szükséges egy ún. Kockázatfelelős hozzárendelése. Ő lesz a felelős azért, hogy a hozzárendelt kockázatokat értékelje, felügyelje és kezelje. A Táblázat „O" oszlopába kell kerülnie.

A HATÁRIDŐ

A Hivatalnak meg kell határoznia, hogy milyen időintervallumon belül hajtja végre a kockázat kezeléséhez szükséges intézkedéseket. Ehhez az „N" oszlopot, a „Határidő" -t kell igénybe venni.

KÉSZENLÉTI TERV

A készenléti terv olyan dokumentum, amely meghatározza, hogy hogyan kell cselekedni váratlan események, vagy válsághelyzetek esetén. Ha a kockázatelemzés részeként elkészítették az esetleges kockázatok és veszélyforrások azonosítását, akkor a készenléti terv ezen felismerésekre építve kínálhat cselekvési tervet az esetleges problémákra. Jelentősen befolyásolhatja egy kockázat mértékét, ha rendelkezünk megfelelő készenléti tervvel.

FIGYELÉS- ÉS FELÜGYELET (KOCKÁZAT-MONITORING)

STÁTUSZ ÉS FRISSÍTÉS

Minden kockázathoz tartozik egy státusz, egy állapot, amely azt mutatja, hogy a jelenleg milyen folyamatok történtek (illetve történtek-e) az adott kockázat kezelésével kapcsolatban, vagy azt már lezártnak tekinthetjük.

Jelen módszertan ötféle státuszt különböztet meg, ezek a következők:

1. Aktív (nem indult)
   A Hivatal azonosított és értékelt egy kockázatot, de jelenleg még választerv nincs, illetve válaszlépéseket nem foganatosított. A kockázatot mindemellett aktívan figyelik és ellenőrzik.
2. Aktív (folyamatos)
   A Hivatal az azonosított kockázatot aktívan figyeli és a válaszlépések folyamatban vannak.
3. Aktív (teljesült)
   A Hivatal az azonosított kockázatot aktívan figyeli, a válaszlépések már lezárultak.
4. Alvó (nem indult)
   Az adott kockázat jelenleg nem kiemelt prioritás, de a jövőben aktívvá válhat.
5. Lezárt (teljesült)
   A kockázat a kockázatkezelő intézkedéseknek (vagy egyéb tényezők változásainak) köszönhetően többé nem jelent veszélyt a Hivatalra nézve.

A státuszhoz szervesen kapcsolódik az utolsó frissítés dátuma, amely az időpontot jelöli, amikor utoljára frissítették, vagy felülvizsgálták a kockázatok státuszát a kockázatkezelési rendszerben.

Ennek a dátumnak több szerepe is lehet:

- ***Aktualitás*** - Az utolsó frissítés dátuma azt jelzi, hogy a kockázatokkal kapcsolatos információk naprakészek és aktuálisak-e. Ezzel segít biztosítani, hogy a döntéshozók mindig a legfrissebb adatokkal rendelkezzenek a kockázatok állapotáról.
- ***Nyomon követés*** - A dátum nyomon követése lehetővé teszi a Hivatal számára, hogy lássa, milyen gyakran ellenőrzik és frissítik a kockázatokat. A rendszeres frissítések fontosak a változó kockázati környezet kezelése és a hatékony válaszok biztosítása érdekében.
- ***Döntéshozatali támogatás*** - Az aktuális kockázatstátusz a döntéshozatal alapja lehet. Az utolsó frissítés dátuma segíthet a döntéshozóknak abban, hogy megbecsüljék, milyen régi vagy friss az információ, és hogy szükség lehet-e további vizsgálatokra vagy frissítésekre.

NYOMON KÖVETÉS, KAPCSOLÓDÓ MEGJEGYZÉSEK

Az eddig elvégzett kockázattal, illetve kockázatkezeléssel kapcsolatos tevékenységeket kell a Táblázat „S" oszlopába leíró formában feljegyezni. Ez is szervesen kapcsolódik a Státuszhoz, hiszen a Kockázatfelelős itt fejti ki részletesebben a kockázattal kapcsolatos fejleményeket.

Azáltal, hogy rendszeresen rögzítik és nyomon követik a kockázatokkal kapcsolatos megjegyzéseket, a Hivatal képes marad reagálni a változó kockázati környezetre és hatékonyabban kezelni a potenciális kockázatokat. Itt

dokumentálják a változásokat, melyek megkönnyítik a nyomon követést, illetve döntéstámogatási, döntéselőkészítési szerepük van.

EREDMÉNYEK ÉRTÉKELÉSE

A kockázatok kezelésének hatékonyságát azok lezárásáig éves szinten, vagy változások esetén (pl: státuszmódosítás) értékelnünk kell. Az értékelésnek szöveges formában a „T" oszlopba kell kerülnie.

Minden esetleges változást, vagy változtatást jelezni kell a Kockázatkezelési vezetőnek.

KOCKÁZATELEMZÉS-JELENTÉS

A jelentés célja, hogy összefoglalja az azonosított kockázatokat, értékelje azokat, és ajánlásokat tegyen a kockázatok kezelésére. A kockázatelemzés-jelentésnek az érintett felek számára könnyen érthetőnek és áttekinthetőnek kell lennie, és az ajánlásoknak konkrétnak és végrehajthatónak kell lenniük.

Évente legalább egy alkalommal összefoglaló jelentést kell készíteni a nem lezárt kockázatokról.

FELELŐSSÉGEK ÉS FOLYAMATOK A KOCKÁZATKEZELÉS KAPCSÁN (RACI MÁTRIX)

Engedélyezési folyamat	IBF	Szervezet vezetője	Kockázat-menedzser	IT vezető Rendszergazda	Folyamatgazda munkahelyi vezető	Belső ellenőrzés auditor	Érintett munkatárs
Új kockázat azonosításának jóváhagyása	R	A	C	I	C	I	I
Kockázatértékelés eredményének elfogadása	R	A	C	I	C	I	I
Kockázatkezelő intézkedés végrehajtásának jóváhagyása	R	A	C	C	R	I	I
Maradványkockázat elfogadása	C	A	R	I	C	I	I
Kivételek engedélyezése	R	A	C	I	C	I	I
Kockázatkezelési folyamat módosításának jóváhagyása	R	A	C	I	C	C	I
Kockázatelemzési jelentések	R	A	C	I	C	I	I

IBF: felelős az információbiztonsági megfelelésért, dokumentációért, és az engedélyezési folyamat koordinálásáért.

Szervezet vezetője: végső döntéshozó és felelős a maradvány-kockázatok elfogadásáért.

Kockázatmenedzser: az értékelések és kockázatkezelési tervek szakmai felelőse.

IT vezető / rendszergazda: technikai megvalósításért felelős.

Folyamatgazda / munkahelyi vezető: a területileg érintett folyamatokért felelős.

Belső ellenőrzés / auditor: felülvizsgálja az engedélyezési folyamatok megfelelőségét.

Érintett munkatárs: informált a döntésekről, végrehajtja az előírásokat.

16. RENDSZER- ÉS SZOLGÁLTATÁSBESZERZÉS (A8.25)

16.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Az eljárásrend célja, hogy meghatározza a beszerzési folyamat lépéseit, ideértve az alkalmazandó védelmi intézkedések funkcionális tulajdonságait és a biztonsági tervezési elveket. Emellett figyelembe veszi a külső szolgáltatóktól érkező információs rendszerek szolgáltatásait és a fejlesztési folyamatot, szabványokat és eszközöket. Ezáltal garantálja a biztonságos és hatékony informatikai infrastruktúra kialakítását és fenntartását a Hivatal számára.

Felelős: IT vezető, IBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

16.2. ERŐFORRÁSOK RENDELKEZÉSRE ÁLLÁSA

Az éves költségvetési tervben, vagy a beruházási tervekben nevesítve szerepeltetni kell az EIR és szolgáltatások védelméhez szükséges erőforrásokat.

16.3. A RENDSZER FEJLESZTÉSI ÉLETCIKLUSA (A8.25)

Figyelemmel kell kísérni az informatikai biztonsági helyzetet az EIR-einek teljes életútján, azok minden életciklusában.

Meg kell határozni és dokumentálni az információbiztonsági szerepköröket és felelősségeket a fejlesztési életciklus egészére. Mindemellett ki kell jelölni az információbiztonsági szerepköröket betöltő felelős személyeket.

A rendszer életciklus szakaszai a következők:

- Követelmények meghatározása
- Fejlesztés vagy beszerzés
- Megvalósítás vagy értékelés
- Üzemeltetés és fenntartás
- Kivonás (archiválás, megsemmisítés).

16.7. BESZERZÉSEK (A8.4)

A BESZERZÉSI KÖVETELMÉNYEK MEGHATÁROZÁSA (A8.26)

A Hivatal az EIR-re, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben szerződéses követelményként meghatározza az alábbiakat:

A beszerzésre kerülő rendszerek az alapvető, a szabványi és más jogszabályokban megkövetelt működési elvárásait teljesítenie kell. Az érintett rendszer esetleges cseréje esetén gondoskodni kell az előzetes felkészülésről, hogy a korábban használt, illetve szükséges folyamatok az új rendszerben hogyan érhetőek el.

A garanciális biztonsági követelmények:

a) A beszerzésre kerülő rendszerek biztonsági funkciói nem gyengülhetnek sem az elvárások, sem a korábbi rendszer paramétereinek tekintetében.

b) Figyelembe kell venni a változó jogszabályi előírásokat
c) A beszerzést megelőzően nem adható ki „valós alapú" tesztadat
d) Vizsgálni kell a termék előállítójának alkalmazott eljárásait, szabványait
e) Az előzetes tesztelés kötelező

Rögzíteni kell az adott rendszer biztonsági osztályát és az ahhoz tartozó követelményeket.

A biztonsággal kapcsolatos dokumentációs követelményeket előzetesen meg kell fogalmazni. A rendszerrel kapcsolatosan alapvető elvárás, hogy a felhasználói, és a biztonsági dokumentáció különállóan jelenjen meg, és önállóan is értelmezhetők legyenek.

A fejlesztésekre vonatkozó szerződéseknek, ill. a szerződésekhez tartozó műszaki specifikációknak, ill. a fejlesztési projektekhez tartozó megállapodásoknak ki kell térniük az informatikai biztonsági követelményekre és azokra az átadás-átvételi feltételekre, amelyek alapján ezek ellenőrzésre kerülnek (A8.30).

A fejlesztés tervezése során az informatikai biztonsági követelményeket a fejlesztésért felelős az IT vezetővel együttműködve azonosítja, és illeszti a specifikációba. meghatározzák, hogy a rendszer működése során milyen bemenő adat ellenőrzési, feldolgozás ellenőrzési, titkosítási, üzenet sértetlenség ellenőrzési, kimenő adat ellenőrzési követelmények fogalmazódnak meg, és a kapcsolódó követelményeket szintén beépítik a specifikációba. A specifikációt elfogadás előtt írásban véleményezi az IT vezető.

Minden egyedi fejlesztés esetén biztosítani kell a forráskód közvetlen, vagy közvetett rendelkezésre állását, valamint feltüntetni a fejlesztői környezetet, melyek hozzáférhetősége, adatai a szerződésben feltüntetésre kell kerüljenek. (A8.27)

A bevezetésre kerülő rendszereket bevezetés előtti tesztelni szükséges. A tesztelésnek ki kell térnie a bevezetés által érintett kapcsolódó rendszerek tesztelésére is. A tesztelések és a bevezetés során a rendszergazdának kell gondoskodnia arról, hogy éles rendszeren csak engedélyezett és felügyelt módosítás történhessen. Ugyancsak a rendszergazdának kell gondoskodnia arról, hogy a megfelelőség ellenőrzéséhez használt teszt adatokhoz, illetve a forráskódokhoz illetéktelen ne férjen hozzá.

Amennyiben külső fejlesztők működnek közre a fejlesztésben, a fejlesztéshez ki kell jelölni egy projektvezetőt, akinek a feladata az információ kiszivárgás kockázatának csökkentése és a fejlesztőkkel együttműködés során a biztonsági követelmények betartása, betartatása. E célból együtt kell működnie az IT vezetővel.

Annak érdekében, hogy az EIR-nek a biztonság szerves részét képezze, a biztonsági követelményeket már az életciklus tervezési, fejlesztési, beszerzési szakaszában figyelembe kell venni. Az üzemeltetés és karbantartás során az információbiztonsági teljesülését biztosítani kell.

16.8. BESZERZÉSEK – ALKALMAZANDÓ VÉDELMI INTÉZKEDÉSEK FUNKCIONÁLIS TULAJDONSÁGAI

Meg kell követelni a fejlesztőtől az adatvédelem, a hálózati biztonság, a hozzáférési ellenőrzés vagy más olyan biztonsági intézkedések leírását, amelyek szükségesek az adott rendszer biztonságának biztosításához.

16.15. AZ EIR-RE VONATKOZÓ DOKUMENTÁCIÓ (A5.37)

ADMINISZTRÁTORI, VAGY ÜZEMELTETÉSI DOKUMENTÁCIÓ

Ha a rendszer üzemeltetése a Hivatal hatókörébe tartozik, akkor megköveteli és birtokába veszi az EIR-re, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori, vagy üzemeltetési dokumentációt, amely tartalmazza az alábbiakat:

a) A rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését leíró adatokat, folyamatokat, specifikációkat.
b) Biztonsági funkciók (hardening)
c) A biztonsági funkciók hatékony alkalmazásának és fenntartásának leiratait.
d) A konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket, gyengeségeket (kockázatelemzés, hatásvizsgálat)

Ezen dokumentációt a Rendszergazda rendelkezésére kell bocsátani.

FELHASZNÁLÓI DOKUMENTÁCIÓ

A Hivatal megköveteli és birtokába veszi az EIR-re, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amely tartalmazza:

a) A Felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját, ellenőrzését.
b) A rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit.
c) A Felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához.

Ezen dokumentációt a Felhasználók rendelkezésére kell bocsátani.

Amennyiben valamely dokumentáció nem áll rendelkezésre, akkor az IT vezetőnek dokumentálnia kell a dokumentáció beszerzésére tett kísérleteket.

16.16. BIZTONSÁGTERVEZÉSI ELVEK

A Hivatal az általa használt biztonságtervezési elveket ugyanúgy megköveteli a specifikáció, a tervezés, a fejlesztés, a megvalósítás és módosítás során is.

16.49. KÜLSŐ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK SZOLGÁLTATÁSAI (A5.23)

A Hivatal a külső szolgáltató által biztosított elektronikus információs rendszerek (külső EIR-ek) igénybevételét úgy szervezi meg, hogy az megfeleljen a Hivatal információbiztonsági és adatvédelmi követelményeinek, valamint a vonatkozó jogszabályi és szerződéses előírásoknak.

KÜLSŐ EIR IGÉNYBEVÉTELÉNEK FELTÉTELEI

Külső szolgáltató által biztosított elektronikus információs rendszer csak előzetes információbiztonsági és adatvédelmi kockázatértékelést követően vehető igénybe. A szolgáltatóval kötött szerződésnek ki kell térnie

- az adatok tulajdonjogára, kezelésére, visszaszolgáltatására vagy törlésére vonatkozó feltételekre,
- a szolgáltató által alkalmazott információbiztonsági tanúsítványokra vagy megfelelőségi igazolásokra (ISO/IEC 27001, SZTFH igazolás),
- incidenskezelési, mentési, naplózási és helyreállítási kötelezettségekre,
- az adatkezelés helyére és az alkalmazandó joghatóságra,
- valamint alvállalkozók vagy további szolgáltatók bevonásának feltételeire.

HOZZÁFÉRÉS- ÉS JOGOSULTSÁGKEZELÉS

A külső EIR-ek elérését a Hivatal által meghatározott hitelesítési és hozzáférés-kezelési szabályok szerint kell biztosítani. Az adminisztrátori jogosultságokat a szükséges minimumra kell korlátozni.

A hozzáféréseket és az adminisztratív műveleteket naplózni kell, valamint biztosítani kell a felhasználói tevékenységek egyedi azonosíthatóságát és visszakövethetőségét.

Dokumentálni kell a külső rendszer felügyeletét ellátó személyek, illetve a felhasználók feladatait és kötelezettségeit a külső rendszerrel kapcsolatban.

ADATVÉDELEM ÉS TITKOSÍTÁS

A külső EIR-ben kezelt adatok védelmét megfelelő technikai és szervezési intézkedésekkel kell biztosítani. Az érzékeny adatok átvitel és tárolás során titkosítással védendők.

A titkosítási kulcsok kezelésének felelősségét és módját egyértelműen rögzíteni kell. A szolgáltatás megszűnésekor biztosítani kell az adatok biztonságos visszaszolgáltatását vagy törlését.

FOLYAMATOS FELÜGYELET ÉS MEGFELELŐSÉG

A Hivatal rendszeresen ellenőrzi a külső szolgáltató által biztosított rendszer biztonsági és működési megfelelőségét. Ennek keretében folyamatosan vizsgálni kell

- a szolgáltatás rendelkezésre állását és a szolgáltatási szintek (SLA) teljesülését,
- a biztonsági eseményekkel kapcsolatos értesítéseket és jelentéseket,
- a naplóadatok és auditinformációk rendelkezésre állását.
- A külső szolgáltatás biztonsági szintjét legalább évente felül kell vizsgálni.

ÜZLETMENET-FOLYTONOSSÁG ÉS HELYREÁLLÍTÁS

A külső szolgáltató által biztosított rendszernek támogatnia kell a Hivatal üzletmenet-folytonossági és helyreállítási követelményeit. A szolgáltatásnak biztosítania kell a mentések, a helyreállíthatóság és a szükséges redundancia lehetőségét.

A szolgáltatás kiesése esetére alternatív működési vagy helyreállítási eljárást kell meghatározni.

KILÉPÉSI STRATÉGIA ÉS ADAT-VISSZANYERÉS

A szolgáltatóváltás vagy a szolgáltatás megszűnése esetén biztosítani kell a Hivatal adatainak teljes és ellenőrizhető visszanyerését. A szolgáltatónak lehetővé kell tennie az adatok exportját szabványos, feldolgozható formátumban, valamint gondoskodnia kell a Hivatal adatait tartalmazó példányok biztonságos törléséről.

16.99. TÁMOGATÁSSAL NEM RENDELKEZŐ RENDSZERELEMEK

Azon rendszerelemeknek (szoftver, hardver) amelyeknek már nem elérhető a fejlesztői, vagy szállítói támogatás,

a) le kell cserélni támogatottra;
b) ki kell vezetni, ha már nincs rá szükség;
c) alternatív támogatást kell biztosítani belső, vagy külső szolgáltatók bevonásával;

17. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM (A8.20, A8.21)

17.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend célja a Hivatal EIR-nek és kommunikációs csatornáinak hatékony védelme a külső és belső fenyegetésekkel szemben. Részletesen meghatározza a rendszer és felhasználói funkciók szétválasztásának módját, valamint az osztott használatú rendszererőforrások biztonságos kezelését. Emellett előírja a határvédelmi intézkedéseket, ideértve a hozzáférési pontok és a külső infokommunikációs szolgáltatások védelmét. Kiemelt figyelmet fordít az adatátvitel bizalmasságára és sértetlenségére.

Felelős: IT vezető, IBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

17.12. SZOLGÁLTATÁSMEGTAGADÁSSAL JÁRÓ TÁMADÁSOK ELLENI VÉDELEM

Az EIR-t fel kell készíteni a szolgáltatás megtagadás alapú (Denial of Service) támadásokkal szemben.

A szolgáltatás megtagadó, más néven túlterheléses támadás során a támadó célja, hogy a felhasználók ne tudjanak elérni egy bizonyos szolgáltatást (pl.: a levelezést, bizonyos webhelyeket, online felhasználói fiókokat). Ennek során a támadó felesleges kérésekkel árasztja el és túlterheli a rendszert, amely így nem tudja a felhasználói kéréseket kiszolgálni.

A védelem érdekében biztosítani kell az EIR-t alkotó szoftverek naprakészségét a 10. Karbantartás fejezetben leírtak szerint.

Az informatikai rendszer kártevők elleni védelmét a 18.8. Kártékony kódok elleni védelem pontban leírtak szerint kell megvalósítani.

A határok védelmét a 17.17. A határok védelme fejezet alapján kell kialakítani.

Szegmentált hálózatot kell kialakítani, amelyben a felhasználói tevékenységek céljából külön alhálózatban kell elhelyezni a szervereket és a felhasználói munkaállomásokat, illetve külön menedzsment alhálózatot kell létrehozni az üzemeltetési tevékenységek (pl.: hálózati eszközök, szerverek, tároló rendszerek stb. menedzselése) céljából.

Az EIR-t – a 6.26. Legszűkebb funkcionalitás pont előírásai szerint – úgy kell konfigurálni, hogy csak a minimálisan szükséges szolgáltatások, portok és protokollok legyenek engedélyezve.

17.17. A HATÁROK VÉDELME

Az EIR Internet felőli – és kulcsfontosságú pontokon belső – határvédelmét tűzfalakkal kell biztosítani oly módon, hogy a tűzfalon keresztül csak az engedélyezett szolgáltatások legyenek elérhetők.

A nyilvánosan hozzáférhető rendszerelemeket szeparált hálózaton kötelező elhelyezni, elkülönítve a belső hálózattól. A szeparált (nyilvános) hálózatról a belső (szervezeti) hálózat elérését tűzfalakkal kell biztosítani.

A tűzfalak szabályrendszereinek kialakítása, a beállítások folyamatos karbantartása, a tűzfalak folyamatos felügyelete, az eseménynaplók elemzése, a betörési kísérletek kiszűrése és a szükséges intézkedések megtétele a Rendszergazda feladata.

A határvédelmi eszközök üzembiztonságáért, az eszközök karbantartásáért és javításáért, a beállítások mentéséért a Rendszergazda felel.

A rendszer külső határain olyan határvédelmi (tűzfal) megoldást kell alkalmazni, amely:

- alapértelmezett beállításként tilt minden külső kapcsolódást, a külön engedélyezett kapcsolatokon kívül;
- figyeli, naplózza és megakadályozza a kibertámadási kísérleteket;
- képes a túlterhelés alapú támadások felismerésére és hatásainak mérséklésére;
- képes biztonságos VPN kommunikáció biztosítására.

A rendszervédelem további eszközeként:

- blokkolni kell a belső hálózatból a veszélyesként besorolt, vagy kártékony kódot tartalmazó weboldalakhoz történő hozzáférést;
- Az e-mail kommunikációban külső spam szűrő rendszert kell alkalmazni a kéretlen, adathalász és kártékony kódot tartalmazó levelek blokkolására és karanténba helyezésére.

A lehetőségek szerint a Hivatal valamennyi telephelyén törekedni kell a határvédelmi eszközök Alapkonfiguráció szerinti azonos beállítására és a naplózás rendjének betartására.

17.49. KRIPTOGRÁFIAI KULCS ELŐÁLLÍTÁSA ÉS KEZELÉSE (A8.24)

A Hivatal rendelkezik a Nemzeti Média és Hírközlési Hatóság által elfogadott kriptográfiai (titkosító) kulcsokkal, valamint ezen kulcsokból származtatott belső (önaláírt) kriptográfiai kulcsokkal is.

A Hivatal titkos kulcsát csak a Rendszergazda ismeri. A 2 évnél régebbi kulcsokat a Rendszergazda inaktíválja, vagy eltávolítja.

17.53. KRIPTOGRÁFIAI VÉDELEM (A8.24)

Az EIR-ben csak olyan kriptográfiai (titkosítási) megoldás alkalmazható, mely megfelel az elektronikus aláírásról szóló törvény előírásainak, illetve az elektronikus aláírást felügyelő hatóság ajánlásainak és állásfoglalásainak.

Felhasználási területek:

- Adatátvitel védelme (SSL/TLS)
- E-mail titkosítása (S/MIME)
- Jelszóvédelem (HASH)
- VPN (AES-256)
- Wifi hálózatok titkosítása (WPA2/WPA3)
- Hardveres titkosítási modulok (HSM):
- Személyazonosság ellenőrzése (biometrikus adatok):
- Hitelesítési tokenek (OTP)

17.54. EGYÜTTMŰKÖDÉSEN ALAPULÓ INFORMATIKAI ESZKÖZÖK

A Hivatal csak olyan együttműködésen alapuló számítástechnikai eszközöket (pl.: a számítógép kameráját és mikrofonját használó kommunikációs szoftvereket; vagy a számítógép képernyőjének, billentyűzetének és egerének távoli elérését biztosító, távsegítség nyújtására szolgáló szoftvereket) alkalmaz, amelyek:

a) vezérlő szoftvere az engedélyezett szoftverek körébe tartozik;

b) működését a munkatársak ismerik;
c) aktiválásához a Felhasználó jóváhagyása szükséges.

Az engedélyezett alkalmazásokat a 2.100 Távoli hozzáférések pontja taglalja.

17.69. BIZTONSÁGOS NÉV/CÍM FELOLDÁSI SZOLGÁLTATÁS (HITELES FORRÁS)

Az EIR névfeloldási szolgáltatását úgy kell kialakítani, hogy a hiteles forrást biztosító DNS szerver (autoritatív DNS) kriptográfiai (titkosítási) megoldással kiegészített, biztonságos tranzakciókat valósítson meg, amely nemcsak hiteles adatokat biztosít a név/cím feloldási kérésekre, hanem az információ eredetét és sértetlenségét is igazolja.

17.71. BIZTONSÁGOS NÉV/CÍM FELOLDÓ SZOLGÁLTATÁS (REKURZÍV VAGY GYORSÍTÓTÁRAT HASZNÁLÓ FELOLDÁS)

Az EIR névfeloldási szolgáltatását megvalósító rekurzív vagy gyorsítótáras DNS szervereknek kriptográfiai (titkosítási) megoldással kiegészített, biztonságos tranzakciókat kell megvalósítaniuk, amely segítségével a hiteles forrásból származó név/cím feloldó válaszokra vonatkozóan ellenőrizniük kell és maguknak is biztosítaniuk kell az információ eredetének és sértetlenségének igazolását.

17.72. ARCHITEKTÚRA ÉS TARTALÉKOK NÉV/CÍM FELOLDÁSI SZOLGÁLTATÁS ESETÉN

Az EIR név/cím feloldási szolgáltatását redundáns, hibatűrő módon kell kialakítani, azaz tartalék DNS szervert kell alkalmazni, amely biztosítja a szolgáltatás magas rendelkezésre állását.

A külső és a belső szerepköröket szét kell választani, vagyis külön DNS szervert kell használni a belső hálózat kiszolgálására, és külön szervernek kell ellátnia az internetes DNS szerverekkel történő kapcsolattartást.

17.108. A FOLYAMATOK ELKÜLÖNÍTÉSE

Az EIR-ben elkülönített végrehajtási tartományt kell fenntartani minden programfolyamat (process) számára, vagyis az egy számítógépen futó, megosztott erőforrásokat használó folyamatok nem szerezhetnek jogosulatlanul információkat más folyamatoktól.

Ennek érdekében a Hivatalnál csak olyan modern operációs rendszerek alkalmazhatóak, amelyek ezt biztosítják.

18. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG (A8.1)

18.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend célja az EIR és az információk integritásának és biztonságának védelme. Az eljárásrend meghatározza a hibajavítás folyamatát, valamint előírja a kártékony kódok elleni védelmi intézkedéseket. Emellett előírja az EIR monitorozását, részletesen foglalkozik a szoftver- és információsértetlenség ellenőrzésével, a kéretlen üzenetek elleni védelemmel és a bemeneti információk ellenőrzésével.

Felelős: IT vezető

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

18.2. HIBAJAVÍTÁS

A Hivatalnál e-mailes hibabejelentés működik az alábbi feladatok hatékony támogatása céljából:

- a felhasználói oldalon jelentkező, EIR-rel kapcsolatos bejelentések (hibabejelentés, segítségnyújtás kérése, hozzáférési jogosultság igénylés stb.) akár munkaidőn túli fogadására;
- az elvégzett munkák dokumentálására.
- A felhasználók a következő formában tehetik meg a bejelentésüket:
  - remete.karoly@forel.hu e-mail címen,
  - Sürgős esetben telefonon a +36 30 957 1493 mobilszámon
- A bejelentéseknek minden esetben tartalmazniuk kell:
  - a bejelentő nevét, e-mail és/vagy telefonos elérhetőségét;
  - az EIR megnevezését;
  - az igény vagy a hibajelenség pontos leírását;
  - hibabejelentés esetén a hiba felmerülésének helyét, az esetleges hibaüzenetet és a hiba észlelésének időpontját.

Az EIR felhasználója a rendszerhibát e-mailben bejelenti a Rendszergazdának.

A telefonon történt bejelentéseket a későbbiekben minden esetben dokumentált formában is meg kell erősíteni!

A Rendszergazda fogadja a bejelentést, és kiosztja a feladatot az EIR-hez kijelölt, Rendszergazda számára.

Belső üzemeltetésű rendszer esetén:

A kijelölt Rendszergazda megvizsgálja, és szükség szerint pontosítja a hibát, majd gondoskodik a hiba javításáról.

Bizonyos esetekben szükség lehet a hiba kijavításához külső partnerek (pl.: speciális szakismeretet, szerszámokat vagy anyagokat igénylő hardver javítások esetén külső szakszerviz; vagy szoftverhibák esetén a külső szoftverfejlesztő; vagy a rendszer üzemeltetéséhez támogatást nyújtó szerződéses partner) bevonására. Ilyen esetben a Rendszergazda feladata a külső partner által végzett javítás koordinálása, a javított hardver eszközök, illetve szoftverfrissítések éles üzembe állítás előtti tesztelése, a szoftverfrissítések telepítése.

A külső üzemeltetésű rendszerek esetén:

A Rendszergazda a vonatkozó szerződés alapján értesíti a külső üzemeltetőt és koordinálja a hiba kijavítását.

A hibajavítás elvégzéséről a Rendszergazda e-mailben értesíti a bejelentőt.

Szoftver- és firmware frissítések

A hibajavításokkal kapcsolatban szükség lehet szoftverfrissítések telepítésére, amely a változáskezelés hatálya alá esik, ezért ennek során a 6.7 A konfiguráció változások felügyelete (változáskezelés) fejezetben leírtak alkalmazandók.

Biztonsági frissítések

A hardvergyártók és szoftverfejlesztők rendszeresen adnak ki biztonsági frissítéseket a termékükben felfedezett biztonsági hibák javítására. Ezen biztonsági frissítések telepítése kiemelt jelentőséggel bír az EIR biztonsága szempontjából, mert az ismert biztonsági hibák kihasználásával könnyen válhat a rendszer támadás célpontjává.

Az EIR és környezetük biztonsági frissítéseinek telepítése a változáskezelés hatálya alá esik, ezért ennek során 6.7 A konfiguráció változások felügyelete (változáskezelés) fejezetben leírtak alkalmazandók.

a) **Microsoft termékek biztonsági frissítéseinek telepítése**
A Microsoft termékek biztonsági frissítéseinek telepítésére lehetőség szerint a Microsoft által biztosított központi menedzsment szervert kell alkalmazni, mely biztosítja a frissítések ütemezését, a munkaállomások újraindításának kikényszerítését, a telepítési műveletek naplózását. A biztonsági frissítések éles környezetben történő telepítését meg kell előznie egy a Hivatal jellemző eszközeiből felépített reprezentatív tesztkörnyezetben való tesztelésnek. A tesztelést a biztonsági frissítés kiadását követő 1 héten belül el kell végezni. Törekedni kell arra, hogy a biztonsági frissítések a kiadást követő 4 héten belül telepítésre kerüljenek valamennyi érintett eszközön.

b) **Nem Microsoft termékek biztonsági frissítéseinek telepítése (Unix, Linux)**
A nem Microsoft termékek frissítését a gyártói ajánlások figyelembevételével kell elvégezni.

c) **Irodai segédprogramok biztonsági frissítéseinek telepítése**
Törekedni kell a kiegészítő irodai segédprogramok (pl.: Java Runtime Environment, Adobe Acrobat Reader stb.) naprakészségének biztosítására. Különös figyelmet kell fordítani az irodai segédprogramok EIR-rel való együttműködésére, ezért a frissítéseket először tesztelni szükséges. Az EIR fejlesztőjével kötött szerződésbe bele kell foglalni, hogy az EIR-t úgy köteles továbbfejleszteni, hogy az mindig kompatibilis legyen a kiegészítő irodai segédprogramokkal.

18.8. KÁRTÉKONY KÓDOK ELLENI VÉDELEM (A8.7)

VÍRUSVÉDELEM

A vírusok és egyéb kártevők (pl.: férgek, kémprogramok, trójai programok stb.) jelentős veszélyforrást jelentenek az EIR-re és az általunk kezelt adatokra, ezért az ellenük való védekezés elengedhetetlen.

A kártevők általi fertőzés elleni védekezés során a következőkről kell gondoskodni:

A fertőzés elkerülése, illetve megbízható megszüntetése érdekében vírusvédelmi szoftverrel kell ellátni minden szervert és munkaállomást. Vírusvédelmi szoftver nélkül sem hálózati, sem önálló számítógép nem üzemeltethető.

A vírusvédelmi szoftverek vírusdefiníciós adatbázisát a lehető leggyakrabban frissíteni kell, ezért vírusvédelmi szoftvereket úgy kell beállítani, hogy a frissítés letöltése automatizáltan történjen a vírusvédelmi rendszert menedzselő szerverről, amely a vírusvédelmi szoftver és a vírusdefiníciós adatbázis szétosztására szolgál. A frissítések letöltésének időintervalluma nem lehet nagyobb 1 munkanapnál.

A rendszergazdának gondoskodnia kell arról, hogy a vírusvédelmet menedzselő szerveren a vírusvédelmi szoftver lehető legfrissebb program- és vírusadatbázis verziója álljon rendelkezésre.

A vírusvédelmi szoftverhez tartozó szoftverfrissítések telepítése a változáskezelés hatálya alá esik, ezért ennek során a 6.7 A konfiguráció változások felügyelete (változáskezelés) fejezetben leírtak alkalmazása kötelező.

A vírusvédelmi szoftvereket úgy kell telepíteni és beállítani, hogy a háttérben folyamatosan futva (rezidens módban) működjenek, azaz a számítógép indításakor a szoftver aktivizálódjon, és állandó védelmet biztosítson.

A vírusvédelmi szoftvereket úgy kell beállítani, hogy legalább hetente automatikusan időzített, a számítógép valamennyi helyi háttértárolójára kiterjedő, teljes körű vírusellenőrzés történjen. Fájl szerverek esetén a vírusellenőrzést úgy kell beállítani, hogy az esetlegesen nem lezárult vizsgálat után legfeljebb 24 óra múlva újra induljon el.

A cserélhető adathordozókon (pl.: DVD, pendrive, külső merevlemez) a használat előtt minden esetben vírusellenőrzést kell végezni. A vírusvédelmi szoftverek beállításával kell gondoskodni arról, hogy az ellenőrzés automatikusan megtörténjen.

A vírusvédelmi szoftvereket olyan módon kell beállítani, hogy fertőzés esetén a szoftver elsődleges akcióként próbálja megtisztítani, ha az sikertelen, akkor helyezze karanténba vagy törölje a fertőzött fájlokat (a karanténba helyezett fájlok csak a vírusvédelmi szoftver által elérhetők, és később egy újabb vírusdefiniciós adatbázissal a szoftver képes lehet a karanténba helyezett fájlok megtisztítására). Minden ilyen intézkedésről riasztást kell, hogy küldjön a Rendszergazdának.

Amennyiben a Rendszergazda téves riasztást feltételez, azt jeleznie kell az IBF részére, aki meghatározza az esetleges további teendőket.

18.13. AZ EIR MONITOROZÁSA (A8.12)

A rendszer kiszolgálóira felügyeleti eszközöket kell telepíteni, hogy a Hivatal időben észlelhesse a rendellenességeket.

A felügyeleti eszközök segítségével Rendszergazdáknak folyamatosan monitorozniuk kell a rendszert, hogy

a) felfedezzék a támadásokat, vagy potenciális támadásra utaló jeleket;
b) felfedezzék az engedély nélküli hálózati kapcsolatokat;
c) azonosítsa a rendszer jogosulatlan használatát;
d) haladéktalanul értesüljenek a rendszerelemek működési zavarairól

Az észlelt eseményeket elemezni kell, az események súlyától függően a Rendszergazdának értesítenie kell az IT vezetőt, illetve az IBF-t.

A Hivatal köteles a kiberbiztonsági intézkedések és a felügyeleti mechanizmusok szintjét felülvizsgálni, és szükség esetén módosítani annak érdekében, hogy a védelem mindig arányos maradjon az aktuális kockázati szinttel.

Amennyiben szükséges, jogi állásfoglalást is kérhet a tevékenységgel kapcsolatban.

18.37. BIZTONSÁGI RIASZTÁSOK ÉS TÁJÉKOZTATÁSOK

Az IBF az illetékes hatóságok informatikai biztonsági riasztásait, ill. az informatikai szakportálokon megjelenő biztonsági figyelmeztetéseket folyamatosan nyomon követi és a szükséges intézkedéseket megteszi.

Folyamatosan nyomon követi a Kiberbiztonsági incidenskezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket, valamint az informatikai szakportálokon megjelenő biztonsági figyelmeztetéseket.

Szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki, tanácsokat és iránymutatásokat készít.

A biztonsági iránymutatásoknak megfelelően megteszi a megfelelő ellenintézkedéseket és válaszlépéseket.

18.67. INFORMÁCIÓ KEZELÉSE ÉS MEGŐRZÉSE

Az EIR be- és kimeneti információinak (pl.: számlák, adatszolgáltatások) kezelésével kapcsolatban a következők az előírások:

a) Gondoskodni kell a be- és kimeneti információk tartalmi ellenőrzéséről.
b) Gondoskodni kell arról, hogy a kimeneti információkhoz történő fizikai és logikai hozzáférés csak az arra jogosult személyekre korlátozódjon.
c) Gondoskodni kell arról, hogy a jogosult személyek időben megkapják az elkészült kimeneti információkat.
d) Biztosítani kell, hogy a megsemmisítési eljárások során a kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.
e) A kimeneti információkat (pl. számlákat) a vonatkozó jogszabályok, szabályzatok szerint kell megőrizni.

A Hivatal az EIR kimeneti információit nyomtatott formában, elzártan vagy hiteles elektronikus formában őrzi meg.

19. ELLÁTÁSI LÁNC KOCKÁZATKEZELÉSE (A5.19)

19.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend célja a beszállítói lánc kockázatainak kezelése és minimalizálása. Az eljárásrend meghatározza a beszállítói láncra vonatkozó kockázatkezelési szabályokat és követelményeket, emellett előírja az alvállalkozókra vonatkozó ellenőrzéseket és a beszerzési stratégiák kidolgozását. Kiemelt figyelmet fordít a beszállítók értékelésére és felülvizsgálatára, valamint a rendszerek vagy rendszerelemek hitelességének biztosítására.

Felelős: IBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, a Rendszergazdával, valamint a Kockázati szereplőkkel (1.7.2.) minden esetben ismertetni kell.

19.2. ELLÁTÁSI LÁNCRA VONATKOZÓ KOCKÁZATKEZELÉSI SZABÁLYZAT

Az ellátási láncra vonatkozó kockázatkezelési szabályok megegyeznek az általános informatikai kockázatkezelési szabályokkal.

Ki kell alakítani egy folyamatot annak érdekében, hogy azonosítani és kezelni lehessen a gyengeségeket vagy hiányosságokat a meghatározott EIR-ek ellátási láncának elemeiben és folyamataiban.

Biztosítani kell, hogy az ellátási láncért felelős személyek részt vegyenek a gyengeségek és hiányosságok azonosításában és kezelésében, valamint az erre vonatkozó folyamatok kidolgozásában és végrehajtásában. Ezen személyeket be kell vonni a kockázatkezelésbe.

Ellátási Lánccal Kapcsolatos Kontrollok Alkalmazása

Alkalmazni kell a meghatározott ellátási lánccal kapcsolatos kontrollokat annak érdekében, hogy védeni lehessen a rendszerelemet vagy rendszer szolgáltatást az ellátási lánccal kapcsolatos kockázatokkal szemben.

Ilyen fenyegető tényezők lehetnek:
- Kutatás-fejlesztés elakadása
- Tervezési hiba
- Gyártási hiba
- Beszerzési probléma
- Szállítás nehézségei
- Üzemeltetés zavara, vagy hibája
- Karbantartás hiányosságai
- Kivezetés/Selejtezés problémái

Csökkenteni lehet az ellátási lánccal kapcsolatos eseményekből eredő károkat és következményeket a meghatározott kontrollok hatékony alkalmazásával.

Abban az esetben, ha a beszállítók megváltoznak, a beszállítói kockázatelemzéseket soron kívül el kell végezni.

Az ellátási lánccal kapcsolatos kockázatok és kezelésük a [*VPH_Kockázat-menedzsment*] dokumentumban találhatók.

19.4. ELLÁTÁSI LÁNCRA VONATKOZÓ KÖVETELMÉNYEK ÉS FOLYAMATOK

A külső partnerek képviselőivel a mindenkor hatályos IBSZ vonatkozó részeit a feladatnak megfelelő mértékben ismertetni kell. A betekintés mélységének meghatározása az Adatgazda felelőssége. A szerződéskötés és az

együttműködés során biztosítani kell, hogy a külső partner (fejlesztő cég, szállító) az általa gyártott, telepített, fejlesztett EIR-t és rendszerelemet úgy konfigurálja, hogy annak minden eleme és egésze eleget tegyen az IBSZ-ben előírtaknak.

A már meglévő rendszerek cseréje, megújítása esetén meg kell vizsgálni, és szükség esetén az aktuális kockázatoknak megfelelően módosítani kell a belső besorolást. Új rendszerek bevezetésénél el kell végezni a rendszerek besorolását.

19.7. ELLÁTÁSI LÁNC ELLENŐRZÉSEK ÉS FOLYAMATOK – ALVÁLLALKOZÓK (A5.22)

Bármely informatikához kapcsolódó szolgáltatást nyújtó szolgáltató, ill. alvállalkozó, valamint más együttműködő partnerrel való együttműködés megkezdése előtt a szerződést előkészítő munkatárs az IT vezető bevonásával megvizsgálja a felmerülő informatikai biztonsági kockázatokat, hozzáférési igényeket, és a szükséges kontrollokat beépíti a partnerrel kötött szerződésbe, kapcsolódó megállapodásba. Szolgáltató, ill. alvállalkozó bevonása miatt fellépő új kockázat felmerülésekor a kockázatot az IBF a kockázat-felmérési eljárások során kezeli.

19.13. BESZERZÉSI STRATÉGIÁK, ESZKÖZÖK ÉS MÓDSZEREK (A5.20)

Vizsgálatnak kell alávetni potenciális beszállítókat, hogy meggyőződjünk arról, hogy megfelelnek a Hivatal által meghatározott biztonsági és minőségi követelményeknek. Ez magában foglalja az üzleti hátterük, referenciáik és minősítéseik ellenőrzését.

Fontos, hogy a szerződésekben szerepeljenek olyan záradékok, amelyek biztosítják a beszállítók felelősségét és kötelezettségét az adatvédelem, az információbiztonság és más kapcsolódó biztonsági kérdések tekintetében.

A kritikus beszállítók kiválasztásánál és felhasználásánál fontos, hogy a Hivatal ne támaszkodjon kizárólag egyetlen beszállítóra. A különböző beszállítók és források felhasználása csökkenti az egyetlen beszállítótól való függőséget és az ezzel járó kockázatot.

Rugalmas szerződési feltételek bevezetése szükséges, amelyek lehetővé teszik a szerződések módosítását vagy felmondását bizonyos kockázati események bekövetkezte esetén, például egy beszállító hanyagsága vagy károkozása esetén.

Rendszeres ellenőrzések és felügyeleti mechanizmusok bevezetése kell az ellátási lánc különböző szakaszaiban annak érdekében, hogy azonosítsák és kezeljék az esetleges kockázatokat és problémákat.

19.19. ÉRTESÍTÉSI MEGÁLLAPODÁSOK

A beszállítói láncban részt vevő szervezetekkel olyan megállapodás szükséges, amely kitér a kommunikációra, információ áramlásra, az ellenőrzésekre a Hivatal és a beszállítók között.

19.22. RENDSZEREK VAGY RENDSZERELEMEK VIZSGÁLATA (A5.21)

A Hivatal az ellenőrzéseket a beüzemelés alkalmával történő vizsgálatra korlátozza, elfogadottak a gyártói tesztek.

19.23. RENDSZERELEM HITELESSÉGE

A rendszerelemek hamisítás elleni vizsgálata kötelező a rendszerbe illesztés előtt. A különböző rendszerelemeket többféle módszerrel kell vizsgálni:

Hardverkomponensek: fizikai ellenőrzéssel (szemrevételezés) kell vizsgálni. Figyelni kell az idegen címkéket, forrasztásokat vagy változásokat a külső megjelenésben. Ellenőrizni kell az alkatrészek eredetiségét és hitelességét, amelyeket védjegyek vagy tanúsítványok igazolnak.

Szoftverkomponensek: ha lehetőség van rá, akkor forráskód-ellenőrzést kell végezni. Amennyiben nincs. úgy a digitális aláírások hiánya vagy érvénytelensége jelezheti a hamisítást.

Firmware, vagy BIOS: ellenőrizni kell a firmware és BIOS verzióját a gyártó hivatalos weboldalán vagy a rendszer dokumentációjában. Amennyiben van rá lehetőség, akkor a gyártó által rendelkezésre bocsátott speciális firmware vagy BIOS ellenőrző eszközt kell használni. Át kell nézni a BIOS beállítását, amelyben nem jóváhagyott beállításokat kell keresni.

Amennyiben hamisításra utaló nyomokat találunk a rendszerelemekben, úgy azt jelezni kell a rendszerelem szállítójának, illetve az IBF-nek, aki dönt a további lépésekről.

19.24. RENDSZERELEM HITELESSÉGE – HAMISÍTÁS ELLENI KÉPZÉS

A Rendszergazdát képezni kell a hamisítások felismerésére. Ezen képzések megszervezése és lebonyolítása az IT vezető feladata.

19.25. RENDSZERELEM HITELESSÉGE – KONFIGURÁCIÓFELÜGYELET

Különös odafigyelést igényelnek a szervizelt, vagy javított rendszerelemek. Az újbóli üzembeállítás előtt a konfigurációs beállításokat össze kell vetni a konfigurációfelügyeletet ellátó rendszer – illetve az automatikus leltár - által dokumentálttal és ellenőrizni kell a nem jóváhagyott változtatásokat.

19.27. RENDSZERELEM SELEJTEZÉSE, MEGSEMMISÍTÉSE

Biztonságosan selejtezni az adatokat, dokumentációkat, eszközöket és rendszerelemeket a következő módszerekkel kell selejtezni (vagy megsemmisíteni):

Adatok és dokumentációk megsemmisítése: A bizalmas adatok és dokumentációk megsemmisítésére biztonságos módszereket kell használni: iratmegsemmisítő gépeket, vagy adathordozó megsemmisítő gépeket.

Adatok és dokumentációk biztonságos törlése: Ha az adatok elektronikus formában vannak, adatmegsemmisítő szoftvereket vagy eszközöket kell alkalmazni, amelyekkel elérhető az adatok és adathordozók visszaállíthatatlan törlése.

Adatok és dokumentációk titkosítása: Ha az adatok és dokumentációk tartalmaznak bizalmas információkat, el lehet végezni azok titkosítását.

Fizikai eszközök selejtezése: A fizikai eszközök (pl. számítógépek, merevlemezek, nyomtatók) selejtezését úgy kell végrehajtani, ha a Rendszergazda előtt meggyőződik arról, hogy a merevlemezeket vagy más adattároló eszközöket visszaállíthatatlan technikával törölték vagy fizikailag megsemmisítették.

Rendszerelemek fizikai megsemmisítése: Ha a rendszerelemeket nem lehet újra hasznosítani vagy újra használni, akkor a hardvert fizikailag meg kell semmisíteni, hogy a Hivatal elkerülje azok visszaállítását vagy visszafejtését.

Dokumentálás és nyilvántartás: a selejtezési folyamatot a Rendszergazdának dokumentálni kell, és a dokumentumon szerepeltetni kell:

a) az összes selejtezett elemet;
b) az elemek selejtezési dátumát;
c) a folyamatot végrehajtó személyt;
d) az eljárás részleteit;

Ez segít megfelelni a jogszabályi előírásoknak és auditoknak.

20. ÜZEMELTETÉSI INTÉZKEDÉSEK (A5.4)

Az üzemeltetési intézkedések a Hivatal, valamint a felhasználók – és az informatikai rendszerüzemeltetési szolgáltatás ügyfelei – számára meghatározott az EIR-ek üzemeltetésére, illetve használatára vonatkozó szabályok, eljárások.

20.1 A HÁLÓZAT ÜZEMELTETÉSE, HASZNÁLATA

A felhasználói munkaállomások a hálózat segítségével kapcsolódnak a különböző szolgáltatásokat nyújtó szerverekhez (pl.: fájl szerverhez, levelező szerverhez stb.), egyéb hálózati eszközökhöz (pl. hálózati nyomtatókhoz), férnek hozzá az Internethez és a hálózaton elérhető alkalmazói rendszerekhez.

20.1.2. FIZIKAI CSATLAKOZÁS A HÁLÓZATHOZ

Az informatikai eszközök, berendezések vezetékes hálózatra való fizikai csatlakoztatását – ezzel összefüggésben az informatikai eszközök másik tárolóhelyre történő áthelyezését – csak a Rendszergazda végezheti.

A mobil eszközök vezeték nélküli hálózati hozzáférésére a **Vezeték nélküli hozzáférés** pontban leírtakat kell alkalmazni.

Nem a Hivatal tulajdonában lévő informatikai eszközöket, berendezéseket csatlakoztatni a Hivatal hálózatához kizárólag az IT vezető tudtával és engedélyével lehet.

20.1.3. KÖZÖS HÁLÓZATI MAPPÁK HASZNÁLATA

A Hivatal a közös munkavégzéséhez, a közösen használt fájlok, dokumentumok tárolására a fájl szerveren kialakított közös hálózati mappákat biztosít a felhasználók részére.

A közös mappák kialakítására és használatára vonatkozóan az alábbiakat kell alkalmazni:

- A közös mappákat szervezeti egységek és közös feladatok (pl. projektek) szerint van kialakítva.
- A közös mappákhoz való hozzáférést jogosultságokkal van szabályozva. A mappák és a jogosultságok kialakításával biztosítjuk, hogy a felhasználók csak a feladatellátásukhoz szükséges mappákhoz rendelkezzenek módosítás jogosultsággal.
- A központi tárhely takarékos használata érdekében a közös mappákban csak a feltétlenül szükséges, és többek által használt dokumentumokat szabad tárolni. Magánjellegű fájlokat (pl.: fényképeket, zenéket, filmeket) a közös mappákban tárolni tilos!
- Tilos a közös mappákban futtatható (pl.: .exe, .com kiterjesztésű) fájlokat tárolni és onnan a futtatni
- A közös mappák felhasználható mérete korlátozott. A korlátok eredményes betartása érdekében a nagyméretű fájlokra (pl.: videókra, fotókra) kell elsősorban figyelni, és a felhasználóknak rendszeresen törölniük kell a munkájukhoz tartozó, már elavult és szükségtelen fájlokat.

Felelős: rendszergazda

20.1.4. SAJÁT MAPPA HASZNÁLATA

A hálózati hozzáféréssel együtt a Hivatal a felhasználók rendelkezésére bocsájt egy felhő alapú, mások által nem elérhető, saját használatú mappát.

Ezen mappák használatára az alábbiak vonatkoznak:

- A mappában helyezhetők el a felhasználók saját használatú, munkavégzéssel kapcsolatos fájljai, dokumentumai, de rendszerektől függően ide kerülhetnek a felhasználói beállítások és a felhasználó által készített listák, lekérdezések is.

- A mappák felhasználható mérete korlátozott ezért, ha a korlát túllépésére vonatkozó figyelmeztetést kap a felhasználó, akkor törölnie kell a szükségtelen lekérdezésekből vagy az általa elhelyezett egyéb fájlokból olyan módon, hogy a mappa mérete ne haladja a korlátot.

20.1.5. TILTOTT HÁLÓZATI TEVÉKENYSÉGEK

A Hivatal hálózata nem használható az alábbi tevékenységekre:

- Szigorúan tilos minden jogszabályokba ütköző tevékenység, így különösen mások személyiségi jogainak megsértése (pl. rágalmazás), a szerzői jogok megsértése (pl. szoftverek, filmek, zenék illegális terjesztése), tiltott haszonszerzésre irányuló tevékenység (pl. piramisjáték).
- Szigorúan tilos minden, a Hivatal jó hírnevét veszélyeztető, a közízlést sértő, mások vallási, etnikai, politikai vagy más jellegű érzékenységét bántó tevékenység (pl. pornográf, pedofil anyagok közzététele).
- Tilos a magáncélú haszonszerzésre irányuló, direkt üzleti célú tevékenység és reklám.
- Tilos a hálózatot és erőforrásait indokolatlanul, túlzott mértékben, pazarló módon igény bevevő tevékenység (pl.: nem hivatali körlevelek, hálózati játékok, kéretlen reklámok).
- Tilos a hálózat és erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információk és szoftverek terjesztése.
- Tilos a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, számítógépek/szolgáltatások – akár tesztelés céljából történő – túlzott mértékben való szisztematikus próbálgatása (pl. TCP port scan).
- Tilos a hálózati erőforrások, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére vagy bármely egyéb károkozásra irányuló tevékenység.
- Tilos a hálózati eszközök, üzenetek hamisítása, olyan látszat keltése, mintha egy üzenet más eszköztől vagy felhasználótól származna.

20.2 A HÁLÓZAT ÜZEMELTETÉSE

20.2.1 A HÁLÓZAT FIZIKAI KIALAKÍTÁSA, MÓDOSÍTÁSA

A hálózati rendszer bővítése vagy átalakítása

Ilyen tevékenységet kizárólag a Rendszergazda, vagy az IT vezető által ezzel megbízott külső partnerek alkalmazottai végezhetik.

Illetéktelen személy a kialakított hálózati rendszeren nem változtathat:

- hálózati végpontot nem helyezhet át;
- aktív hálózati eszközt vagy szerverfeladatokat ellátó eszközt a hálózatra nem kapcsolhat rá;
- a hálózat elemeit (pl.: fali aljzatokat, csatlakozókat, hálózati kábeleket stb.) nem bonthatja meg.

A hálózat működési biztonsága szempontjából alapvető jelentőségű a hálózat kábelezése, amelyre vonatkozóan a következőket kell figyelembe venni:

- A hálózat tervezésénél, kiépítésénél strukturált felépítést kell alkalmazni.
- A hálózat kiépítése során külön kábelcsatornában vagy tálcában kell haladniuk az áramellátást, illetve az adatkommunikációt biztosító vezetékeknek.
- A kábeleket csatornán kívül vezetni – még ideiglenes megoldásként – sem szabad.

Szegmentált hálózat kialakítása

A hálózati forgalom növekedése a hálózat túlterheléséhez vezethet. Ez ellen a hálózat szegmentálásával, azaz a területi (pl. telephelyek szerinti) felosztásával, alhálózatok kialakításával kell védekezni

A hálózat szegmentálása fizikai, területi alapon túl történhet logikai alapon is VLAN (virtuális helyi hálózat) szeparációs technológia alkalmazásával.

VLAN-ok kialakításával kell szétválasztani egymástól:

- a normál felhasználói tevékenységekhez tartozó adatforgalmat (szerverek, munkaállomások);
- az üzemeltetési tevékenységek (pl.: hálózati eszközök, szerverek, tárolórendszerek stb. menedzselése) céljára szolgáló menedzsment hálózat adatforgalmát;
- a külső hozzáférések (pl. vendég WiFi) adatforgalmát;
- a hálózati forgalom funkcionálisan elkülönülő részeit (pl.: IP telefonhálózat, kamera rendszer stb.).

A VLAN-ok használata biztosítja, hogy egy támadás esetén az esetleges kár csak az adott részterületre korlátozódjék.

Felelős: IT vezető

20.2.2 INFORMATIKAI ESZKÖZÖK ÜZEMELTETÉSE, HASZNÁLATA

A felhasználói oldali informatikai eszközök (számítógépek és tartozékok) üzemeltetésére és használatára vonatkozóan a következő eljárásrendet kell alkalmazni:

INFORMATIKAI ESZKÖZÖK HASZNÁLATA

Az informatikai eszközök használatára az alábbiak vonatkoznak:

- A munkahelyeken elhelyezett informatikai eszközöket a Felhasználók csak a kiadott feladatok elvégzése céljából használhatják. A meghatározott feladatokon kívüli tevékenységre (pl.: magáncélú felhasználásra, játékra, szórakozásra stb.) az eszközöket használni tilos!
- A felhasználók a használat ideje alatt az informatikai eszközök rendeltetésszerű működtetéséért egy személyben felelősek.
- A munka befejeztével – az alkalmazói szoftverekből, valamint az operációs rendszerből és a hálózatból való kilépés után – a felhasználóknak a számítógépet és egyéb eszközöket ki kell kapcsolniuk. Ez alól kivételt képeznek a folyamatos működést igénylő szoftvereket futtató számítógépek és a hálózati nyomtatók.
- Szintén nem szükséges az eszközöket kikapcsolni, ha azokat több műszakban használják.
- A felhasználó feladata az eszközök tisztán tartása, állagának megőrzése. Javításra vagy cserére leadni csak külsőleg megfelelően megtisztított eszközt lehet!
- Az informatikai eszközök meghibásodása vagy rendellenes működése esetén a hiba elhárítását is e-mailben kell igényelni.

INFORMATIKAI ESZKÖZÖK ÜZEMBE HELYEZÉSE

BESZERZÉST KÖVETŐ ELSŐ ÜZEMBE HELYEZÉS

Az informatikai eszközök üzembe helyezését a Rendszergazda, vagy az IT vezető által ezzel megbízott külső partnerek alkalmazottai végezhetik.

Az üzembe helyezés helyét és az eszközért felelős felhasználó személyét a Munkahelyi vezető jelöli ki.

Az üzembe helyezés során:

- jól látható helyen (lehetőleg az eszköz előlapján) el kell helyezni az eszköz egyedi azonosítására szolgáló informatikai azonosítót;
- a számítógépeken be kell állítani az Alapkonfiguráció szerinti egységes szoftver környezetet;
- és telepíteni kell a Hivatal által biztosított egyéb szoftvereket.

Az üzembe helyezést végző munkatársnak az üzembe helyezett eszköz hardver/szoftver konfigurációját az Átadás/átvételi jegyzőkönyvben kell rögzítenie, és a jegyzőkönyvet az eszközért felelős felhasználóval aláíratva kell az eszközt átadnia.

Ezt követően az eszköz számlája és a jegyzőkönyv alapján a hardver konfiguráció adatait, a telepített licencköteles szoftvereket, valamint az eszköz tárolóhelyét és az eszközért felelős felhasználó személyét fel kell vezetni a Hardver- és Szoftver nyilvántartásokba.

A befektetett eszközök nyilvántartásban az informatikai eszközök megnevezése mellett az informatikai azonosítót is rögzíteni kell, amely megkönnyíti a számviteli és az informatikai nyilvántartások egyeztetését és az eszközök leltározását.

JAVÍTÁST, KARBANTARTÁST KÖVETŐ ÜZEMBE HELYEZÉS

Az informatikai eszközök javítást, karbantartást követő üzembe helyezését szintén a rendszergazda, vagy az IT vezető által ezzel megbízott külső partnerek alkalmazottai végezhetik.

A javítás, karbantartás során változhat az eszközök hardver konfigurációja, cserélődhetnek a tartozékai. Ilyen esetben az üzembe helyezést végző munkatársnak az eszköz megváltozott konfigurációját az rögzítenie kell a Hardver- és Szoftver nyilvántartásokban.

ÁTADÁS/ÁTVÉTELI JEGYZŐKÖNYV

Az Átadás/átvételi jegyzőkönyv fő célja, hogy rögzítse a felhasználók felelősségét a használatukba adott informatikai eszközökre vonatkozóan.

A felhasználóknak jegyzőkönyvvel átadott informatikai eszközök konfigurációját a Hivatal a szoftver leltárhoz kapcsolódóan vagy szúrópróbaszerűen bármely karbantartás vagy javítás alkalmával ellenőrizheti.

ESZKÖZÖK elhelyezését befolyásoló tényezők

A számítógépes munkahelyek kialakításakor minden esetben figyelembe kell venni a képernyő előtti munkavégzés minimális egészségügyi és biztonsági követelményeiről szóló 50/1999. (XI.3.) EüM rendelet rendelkezéseit, valamint az alábbi elhelyezést befolyásoló tényezőket:

- Az informatikai eszközöket úgy kell elhelyezni, hogy azok karbantartása, javítása során a hozzáférhetőség biztosított legyen. Javasolt elhelyezés az asztal tetején, vagy az asztal mellett. Tilos a számítógépet az asztal alatt vagy annak beépített polcán úgy elhelyezni, hogy a számítógépház oldalát csak a csatlakozók kihúzását követően lehessen eltávolítani!
- Az elhelyezés során biztosítani kell a melegedő eszközök hűtését, ezért tilos az eszközön lévő szellőző réseket eltakarni (pl. az eszköz zárt helyre beépítésével vagy az eszközre történő rápakolással).
- A monitorok elhelyezését úgy kell megoldani, hogy üzemelés alatt a jogosulatlan személyek rálátása kizárt legyen.
- Az egymáshoz közel elhelyezett informatikai eszközök működése sem fizikailag, sem elektromágneses sugárzással a másik eszköz működését nem zavarhatja.
- A számítógépes munkahelyek működéséhez antisztatikus környezetet kell kialakítani. Ezekben a helyiségekben kerülendők a műszálas szőnyegpadlók, bútorszövetek, ruhák.

- Az informatikai eszközök üzembe helyezése előtt felül kell vizsgálni a villamos hálózaton alkalmazott vezetékeket, biztosítékokat abból a szempontból, hogy a szükséges áramerősség biztosítható-e az összes terhelés egyidejű bekapcsolása mellett.
- Az informatikai eszközöknek mindenféle előre betervezhető természeti, illetve emberi fenyegetésből származó rongálódásokkal szemben a biztonságban kell lenniük.

SZÁMÍTÓGÉPET TARTALMAZÓ HELYISÉGEK VÉDELME

Az EIR-ekbe történő illetéktelen behatolás elkerülése érdekében a számítógépet tartalmazó helyiségek esetében szigorúan be kell tartani a Hivatal helyiségek zárására vonatkozó előírásait, amely a tulajdonvédelmen túl ilyen esetben adatvédelmi szempontokat is szolgál.

Ha a felhasználó utolsóként távozik a helyiségből, az előírásoknak megfelelően zárnia kell a helyiséget.

A MEGELŐZÉS FONTOSSÁGA (A7.7 – A7.8)

„Tiszta asztal, tiszta képernyő policy"

Minden szempontból védeni kell a Hivatal információs vagyonát, úgy a számítógépen tárolt elektronikus adatokat, mint a munkavállalók íróasztalán elhelyezett érzékeny, papír alapú információkat.

A monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és semmiképpen se legyen látható az épületen kívülről (ha monitor elhelyezéssel nem biztosítható, akkor sötétítő függöny használatával). A Felhasználóknak zárolniuk kell a munkaállomást, (pl.: a Ctrl +Alt +Del billentyűk, majd a Zárolás gomb lenyomásával), ha azt rövidebb időre őrizetlenül hagyják. Ügyfél nem maradhat felügyelet nélkül az irodában, illetve otthoni munkavégzés, vagy távmunka esetén is figyelni kell arra, hogy pl. gyermek ne férjen hozzá az EIR-ekhez.

A munkafázis végeztével a Felhasználóknak ki kell jelentkezni az alkalmazásokból, majd leállítani a számítógépet. Minden érzékeny információt tartalmazó anyagot (papír alapú anyagokat, valamint elektronikus adathordozókat) el kell tenni az asztalokról, és zárható helyen kell tárolni. Gondoskodni kell arról, hogy a nyomtatókból, fénymásolóból kijövő dokumentumokhoz illetéktelenek ne férjenek hozzá, illetve ügyelniük kell, hogy érzékeny információt tartalmazó dokumentum ne maradjon pl. a fénymásolóban.

Az iroda elhagyása esetén a Felhasználóknak meg kell győződniük arról, hogy nem maradt-e valami érzékeny információt tartalmazó dokumentum, vagy adathordozó az asztalunkon. Csak ezután lehet elhagyni az irodát.

INFORMATIKAI ESZKÖZÖK ÁTHELYEZÉSE

A nem mobil informatikai eszközöket csak a rendszergazda helyezheti át másik tárolóhelyre. Az áthelyezést e-mailben kell igényelni.

A fentiek alól funkciójuknál fogva kivétel képez a hordozható számítógépek, projektorok, mobil adathordozók (pl.: pendrive, külső merevlemez) ideiglenes mozgatása, amit vezetői engedélyezés esetén a felhasználók is végezhetnek.

Az is eszköz áthelyezésnek számít, ha fizikailag nem változik az informatikai eszköz helye, de módosul az eszközért felelős felhasználó személye.

Az áthelyezést végző munkatársnak az eszköz megváltozott tárolóhelyét és/vagy az eszközért felelős felhasználó változását a kapcsolódó nyilvántartásokban rögzíti.

Felelős: rendszergazda

MUNKAVÉGZÉS BIZTONSÁGI TERÜLETEKEN

A fokozottan és kiemelten védett területeken csak szakképzett személyzet végezhet munkát.

Ezeken területeken a bizalmas információkat elzárt helyen kell tárolni, megakadályozva azok illetéktelen hozzáférését. Ezen a területen más személy csak az oda beosztott munkatársakkal együtt tartózkodhat.

Azokon a munkahelyeken, ahol ügyfélforgalom lehetséges, a munkahely rövid idejű elhagyásakor a számítógépet zárolni kell (pl. jelszóval védett képernyőkímélő). Ha a munkahelyet hosszabb időre elhagyják, vagy napi munka végén, a számítógépet ki kell kapcsolni. Ez alól kivételt képez az az eset, ha hosszan futó adatfeldolgozás van folyamatban, ilyenkor viszont a jelszavas képernyővédőt aktivizálni kell.

Az asztali számítógépeknek a Hivatal területéről történő kivitele tilos.

Felelős: Felhasználó

20.3 SZOFTVEREK ÜZEMELTETÉSE, HASZNÁLATA

A szoftverek bevezetésére, módosítására, telepítésére és használatára vonatkozóan a következő eljárásrendet kell alkalmazni:

20.3.1 SZOFTVEREK HASZNÁLATA

MUNKAÁLLOMÁSOK HELYI BEÁLLÍTÁSAI

Tilos a munkaállomásokon a Hivatal által kialakított rendszerbeállításokat (pl.: az Internet-, tűzfal-, biztonsági frissítések beállításait) megváltoztatni, vagy a számítógép megjelenési tulajdonságait a Hivatalnál alkalmazott egységes megjelenéshez képest olyan mértékben megváltoztatni, testre szabni, hogy az akadályozza a Hivatalon belüli közös munkát, vagy a telefonos-, esetleg távoli segítségnyújtását.

Ha a felhasználó változtat a helyi beállításokon, úgy őt terheli a felelősség az ebből eredő károkért.

A tiltó rendelkezésen túl törekedni kell arra, hogy a helyi beállítások központosított módon (pl. tartományi szintű csoportházirend alkalmazásával) jussanak érvényre és védettek legyenek a felhasználók általi módosítástól.

Felelős: IT vezető

DOKUMENTUMOK HELYI TÁROLÁSA ÉS MENTÉSE

A munkaállomások helyi adattárolóin történő adattárolást kerülni kell.

Az üzleti dokumentumokat elsődlegesen a fájl szerveren kialakított közös hálózati mappákban, vagy a felhasználó saját, OneDrive mappájában kell tárolni. A Rendszergazda feladata arról gondoskodni, hogy a szerverekben lévő adattárolók megfelelő védelemmel rendelkezzenek a hardver meghibásodások ellen és tartalmuk rendszeresen mentésre kerüljön.

Ugyanakkor a felhasználóknak lehetőségük van a dokumentumaikat a munkaállomáson helyileg is tárolni (pl.: az éppen szerkesztett dokumentumokat és a kapcsolódó munkaanyagokat; vagy az elsődlegesen a fájl szerveren tárolt dokumentumok másolatait a hordozható számítógépek hálózattól független használatához).

A munkaállomásokban lévő adattárolók nincsenek védve a hardver meghibásodások ellen, ezért gondoskodni kell a rajtuk tárolt dokumentumok mentéséről. A munkaállomáson helyileg tárolt dokumentumok mentéséért és a mentés adathordozók előírásnak megfelelő tárolásáért a felhasználó a felelős.

ALKALMAZÓI SZOFTVEREKBŐL KILÉPÉS SZÜKSÉGESSÉGE

A felhasználók adatvédelmi okokból nem hagyhatják bejelentkezett állapotban felügyelet nélkül a számítógépeket.

Mindig ki kell lépni az alkalmazói szoftverekből, ha a felhasználó:

- távozik a számítógéptől;
- vagy befejezi a szoftver használatát.

Ha a felhasználó rövid időre (5-10 percre), ideiglenesen távozik a számítógéptől, az alkalmazói szoftverekből kilépés után elegendő zárolni a számítógépet.

Ha a felhasználó hosszabb időre távozik a számítógéptől vagy befejezi a munkát, ki kell lépnie az operációs rendszerből és a hálózatból és – a folyamatos működést igénylő szoftvereket futtató számítógépek és a több műszakban használt számítógépek kivételével – kell kapcsolnia a számítógépet.

A munkaállomáson helyileg futó alkalmazói szoftverek (pl. Office irodai szoftverek) használata esetén is érdeke a felhasználónak, hogy a számítógéptől való távozás esetén a nyitott fájlokat, dokumentumokat bezárja és a szoftverekből kilépjen, hogy egy esetleges áramszünet esetén elkerülje az adatvesztést.

Felelős: Felhasználó

SZABÁLYOS KILÉPÉS A SZOFTVEREKBŐL ÉS A LEFAGYÁSOK KEZELÉSE

Tilos a szoftverek futását a számítógép kikapcsolásával vagy hardveres újraindításával (a Reset gombbal) megszakítani! A számítógép kikapcsolása előtt mindig ki kell lépni az alkalmazói szoftverekből, az operációs rendszerből és a hálózatból.

Amennyiben a felhasználó a számítógép lefagyására gyanakszik, akkor is próbálkozzon előbb

- szabályos módon kilépni az alkalmazói szoftverekből;
- a nem válaszoló programokat az operációs rendszer feladatkezelőjének segítségével bezárni;
- majd az operációs rendszert újraindítani;
- és csak legvégső esetben indítsa újra hardveresen a számítógépet.

20.3.2. SZOFTVEREK TELEPÍTÉSE

Alkalmazói szoftvereket kizárólag a rendszergazda, illetve az IT vezető által ezzel megbízott külső partnerek alkalmazottai telepíthetnek a felhasználói munkaállomásokra.

A felhasználóknak az már bevezetett szoftverek munkaállomásokra történő telepítését vagy eltávolítását e-mailben kell igényelniük.

A licencköteles (vásárolt, bérelt vagy fejlesztett) szoftverek licenceit a Szoftver nyilvántartásban kell nyilvántartani. Az ilyen szoftverek telepítése előtt a telepítést végző munkatársnak a nyilvántartás alapján ellenőriznie kell, hogy az adott szoftverre vonatkozóan a Hivatal rendelkezik-e felhasználható szoftverlicenccel. Tilos a szoftvereket a licenc által megengedett darabszámot meghaladó számban használni! Ha nincs rendelkezésre álló licenc, a szoftver telepítését nem lehet elvégezni!

Ha a már bevezetett kereskedelmi szoftverek esetén nincs felhasználható szoftverlicenc, a Hivatal vonatkozó beruházási és beszerzési eljárása szerint le kell folytatni a szoftver (vagy mennyiségi szoftverlicenc) beszerzését és csak ezt követően engedélyezett a szoftver telepítése.

A licencköteles szoftverek telepítésével egyidejűleg a telepítést végző munkatársnak a Szoftver nyilvántartásban rögzítenie kell a szoftverlicenc felhasználását.

A szabad szoftverek telepítése előtt ellenőrizni kell, hogy a szoftver szerepel-e az Engedélyezett szabad szoftverek nyilvántartásában, és milyen korlátozásokkal használható. A szoftver telepítését nem lehet elvégezni, ha a szoftver nem szerepel a nyilvántartásban, vagy a licenc korlátozása nem teszi a telepítést lehetővé! Ha a felhasználó olyan új, feltételezhetően szabad szoftver telepítését igényli, amely még nem került vizsgálatra, az Szabad szoftverek bevezetése pont szerint végre kell hajtani a szoftver engedélyezési folyamatát.

A szoftverekhez tartozó dokumentációt (pl.: Felhasználói kézikönyv, Üzemeltetési kézikönyv, licencszerződés, licencengedély, telepítő adathordozó stb.) a rendszergazdának kell átadni, aki, mint az EIR-ek üzemeltetője kezeli és őrzi ezeket.

20.3.3 ALKALMAZÓI SZOFTVEREK MÓDOSÍTÁSA

A már üzemelő, belső vagy külső fejlesztéssel készült alkalmazói rendszereknél utólag felmerülhet a szoftver módosításának igénye.

A felmerülő fejlesztési, módosítási igényeket a rendszer kulcsfelhasználója fogja össze és képviseli a belső, illetve a külső fejlesztők felé.

Amennyiben a módosítás más kapcsolódó alkalmazói rendszereket is érint, a rendszer kulcsfelhasználója egyeztető megbeszélést hív össze az érintett szakterületek részére. A megbeszélésen közös véleményt kell kialakítani a módosítás pontos tárgyáról.

A módosítási igényt a kulcsfelhasználó hagyja jóvá és belső fejlesztés esetén a Jira rendszerben adja át.

A módosítás során belső fejlesztésnél a Belső fejlesztés pontban, külső fejlesztés esetén pedig a Külső cég általi fejlesztés pontban leírt, új szoftver fejlesztésére vonatkozó lépéseket kell értelemszerűen, részben vagy egészben végrehajtani.

Amennyiben a módosított adatállományok száma eléri vagy meghaladja az adatállományok teljes számának egyharmadát, a tesztelésnek nemcsak a módosított programfunkcióra, hanem a teljes szoftverre ki kell terjednie. Csak a minden tekintetben ellenőrzött, hibátlanul működő szoftvert szabad használatra.

A szoftver fejlesztőjének új verziószámmal kell ellátni a módosított szoftvert, és az új verzióban történt változásokról a felhasználóknak tájékoztatást kell adnia.

Az új szoftververzió éles üzembe állítása a változáskezelés hatálya alá esik, ezért ennek során a 6.7 A konfigurációváltozások felügyelete pontban leírtak alkalmazása kötelező.

20.4 E-MAIL HASZNÁLATA

A Hivatal alkalmazottai, amennyiben munkájuk indokolja, hozzáférést kaphatnak az elektronikus levelezési rendszerhez.

A központi levelezőrendszer kizárólagos célja a munkavégzés. A felhasználó nem jogosult magáncélra használni a levelezőrendszert.

A Hivatal által kiosztott minden e-mail cím a munkavégzést, ügyek intézését szolgálja függetlenül attól, hogy egy-egy felhasználó személyéhez kötött az elnevezés. A levelezésbe a munkáltató betekinthet. A Hivatal jogosult az e-mail címmel és az ottani adatokkal minden egyéb műveletre is, például, de nem kizárólag: átirányítani, megszüntetni, automatikus válaszüzenetet applikálni, biztonsági mentést készíteni a levelekről, azokat tárolni, letörölni, publikálni, megosztani más felhasználókkal a céges munkavégzés céljából.

A munkaállomásokon szigorúan tilos a magánlevelezés mellékleteinek, csatolmányainak megnyitása, illetve ezek tárolása.

A fogadott levelekben szigorúan tilos megnyitni a nem ellenőrzött tartalmú mellékleteket, ismeretlen linkeket.

20.4.1 AZ ELEKTRONIKUS LEVELEZÉS BIZTONSÁGI ELŐÍRÁSAI

Az elektronikus levelezés a Hivatal informatikai rendszereinek biztonságára nézve az egyik fő veszélyforrás, ezért az elektronikus levelezés biztonsága érdekében az alábbi előírásokat kell betartani:

- A számítógépre telepített, naprakész (legalább naponta frissülő) vírusadatbázissal rendelkező vírusvédelmi szoftver nélkül tilos az elektronikus levelezés használata. Jelenteni kell a Rendszergazdának, ha valamilyen oknál fogva a számítógépen nem fut vírusvédelmi szoftver, vagy nem frissül a vírusdefiníciós adatbázisa és a szoftver azt jelzi, hogy az adatbázis elavult.
- Tilos megnyitni a vírusvédelmi szoftver által fertőzöttnek jelzett leveleket, ezeket megnyitás nélkül törölni kell.
- Az elektronikus levélben küldött vírusok általában csatolt fájlként érkeznek. Mivel a vírusvédelmi szoftverek nem ismernek fel azonnal minden új vírust vagy vírusváltozatot, a számítógép akkor is megfertőződhet, ha naprakész a vírusvédelmi szoftver vírusadatbázisa, ezért a csatolt fájlok megnyitásakor az elektronikus levelezés biztonsági előírásainak betartására fokozott figyelmet kell fordítani.
- A fokozott vírusveszély miatt tilos a nem megbízható forrásból származó levelet, azok levélmellékletét megnyitni, a levélben található internetes hivatkozásokra (linkekre) kattintani. A forrást nem megbízhatónak kell tekinteni, ha
    - a levél nyelve nem várt, nem külföldi partnerrel folytat a felhasználó levelezést (a sok veszélyes levél idegen nyelvű, ezért ezeket a leveleket fokozott figyelemmel kell vizsgálni);
    - a levél címzettje közt sok, nem ismert személy szerepel;
    - a levél tárgya nem illeszkedik a Hivatal ügyviteli folyamataihoz;
    - levélszemétre jellemző csalogató szövegeket tartalmaz nyereményről vagy pikáns képekről, vagy valamely megvásárolható terméket vagy szolgáltatást reklámoz, stb.;
    - a felhasználó számára ismeretlen kiterjesztésű vagy tiltott csatolt fájlokat tartalmaz.

A „Levélszemét" mappába érkező leveleket a kéretlen leveleket szűrő szoftver minősítette levélszemétnek. A szoftver nem minden esetben dolgozik helyesen, lehetnek az ügyviteli folyamathoz tartozó levelek is a mappában. Az itt található levelek megbízhatóságát fokozott figyelemmel kell vizsgálni.

Tilos válaszolni olyan levelekre, amelyek arra szólítanak fel, hogy a Hivatal biztonsági rendszeréről vagy a felhasználó saját hozzáférési adatairól (felhasználónév, jelszó) adjon tájékoztatást.

A levelező szervert is el kell látni olyan hatékony vírusvédelmi szoftverrel, amely megakadályozza a fertőzések elektronikus levelekben történő terjedését.

20.4.2 TILTÓ RENDELKEZÉSEK AZ ELEKTRONIKUS LEVELEZÉSRE VONATKOZÓAN

Az elektronikus levelezés használata során nem engedélyezettek az alábbi tevékenységek:

- Szigorúan tilos a levelezési rendszeren keresztül olyan tartalmú levelet küldeni, amely más természetes vagy jogi személy személyiségi, illetve egyéb jogait sérti (pl.: rágalmazás, szerzői jogok megsértése).
- Szigorúan tilos a Hivatal jó hírnevét veszélyeztető, a közízlést sértő, mások vallási, etnikai, politikai vagy más jellegű érzékenységét bántó tartalmú levelek küldése.
- Tilos a levelező rendszeren keresztül belső használatú, bizalmas vagy titkos dokumentumokat, adatokat a Hivatalból engedély nélkül kijuttatni, illetéktelen személyek részére hozzáférhetővé tenni.
- Tilos a beérkező leveleket a Hivatalon kívüli postafiókban kezelni.
- Tilos a levelező rendszerben lánclevelet, azaz olyan levelet továbbítani, amely arra szólít fel, hogy minél több címzettnek küldjünk tovább.

- Tilos feliratkozni nem szakmai jellegű, nem az ügyviteli munkát segítő hírlevél küldő szolgáltatásra.
- Tilos engedély nélkül a Hivatal teljes címtára felhasználásával szervezeti szintű körlevelet küldeni. Szervezeti szintű körlevelet csak az erre kijelölt (és megfelelő jogosultságot kapott) személyek küldhetnek, ilyen igény esetén a küldendő levélmintát nekik kell eljuttatni.
- Tilos másvalaki nevében levelet küldeni, kivéve felelős vezetői utasítás alapján.

20.4.3 KORLÁTOZÁSOK AZ ELEKTRONIKUS LEVELEZÉS HASZNÁLATÁBAN

Az elektronikus levelezés biztonsága és a levelező szerver védelme érdekében az alábbi levelezésre vonatkozó korlátozások vannak érvényben:

- A postafiókok mérete fő szabály szerint 50 Gb..
- A beérkező levelek maximális megengedett mérete 20 Mb.
- A küldött levelek maximális megengedett mérete 20 Mb.
- A levelezésben nem fogadhatók és küldhetők levélmellékletként (még tömörített csomagban sem) az alábbi formátumú fájlok a vírusfertőzés veszélye miatt:
    - futtatható fájlok (pl.: .exe, .com, .bat, .cmd, .vbs);
    - egyéb programkódot tartalmazó veszélyes fájlok (pl.: .dll, .sys, .inf, .bin, .hta, .docm, .xlsm).

A felhasználók feladata gondoskodni a szerveren biztosított tárhely elfogyásakor a levelek archiválásáról. Az archiválás végrehajtásához a Rendszergazdának bejelentve kérhető segítség.

20.4.4 AZ ELEKTRONIKUS LEVELEZÉS MAGÁNCÉLÚ HASZNÁLATA

Mivel minden levelezést a Hivatal tulajdonát képező vagy általa bérelt informatikai erőforrások biztosítanak, ezért a levelek is a Hivatal tulajdonát képezik. Így a Hivatal fenntart minden jogot a levelek kezelésével kapcsolatban. A magáncélú használat nem engedélyezett.

A fentieken túl kerülni kell az Interneten elérhető ingyenes levelezési oldalak vagy magán előfizetésekhez tartozó postafiókok belülről történő használatát. Ezeket hivatalos ügyekben használni tilos.

A lánclevelek elkerülése érdekében a Hivatal kivétel listát alkalmaz a minden felhasználó csoportnak történő küldéshez. A lista Jegyzői jóváhagyással módosítható.

20.4.5 AZ ELEKTRONIKUS LEVELEZÉS ELLENŐRZÉSE

A Hivatal fenntartja a jogot a levelezés forgalmának naplózására, a levelezés méretének, gyakoriságának, és ha szükséges tartalmának ellenőrzésére, korlátozására a levelezőszerver, és az Internet kapcsolat sávszélességének hatékonyabb kihasználása, valamint a Hivatal informatikai rendszereinek biztonsága érdekében.

A fenti ellenőrzéseket a Rendszergazda az IBF kérése esetén végzi.

20.5 AI ESZKÖZÖK HASZNÁLATA (A5.32)

Az AI, mint eszköz nem tiltott a Hivatalnál, de a következő szigorú szabályozás vonatkozik a használatára:

FELHASZNÁLÓK - AI-ESZKÖZÖK (CHATGPT, COPILOT, GEMINI, CLAUDE, MISTRAL)

Szabályok:

- AI csak a Hivatal tulajdonában levő eszközzel használható.
- Tilos bizalmas, személyes, üzleti vagy ügyféladatokat megadni AI-eszközben, kivéve, ha a Hivatal írásban engedélyezte az adott platformot, és a használat adatvédelmi feltételei biztonságosan szabályozottak.

- Minden AI által generált tartalom hitelességét és pontosságát ellenőrizni kell, mielőtt azt belső vagy külső kommunikációban felhasználják.
- Az AI által létrehozott kimenet nem tekinthető hivatalos szervezeti állásfoglalásnak és nem szolgálhat önálló döntéstámogató anyagként, csak szakértői kontroll után.
- Az AI-eszközök használata során kötelező betartani a GDPR-t, szerzői jogi és etikai előírásokat, különösen akkor, ha a tartalom harmadik félnek továbbításra kerül.
- Minden AI-használattal kapcsolatos rendellenességet (pl. gyanús adatkérés, hibás működés, adatvesztés, adatszivárgás) haladéktalanul jelenteni kell az informatikai vagy információbiztonsági felelősnek.

RENDSZERGAZDÁK - AI-INTEGRÁCIÓ ÉS ÜZEMELTETÉS

Szabályok:

- AI-rendszer vagy AI-funkció csak jóváhagyott, dokumentált, biztonsági szempontból ellenőrzött módon integrálható a Hivatal informatikai környezetébe.
- API-kulcsok, hitelesítő tokenek és hozzáférési adatok tárolása csak titkosított jelszó- vagy titokkezelő rendszerben engedélyezett.
- Az AI-eszközök kommunikációja csak titkosított hálózati csatornán (pl. TLS) és szűrt hozzáférés-vezérléssel működhet.
- Minden hozzáférést és API-hívást naplózni kell, a naplókat biztonságosan meg kell őrizni és rendszeresen vizsgálni kell biztonsági szempontból.
- AI-eszközök bevezetése és üzemeltetése előtt kötelező kockázatértékelést végezni, amely magában foglalja az adatok típusát, a külső szolgáltatók szerepét és a potenciális kockázatokat.
- Külső AI-szolgáltató használata esetén érvényes adatfeldolgozási megállapodásnak (DPA) és szerződéses biztonsági feltételeknek kell rendelkezésre állnia, és ennek betartását folyamatosan felügyelni kell.

21. ZÁRÓ RENDELKEZÉSEK (A5.4)

A Hivatal vezetője gondoskodik arról, hogy az IBSZ-ben foglaltakat valamennyi a Hivatal feladatellátásában részt vevő alkalmazott megismerje.

Új alkalmazott Szervezethez történő felvétele esetén a Személyügy gondoskodik arról, hogy az alkalmazott a munkaszerződés aláírása előtt megismerje a szabályzat munkaköréhez kapcsolódó fejezeteit.

A Hivatal alkalmazottai tevékenységük ellátása során kötelesek alkalmazni IBSZ-ben foglalt rendelkezéseket, valamint ennek megfelelően kell kialakítaniuk a munkafolyamataikat.

22. MELLÉKLETEK

ALKALMAZOTT MEGNEVEZÉSEK, KIFEJEZÉSEK:

A jelen szabályzatban alkalmazott megnevezések és rövidítések a következők:

- **IBSZ:** Információbiztonsági Szabályzat, jelen eljárásgyűjtemény.
- **adatgazdai terület:** az a szervezeti egység, amelyhez az informatikai rendszerben tárolt adatok kezelése rendelhető, illetve ahol az adat keletkezik.
- **alaprendszer**: az alkalmazói szoftverek működéséhez szükséges alap informatikai szolgáltatásokat megvalósító informatikai rendszerek (pl.: központi címtár, fájl szerver szolgáltatások, levelező rendszer stb.).
- **alkalmazói rendszer**: a Hivatal tevékenységét közvetlenül támogató informatikai rendszer (pl.: Jira, stb.).
- **beépített rendszergazdai fiók:** a szoftverek és hardver eszközök kiemelt jogosultságú, gyárilag beépített rendszergazdai fiókja (pl.: admin, administrator, root, superuser, SA, stb.), amelyek segítségével a rendszerelem felügyelhető, adminisztrálható.
- **belső fejlesztés**: a Hivatal által történő szoftverfejlesztés.
- **elektronikus információs rendszerek biztonságáért felelős személy (IBF):** a Hivatal elektronikus információs rendszerei biztonságáért felelős személy.
- **hálózati megosztás:** a szerveren elhelyezkedő, programokat vagy dokumentumokat tartalmazó fájl mappa, amelyhez a felhasználók jogosultságokkal szabályozható módon hozzáférhetnek.
- **hálózati nyomtató:** közvetlenül a hálózatra kapcsolódó nyomtató vagy multifunkciós (fénymásolásra és szkennelésre is alkalmas) nyomtató.
- **home mappa:** a felhasználók saját használatú fájljai, dokumentumai, felhasználóhoz kötődő beállításai, lekérdezései tárolására a felhasználók rendelkezésére bocsájtott, mások által nem elérhető mappa.
- **illegális szoftver**: érvényes használati engedély (szoftverlicenc) nélkül, vagy nem a licencszerződésnek megfelelően használt szoftver.
- **informatikai azonosító:** az informatikai eszközhöz a Hivatalnál alkalmazott egységes névkonvenció szerint rendelt egyedi azonosító.
- **informatikai erőforrások:** az informatikai rendszer hardver, szoftver, hálózati és környezeti infrastruktúra elemeinek összessége.
- **informatikai eszköz**: számítógép, számítógéphez kapcsolódó periféria (pl.: monitor, billentyűzet, egér, nyomtató, szkenner, pendrive, külső merevlemez stb.) vagy egyéb olyan hardver eszköz (pl. hálózati eszköz), amely az informatikai rendszer működéséhez szükséges.
- **informatikai rendszer:** azon elektronikus információs rendszer, amely magában foglalja a hardver eszközöket, a szoftvereket, a hálózati és környezeti infrastruktúra elemeit, valamint tágabb értelemben a szoftverekben kezelt adatokat, az adathordozókat, a dokumentációkat, szabályzatokat és a rendszert kezelő személyeket.
- **Infotv.**: 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.
- **IT vezető:** az informatikai üzemeltetés, fejlesztés felügyeletével megbízott személye
- **Kiberbiztonsági incidenskezelő központ:** a kijelölt nemzeti kiberbiztonsági incidenskezelő központ, amelynek feladatait a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézetének egy biztonsági eseményekkel foglalkozó akciócsoportja, más néven a nemzeti CSIRT (Computer Security Incident Response Team) látja el.
- **kiemelt kódrendszer**: informatikai rendszerben alkalmazott kiemelt jelentőségű kódrendszer, amelyeket több informatikai rendszer közösen használ és kapcsolódási pontot jelent az egyes informatikai rendszerek között.
- **központi címtár**: a hálózati rendszer felhasználóinak adatait tároló központi adatbázis.

- **kulcsfelhasználó:** az informatikai rendszerhez az adatgazdai terület részéről kijelölt, a rendszerben tárolt adatok védelméért, a rendszer funkcionális működéséért felelős felhasználó.
- **külső fejlesztés**: a Hivatalon kívül egyéb külső fejlesztő cég bevonásával történő szoftverfejlesztés.
- **legális szoftver, jogtiszta szoftver**: érvényes használati engedéllyel (szoftverlicenccel) rendelkező, a licencszerződésnek megfelelően használt szoftver. A vásárolt, bérelt, illetve külső fejlesztésű szoftverek esetében a számla, felhasználói licencszerződés/licencigazolás és az eredeti telepítő adathordozók együttes vagy részbeni meglétével kell hitelt érdemlően bizonyítani a használat jogosságát (számlának minden esetben lennie kell). A belső fejlesztésű szoftverek esetén a szoftverlicenc igazolásához a forrásprogram megléte szükséges.
- **licencköteles szoftver**: olyan szoftver, amely használata használati engedélyhez (szoftverlicenchez) kötött, és amelyért a szoftver szerzője használati díjat kér. Ide tartoznak a vásárolt, bérelt vagy belsőleg fejlesztett, illetve külső fejlesztő cég bevonásával fejlesztett szoftverek.
- **mobil adathordozó**: informatikai eszköznek minősülő, cserélhető adathordozó (pl.: pendrive, külső merevlemez).
- **mobil eszköz:** hordozható számítógép (laptop, notebook) vagy egyéb informatikai és kommunikációs feladatok ellátására használható, operációs rendszerrel, kommunikációs szolgáltatásokkal rendelkező, hordozható eszköz (pl.: mobiltelefon, PDA, táblagép).
- **munkaállomás**: olyan személyi számítógép (PC), amelyet a felhasználó a napi munkája során használ, és amellyel igénybe veheti a szerverek szolgáltatásait. Lehet asztali számítógép (desktop PC) és hordozható számítógép (laptop, notebook).
- **rendszergazda**: az informatikai rendszer felett felügyeletet gyakorló személy.
- **szabad szoftver**: olyan szoftver, amelynek licencszerződéséből kétséget kizáróan megállapítható, hogy a szerző vagyoni jogairól lemond, a szoftver használatáért díjat nem kér (freeware szoftverek), illetve bizonyos korlátozásokkal engedélyezi a szoftver használatát díj fizetése nélkül (shareware vagy demo szoftverek).
- **Szjt:** 1999. évi LXXVI. törvény a szerzői jogról.
- **távoli hozzáférés:** minden olyan hozzáférés a Hivatal informatikai rendszeréhez (felhasználó vagy másik informatikai rendszer által), amelyben a kommunikáció egy külső, nem a Hivatal által ellenőrzött hálózaton (pl. Interneten) zajlik.
- **technikai felhasználói fiók**: nem személyhez, hanem szoftverhez, szolgáltatáshoz vagy hardver eszközhöz kötődő felhasználói fiók, amelyet belsőleg használnak valamely más rendszer szolgáltatásának eléréséhez (pl.: egy alkalmazói szoftver használja adatok tárolásához az adatbáziskezelő szerveren; vagy egy multifunkciós nyomtató szkennelt dokumentumok e-mail-ben történő küldéséhez; stb.).
- **Hibabejelentés (e-mail)**: a Hivatal által alkalmazott, e-mail alapú bejelentési mód, amelynek célja a (külső és belső) felhasználók részéről érkező, informatikai rendszerekkel kapcsolatos hibák és észrevételek fogadása, nyilvántartása és kezelése.
- **Jegyző**: a Hivatal vezetője.
- **védett terület**: az informatikai eszközöket koncentráltan tartalmazó helyiségek (pl.: szerverterem, hálózati rendező helyiség), vagy bizalmas iratokat tartalmazó helyiségek (pl. irattár), illetve a nem védett területnek számító helyiségben elhelyezett egyedi hálózati rack szekrények.
- **vírusvédelmi szoftver**: a vírusok és egyéb kártevők (pl.: férgek, kémprogramok, trójai programok) elleni védekezésre szolgáló program, amely képes felismerni, és a legtöbb esetben eltávolítani a fertőzött számítógépről a kártékony programokat.