Balatonszabadi Polgármesteri Hivatal

Információbiztonsági szabályzata (IBSZ) K7 v3.2

Készült:	2017. december 1.
Utolsó módosítás:	2018. január 17.
Módosította:	Vékás Sándor
Azonosító:	IBSZ v3.2
Oldalak száma:	51

1. ÁLTALÁNOS RENDELKEZÉSEK

1.1. A Szabályozás célja

Balatonszabadi Polgármesteri Hivatal (a továbbiakban: hivatal) Információbiztonsági Szabályzatának (a továbbiakban: IBSZ) célja, hogy a vonatkozó jogszabályokkal (2013. évi L. törvény, 41/2015. (VII. 15.) BM rendelet, 257/2016. (VIII. 31.) Kormányrendelet, 679/2016. EU rendelet) és a hivatal belső rendelkezéseivel összhangban meghatározza a hivatal informatikai rendszerei által kezelt információvagyon bizalmassága, hitelessége, sértetlensége, valamint rendelkezésre állásának biztosítása, funkcionalitása és üzembiztonsága megőrzése érdekében betartandó elveket. Az IBSZ meghatározza az informatikai vezető és az információbiztonságért felelős személy feladatait, valamint az információs rendszer működtetői és felhasználói számára kötelező szabályokat. Az IBSZ kiemelt célja, hogy a hivatal informatikai rendszereinek zavartalan működése biztosítva legyen.

Jelen szabályzat a fentiek keretében védelmi eljárásokat határoz meg, intézkedési jogosultságot állapít meg, valamint ellenőrzési mechanizmusokat állít fel a szabálytalanságok felderítésére és a felelősség megállapítására.

1.2. A Szabályozás hatálya

1.2.1. Az IBSZ személyi hatálya

Az IBSZ személyi hatálya a hivatal valamennyi teljes- vagy részmunkaidős, valamint szerződéses dolgozójára kiterjed. Az IBSZ hatálya kiterjed a hivatal informatikai rendszerének üzemeltetésében és karbantartásában résztvevő cégekre, vállalkozókra, illetve magánszemélyekre (a továbbiakban: Szerződéses partnerek) ***(B01 Szerződéses partnerek listája)*** Az érintettekkel az IBSZ megfelelő pontjait ismertetni kell ***(B03 IT felhasználói szabályzat)***, továbbá nyilatkozniuk kell az IBSZ rájuk vonatkozó előírásainak elfogadásáról és betartásáról az előírások szerinti munkavégzésükhöz ***(B02 Nyilatkozat az IT biztonsági szabályok elfogadásáról)***.

Az IBSZ hatálya kiterjed minden olyan magánszemélyre, illetve gazdasági szervezetre, aki/ami munkavégzése kapcsán bármilyen informatikai eszközzel a hivatal informatikai infrastruktúrájához csatlakozik, illetve azt igénybe veszi. A csatlakozás kizárólag hivatali érdekből történhet.

1.2.2. Az IBSZ tárgyi hatálya

Az IBSZ tárgyi hatálya kiterjed:

- a védelmet élvező adatok teljes körére, felmerülési és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül;
- a hivatal tulajdonában lévő, illetve az általa bérelt, vagy használt valamennyi informatikai berendezésre (számítógépekre, azok tartozékaira és perifériáira);
- a különböző adathordozókra;
- a hivatal számítógépes hálózatára és annak elemeire;
- a számítógépes hálózathoz való kapcsolódást biztosító eszközökhöz tartozó modemekre (szolgáltatói modem, mobil stickek), hálózati útválasztókra (routerek), aktív elemekre és egyéb

olyan speciális eszközökre, melyek az informatikai eszközökhöz, illetve a hálózathoz illeszthetők (pl. switch, hub, pendrive, mobil adattároló, mobiltelefon, digitális fényképezőgép stb.);
- az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, üzemeltetési stb.);
- a rendszer- és felhasználói programokra;
- az adatok felhasználására vonatkozó utasításokra;
- az adathordozók tárolására és felhasználására;
- tulajdonviszonytól függetlenül (tulajdonolt, bérelt stb.) a hivatal területén (állandóan vagy ideiglenes jelleggel) telepített informatikai eszközökre, az azokkal kapcsolatos tevékenységre.

Az IBSZ a tárgyi hatálya alá tartozó elemek teljes életciklusára kiterjed, amely az alábbi szakaszokból áll:
- tervezési szakasz: a rendszer iránti igény, a rendszer célja és a vele szemben támasztott követelményeknek a leírása;
- fejlesztési/beszerzési szakasz: a rendszer fejlesztése, programozása, létrehozása, beszerzése;
- megvalósítási szakasz: a rendszer tesztelése, telepítése, testre szabása;
- üzemeltetés/karbantartás: a rendszer üzemelése, üzemeltetése, hardver- és szoftver-módosítások, karbantartás, események kezelése;
- visszavonás/selejtezés/megsemmisítés szakasz: információk, hardver és szoftver visszavonása az üzemelésből, törlése, megsemmisítése és hosszabb távú megőrzésre való felkészítése.

1.2.3. Az IBSZ időbeli hatálya

Az Információbiztonsági Szabályzatot évente vagy jelentősebb infrastrukturális változás, illetve jogszabályváltozás esetén felül kell vizsgálni és szükség esetén módosítani szükséges, mind hivatali, mind informatikai szakmai szempontok szerint.

1.3. Az IBSZ alapelvei

A hivatal informatikai rendszereiben biztosítani kell informatikai és nem informatikai eszközök és módszerek kombinációjával az érzékeny adatok adatbiztonságát és az ilyen adatokat tároló, feldolgozó, továbbító rendszerek üzembiztonságát. Az egyes rendszerek tervezése és megvalósítása során – *a rendszerben kezelt adatok biztonsági osztályba sorolásának megfelelően* – kell a konkrét IT biztonsági ellenintézkedéseket meghatározni.

A bizalmasság biztosítása lehetővé teszi, hogy az információ a jogosulatlan informatikai egyedek (személyek, csoportok, programok, folyamatok stb.) számára ne legyen elérhető, ne kerüljön nyilvánosságra. Érvényesülnie kell a hivatal és szervezetei által kezelt, felhasznált adatokhoz való hozzáférés tekintetében, elsősorban a szervereken és a felhasználói munkaállomásokon történő adathozzáférések és az adatkezeléseknél felhasznált adathordozók tekintetében, valamint a kommunikáció során.

Az egyedi elszámoltathatóságot a hivatali rendszerekben a felhasználókat egyértelműen azonosító és hitelesítő mechanizmusok megvalósításával és az egyes rendszerekben naplózandó események, a naplórekordok tartalmának meghatározásával és rögzítésével kell biztosítani, amennyiben az adott alrendszer technikailag ezt lehetővé teszi. A naplókat védeni kell a jogosulatlan hozzáférés, módosítás és törlés ellen.

Az információ és a rendszerek rendelkezésre állása érdekében a hivatali rendszerekben biztosítani kell a tárhelyek sértetlenségét, azonosítani kell a rendszerkomponenseket és rendszerkapcsolatokat. Eljárások és mechanizmusok akadályozzák meg a kártékony kódok rendszerbe jutását és az ottani károkozást. Mentési eljárásokat kell kidolgozni az adatokra, dokumentumtárakra, szoftverekre. Az eljárásokat tesztelni, dokumentálni kell. A mentéseknél a rendelkezésre állás biztosításán kívül a bizalmasság és sértetlenség követelményeit is biztosítani kell. Olyan alapszoftvereket és alkalmazásokat kell használni a hivatali rendszerekben, amelyek biztosítják, hogy a rendszer működésének megszakadása után minimális veszteséggel álljon vissza biztonságos állapotba.

A dokumentáltság elve érvényre juttatása érdekében a rendszerek adminisztrátorai számára a biztonságos konfiguráláshoz, használathoz szükséges ismereteket (telepítési, üzemeltetési leírások) tartalmazó telepítési- és használati leírást kell rendelkezésre bocsátani. Felhasználói leírást kell biztosítani az átlagos/általános felhasználó számára. A leírásokat hivatali fejlesztési erőforrások alkalmazása esetén az adott rendszer fejlesztését, kialakítását végző hivatali egységnek kell elkészíteni. Külső fejlesztő közreműködése esetén a fejlesztést végző külső munkatárs készíti el, együttműködve a fejlesztésért felelős hivatali egységgel.

A hitelesség biztosítása érdekében – ahol a hitelesség egy entitás (IT rendszeren belül elkülöníthető tulajdonsággal bíró személy, program, folyamat, adat stb.) olyan tulajdonsága, amely egy vagy több hozzá kapcsolódó tulajdonságot más egyed számára bizonyíthatóvá tesz - a hivatal belső kapcsolataiban a kommunikáló felek, hivatali egységek kölcsönösen és kétségtelenül ismerjék fel egymást és ez az állapot a kapcsolat egész idejére változatlanul fenntartható legyen.

A szükséges és elégséges ismeret elve alapján a rendszer minden felhasználónak biztosítja azokat – de csak azokat – az információkat és funkciókat, amelyek az adott felhasználó feladatainak ellátáshoz szükségesek. A hivatali rendszerekben a felhasználó csak azonosítás és hitelesítés után férhet hozzá a rendszerszolgáltatásokhoz.

Az információtartalom sértetlenségét biztosítani kell a hivatal rendszereiben az adattárolás, kezelés és továbbítás folyamán, azaz adatokat, dokumentumokat, programokat, hardvert és szoftvereszközöket, és ezek konfigurációit csak az arra jogosultak kezelhetik. Ezen elemek észrevétlenül nem módosulhatnak, törlődhetnek. Biztosítani kell, hogy a jogosultak a pontos és helyes információkat dolgozzák fel tevékenységük során.

Folyamatos ellenőrzés biztosítása

Az érintett hivatal folyamatba épített ellenőrzést vagy ellenőrzési tervet hajt végre, amely tartalmazza:

- az ellenőrizendő területeket;
- az ellenőrzések, valamint az ellenőrzéseket támogató értékelések gyakoriságát;
- az érintett hivatal ellenőrzési stratégiájához illeszkedő folyamatos biztonsági értékeléseket;
- a mérőszámok megfelelőségét;
- az értékelések és az ellenőrzések által generált biztonsággal kapcsolatos adatok összehasonlító elemzését;
- az érintett hivatal reagálását a biztonsággal kapcsolatos adatok elemzésének eredményére;
- az érintett hivatal döntését arról, hogy milyen gyakorisággal kell az elemzési adatokat az általa meghatározott személyi- és szerepkörökkel megismertetni (ideértve azok változásait is).

A rendszer életciklus szakaszaiba épített biztonság elvének teljesítése céljából a rendszer teljes életciklusában érvényesülnie kell az információbiztonsági szempontoknak.

A feladatok elkülönítése elvének teljesítése érdekében a szerepkörök kialakítása során a feladatokat úgy kell szétosztani az érintettek között, hogy ne egyetlen személy kezében összpontosuljon a hivatal informatikai rendszereinek adminisztrálása és biztonsági ellenőrzése.

A hivatal elektronikus információs rendszerének kapcsolódása szempontjából szabályozza és belső engedélyhez köti az elektronikus információs rendszerének kapcsolódását más elektronikus információs rendszerekhez, dokumentálja az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.

A hivatal elektronikus információs rendszerének kapcsolódása szempontjából belső engedélyhez köti az elektronikus információs rendszereinek összekapcsolását.

A hivatal külső elektronikus információs rendszerekhez való kapcsolódásokhoz az információbiztonsági szabályzatában szabályrendszert állít fel és alkalmaz, amelynek eredménye lehet az összes kapcsolat engedélyezése vagy tiltása, meghatározott kapcsolatok engedélyezése, meghatározott kapcsolatok tiltása.

A hivatal cselekvési tervet készít, ebben mérföldköveket és felelősöket határoz meg. A kockázatkezelési stratégia és a kockázatokra adott választevékenységek prioritása alapján meghatározott időnként felülvizsgálja és karbantartja a cselekvési tervet. Ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni a hiányosság megszüntetése érdekében. Ha a meghatározott biztonsági szint alacsonyabb, mint az érintett hivatalra érvényes szint, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni az előírt biztonsági szint elérése érdekében.

Előzetes tesztelés és megerősítés

A hivatal kifejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét. A konfiguráció megváltoztatása előtt az új verziót tesztelni kell, ezután dönteni kell annak megfelelőségéről, továbbá dokumentálni kell az elektronikus információs rendszer változtatásait az éles rendszerben történő megvalósítása előtt.

A hivatal megvizsgálja az elektronikus információs rendszerben tervezett változtatásoknak az információbiztonságra való hatását még a változtatások megvalósítása előtt.

1.4. Szerepkörök, tevékenységek, felelősségek

Az informatikai biztonsággal kapcsolatos feladatok szerepkörökhöz rendeltek. A szerepkörök szerinti felelősök kijelölése elsősorban a munkaköri leírásokban történik. Az informatikai infrastruktúra biztonságos működtetésében, illetve az informatikai rendszerekben kezelt adatok védelmének tárgykörében a következő szerepkörök kerülnek meghatározásra:

1.4.1. A hivatal vezetője

A hivatal vezetője a Jegyző (továbbiakban: a hivatal vezetője). Felelős az informatikai rendszerben tárolt adatok védelméért és az adatok biztonságáért. Hatáskörében jogosult a számítógépes adatvédelem és az adatbiztonság megszervezésére és ellenőrzésére.

Feladatai:

- Az irányadó biztonsági osztály tekintetében biztosítja a jogszabályban meghatározott követelmények teljesülését a hivatalra és információs rendszerre vonatkozóan is.
- Biztonságért felelős személyt nevez ki ***(B04 IT Biztonsági Felelős megbízása)***, erről a hatóságok felé tájékoztatást nyújt (***NEIH_REG_1465381745324.frm.enyk***)
- Meghatározza a hivatal elektronikus információs rendszereinek felhasználóira vonatkozó szabályokat ***(B07 Információbiztonsági Szabályzat)***.
- Meghatározza a hivatal elektronikus információs rendszerei védelmének felelőseire, feladataira, és az ehhez szükséges hatáskörre vonatkozó szabályokat, illetve kiadja az információbiztonsági szabályzatot *(B07 Információbiztonsági Szabályzat)*.
- Gondoskodik az oktatásról, az információbiztonsági ismeretek szinten tartásáról ***(B08 IT biztonsági oktatási terv és napló)***.
- Kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik a megfelelésről ***(B09 IT kockázatértékelés)***.
- Gondoskodik az események nyomon követhetőségéről ***(B10 IT biztonsági események naplója)***.
- Biztonsági esemény bekövetkezésekor gondoskodik a gyors és hatékony reagálásról, ezt követően a biztonsági esemény kezeléséről, az érintettek haladéktalan tájékoztatásáról *(B10 IT biztonsági események naplója)*.
- Ha külsős erőforrást vesz igénybe, akkor szerződéses kötelemként gondoskodik a törvényben foglaltak teljesüléséről. A hivatal vezetője ebben az esetben is felelős a meghatározott feladatokért, kivéve, ha jogszabály által kijelölt központosított szolgáltatót kell igénybe venni. Ebben az esetben a szolgáltató felett felügyeletet gyakorló miniszter a felelős.
- Megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.
- A hatóságok felé az ellenőrzéshez lefolytatásához szükséges feltételeket biztosítja.

1.4.2. Az elektronikus információs rendszerek biztonságáért felelős személy

Az elektronikus információs rendszerek biztonságáért felelős személyt (továbbiakban: IBF) a hivatal vezetője nevezi ki *(B04 IT Biztonsági Felelős megbízása)*. Az IBF felel a hivatalnál előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:

- A hivatal vezetőjének közvetlen adhat tájékoztatást, jelentést.
- Gondoskodik a hivatal elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról.
- Elvégzi vagy irányítja a fenti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését.
- Előkészíti a hivatal elektronikus információs rendszereire vonatkozó Információbiztonsági Szabályzatot (IBSZ).
- Meghatározza a rendszerek biztonsági beállításaival kapcsolatos elvárásokat, jogokat, feladatokat.
- Véleményezi az elektronikus információs rendszerek biztonsága szempontjából a hivatal ezen tárgykört érintő szabályzatait és szerződéseit.
- Biztosítja a 2013. évi L. törvény és a 41/2015. (VII. 15.) BM rendelet szerinti követelmények teljesülését.

Az elektronikus információs rendszer biztonságáért felelős személy a 2013. évi L. törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről köteles tájékoztatni a hivatal vezetőjét és a jogszabályban meghatározott szervet.

Az elektronikus információs rendszer biztonságáért felelős személy a hivatal vezetőjének támogatásával biztosítja az e szabályzatban meghatározott követelmények teljesülését. A hivatal valamennyi elektronikus információs rendszerének a tervezésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében közreműködik.

Ha a hivatal az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, akkor az elektronikus információs rendszer biztonságáért felelős személy jogosult a közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatokat, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.

Az elektronikus információs rendszer biztonságáért felelős személy e szabályzat szerinti feladatai és felelőssége más személyre át nem ruházható.

1.4.3. Üzemeltető, informatikus/rendszergazda

Feladata az informatikai infrastruktúra üzemeltetése, fejlesztése és biztonságos működésének elősegítése.

Felelős

- a szerverek és a rajtuk futó alapszoftverek, operációs rendszerek, szolgáltatások, adatbáziskezelők, fájl- és nyomtatószerverek működtetéséért;
- a hivatal mentési rendjében foglaltak szerint az adatmentések elvégzéséért, a mentett adatok biztonságos tárolásáért, a szükséges visszaállításokért;
- a standard felhasználói alkalmazáskörnyezet és az általa nyújtott szolgáltatások és segédalkalmazások, továbbá a ráépülő általános irodai alkalmazások komponensei, továbbá a hivatal felhasználói környezetében már megszokott általános alkalmazások és felhasználói segédprogramok, valamint a hálózati nyomtatók működtetéséért;
- az aktív és passzív hálózati eszközök működtetéséért, rendelkezésre állásáért;
- az adatbázisban tárolt adatok és szoftverek rendelkezésre állásáért, a hozzáférők adminisztrálásért.

1.4.4. Honlaptartalom kezelő

A hivatal honlapjának tartalomkezelését a Polgármesteri Hivatal kijelölt ügyintézője végzi.

A jogszabály által előírt kötelezően nyilvános közadatokat - változás esetén - a közzétételi egységekhez rendelt ügyintéző vagy irodavezető továbbítja elektronikus levélben az erre felhatalmazott honlaptartalom kezelőhöz.

1.4.5. Felhasználó

A hivatali rendszerek nem üzemeltető felhasználója.

- Ismernie kell az Információbiztonsági Szabályzatban szereplő előírásokat, illetve azokat maradéktalanul be kell tartania.
- Rendelkeznie kell az általa használt berendezésekre és szoftverekre vonatkozó előírásokkal, valamit ismernie kell azok tartalmát.
- Tevékenysége megkezdésekor ellenőriznie kell, hogy az általa használt eszközök üzemképesek-e és azok beállítása az előírásoknak megfelelő-e.
- Köteles figyelemmel kísérni az általa használt berendezések és szoftverek állapotát és az esetleges meghibásodást vagy helytelen működést azonnal jeleznie kell a közvetlen vezetőnek.
- Munkája során figyelnie kell arra, hogy illetéktelen személyek lehetőleg ne tartózkodjanak az adat/információ feldolgozása során a helyiségben.
- Tevékenysége befejezésekor a használt programokból szabályszerűen ki kell lépjen.
- Hálózati információ igénybevételét követően a hálózatból szabályosan ki kell lépjen.
- A berendezéseket szükség esetén az előírásoknak megfelelően le kell állítania, illetve az áramellátásukat meg kell szüntetnie.
- A helyiségből utolsóként való távozáskor meg kell győződnie a helyiség biztonságos lezárásáról.

1.5. A vezetőség elkötelezettsége, a pénzügyi erőforrások biztosítása

A hivatal vezetősége elkötelezett az információbiztonság menedzselése iránt. Ennek megfelelően:

- Az információbiztonság ügyének szükséges mértékű publicitást biztosít a hivatal keretein belül, valamint gondoskodik a munkatársak megfelelő felvilágosításáról, tájékoztatásáról, oktatásáról;
- A szükséges anyagi-, humán- és technikai erőforrásokat biztosítja;
- A beruházások, beszerzések során tervezi az információbiztonsági stratégia megvalósításához szükséges forrásokat, dokumentálja e követelmény alá eső kivételeket.
- Az információbiztonság irányítására felelőst delegál és ruház fel a szükséges jogokkal;
- Gondoskodik a biztonsági dokumentációkban található előírások betartásáról, auditot folytat le (***B11 IT Biztonsági auditjelentés***) és be nem tartás esetére szankciókat határoz meg, illetve foganatosít a köztisztviselőkre vonatkozó törvények (2011. évi CXCIX. törvény, 31/2012 (III. 7.) Kormányrendelet) szerint;
- Támogatja a rendszer használóinak az információbiztonságot fejlesztő törekvéseit.

Mivel a hivatali információvagyon biztonsága nem kizárólag az annak kezelésével megbízott személyek feladata és felelőssége, ezért a vezetőség elvárja, hogy a hivatal minden dolgozója és szerződéses partnere sajátjának tekintse az információ biztonságának ügyét, és azt külön utasítás nélkül támogassa feladatán és hatáskörén belül.

1.6. Az IBSZ jogi háttere

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 41/2015. számú BM rendelet - az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről

- 257/2016. (VIII. 31.) Kormányrendelet az önkormányzati ASP rendszerről
- 679/2016. EU rendelet (GDPR)
- 466/2017. (XII. 28.) Kormányrendelet az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról

2. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

2.1. Információbiztonsági politika

A hivatal megfogalmazza és kihirdeti az információbiztonsági politikát (a továbbiakban IBP) ***(B06 Információbiztonsági Politika)***, melyben meghatározza a kiberbiztonsági célokat, kifejti az alkalmazott biztonsági alapelveket és megfelelőségi követelményeket, valamint bemutatja a vezető beosztású tagjainak elkötelezettségét a biztonsági feladatok irányítása és támogatása iránt.

Az IBP felülvizsgálata és esetleges frissítése évente vagy az elektronikus információs rendszert érintő változások, illetve jogszabályváltozás esetén esedékes.
Felelős: a hivatal vezetője

2.2. Információbiztonsági stratégia

A hivatal megfogalmazza és kihirdeti az információbiztonsági stratégiát (a továbbiakban IBS), ***(B05 Információbiztonsági Stratégia)*** amely meghatározza a biztonságpolitikai célok megvalósításának módszerét, eszközrendszerét, ütemezését. Az IBS illeszkedik a hivatal más stratégiáihoz, így különösen a költségvetési és humánerőforrás tervezéshez, fejlesztéshez, jövőképhez, illetve a működtetett minőségirányítási, vagy információbiztonság-irányítási rendszerekhez.

Az IBS felülvizsgálata és esetleges frissítése évente, vagy az elektronikus információs rendszert érintő változások esetén, illetve jogszabály változás esetén esedékes.
Felelős: a hivatal vezetője

2.3. Az elektronikus információs rendszerek nyilvántartása

A hivatal az elektronikus információs rendszereiről nyilvántartást vezet ***(B12 IT leltár)***. A nyilvántartást elektronikus formában vezeti és gondoskodik annak naprakészségéről.

A nyilvántartásnak minden rendszerre nézve tartalmaznia kell:
- annak alapfeladatait;
- a rendszerek által biztosítandó szolgáltatásokat;
- az érintett rendszerekhez tartozó licenc számot (amennyiben azok a hivatal kezelésében vannak);
- a rendszer felett felügyeletet gyakorló személy azonosító- és elérhetőségi adatait;
- a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító- és elérhetőségi adatait, valamint ezen hivatalok rendszer tekintetében illetékes kapcsolattartó személyeinek azonosító- és elérhetőségi adatait.

A különböző adatokat nem szükségszerűen egy nyilvántartásban kell tárolni, hanem logikus módon szétválaszthatók. Az adatok feltöltéséről mindig az adott rendszerrel kapcsolatos feladatot elvégző informatikus gondoskodik.

Minden rendszereszközt a beszerzéssel egyidejűleg fel kell venni a nyilvántartásba. A nyilvántartásból rendszereszközt kivenni csak annak selejtezésekor lehet.

2.3.1. Elektronikus információs rendszerelem leltár

A hivatal az elektronikus információs rendszerének elemeiről elektronikus formában vezetett nyilvántartást vezet, mely az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet tartalmazza. Rendszeres felülvizsgálatokkal gondoskodni kell arról, hogy a nyilvántartás mindig naprakész legyen, pontosan tükrözze az elektronikus információs rendszer aktuális állapotát. *(B12 IT leltár)*
Felelős: Üzemeltetői csoport

2.4. Biztonsági osztályba sorolás

Adatbiztonság szempontjából a hivatal kezelésében lévő elektronikus formában tárolt információkat, eszközöket, erőforrásokat és szolgáltatásokat a kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából 1-től 5-ig terjedő skálán – a kockázat növekedésével arányosan növekvő - biztonsági osztályokba kell sorolni. A besorolás eredményét melléklet formában rögzíteni kell az információbiztonsági szabályzatban is. *(B12 IT leltár)*

A besorolást minimum kétévente, de minden, az elektronikus információs rendszereket érintő változás után, illetve jogszabályváltozás esetén felül kell vizsgálni és szükség esetén ismételten el kell végezni.

2.5. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás

Az új belépő munkatársak a belépéskori oktatás *(B08 IT biztonsági oktatási terv és napló)* és a titoktartási nyilatkozat ***(B14 Titoktartási nyilatkozat)*** aláírása után kaphatnak hozzáférést a rendszerekhez. A belépő munkatárs új hozzáférési jogkörét, illetve nem új belépő munkatárs hozzáférési jogkör változtatását a felettes vezetője határozza meg.

A meghatározás során az érintett vezető a ***B15 Hozzáférések igénylése és letiltása*** formanyomtatványon összegzi az általa szükségesnek tartott hozzáféréseket és azokat jóváhagyatja a hivatal vezetőjével. Amennyiben a hivatal vezetője nem járul hozzá a kért jogosultságok kiadásához, úgy az ahhoz való hozzáférést megtilthatja, de ezen döntését indokolnia kell az igénylő felé, aki az IBF döntését kérheti a jogosultság kiadásának kérdésében.

A jóváhagyott formanyomtatványt az igénylő vezető továbbítja az érintett rendszer adminisztrátora felé, akinek felelőssége, hogy csak a jóváhagyott jogosultságokat állítsa be. A rendszergazdának tilos az engedélyben nem szereplő jogosultságot beállítani. A beállítások megfelelőségét az IBF szúrópróbaszerűen ellenőrizheti.

Amennyiben az információbiztonsági szabályozásban, feladat- vagy felelősségi köröket érintő változások következnek be, úgy a változtatásokat vezetői jóváhagyás után át kell vezetni a munkaköri leírásokba és azokat aláírással érvényesíttetni az érintettekkel. Amennyiben a módosított munkaköri leírásokkal kapcsolatban az érintett munkavállalóknak észrevétele van, azt az IBF felé tehetik meg.

Amennyiben a változások vállalkozói szerződéseket érintenek, úgy a hivatal vezetése kezdeményezi az érintett vállalkozói szerződések módosítását, illetve kiegészítését a biztonsági követelményeknek megfelelően és menedzseli a szerződések módosítását és azok aláírással történő érvényesítését.

Új munkakörök kialakítása során a hivatal vezetője tájékoztatja az IBF-et a munkakör feladatairól és tervezett jogosultságairól. Az IBF javaslattal élhet a munkakör feladatainak biztonsági vonatkozásait illetően.

2.6. Biztonságtervezési eljárásrend

A hivatal...

- megfogalmazza, a hivatalra érvényes követelmények szerint dokumentálja, és a munka- és feladatkörük miatt érintettek számára kihirdeti a biztonságtervezési eljárásrendet mely a biztonságtervezési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
- a biztonságtervezési eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a biztonságtervezési eljárásrendet.

Biztonságtervezési szempontból a hivatal az alábbi időszakokat definiálja az információs rendszerek életciklusának tekintetében:

- követelmény meghatározás;
- fejlesztés vagy beszerzés;
- megvalósítás vagy értékelés;
- üzemeltetés és fenntartás;
- kivonás (archiválás, megsemmisítés).

A rendszerbiztonság tervezésekor a hivatal az információs rendszerek valamennyi életciklusára vonatkozóan szem előtt tartja a *B06 Információbiztonsági Politikában* megfogalmazott célokat és követelményeket, valamint a gyártói és iparági előírásokat, ajánlásokat.

A hivatal vezetője évente legalább egyszer felülvizsgálja és frissíti a biztonságtervezési eljárásrendet.

2.7. Rendszerbiztonsági terv

A hivatal az elektronikus információs rendszeréhez rendszerbiztonsági tervet készít ***(B17 Rendszerbiztonsági terv)***, amely...

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

- gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és szerepkörökben dolgozók megismerjék (ideértve annak változásait is);
- belső szabályozásában, vagy a rendszerbiztonsági tervben meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszer rendszerbiztonsági tervét;
- frissíti a rendszerbiztonsági tervet az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások, és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén;
- elvégzi a szükséges belső egyeztetéseket;
- gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

Ha egy adott információs rendszer jelentősége nem indokolja, illetve a jogi-, szabályozási- és üzemeltetési körülmények nem teszik lehetővé, a hivatal vezetője az IBF egyetértésével eltekinthet az adott rendszerre vonatkozó rendszerbiztonsági terv készítésétől.

2.8. Személyi biztonság

A hozzáférési jogosultságot igénylő felhasználóval szembeni elvárásokat, a rá vonatkozó szabályokat, felelősségeket, az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységeket jelen dokumentum, valamint az adott rendszerdokumentáció tartalmazza. A hozzáférés engedélyezése előtt a hozzáférési jogosultságot igénylő személynek írásbeli nyilatkozatot (*B02 Nyilatkozat az IT biztonsági szabályok elfogadásáról*) kell tennie arról, hogy az érintett rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja.

2.9. Rendszer és szolgáltatás beszerzés

2.9.1. Beszerzési eljárásrend

A hivatal...

- megfogalmazza és a hivatalra érvényes követelmények szerint dokumentálja, valamint a hivatalon belül kihirdeti a beszerzési eljárásrendet (***B18 Beszerzési eljárásrend***), mely a hivatal elektronikus információs rendszerére, az ezekhez kapcsolódó szolgáltatások és információs rendszer biztonsági eszközök beszerzésére vonatkozó szabályait fogalmazza meg (akár az általános beszerzési szabályzat részeként), és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
- a beszerzési eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a beszerzési eljárásrendet.

2.9.2. A rendszer fejlesztési életciklusa

Az informatikai eszközök különböző beszerzési eljárásmódjainak alkalmazásánál fokozottan szem előtt kell tartani, hogy a szóban forgó eszköz megfeleljen a jelen szabályzatban rögzített információbiztonsági követelményeknek.

A hivatal az elektronikus információs rendszereinek teljes életútján, azok minden életciklusában figyelemmel kíséri információbiztonsági helyzetüket. Fejlesztés esetén már a rendszer tervezésénél fokozottan figyelembe kell venni az információbiztonsági előírásokat, ajánlásokat. A hivatal a fejlesztési életciklus egészére meghatározza és dokumentálja az információbiztonsági szerepköröket és

felelősségeket, valamint a hivatalra érvényes szabályok szerint kijelöli az ezen szerepköröket betöltő, ezekért felelős személyeket.

Az informatikai üzemeltetés az általa kiadott/telepített informatikai eszközökről (hardver, szoftver, fejlesztett rendszerek kiadása, telepítése, verziókövetés) naprakész nyilvántartást vezet *(B12 IT leltár).*

2.10. Biztonságelemzési eljárásrend

A hivatal megfogalmazza, és az érintett hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett hivatalon belül kihirdeti a biztonságértékelési eljárásrendet, amely a biztonságértékelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő, valamint a biztonságértékelési eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a biztonságértékelési eljárásrendet.

A hivatal biztonságértékelési tervet készít, melyben meghatározott gyakorisággal értékeli az elektronikus információs rendszer és működési környezete védelmi intézkedéseit, kontrollálja a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelő működését, elkészíti a biztonságértékelés eredményét összefoglaló jelentést, valamint gondoskodik a biztonságértékelés eredményét összefoglaló jelentésnek az érintett hivatal által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismeréséről.

A biztonsági értékelés tartalmazza:

- az értékelendő (adminisztratív, fizikai és logikai) védelmi intézkedéseket;
- a biztonsági ellenőrzések eredményességét meghatározó eljárásrendeket;
- az értékelési környezetet, az értékelő csoportot, az értékelés célját, az értékelést végzők feladatát.

Az érintett hivatal kifejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét.

2.11. Tesztelés, felügyelet

A hivatal megfogalmazza és dokumentálja, valamint kihirdeti az elektronikus információs rendszer tesztelésével, képzésével és felügyeletével kapcsolatos eljárásokat, amelyek támogatják a tesztelési, képzési és felügyeleti tevékenységek fejlesztését és fenntartását, valamint folyamatos időbeni végrehajtását. A hivatal felülvizsgálja a tesztelési, képzési és ellenőrzési terveket a kockázatkezelési stratégia és a lehetséges, vagy bekövetkezett biztonsági események súlya alapján.

Az érintett hivatal kifejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét.

A hivatal az elektronikus információs rendszerei és alkalmazásai tekintetében legalább kétévente sérülékenység tesztet végeztet, ha azt az elektronikus információs rendszerfejlesztési, üzemeltetési és használati körülményei lehetővé teszik, valamint olyan esetben, amikor új, lehetséges sérülékenység merül fel az elektronikus információs rendszerrel vagy alkalmazásaival kapcsolatban.

A sérülékenység tesztet külső hivatal bevonásával azon elektronikus információs rendszerek tekintetében végezteti el, amelyek az érintett hivatal felügyelete, irányítása alatt állnak. Az elektronikus információs rendszer különleges jogosultsághoz kötött - úgynevezett privilegizált -

hozzáférést biztosít az érintett hivatal által kijelölt rendszerelemekhez a sérülékenység teszt végrehajtásához.

A tesztet végző...

- kimutatást készít a feltárt hibákról, valamint a nem megfelelő konfigurációs beállításokról;
- végrehajtja az ellenőrzési listákat és tesztelési eljárásokat;
- felméri a sérülékenység lehetséges hatásait;
- elemzi a sérülékenység teszt eredményét;
- megosztja a sérülékenység teszt eredményét a jegyzővel és a rendszergazdával;
- olyan sérülékenységi teszteszközt alkalmaz, melynek sérülékenység feltáró képessége könnyen bővíthető az ismertté váló sérülékenységekkel;
- meghatározza, hogy egy támadó milyen információkat képes elérni az elektronikus információs rendszerben, és ennek elhárítására javítási javaslatokat tesz.

Hivatalos sérülékenység vizsgálatot kizárólag a Kormányzati Eseménykezelő Központ (GovCERT-Hungary) végezhet. A teszt eredményének függvényében az informatikai vezető utasításokat ad a rendszergazdának a feltárt hiányosságok megszüntetésére vonatkozóan.

2.12. Biztonsági eseménykezelési eljárásrend

A hivatal eseménykezelési eljárást dolgoz ki a biztonsági eseményekre, amelyek magukban foglalják az előkészületet, az észlelést, a vizsgálatot, az elszigetelést, a megszüntetést és a helyreállítást;

- egyezteti az eseménykezelési eljárásokat az üzletmenet-folytonossági tervéhez tartozó tevékenységekkel;
- az eseménykezelési tevékenységekből levont tanulságokat beépíti az eseménykezelési eljárásokba, a fejlesztési és üzemeltetési eljárásokba, elvárásokba, továbbképzésekbe és tesztelésbe;
- nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági eseményeit;
- mindenkitől, aki az elektronikus információs rendszerrel, vagy azok elhelyezésére szolgáló objektummal kapcsolatban áll megköveteli, hogy jelentsék a biztonsági esemény bekövetkeztét, vagy ha erre utaló jelet, vagy veszélyhelyzetet észlelnek;
- jogszabályban meghatározottak szerint jelenti a biztonsági eseményekre vonatkozó információkat az elektronikus információs rendszerek biztonságának felügyeletét ellátó szerveknek;
- tanácsadást és támogatást nyújt az elektronikus információs rendszer felhasználóinak a biztonsági események kezeléséhez és jelentéséhez;
- biztonsági eseménykezelési tervet dolgoz ki, amely...
  - az érintett hivatal számára iránymutatást ad a biztonsági esemény kezelési módjaira;
  - ismerteti a biztonsági eseménykezelési lehetőségek struktúráját és hivatalát;
  - átfogó megközelítést nyújt arról, hogy a biztonsági eseménykezelési lehetőségek hogyan illeszkednek az általános hivatalba;
  - kielégíti az érintett hivatal feladatkörével, méretével, hivatali felépítésével és funkcióival kapcsolatos egyedi igényeit;
  - meghatározza a bejelentésköteles biztonsági eseményeket;
  - meghatározza és folyamatosan pontosítja a biztonsági események kiértékelésének, kategorizálásának (súlyosság stb.) kritériumrendszerét;

- támogatást ad a biztonsági eseménykezelési lehetőségek belső mérésére;
- meghatározza azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására;
- kihirdeti és tudomásul veteti a biztonsági eseménykezelési tervet a biztonsági eseményeket kezelő (névvel és/vagy szerepkörrel azonosított) személyeknek és hivatali egységeknek;
- meghatározott gyakorisággal felülvizsgálja a biztonsági eseménykezelési tervet;
- frissíti a biztonsági eseménykezelési tervet, figyelembe véve az elektronikus információs rendszer és a hivatal változásait vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat;

- gondoskodik arról, hogy a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető, módosítható.
- biztonsági eseménykezelési képzést biztosít az elektronikus információs rendszer felhasználóinak a számukra kijelölt szerepkörökkel és felelősségekkel összhangban;
- a képzést a biztonsági eseménykezelési szerepkör vagy felelősség kijelölését követő, meghatározott időtartamon belül, vagy amikor ezt az elektronikus információs rendszer változásai megkívánják, vagy meghatározott gyakorisággal tartja.

3. ADATOK ÉS IT RENDSZEREK VÉDELME, BIZTONSÁGA

Jelen fejezet alkalmazása során figyelemmel kell lenni a más jogszabályban meghatározott tűz-, vagyon- és személyvédelmi, valamint a személyes adatok kezelésére vonatkozó rendelkezésekre, valamint arra, hogy e fejezet rendelkezései az adott létesítmény bárki által szabadon látogatható vagy igénybe vehető területeire nem vonatkoznak.

3.1. Fizikai védelmi intézkedések

Azon helyiségek kijelölése, illetve kialakítása során, amelyekben a hivatal kiemelt fontosságú kiszolgáló számítógépei (szerverei) kerülnek elhelyezésre, különös figyelmet kell fordítani a fokozott biztonságra. A helyiség (szerverszoba) közelében nem üzemelhet tűz- és robbanásveszélyes raktár. A helyiségben független áramellátással működő tűzjelző rendszert kell kiépíteni, a bejárat közelében az informatikai eszközökhöz megfelelő oltóberendezést kell elhelyezni. A berendezések üzembiztonságát az előírásoknak megfelelően időszakosan ellenőrizni kell. A szerverszobában az erőforrások biztonságos működéséhez szükséges szinten kell tartani a hőmérsékletet és páratartalmat (klímaberendezés), valamint figyelni kell ezek szintjét.

3.1.1. Fizikai védelmi eljárásrend

A fizikai és környezeti biztonságra vonatkozó óvintézkedések a hivatali rendszereknek helyet adó létesítmények, a rendszer-erőforrások és a működést biztosító alapszolgáltatások védelmével kapcsolatban fogalmaznak meg szabályokat annak érdekében, hogy a számítástechnikai szolgáltatások megszakadását, eszközök ellopását, a fizikai károkozást, az információk jogosulatlan felfedését, a rendszer sértetlenségének elvesztését megakadályozzák.

A hivatal legalább éves gyakorisággal felülvizsgálja és frissíti a fizikai védelmi eljárásrendet.

A hivatali számítógépek és adathordozók fizikai védelmét biztosítani kell a hivatalban lopás, rongálás, megsemmisülés ellen értékarányos módszerekkel és eljárásokkal (pl. élőerős védelem és fizikai védelem – rácsok, ajtók, riasztóberendezés).

A hardverek és adatok részleges vagy teljes megsemmisülésével fenyegető tüzek megelőzése és elhárítása a *Tűzvédelmi Szabályzat* rendelkezései szerint történik.

Az infrastrukturális gyengeségek és hiányosságok kivédése érdekében az egyes rendszerek biztonsági osztályba sorolása után gondoskodni kell a megfelelő infrastruktúra biztosításáról. Ilyenek lehetnek a következők: szünetmentes áramellátás, hőmérséklet és páratartalom szabályozó rendszer, beléptető rendszer stb.

A hivatal informatikai rendszeréhez nem a hivatali infrastruktúrájához tartozó (pl. magántulajdonú) számítástechnikai, kommunikációs, multimédiás berendezést vagy adathordozót kapcsolni tilos! Amennyiben hivatali érdekből szükséges ilyen eszköz használata, úgy az csak a hivatal vezetőjének vagy az IBF-nek az engedélye alapján, az informatikus bevonásával, dokumentálási kötelezettség mellett végezhető el ***(B21 Idegen eszköz használatának engedélyezése)***.

A hivatal tulajdonában lévő vagy bérelt számítástechnikai berendezések behozatala, kivitele (javítás céljából, máshol történő használatra stb.) csak hivatali céllal lehetséges, amelyet az IBF vagy a hivatal vezetője engedélyezhet ***(B22 IT eszköz kiviteli-behozatali engedélye)***. Ezeket az eseteket dokumentálni kell. Nem kell alkalmanként dokumentálni a személyes használatra, név szerint, tartósan átadott eszközök mozgatását (pl. hivatali laptopok, telefonok stb.) *(B28 IT eszközök használatba adása és visszavétele)*.

A javítás céljából a hivatalból kikerülő eszközök esetében biztosítani kell, hogy a hivatal által kezelt adatok ne kerüljenek ki. Olyan meghibásodott eszközök (PC, mobil eszköz, szerver stb.), amelyekben az adathordozók védendő adatokat tartalmazhatnak, nem kivihetők az adathordozó alkatrésszel. Ebben az esetben az adathordozót (merevlemez, statikus memória egység stb.) a javítás idejére cserealkatrésszel kell a gépben helyettesíteni, vagy ha nem szükséges ez az alkatrész a működéshez, akkor az eredeti adathordozó és cserealkatrész nélkül kell javítási célból kivinni a hivatalból. Az eredetileg használt adathordozót a javítás után vissza kell helyezni az eszközbe, vagy arról az adatokat az új eszközre át kell tenni. Amennyiben az eredeti adathordozó alkatrész nem kerül vissza az adott eszközbe, úgy az adathordozót a szabályzat „4.4 Adathordozók védelme" fejezetében meghatározottak szerint kell kezelni.

3.1.2. Fizikai belépés ellenőrzése, belépési engedélyek

A hivatal székhelyén 3 biztonsági zóna van elkülönítve:

1. zóna A bejutás ellenőrzötten lehetséges, látogató felügyelet nélkül bent tartózkodhat. Informatikai eszköz nem lehet a zónában. A zónába tartozó helyiségek: *folyosó, lépcsőház*

2. zóna A bejutás kulccsal vagy beléptető rendszerrel lehetséges, látogató csak felügyelettel tartózkodhat a területen. A zónába tartozó helyiségek: *iroda, tárgyaló*

3. zóna A bejutás kulccsal vagy beléptető eszközzel, csak ideiglenesen, belépési naplót vezetve lehetséges. A kiemelt fontosságú informatikai eszközöket itt kell elhelyezni. Kizárólag az

informatikus tartózkodhat bent kíséret nélkül, másokat az informatikusnak kell kísérni. A zónába tartozó helyiségek: *szerverszoba*

A 2. és 3. zónába tartozó helyiségeket – amennyiben nem folyik bennük munkavégzés – kulcsra zárva kell tartani vagy elektronikus beléptetőrendszerrel kell védeni. A helyiségek kulcsait elzárva kell tartani és csak az arra jogosultaknak szabad kiadni. A kulcsok kiadását és visszavételét dokumentálni kell.

Az új belépő munkatársak kulcsokat és/vagy kártyákat csak a belépést követő oktatás *(B08 IT biztonsági oktatási terv és napló)* megtörténte és a titoktartási nyilatkozat *(B14 Titoktartási nyilatkozat)* aláírása után kaphatnak. A belépő munkatárs új belépési jogosultságait, illetve nem új belépő munkatárs belépési jogosultságainak változtatását az érintett terület vezetője határozza meg. A meghatározás során a terület vezetője a *B15 Hozzáférések igénylése és letiltása* formanyomtatványon összegzi az általa szükségesnek tartott belépési jogosultságokat és azokat jóváhagyatja a hivatal vezetőjével.

A jóváhagyott *B15 Hozzáférések igénylése és letiltása* formanyomtatvány továbbításra kerül a kulcsok/azonosító kártyák/kódok kiosztásának felelőse felé, akinek felelőssége, hogy csak a vezetőség által jóváhagyott jogosultságokat állítsa be, csak a megfelelő kulcsokat/kódokat adja ki. Amennyiben felmerül a jóváhagyás hiteltelenségének gyanúja, úgy azt köteles a kulcskiadás előtt igazoltatni a vezetőség megkérdezésével. A kulcsokat vagy kódokat évente cserélni kell, a jogosultságok felülvizsgálatával együtt.

A helyiség (szerverszoba) közelében nem üzemelhet tűz- és robbanásveszélyes raktár. A helyiségben tűzjelző rendszert kell kiépíteni, amelynek üzembiztonságát az előírásoknak megfelelően időszakosan ellenőrizni kell.

A helyiséget mindig zárva kell tartani. A helyiség kulcsait munkaidőben csak az informatikai vezető, illetve az általa felhatalmazott informatikus veheti fel, mivel a szerver sértetlensége, rendelkezésre állása az ő felelősségük. A felvétel tényét minden esetben nyilván kell tartani a ***B25 Szerverszoba belépési nyilvántartás*** nyomtatványon. A nyomtatványt legalább egy évre visszamenőleg meg kell őrizni. Munkaidőn kívül a kulcsokat elzártan kell tartani. A helyiségben idegen személy felügyelet nélkül nem tartózkodhat. A belépések rögzítése történhet elektronikus beléptető rendszer használatával is. Ebben az esetben csak az informatikai vezető és az általa felhatalmazott informatikus kártyája nyithatja az ajtót, illetve ők ismerhetik az ajtónyitó kódokat.

A belépésre jogosultak listáját mindig naprakészen kell tartani (***B23 Belépésre jogosultak***), akinek a belépése már nem indokolt, el kell távolítani a listáról, a belépési jogosultságot igazoló dokumentumait/eszközeit vissza kell vonni.

A belépési jogosultságokat a belépési pontokon a portaszolgálat ellenőrzi, a látogatók (vendégek, ügyfelek) belépéseiről nyilvántartást vezet a látogatóktól elkért fényképes igazolvány alapján. A belépési nyilvántartás tartalmazza a látogató nevét és személyi igazolványának számát. A nyilvántartás adatvédelmi okokból egy hónap után megsemmisítendő. A látogatók csak kísérettel mozoghatnak a hivatal 2. és 3. zónába tartozó területein. A zónahatárokon biztosági kamerát vagy elektronikus beléptetőrendszert kell üzemeltetni.

Az elektronikus információs rendszereknek helyt adó létesítményekbe belépésre jogosultakról a hivatal nyilvántartást vezet a *B23 Belépésre jogosultak* listáján, és belépési jogosultságot igazoló eszközöket (pl. kitűzők, azonosító kártyák) bocsát ki a részükre ***(B24 Azonosító kártya)***.

A hivatal által meghatározott ideig (de legalább egy évig) megőrzi az elektronikus információs rendszereknek helyt adó létesítményekbe történt látogatói belépésekről szóló információkat. A hivatal azonnal átvizsgálja a látogatói belépésekről készített információkat és/vagy felvételeket, ha a rendelkezésre álló információk jogosulatlan belépésre utalnak.

A hivatal helyiségeiben a hatályos előírásoknak megfelelő vészvilágítást és menekülési útvonal jelzéseket kell elhelyezni, illetve üzemeltetni.

3.2. Hivatali és személyzeti szabályok

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

3.2.1. Felvételi eljárás során követendő szabályok, személyes követelmények

A hivatal meghatározza a felvételi eljárás során követendő szabályokat ***(B26 Felvételi eljárásrend)***, személyes követelményeket. A követelményeket a Munkaköri leírásokban rögzíti.

3.2.2. Képzési eljárásrend

A felhasználói állományt az informatikai biztonság megvalósítása érdekében munkakörüknek megfelelően képezni kell, a fejlesztői, üzemeltetői állománynak pedig folyamatosan szinten kell tartania és fejlesztenie kell az informatikával és informatikai biztonsággal kapcsolatos ismereteit. A felhasználói személyi állományt új rendszerek bevezetésekor képezni kell. A hivatalban alkalmazott új dolgozót - vezetője kérése alapján- soron kívül kell oktatni a rendszer használatáról.

A követelmények és a ténylegesen rendelkezésre álló erőforrások összevetése alapján évente oktatási terv *(B08 IT biztonsági oktatási terv és napló)* készül. Ez tartalmazza a szükséges oktatásban résztvevők körét, az oktatás/képzés témakörét és követelményeit. A tervezett képzéseknél figyelembe kell venni a minőségi, környezeti, a munkahelyi egészségvédelmi és biztonsági, illetve az információbiztonsági célok kapcsán megfogalmazott, jövőben elvárt kompetenciákat.

Ezeken túlmenően a hivatal nyitott munkatársainak egyéni teljesítményét javító igények tekintetében is, és ezért – eseti elbírálás alapján – figyelembe veszi a vezetők és a beosztottak saját továbbképzési igényét is, ha azok összhangban vannak a hivatal hosszú távú stratégiájával.

Az oktatás mellett a teljes felhasználói állománnyal ismertetni kell az IBSZ rájuk vonatkozó előírásait (*B03 Információbiztonsági Szabályzat (IFSZ)*). A felhasználók nyilatkozatot adnak arról, hogy az ismertetés megtörtént, a szabályzatban foglaltakat megértették és azokat maradéktalanul betartják *(B02 Nyilatkozat az IT biztonsági szabályok elfogadásáról)*.

3.2.3. Biztonság tudatosság képzés

A hivatal annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára:

- az új felhasználók kezdeti képzésének részeként (*B08 IT biztonsági oktatási terv és napló*);
- új szerepkörbe vagy felelősségbe kerülésükkor
- amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;
- legalább évente informatikai és IT-biztonsági képzés, ismeret-felfrissítés (*B08 IT biztonsági oktatási terv és napló*).

3.2.4. Fegyelmi intézkedések

A biztonsági előírásokat megsértőkkel szemben fegyelmi eljárás indul. Fegyelmi eljárást az érintett munkavállaló közvetlen vezetője, az IBF, illetve a hivatal vezetője kezdeményezhet írásban ***(B27 IT biztonsági fegyelmi eljárás kezdeményezése és jegyzőkönyve)***. A kezdeményezésnek tartalmaznia kell:

- a fegyelmi eljárást kezdeményező nevét, beosztását;
- a valószínűsíthető fegyelmi vétséget elkövető (érintett) nevét, beosztását;
- az észlelés idejét, módját;
- a fegyelmi vétség elkövetésének idejét, módját, körülményeit;
- a keletkező károk és egyéb következmények kifejtését;
- a kezdeményezés idejét.

A hivatal vezetője a kezdeményezést elbírálja, melyről értesítést küld a kezdeményezőnek és az IBF-nek. Kitűzi továbbá a fegyelmi eljárás feltáró megbeszélésének időpontját és meghatározza az azon résztvevő személyek körét.

A fegyelmi eljárás az alábbi szakaszokra tagolódik:

- feltáró megbeszélés;
- adatgyűjtés, adatértékelés;
- záró megbeszélés.

A feltáró megbeszélésen jelen van:

- a hivatal vezetője;
- az eljárást kezdeményező;
- az eljárásban érintett személy;
- az IBF, amennyiben biztonságot érintő fegyelmi vétségről van szó;
- az eseményben érintett egyéb személyek;
- azok, akiket erre a megbeszélésre a hivatal vezetője meghív.

A feltáró megbeszélést a hivatal vezetője vezeti. A megbeszélés során az eljárást kezdeményező személy felvázolja az általa tapasztalt vélhető fegyelmi vétséget. Az ismertetés során a kezdeményező személynek prezentálnia kell az eseményről begyűjtött bizonyítékait, illetve meg kell neveznie azokat a személyeket, akik érintettek, illetve egyéb bizonyítékokat tudnak szolgáltatni.

Ezt követően a fegyelmi eljárásban érintett személy reagál a kezdeményező személy által felvázoltakra. Ennek során meg kell neveznie azon pontokat, amelyekkel egyetért, amelyekkel nem ért egyet, illetve

amelyekkel részben ért egyet. Ezen kifejtés során a kezdeményezőnek nincs lehetősége azonnali interakciókra. A hivatal vezetőjének feladata és felelőssége, hogy biztosítsa az érintettnek a teljes kifejtés lehetőségét. Ezt követően a jelenlévők véleményezik, megvitatják a helyzetet. A feltáró megbeszélésről jegyzőkönyvet *(B27 IT biztonsági fegyelmi eljárás kezdeményezése és jegyzőkönyve)* kell készíteni, mely tartalmazza:

- a fegyelmi eljárás kezdeményezésének hivatkozási számát;
- a fegyelmi eljáráson jelenlévőket;
- a fegyelmi eljárás lefolytatásának idejét, helyét;
- a fegyelmi eljáráson elhangzottakat, meghivatkozva a személyt.

Amennyiben szükséges, a feltáró megbeszélést követően újabb adatok begyűjtése kezdeményezhető az esetleges tisztázatlan körülmények tisztázására. A rendelkezésre álló adatok alapján az eljárást vezető döntést hoz a fegyelmi eljárás tárgyát képező témában, mely során állásfoglalást alakít ki azt illetően, hogy

- a fegyelmi vétség megvalósult-e, ha igen, akkor milyen formában nyilvánult meg;
- kik érintettek a fegyelmi vétségben, kik felelősök annak megvalósulásában és milyen mértékben;
- a meghatározott felelősségek milyen szankcionálási eljárást vonnak maguk után;
- szükséges-e a büntetőjogi felelősségeket vizsgálni, s ha igen, azt mi módon kezdeményezi a hivatal.

A záró megbeszélésen részt vesznek:

- a hivatal vezetője;
- az eljárást kezdeményező;
- az eljárásban érintett személy;
- az IBF, amennyiben biztonságot érintő fegyelmi vétségről van szó;
- azok, akiket erre a megbeszélésre a hivatal vezetője meghív.

A záró megbeszélésről jegyzőkönyv készül, mely tartalmazza:

- a fegyelmi eljárás kezdeményezésének hivatkozási számát;
- a fegyelmi eljáráson jelenlévőket;
- a fegyelmi eljárás lefolytatásának idejét, helyét;
- a hivatal vezetője állásfoglalását a fentiekben részletezett kérdésekben.

A jegyzőkönyvről másolatot kap az érintett személy, az eredetit pedig a hivatal őrzi meg.

Fegyelmi eljárás érvényesítése

Az érvényesítés során a hivatal vezetőjének állásfoglalására alapozva a szükséges teendők meghatározásra kerülnek, kijelölik azok elvégzésének felelőseit és az elvégzés határidejét. Ezen feladatokat a fegyelmi eljárás jegyzőkönyvére kell felvezetni *(B27 IT biztonsági fegyelmi eljárás kezdeményezése és jegyzőkönyve)*, de a kiadott másolaton ezeket nem kell szerepeltetni.

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

3.2.5. Eljárás a jogviszony megszűnésekor

A munkavállaló jogviszonyának megszűnése esetén a munkavállaló felettes vezetője gondoskodik a kilépő információs rendszerrel vagy annak biztonságával kapcsolatos feladatainak ellátásáról a jogviszony megszűnését megelőzően. A jogviszony megszűnésekor a jogviszonyt megszüntető személy gondoskodik arról, hogy a kilépő esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását megelőzze (hozzáférések megszüntetése, jogosultságok visszavonása).

A hivatal ellenőrzi, hogy a kilépő felhasználó személyes használatában található-e informatikai eszköz, illetve gondoskodik ezek visszavételéről ***(B28 IT eszközök használatba adása és visszavétele)***. A hivatal a kilépő számára igazolja, hogy a hozzáférési jogokat törölte, illetve a felhasználó a hivatal felé elszámolt. A kilépőt tájékoztatni kell az esetleg rá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről.

A hivatal meghatározott ideig megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és hivatali információkhoz. Adatvédelmi okokból a hivatali felhasználóneveket/azonosítókat úgy szükséges létrehozni, hogy azok személyes adatot ne tartalmazzanak (pl. ugyintezo1@hivatal.hu).

3.3. Azonosítás és hitelesítés

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a hivatal felhasználóit, a felhasználók által végzett tevékenységet.

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a különleges jogosultsághoz kötött - úgynevezett privilegizált - felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

3.3.1. Azonosítási és hitelesítési eljárásrend

A hivatalban alkalmazott informatikai rendszerekben felhasználói azonosítást és hitelesítést kell alkalmazni a jogosulatlan személyek tevékenységének megakadályozása és az elszámoltathatóság megvalósítása érdekében.

Az alábbi követelmények szerint az azonosítási folyamatban a felhasználó megadja azonosságát a rendszer felé, melyre a felhasználói azonosító szolgál.

A hitelesítés a felhasználó állítólagos azonosságának a bizonyítására szolgál. A hivatal informatikai rendszereiben legalább tudás alapú (jelszavas) hitelesítést kell alkalmazni. A hitelesítési adatokhoz való hozzáférés korlátozása érdekében az ilyen adatokat védeni kell a jogosulatlan megismerés, módosítás, törlés ellen.

Az azonosítási és hitelesítési adatok és eszközök kezelésére, az azonosítás és hitelesítési folyamatra az alábbi általános szabályokat minden rendszerben/alrendszerben be kell tartani:

- A hivatal kijelölt informatikusai gondoskodnak arról, hogy a rendszerben szereplő minden felhasználói azonosító valós, engedélyezett felhasználóhoz tartozzon.
- A rendszergazdai feladatokat ellátó személyek részére az adminisztratív és a felhasználói feladatok ellátására külön azonosítót kell létrehozni, az adminisztrátori azonosítót csak rendszergazdai feladatok ellátására szabad használni!

- A hivatal kijelölt informatikusainak az azonosítási adatokat naprakészen kell tartani: az új felhasználókat be kell vezetni a rendszerbe, a hivatalból, hivatali egységből, munkakörből stb. eltávozott munkatársak jogait vissza kell vonni.
- A hitelesítő eszközök személyre szólóan kerülnek kiadásra és nyilvántartásra, így kezelésükért, használatukért és tárolásukért a felhasználók felelnek.
- A hivatal informatikai rendszereihez hozzáférő felhasználóknak egyedi módon azonosítaniuk kell magukat. Más felhasználók azonosítóinak használata TILOS!
- Az azonosító/hitelesítő eszközöket TILOS másnak odaadni, a jelszavakat másnak átadni, elmondani és/vagy leírni. A tiltás teljes mértékben vonatkozik arra is, hogy az egyedi eszközt/jelszót vezetőnek, rendszergazdának, külső informatikai szakembernek sem szabad átadni, még abban az esetben sem, ha azt kifejezetten kérik!
- Jelszó használata esetén a felhasználó által választott jelszónak megfelelő biztonságúnak kell lennie. A megfelelő jelszavakra (legalább) az alábbi kritériumok igazak (ezt technológiai eszközökkel bizonyos rendszerek kényszeríthetik is):
  - legalább 8 karakter hosszú;
  - nem szótári szó, illetve annak egyszerű kiegészítése, pl. anna78;
  - nem egyszerű sorozat (pl. 123456, abcdef, asdfgh);
  - tartalmaz számokat, kis- és nagybetűket.
- Amennyiben egy hivatali munkaállomáson több felhasználó is jogosult dolgozni, úgy a feladat elvégzése után (mielőtt másik felhasználó a géphez hozzáférne) a rendrendszerből ki kell jelentkezni!
- Megosztott, vagy csoport felhasználói fiókokhoz tartozó hitelesítő eszközöket vagy adatokat a csoport tagjainak változása esetén vissza kell vonni, majd újra kell generálni az aktuális állapotnak megfelelően.
- A saját egyéni munkaállomás időleges elhagyásakor nem lehet a számítógépet bárki által hozzáférhetően hagyni, védelméről gondoskodni kell (kikapcsolás, kijelentkezés, jelszavas képernyővédelem stb.)!
- A felhasználói jelszavakat legalább háromhavonta meg kell változtatni.

A felhasználó távollétében történő elkerülhetetlen hozzáférést az illetékes vezető kezdeményezhet az IBF-nél. Amennyiben a hozzáférést az IBF engedélyezi, úgy azt a hivatal kijelölt munkatársa lehetővé teszi a következő módon:

- rendszergazdai hozzáféréssel megváltoztatja a felhasználó jelszavát;
- a felhasználó hozzáférésével végrehajtja az engedélyezett feladatot;
- a megváltoztatott jelszót az illetékes közvetlen vezetője kapja meg;
- ezt a felhasználó visszatérésekor az első rendszerbe lépéskor a felhasználónak meg kell változtatnia.

3.3.2. Azonosításra, hitelesítésre szolgáló eszközök kezelése

Az azonosításra, hitelesítésre szolgáló eszközök kiadása előtt az azt végző munkatárs vagy hivatal:

- meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát (pl. kezdeti jelszó), melyet az adott rendszer telepítése során a végfelhasználónak meg kell változtatni;
- kiosztáskor ellenőrzi az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát, illetve biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;

- meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit;
- a hitelesítésre szolgáló eszköztípusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket;
- dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, kompromittálódott vagy a sérült eszközöket;
- megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;
- megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét;
- lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.

Az elektronikus információs rendszer fedett visszacsatolást biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.

Sikertelen belépés esetén a hivatal által meghatározott esetszámkorlátot alkalmaz a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire. Amennyiben a sikertelen bejelentkezési kísérletekre felállított esetszámkorlátot a felhasználó túllépi, automatikusan zárolja a felhasználói fiókot vagy csomópontot meghatározott időtartamig, vagy meghatározott módon késlelteti a következő bejelentkezési kísérletet.

A felhasználói azonosítók/jelszavak elvesztését/elfelejtését, illetve vélelmezett kompromittálódását azonnal jelezni kell a hivatal vezetője vagy az IBF felé. Elfelejtett jelszó esetében a rendszergazda új kezdeti jelszót állít be, amelyet az első bejelentkezéskor meg kell változtatni. Azonosító kompromittálódása esetén a kompromittált azonosítóhoz tartozó jogokat azonnal le kell tiltani és ki kell vizsgálni, hogy történt-e jogosulatlan hozzáférés az informatikai rendszerhez. Az IBF engedélyével a rendszergazda a kompromittálódott azonosító helyett az érintett felhasználónak a munkájához szükséges másik azonosítót biztosít.

A szerepköröknek megfelelő, leginkább az üzemeltetéshez köthető rendszergazdai és bizonyos rendszereknél a rendszer-visszaállítási jelszavakat tárolni kell a következő módon:

- Minden ilyen jogosultsági adatot (rendszer neve, hozzáférés módja, felhasználónév, jelszó) redundánsan, két darab külön adathordozóra mentve, megfelelő titkosítású jelszótároló programban rögzítetten, szerepkörönként külön adatbázisban, melynek mesterkulcsát (jelszavát) az adathordozó mellett, szerepkörönként lezárt, lepecsételt és legalább két jogosult személy által aláírt borítékban kell tárolni.
- A borítékba az adatokat úgy kell elhelyezni, hogy azok ne legyenek „átvilágíthatók", felbontás nélkül ne legyenek olvashatók. A borítékokra kívül rá kell írni az utolsó módosítás dátumát és a megbontás okát (pl. audit vagy jogosult távolléte miatti vezetői bontás), ilyen eseteket követően a szerepköri jogosultaknak célszerű a jelszavakat lecserélni.
- A jelszótárolóban a korábbi jelszavak a History alatt, időmegjelöléssel megtalálhatók. A változtatást végző jogosult köteles a hasonló szerepkörűeknek jelezni a változtatás tényét, adattartalmát. Ha a szerepkörhöz rendelt jogosult végez szabályzatban előírt kötelező jelszóváltást a tárolt adatokban, akkor nincs szükség borítékbontásra.
- A borítékot zárt biztonsági szekrényben kell tárolni az illetéktelen hozzáférés elkerülése érdekében.

3.3.3. hivatalon kívüli felhasználók azonosítása és hitelesítése

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a hivatalon kívüli felhasználókat és tevékenységüket.

Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság (NMHH) elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványokat fogadhatja el a hivatalon kívüli felhasználók hitelesítéséhez.

3.4. Hozzáférés védelem, jogosultság kezelés

3.4.1. Hozzáférés ellenőrzési eljárásrend

A hivatal minden informatikai rendszerében, erőforrásaival, szolgáltatásaival kapcsolatban, az adott eszköz, erőforrás, adat, dokumentumtár stb., biztonsági osztályától függően, a szükséges és elégséges ismeret elvének betartásával kell alkalmazni a hozzáférés-védelmi és a jogosultságkezelési intézkedéseket. Minden, az IBSZ hatálya alá eső adatot a központi informatikai rendszerben, a központi logikai, fizikai rendszerek védelme alatt, központi hozzáférés-védelmi és jogosultságkezelési rendszer ellenőrzése mellett kell menedzselni az egyedi elszámoltathatóság elvének érvényre juttatásával. A hozzáférés-védelmi követelmények a hivatal informatikai rendszereiben alkalmazandó rendszertől függenek.

Az információkhoz való hozzáférési lehetőséget (jogosultságot) a felhasználó által betöltött munkakör (szerepkör) alapján kell meghatározni (szerepkör alapú hozzáférés). A szerepkörök definiálása a hivatal munkafolyamatain, hivatali struktúráján, a hierarchikus és funkcionális kapcsolatokon alapul.

A hivatalba újonnan belépő felhasználók informatikai rendszerhez történő hozzáférését az erre szolgáló igénylőlapon *(B15 Hozzáférések igénylése és letiltása)* az érintett hivatali egység vezetője kezdeményezi. A felhasználói hozzáférést és az indokoltan kért jogosultságokat a hivatal vezetőjének engedélye után a rendszergazda adja meg.

A hivatal informatikai rendszereiben működő szolgáltatások (pl. megosztott könyvtárak) esetén a szolgáltatás indítását engedélyező dokumentumban meg kell jelölni a szolgáltatásért (logikailag) felelős vezetőt, és a szolgáltatás tulajdonosát. Amennyiben a feldolgozott adatok, illetve a szolgáltatás jellege alapján a szolgáltatás jellemzően valamelyik szakterületekhez kapcsolható (pl. gazdálkodási adatokról szóló kimutatások, pénzügy, személyügy stb.), úgy annak a területnek a vezetőjét kell szolgáltatás tulajdonosnak kijelölni.

A szolgáltatás tulajdonos által definiált hozzáférés-védelem elve szerint a szolgáltatás tulajdonosa által meghatározott szabályok (engedélyezés) alapján kell az adott szolgáltatáshoz történő hozzáférési jogosultsági kört kialakítani. A szolgáltatás tulajdonosa által megfogalmazott szabályok alapján kell beállítani a megfelelő (pl. könyvtárak esetén: olvasás, írás, törlés) hozzáférési módot. A jogosultságok beállítását az informatikai rendszerben az informatikus végzi el.

A munkaállomásokon és a szervergépeken technikailag is korlátozni kell az úgynevezett alternatív bootolási lehetőségeket (pl. DVD, USB, Ethernet stb.). Ezekre az eszközöket csak karbantartási és javítási célból lehet olyan rendszerrel működtetni, amely nem az üzemszerűen rátelepített operációs rendszer.

A munkaállomásokon és szervereken telepített szoftverek, alkalmazások és szakalkalmazások esetében kiemelt figyelmet kell fordítani az automatikusan létrejövő felhasználókra, hozzáférésekre, jogosultságokra (administrator, guest, root stb.), ezek kezdeti jelszavát meg kell változtatni és/vagy zárolni kell a használatát. Szintén kiemelt figyelmet kell fordítani a teszt jelleggel létrehozott felhasználókra, hozzáférésekre. Ezeket a felhasználókat, hozzáféréseket, amikor használatuk már nem szükséges és indokolt, meg kell szüntetni. Amennyiben a hozzáférések szükségesek (pl. valamilyen rendszerszolgáltatás miatt), úgy legalább a magasabb szintű biztonságukról gondoskodni kell, így vagy át kell őket nevezni, vagy a nem szükséges jogosultságokat el kell venni ezektől a felhasználóktól. Az ilyen felhasználók alapértelmezett jelszavait meg kell változtatni megfelelő erősségű jelszavakra. Szakalkalmazások esetében a fejlesztőknek kerülniük kell az automatikus felhasználói, alapértelmezett jelszóval működő hozzáférések használatát.

A felhasználó szerepkörének megváltozása esetén (pl. más osztályra kerül, munkaköre megváltozik) az informatikus a hivatal vezetőjétől kapott írásos információk alapján a régi szerepkörhöz tartozó jogosultságot a felhasználótól elveszi, majd a szükséges új szerepkörnek megfelelő jogosultságokat megadja. *(B15 Hozzáférések igénylése és letiltása)*

A felhasználó jogviszonyának megszűnése esetén az informatikus vezetője a személyzeti munkatárstól kapott nyomtatványon *(B28 IT eszközök használatba adása és visszavétele)* igazolja, hogy a hozzáférési jogokat törölte, illetve a felhasználó az informatikai vezető felé elszámolt.

Az informatikai rendszerhez, alrendszerekhez történő hozzáférési engedélyeket évente felül kell vizsgálni (pl. távoli hozzáférések, internet elérés, külső levelezés stb.). Az esetlegesen már nem indokolt jogosultságokat, hozzáféréseket meg kell szüntetni.

3.4.2. Felhasználói fiókok kezelése

A felhasználók kizárólag felhasználói jogosultsággal dolgozhatnak a munkaállomásokon, rendszergazdai jogosultságokat nem kaphatnak. Kivételt képeznek e szabály alól azon szakalkalmazások munkaállomásai, ahol a szoftver működéséhez szükségesek az emelt szintű jogok, itt a zavartalan munkavégzés miatt ez engedélyezett. Az így rendelkezésre álló jogokat a felhasználó nem használhatja semmilyen üzemeltetői feladatra (pl. programok telepítése, leállítása stb.), csak és kizárólag a szakalkalmazás használata miatt birtokolhatja ezeket!

A munkaállomásokon a felhasználóknak tilos hálózati szolgáltatásként mappákat/fájlokat megosztani. Amennyiben a megosztás szakmailag indokolt, úgy a közvetlen vezető kezdeményezésére, az IBF jóváhagyásával a megosztást a munkaállomás adminisztrátora hozza létre. Valamennyi megosztás esetén szigorúan kell meghatározni a hozzáféréseket, törekedni kell arra, hogy ne legyenek általános megosztások. Csak azok a felhasználók és munkaállomások kaphatnak jogot az erőforrások elérésére, amelyeknek ez a munkájukhoz valóban szükséges.

A hivatal minden irodájában biztosítani kell a hálózati csatlakozás lehetőségét. A hálózati erőforrásokhoz való hozzáférést különböző szintű hálózati jogosultságok biztosítják. Ezek a jogok az alábbi tevékenységek elvégzését tehetik lehetővé:

- hálózat kezeléséhez szükséges programok közös használata;
- közös nyomtató használata;
- internet böngészés;
- elektronikus levelezés;

- adatbázisok elérésének biztosítása;
- alkalmazások és adatok elérésének biztosítása.

A hálózaton található fájlokra, könyvtárakra (mappákra) kiosztható jogosultságok:

- olvasási jog;
- írási (módosítási, létrehozási) jog;
- törlési jog.

A hivatali informatikai rendszerben az egyes számítástechnikai rendszerek, szoftverek készítői által gyárilag a felhasználók részére biztosított védelmi eljárásokat (pl. a Microsoft Word jelszavas védelme) a felhasználók – a hivatali adatok rendelkezésre állásának biztosítása érdekében – nem használhatják!

A felhasználók számára tilos nem engedélyezett erőforrások, szolgáltatások, jogosultságok megszerzése vagy ennek kísérlete. Tilos más felhasználó munkájának zavarása, állományaikhoz történő bármilyen illetéktelen hozzáférés vagy annak kísérlete.

A hozzáférésvédelmi és jogosultságkezelési elemek, alrendszerek megbízható adminisztrálása érdekében a felhasználói hozzáféréseket megvalósító rendszerek működtetését (ahol a technológia lehetővé teszi) megbízható módon naplózni, és a naplótartalmat az engedélyezett jogosultság-igénylések alapján ellenőrizni kell.

A munkaállomás adminisztrátorát értesíteni kell, ha...

- a felhasználói fiókokra már nincsen szükség;
- a felhasználók kiléptek vagy áthelyezésre kerültek;
- az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak.

A felhasználói fiókok a fiókkezelési szabályokkal összhangban rendszeres időközönként, legalább évente felülvizsgálandók ***(B30 Felhasználói fiókok kiosztása és felülvizsgálata)***.

A hivatal további feladatai:

- meghatározza és azonosítja az elektronikus információs rendszer felhasználói fiókjait és ezek típusait;
- kijelöli a felhasználói fiókok fiókkezelőit;
- kialakítja a csoport- és szerepkör tagsági feltételeket;
- meghatározza az elektronikus információs rendszer jogosult felhasználóit, a csoport- és szerepkör tagságot és a hozzáférési jogosultságokat, valamint (szükség esetén) az egyes felhasználói fiókok további jellemzőit (*B30 Felhasználói fiókok kiosztása és felülvizsgálata*).

3.4.3. Külső rendszerekből történő hozzáférés szabályozása

A hivatal

- meghatározza és dokumentálja felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban;
- külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

Külső cégek folyamatos üzemeltetési feladatainak ellátása érdekében (pl. szerverek és szakalkalmazások karbantartása) a cégek megbízott munkatársai állandó távoli hozzáférést kaphatnak az általuk felügyelt rendszerhez. Ezeket a hozzáféréseket a cégeknek az IBSZ betartásával, bizalmasan és a szakmai normáknak megfelelően kell kezelniük.

Távoli hozzáférést kaphatnak a hivatal azon munkatársai, akik a hivatal által biztosított, távoli munkavégzésre alkalmas eszközzel rendelkeznek.

A távoli hozzáféréshez használt azonosítókat, jogosultságokat a hivatal informatikusa dokumentáltan *(B15 Hozzáférések igénylése és letiltása)* adja ki, az azonosítóért felelős személy pontos meghatározásával. Az azonosítóért felelős személy ezt aláírásával igazolja.

A távoli hozzáférésű munkaállomások biztonságáért minden esetben a távoli gép felhasználója és/vagy üzemeltetője a felelős, így felelős a távoli gépről a hivatal infrastruktúrájában végrehajthatott cselekményekért is.

A hivatal informatikai infrastruktúráját távoli elérése csak titkosított kapcsolaton keresztül történhet. A rendszerhez történő csatlakozás csak a szükséges időre korlátozódhat, a munka végeztével a kapcsolatot bontani kell.

3.4.4. Azonosítás és hitelesítés nélkül engedélyezett tevékenységek

A számítógépes munkahely kialakítását követően a számítógépen dolgozók azonosítására, valamint a jogosultságok meghatározására van szükség. A számítógép használatakor egyedi azonosítókat kell alkalmazni, melyek hiányában a munkaállomásra a belépés nem lehetséges, így az elektronikus információs rendszeren belül semmilyen tevékenységre nincs lehetőség.

3.4.5. Nyilvánosan elérhető tartalom

Nyilvánosan hozzáférhető rendszerként definiálja a hivatal a publikus weboldalát. Az oldal üzemeltetéséért felelős hivatali egység vezetőjének gondoskodni kell az azon publikált információk törvényi megfelelőségéről és valódiságáról, sértetlenségéről. Tilos törvénybe, jogszabályba ütköző, vagy a jó ízlést és közerkölcsöt sértő tartalmat közzétenni. A felkerülő tartalmakat minden esetben ellenőrizni kell a hivatali egység vezetőjének és csak a jóváhagyása után publikálhatók az információk. A publikus weboldalnak gondosan szegmentáltnak kell lennie a hivatal belső hálózatától arra alkalmas eszközzel. Gondoskodni kell a weboldal jogosult használata közben kieszközölhető jogosulatlan elérések megakadályozásáról.

3.4.6. Rendszerhasználat jelzése

A rendszerhez való hozzáférés előtt a felhasználó figyelmeztető üzenetet vagy jelzést kap arról, hogy...

- a felhasználó az érintett hivatal elektronikus információs rendszerét használja;
- a rendszer használatot figyelhetik, rögzíthetik, naplózhatják;
- a rendszer jogosulatlan használata tilos és büntetőjogi vagy polgárjogi felelősségre vonással jár;
- a rendszer használata egyben a felhasználó előbbiekbe történő beleegyezését is jelenti.
- Az elektronikus információs rendszer a figyelmeztető üzenetet vagy jelzést mindaddig a képernyőn tartja, amíg a felhasználó közvetlen műveletet nem végez az elektronikus információs rendszerbe való bejelentkezéshez vagy további rendszer hozzáféréshez.

Nyilvánosan elérhető rendszerek esetén...

- kijelzi a rendszer használat feltételeit, mielőtt további hozzáférést biztosít;
- amennyiben felügyelet, adatrögzítés vagy naplózás történik, kijelzi, hogy ezek megfelelnek az adatvédelmi szabályoknak;

- leírást biztosít a rendszer engedélyezett felhasználásáról.

Vezeték nélküli hozzáférés esetén...

- belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki a vezeték nélküli technológiák kapcsán;
- engedélyezési eljárást folytat le a vezeték nélküli hozzáférés feltételeként.

Az elektronikus információs rendszer a figyelmeztető üzenetet vagy jelzést mindaddig a képernyőn tartja, amíg a felhasználó közvetlen műveletet nem végez az elektronikus információs rendszerbe való bejelentkezéshez vagy további rendszerhozzáféréshez.

Mobil eszközök hozzáférés ellenőrzése

A hivatal belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki az általa ellenőrzött mobil eszközökre és engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást.

3.5. Viselkedési szabályok az interneten

A hivatal e-mail és Internet használati jogokkal rendelkező dolgozói a munkájukkal kapcsolatban használhatják a hivatal által biztosított Internet szolgáltatást.

A belső hálózaton Internet-kapcsolatot létesíteni kizárólag tűzfalon keresztül lehet. Nem megengedett a hivatal informatikai hálózatába kapcsolt hordozható és asztali munkaállomásokról modemes, mobiltelefonos vagy egyéb, nem hivatali kapcsolat létrehozása Internet-szolgáltatókkal.

Az internetszolgáltatás magáncélú használata nem megengedett. Az internetforgalom automatikusan, szoftveres alapon szűrésre kerül, így bizonyos tartalmak nem látogathatók, technológiai eszközzel is tiltásra kerülnek. A technikai szűréstől függetlenül a felhasználóknak az internetszolgáltatás használatának folyamán a következő szabályokat kell betartaniuk:

- Az interneten csak a hivatali munkával kapcsolatos oldalakat lehet látogatni. Tilos a pornográf, online játék, fogadási, csevegő, letöltő és törvénybe ütköző tartalmakat szolgáltató oldalak látogatása, ezekről letölteni, ilyen tartalmakat és helyeken publikálni, adatokat cserélni, adatot tárolni!
- Az Internetről programok letöltése, telepítése és futtatása nem megengedett. Igény esetén az informatikus előzetes bevizsgálás után engedélyezheti programok letöltését és futtatását. A bevizsgálás során ellenőrizni kell...
  - a letölteni kívánt program vírusmentességét;
  - hogy a letölteni kívánt program képes-e működni abban a környezetben, amelybe a letöltést tervezik;
  - hogy a letöltés nem sért-e szerzői jogot.
- Információbiztonsági megfontolásokból tilos a hivatalban a csevegő programok használata (pl. Skype, MSN, Gtalk, IRC, ICQ stb.). Ezen programok futtatása is tilos! A programok hivatali érdekből történő használatára (pl. Skype a kommunikációs költségek csökkentésére) a hivatal vezetője adhat dokumentált módon engedélyt (***B31 Telepíthető nem szakalkalmazások listája***).
- Amennyiben az Interneten keresztüli kommunikáció (főként levelezés) nem titkosított és egyértelműen azonosítható formában (digitális aláírás, fokozott biztonságú elektronikus aláírás)

kerül lebonyolításra, nem megengedett a bizalmas vagy annál magasabb minősítésű, védett információt tartalmazó üzenet küldése kizárólag az Interneten keresztül azonosított feleknek mindaddig, amíg a másik fél megbízható, az Internettől független azonosítása meg nem történik. Az információk minősítését a 2009. évi CLV. törvény és a 243/2016. (VIII.17.) Korm. rendelet szabályozza.

- Tilos a hivatallal kapcsolatos belső információk nyilvános oldalakon való bárminemű közzététele.
- Tilos a munkavégzéssel kapcsolatos adatok továbbítására, tárolására nem magyarországi illetőségű email- és felhőszolgáltatás (pl. Gmail, Dropbox) igénybevétele.

Információbiztonsági vizsgálat, illetve hibakeresés céljából a hivatal informatikai rendszereinek teljes hálózati forgalma megfigyelhető és rögzíthető. A felhasználó az IBSZ ismeretéről és elfogadásáról szóló nyilatkozatával *(B02 Nyilatkozat az IT biztonsági szabályok elfogadásáról)* elfogadja, hogy a rendszer használata egyben a felhasználó beleegyezését is jelenti a figyelésbe és rögzítésbe. Elektronikus levelek esetén a megfigyelés nem terjed ki a levelek tartalmára. A levelek az alábbi technikai tulajdonságok alapján kerülnek vizsgálatra: kéretlen levelek, vírusokat tartalmazó levelek, informatikai támadásokat megvalósító üzenetek, adathalászatot megkísérlő üzenetek.

Ha a dolgozó internethasználata a munka elvégzésének rovására megy (pl. hivatali munkához nem kapcsolódó vagy nagy hálózati terhelést okozó tevékenységet folytat vagy biztonsági fenyegetést jelentő oldalakat látogat), az informatikus jelzi a dolgozó közvetlen vezetőjének, aki megteszi a szükséges intézkedéseket. Amennyiben az intézkedés eredménytelen marad, az érintett munkatárs vezetője utasítására a felhasználó internethozzáférését az informatikus részlegesen vagy teljesen letiltja.

Az internetkapcsolatok üzemeltetéséért felelős vezetőnek joga van az internethozzáférés tartalmi, időbeli, sávszélességbeli és szolgáltatásbeli korlátozásához, amennyiben ez az Internet önkormányzati célú használatának biztosításához szükségessé válik. A korlátozásról a felhasználókat előzetesen tájékoztatni kell.

3.5.1. Elektronikus levelezés (e-mail)

Az e-mail szolgáltatás a hivatal által a felhasználók részére a hivatali elektronikus levelezés céljaira biztosított eszköz. Az e-mail rendszer, valamint a rendszerben előállított, elküldött és megkapott levél is a hivatal felügyelete alá tartozik.

A hivatal elektronikus levelezési rendszere korlátozott mértékben, és a szabályzatban rögzített feltételek betartása mellett használható nem hivatali (személyes) levelezés céljára. Az elektronikus levelező rendszer felhasználója a rendszer használatával automatikusan aláveti magát ezeknek a korlátozásoknak.

A hivatal e-mail rendszerén mindennemű jogszabályellenes tartalom továbbítása és tárolása tilos.

A hivatal nevében folytatott elektronikus levelezésre kizárólag az erre a célra biztosított elektronikus levelezési cím, a rendszeresített levelező (kliens) program, illetve az informatikus által engedélyezett levelezési szolgáltatás használható. A beállítások (működési paraméterek) meghatározásáért és beállításáért az informatikus felelős.

Az elektronikus levelező rendszerben tárolt és továbbított dokumentumok elektronikus kezelésénél is be kell tartani az érvényben lévő ügyviteli, iratkezelési és adatkezelési szabályokat.

Minden elektronikus postaládával rendelkező felhasználó köteles elektronikus postaládájának tartalmát figyelemmel kísérni oly módon, hogy legalább a munkakezdéskor és a munkavégzés befejezését megelőzően meggyőződjön róla, hogy érkezett-e új üzenete, és amennyiben igen, akkor azokat érkeztesse, kezelje (tekintse meg, tegye meg a szükséges egyéb intézkedéseket).

Az elektronikus levelező rendszer használata során nem megengedett:

- nagy mennyiségű és méretű, személyes jellegű üzenetek küldése;
- kéretlen reklámok és hirdetések közzététele;
- lánclevelek terjesztése, továbbítása;
- a felhasználóknak a hivatali e-mail címüket nem hivatalos minőségben használni (pl. magánlevelezés, regisztráció letöltési oldalakon, online játék oldalakon stb.);
- a levelek fejlécének megváltoztatása, hamis levelek küldése;
- olyan üzenetek, illetve csatolt fájlok küldése, továbbítása, amelyek törvénytelenségeket vagy arra való felhívást tartalmaznak, fenyegetők, összességében sértik a hivatal jó hírét, általánosan elfogadott erkölcsi szabályba vagy jogszabályba ütköznek;
- a tévesen címzett, másnak szóló levelek felhasználása;
- a hivatal által biztosított e-mail címre érkező üzenetek átirányítása külső (nem a hivatal elektronikus levelező rendszerében létrehozott) e-mail címre.

A levelezési rendszer személyes célokra az elektronikus levelezésre vonatkozó szabályok betartásával és csak akkor használható, ha az nem sérti a hivatal érdekeit.

Az elektronikus levelek címzése során minden felhasználónak körültekintően kell eljárnia az alábbiak figyelembevételével:

- Csoportos levelező, elosztási lista (pl. „mindenki", „x osztály", „hivatali dolgozók") alkalmazása során meg kell győződni arról, hogy valóban szükséges-e minden, a csoportba tartozó címzett részére elküldeni az üzenetet.
- Titokvédelmi vagy egyéb biztonsági, bizalmassági okokból, amennyiben a levelek címzettjei nem szerezhetnek tudomást egymásról vagy egymás e-mail címéről, akkor a levél „Titkos másolat" (BCC) kategóriáját kell alkalmazni a címzés során.

Csoportos levelező, elosztási lista létrehozása iránti igényt a hivatali egység vezetőjének jóváhagyásával az üzemeltetői csoporthoz kell eljuttatni, amely a szükséges vizsgálatok, egyeztetések elvégzését követően az IBF közreműködésével dönt az igény kielégítéséről és intézkedik annak beállítása érdekében.

A központilag létrehozott csoportos levelező, elosztási listák karbantartása az informatikus feladata. Ennek elvégzéséhez a lista összeállítását kezdeményező hivatali egység, illetve a hivatal munkavállalóinak változása esetén a munkaügyi vezető köteles az informatikus számára adatokat biztosítani.

A hivatal a levelező rendszer működését akadályozó mennyiségű és méretű adat elektronikus levélként való továbbítását korlátozza. A küldhető csatolmányok típusáról és méretéről az informatikus ad kérésre felvilágosítást, valamint segítséget nyújt a nagyméretű fájlok küldésében.

A postaládára vonatkozó korlátozások

A felhasználó e-mail postaládájának mérete korlátozott, melynek méretét az informatikus határozza meg a technikai lehetőségek figyelembe vételével. A meghatározottnál nagyobb postaládára vonatkozó igényt a hivatali egység vezetőjének jóváhagyásával az informatikushoz kell eljuttatni, aki a

szükséges vizsgálatok, egyeztetések elvégzését követően dönt az igény kielégítéséről és intézkedik annak beállítása érdekében.

Amennyiben a hivatali levelezésben – pontos címzés mellett – az elektronikus levelező rendszertől a kézbesítés során kézbesíthetetlenségre utaló hibajelzés érkezik, akkor a felhasználónak – szükség szerint az informatikus megkeresésével – fel kell tárnia ennek okát annak érdekében, hogy üzenete ne vesszen el.

Az elektronikus levelek méretét, valamint a levélhez csatolt fájlok típusát az informatikus korlátozhatja a rosszindulatú kódok terjedésének megakadályozása céljából és azért, hogy biztosítsa a hivatali levelezés megfelelő szolgáltatási szintjét. A korlátozás miatt nem továbbított levelekről, csatolt fájlokról a küldő értesítést kell kapjon.

Ismeretlen feladótól érkező, gyanús csatolt fájlt tartalmazó, vagy ismeretlen linket ajánló (pl. idegen nyelvű, láthatóan reklámcélú, olyan dokumentumra hivatkozó, amiről a címzett nem tud) elektronikus üzenetek csatolmányait, illetve a kapott linkeket nem szabad megnyitni, az ilyen leveleket törölni kell.

4. AZ INFORMATIKAI RENDSZEREK ÜZEMELTETÉSE

4.1. Általános rendelkezések

Az informatikus feladata a felhasználók informatikai támogatása, a szolgáltatások folyamatos, hivatali időben való rendelkezésre állásának biztosítása, a felmerülő biztonsági problémák azonosítása, azok megbízható kezelése és a biztonságért felelős személy tájékoztatása a felmerült problémákról, észlelt jelenségekről.

Az informatikus

- felelős az informatikai rendszer és a hálózat működőképességéért;
- felelős a hálózati szolgáltatások, csatlakozások üzembiztonságáért, koordinálásáért;
- gondoskodik az informatikai eszközök tervszerű megelőző karbantartásáról;
- felelős a folyamatos, hivatali időben való rendelkezésre állásért, a jelentkező hibák mielőbbi szakszerű ellátásáért.

A felhasználóknak tilos a gépek megbontása, a hardver konfigurációk megváltoztatása, a számítógépes hálózat megbontása, átstrukturálása, gépek, eszközök engedély nélküli csatlakoztatása.

A hivatal hálózatára számítógépet csak akkor lehet rácsatlakoztatni, ha a hálózati csatlakozás főbb paraméterei (fizikai és logikai címek, a hálózati struktúrában elfoglalt hely stb.) rögzítésre kerültek, és a csatlakozást az informatikus engedélyezte. Amennyiben valaki számítógépet vagy egyéb számítástechnikai berendezést önhatalmúlag csatlakoztat a hálózatra, úgy az informatikus köteles a berendezést azonnali hatállyal a hálózatról lekötni és az illetéktelen eszközcsatlakozást végrehajtó ellen vezetőjének bevonásával, felelősségének megállapítása érdekében fegyelmi, kártérítési, illetve egyéb eljárást kezdeményezni.

Tilos a felhasználóknak a hálózat kábeleinek szándékos kihúzása a fali csatlakozóból vagy a gépből. Számítástechnikai eszközt és tartozékait helyéről elvinni az informatikus és az eszköznyilvántartással foglalkozó hivatali egység tudta és engedélye nélkül tilos.

A számítógépes hálózathoz és az informatikai szolgáltatásokhoz a hozzáférés munkaidőben biztosított. Az ettől eltérő igényeket legkésőbb három munkanappal korábban kell jelezni az informatikus részére, aki amennyiben az üzemeltető személyzet biztosítható és technikailag is megoldható, akkor a hozzáférést lehetővé teszi.

A munka végeztével a felhasználónak az eszközök működésének megfelelően / üzemszerűen a használt alkalmazásokból ki kell jelentkeznie és ki kell kapcsolnia az informatikai eszközöket. A munkavégzés 15 percnél hosszabb átmeneti felfüggesztése esetén a használt alkalmazásokból, programokból ki kell lépni. Az informatikus által végzendő karbantartási, szoftver frissítési munkák időtartamában az informatikus kérésére az adott alkalmazásokkal történő munkavégzést 15 percen belül üzemszerű kilépéssel és/vagy leállítással be kell fejezni.

Az informatikai eszközöket rendeltetésszerűen kell használni: a számítógépen és perifériáin papírokat és egyéb tárgyakat tárolni nem lehet, a szellőző nyílásokat szabadon kell hagyni, a billentyűzetet védeni kell a szennyeződésektől, a számítógép közelében enni-inni, dohányozni nem szabad!

4.2. Konfigurációkezelés

4.2.1. Konfigurációkezelési eljárásrend

A hivatal...

- megfogalmazza, és a hivatalra érvényes követelmények szerint dokumentálja, valamint a hivatalon belül kihirdeti a konfigurációkezelési eljárásrendet, mely a konfigurációkezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
- a fizikai védelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a konfigurációkezelési eljárásrendet;
- ha hatókörébe tartozik, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely tartalmazza...
  - a rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését;
  - a biztonsági funkciók hatékony alkalmazását és fenntartását;
  - a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket.
- megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amely tartalmazza...
  - a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját;
  - a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit;
  - a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához;
  - gondoskodik arról, hogy az információs rendszerre vonatkozó – különösen az adminisztrátori és fejlesztői – dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható;
  - gondoskodik a dokumentációknak az érintett hivatal által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről.

4.2.2. Alapkonfiguráció

Az érintett adminisztrátorok és adatgazdák az IBF közreműködésével elektronikus információs rendszereikhez egy-egy alapkonfigurációt fejlesztenek ki, dokumentálják és karbantartják azt, leltárba foglalva annak lényeges elemeit ***(B32 Konfigurációkezelési eljárásrend és alapkonfigurációk)***.

A hivatal az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa, valamint meghatározza a tiltott vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatát. (legszűkebb funkcionalitás)

A hivatal...

- meghatározza a működési követelményeknek még megfelelő, de a biztonsági szempontból a lehető leginkább korlátozott módon – a „szükséges minimum" elv alapján – az elektronikus információs rendszerben használt információtechnológiai termékekre kötelező konfigurációs beállítást, és ezt ellenőrzési listaként dokumentálja (***B33 Kötelező konfigurációs beállítások ellenőrző listája***);
- elvégzi a konfigurációs beállításokat az elektronikus információs rendszer valamennyi elemében;
- a meghatározott elemek konfigurációs beállításaiban azonosít, dokumentál és jóváhagy minden eltérést;
- figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait, a hivatal belső szabályzataival és eljárásaival összhangban.

4.2.3. konfigurációváltozások felügyelete (változáskezelés)

A hivatal...

- meghatározza a változáskezelési felügyelet alá eső változástípusokat;
- meghatározza az egyes változástípusok esetén a változáskezelési vizsgálat kötelező és nem kötelező elemeit, előfeltételeit (csatolt dokumentációk, teszt jegyzőkönyvek stb.);
- megvizsgálja a változáskezelési felügyelet elé terjesztett, javasolt változtatásokat, majd kockázatelemzés alapján jóváhagyja, vagy elutasítja azokat;
- dokumentálja az elektronikus információs rendszerben történt változtatásokra vonatkozó döntéseket;
- megvalósítja a jóváhagyott változtatásokat az elektronikus információs rendszerben;
- visszakereshetően megőrzi az elektronikus információs rendszerben megvalósított változtatások dokumentumait, részletes leírását;
- auditálja és felülvizsgálja a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységeket.

Előzetes tesztelés és megerősítés

A konfiguráció megváltoztatása előtt az új verziót tesztelni kell, ezután dönteni kell annak megfelelőségéről, továbbá dokumentálni kell az elektronikus információs rendszer változtatásait az éles rendszerben történő megvalósítása előtt.

4.3. Szoftverhasználat korlátozásai

A hivatal bármely informatikai rendszerére csak az informatikus telepíthet szoftvert, *a felhasználónak szoftvertelepítésre és bizonyos beállítások módosítására nincs sem joga, sem lehetősége.* A hivatal

informatikai eszközeire TILOS illegális és/vagy nem jogtiszta szoftvert telepíteni! A hivatal informatikai infrastruktúrájában a feladatok végrehajtására kizárólag a hivatal által megvásárolt licencű kereskedelmi szoftver termékeket és/vagy szabad szoftvereket lehet alkalmazni. Minden illegális, vagy nem a munkavégzést szolgáló szoftvert, adatot törölni kell a rendszerből. Ezt a műveletet a felhasználó tudtával az informatikus végzi el.

Illegális szoftverek használata esetén a felhasználóval szemben felelősségének megállapítása érdekében fegyelmi, kártérítési, illetve egyéb eljárás indulhat.

A telepítést megelőzően a hivatalban vírusvédelmi célokra üzembe állított eszközzel meg kell vizsgálni a szoftver esetleges vírusfertőzöttségét. Amennyiben technikailag/technológiailag lehetséges, úgy az új szoftvercsomagról biztonsági másolatot kell készíteni. Az installálást csak a munkapéldányról szabad végezni. Az eredeti példányt biztonságos helyen kell tárolni.

A hivatal infrastruktúrájában található eszközökre idegen program, adat másolása tilos!

4.3.1. Felhasználó által telepíthető szoftverek

A felhasználók az informatikai eszközöket hivatali munkavégzés céljára kapják. A felhasználók jogosultsága a belső hálózaton csak a rendszergazda által telepített egységes irodai alkalmazások és szolgáltatások használatára, illetve a munkájukhoz szükséges alkalmazói programok futtatására terjed ki. A hivatal informatikai infrastruktúráját magán célú használatra igénybe venni TILOS!

Ettől eltérni csak a hivatal vezetője vagy az Információbiztonsági Felelős (IBF) írásbeli engedélyével, akkor is kizárólag mobil eszközök esetében szabad (notebook, tablet, mobiltelefon, mobil adathordozók). Az engedély feltétele felhasználói nyilatkozat tétele arról, hogy az adott felhasználó - a tűzfallal leválasztott nyilvános részek (pl. free/vendég wifi) kivételével (*6.2. pont*) - nem használja a hivatal belső informatikai struktúráját ***(B34 IT eszköz kivonási kérelem)***. Ebben az esetben a felhasználót a kockázatokról tájékoztatni kell, aki a nyilatkozattétellel lemond a hivatal nem nyilvános hálózatának bármilyen használati lehetőségéről és a kivont eszköz hardver- és szoftverkarbantartását is átvállalja. Karbantartási kötelezettsége nem terjed ki garanciális javítás ügyintézésére, azt továbbra is az informatikai üzemeltetésért felelős hivatali egység feladata.

4.4. Adathordozók védelme

4.4.1. Adathordozók védelmére vonatkozó eljárásrend

A hivatal által használt hordozható külső adattárolókat (pl. flash diskek, pendrive-ok, memóriakártyák, hordozható HDD-k) egyedi azonosítóval kell ellátni, kivételt képeznek ez alól az optikai adathordozók (CD, DVD) és a hajlékonylemezek, amely tárolók csak számszerűen kerülnek nyilvántartásba. Az egyedi azonosítóval ellátott hordozható adathordozók pontos helyéről naprakész adatbázist kell vezetni ***(B35 Mobil adattárolók nyilvántartása)***.

A használni kívánt adattárolót a tárolásra kijelölt helyről kell kivenni és használatot követően oda kell visszahelyezni. A munkaasztalokon és a számítógépekben csak azok az adathordozók lehetnek, amelyek a munkavégzéshez szükségesek.

Fontos adatokat tartalmazó adathordozókról másolatot kell készíteni, melyeket egymástól elkülönítetten, lehetőleg külön szobában, jól zárható lemezszekrényben kell elhelyezni.

4.4.2. Adathordozók használata, hozzáférés az adathordozókhoz

A hivatali informatikai rendszerekben kezelt adatok, dokumentumok (a 2013. évi L. törvény által definiált) bizalmasságát, hitelességét, sértetlenségét és rendelkezésre állását biztosítani kell, ezért a hivatal nyilvántartást vezet az egyes adathordozó-típusokhoz való hozzáférésre feljogosított személyek köréről, valamint jogosítványuk tartalmáról. A nyilvántartást a hivatal rendszeres időközönként felülvizsgálja, aktualizálja *(B35 Mobil adattárolók nyilvántartása)*.

Minden munkatársnak kötelessége az adattárolók rendeltetésszerű használata. A hivatal adathordozói csak a munkavégzéshez szükséges adatok és szoftverek tárolására hivatottak. A hivatal tulajdonában lévő hordozható külső adattárolók (flash diskek, pendrive-ok, memóriakártyák, hordozható HDD-k) hivatalon kívüli használata csak kivételes esetben, írásbeli vezetői engedéllyel lehetséges.

A felhasználók külső adathordozót az informatikai hálózatra csak a jegyző vagy az informatikus írásbeli engedélyével, vírusellenőrzés után csatlakoztathatják. A vírusellenőrző programot lehetőség szerint úgy kell beállítani, hogy automatikusan elvégezze az ellenőrzést külső eszköz csatlakoztatásakor.

Meghibásodás esetén a munkatársak kötelesek jelenteni azt az informatikus felé. A további felhasználásra alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni. A bizalmas adatokat tartalmazó adathordozókról törlő programokkal kell az adatokat eltávolítani, majd ezt követően kell fizikailag megsemmisíteni. Eszköz külső partner által történő szervizelése esetén a szállítás előtt gondoskodni kell az adathordozó tartalmának visszaállíthatatlan módon történő törléséről. Meghibásodott eszköz cseréje esetén – garanciális esetben is – adathordozó csak úgy vihető ki a hivatal területéről, ha arról minden adat visszaállíthatatlan módon törlésre került.

4.4.3. Adathordozók újrafelhasználása, leselejtezése, megsemmisítése

Az adathordozók biztonságához szorosan kapcsolódik az, hogy adathordozók újrafelhasználása, illetve selejtezése után is biztosítani kell a védendő adatok bizalmasságát.

Amennyiben az adathordozó eszközök (flash diskek, pendrive-ok, memóriakártyák, hordozható HDD-k) újrafelhasználásra kerülnek, úgy biztosítani kell, hogy az új felhasználó(k) jogosulatlanul ne férjenek hozzá a korábban az eszközön tárolt adatokhoz (pl. munkaállomás használható merevlemezének más munkaállomásba szerelése esetén). Ebben az esetben az eszközökön biztonságos törlést kell végrehajtani úgy, hogy a teljes adathordozón található valamennyi adat, partíció legalább háromszor kerüljön felülírásra véletlen adatfolyammal. Azt, hogy az adathordozó törlése sikeres volt-e, a törlést végző minden esetben ellenőrzi. Azokat az adathordozókat, amelyeket nem lehet engedélyezett módon törölni, újra felhasználni tilos, az ilyen eszközöket fizikailag meg kell semmisíteni.

Amennyiben az adathordozó oly mértékben sérült vagy elhasználódott, hogy a további használata lehetetlen vagy célszerűtlen, úgy azt selejtezni, majd fizikailag meg kell semmisíteni.

A selejtezési eljárás folyamán az adathordozókon olyan eljárást kell végrehajtani, amelyek megakadályozzák azt, hogy a későbbiekben ezekről az eszközökről adatokat lehessen visszanyerni. Ennek megfelelően a következő adatmegsemmisítési módszerek kerülnek meghatározásra: FDD, CD, DVD, pendrive, SSD esetén az erre alkalmas adatmegsemmisítő eszközzel be kell zúzni azokat. Merevlemezek esetén a mágneslemezeket el kell távolítani az eszközből, majd az erre alkalmas adatmegsemmisítő eszközzel be kell zúzni azokat.

4.5. Felkészülés a rendkívüli helyzetekre, katasztrófákra

A hivatal teljes informatikai rendszerére ***B36 Informatikai Működésfolytonossági- és Katasztrófa-Elhárítási Terv* készül**, amely megfogalmazza, hogyan lehet a hivatal kritikus funkcióit üzemben tartani vagy biztonságos üzemüket minél hamarabb visszaállítani a különböző mértékű problémák bekövetkezése esetén.

A hivatal...

- összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével;
- meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszerhez kapcsolódó üzletmenet-folytonossági tervet;
- az elektronikus információs rendszer vagy a működtetési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálja az üzletmenet-folytonossági tervet;
- tájékoztatja az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és hivatali egységeket;
- gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető, módosítható;
- meghatározza az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;
- rendelkezik a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről;
- jelöli a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket;
- fenntartja a hivatal által előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is;
- kidolgozza a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

A *B36 Informatikai Működésfolytonossági- és Katasztrófa-Elhárítási Terv* tartalmazza többek között a kritikus fontosságú rendszerek és erőforrások azonosítását, azok alapfeladatait, alapfunkcióit, a rendelkezésre állás biztosításának módját (redundáns rendszerek, tartalékképzés stb.), az ehhez kapcsolódó vészhelyzeti követelményeket, valamit a hivatali adatvagyon mentési- archiválási- és helyreállítási rendjét.

A kidolgozott stratégiák (előkészületek, eljárások dokumentálása, oktatás) megvalósításához a *B36 Informatikai Működésfolytonossági- és Katasztrófa-Elhárítási Terv*ben foglaltak szerint felelősöket kell kijelölni. A tervet az elektronikus információs rendszer vagy a működtetési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálni kell. A terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és hivatali egységeket minden esetben tájékoztatni kell.

4.6. Az elektronikus információs rendszer mentései

A hivatali informatikai rendszerekben kezelt adatok, dokumentumok bizalmasságát, hitelességét, sértetlenségét és rendelkezésre állását biztosítani kell.

A biztonsági mentések gyakoriságának összhangban kell állnia a mentett adatok, illetve programok biztonsági besorolásával, elvesztésük, sérülésük kockázatával és hatásával *(B09 IT kockázatértékelés)*, valamint a hivatal ügyintézési ciklusával.

Az informatikai infrastruktúrában a biztonsági mentési eljárást, annak pontos leírását, valamint az ehhez tartozó feladatokat, szabályokat a ***B37 Mentési rend*** című dokumentum szabályozza részletesen a következő alapelvek betartásával. A dokumentum elkészítésért az informatikus felelős.

Az informatikus feladata a felhasználói rendszerekben leírtakon felüli *rendszeres és időszakos biztonsági mentések elvégzése*. A mentéseket úgy kell végezni, hogy az adatbázisok konzisztenciája biztosítva legyen, illetve az egyéb munkaállomások hálózati munkáját ne akadályozza.

A mentési rendszert a technológiai és gazdasági lehetőségek figyelembevételével a lehető legnagyobb mértékben automatizálni kell, hogy minimalizálni lehessen az emberi tényezőből adódó hibák előfordulásának valószínűségét Ennek koordinációjáért és a szükséges források tervezéséért az informatikus felelős.

A szoftverekről változtatás előtt biztonsági mentést kell készíteni, melynek felelőse a rendszergazda. *A mentést követően az adathordozót a szerver szobától eltérő helyiségben* (lehetőség szerint a szerverszobával nem azonos épületben), erre a célra rendszeresített biztonsági szekrényben, elzárva kell tárolni. Törekedni kell arra, hogy a mentések tárolása fizikailag biztonságos legyen, védeni kell őket az illetéktelen hozzáférésektől, illetve a különböző fizikai behatásoktól (tűz, víz, mágnesesség stb.). A biztonsági mentéseket hibajelzésmentesen, visszatölthető módon kell elkészíteni. Ennek érdekében a mentések felhasználhatóságát, amennyiben technikailag lehetséges, szúrópróbaszerűen tesztelni kell, illetve a mentési eljárásba épített automatikus ellenőrzéseket kell végrehajtani. Ennek betartásáért a biztonsági mentés elvégzésével megbízott rendszergazda tartozik felelősséggel. Sikertelen mentés esetén a lehető legrövidebb időn belül meg kell ismételni a mentést.

A 466/2017. (XII. 28.) Kormányrendeletben foglalt archiválási kötelezettségnek a hivatal az önkormányzati ASP rendszer útján tesz eleget.

4.6.1. A felhasználók adatainak mentése

A felhasználók munkaállomásokon lévő adatait a mentési eljárások nem kezelik, ezért *a felhasználók a munkájukhoz tartozó fontos dokumentumokat a fájlszerverek megfelelő kijelölt területein kötelesek tárolni!*

A mentés elmaradásából eredő, a szerverre nem mentett adatok helyreállításának hibáiért, vagy ennek lehetetlenségéért a felhasználó a felelős. A hivatal által kiadott notebook-ok adatainak mentését az informatikus kérésre elvégzi, a felhasználókkal történt előzetes egyeztetés után. A felhasználók adatainak DVD-re írását, - ha az iroda nem rendelkezik saját DVD-íróval, - kérésre az informatikus végzi. A felhasználók által írt adathordozókon található adatok jogtisztaságáért a felhasználó a felelős.

A munkaállomások a felhasználó munkakörétől és jogosultságtól függően tartalmazhatnak adat be- és kiviteli eszközöket (FDD, CD, DVD, USB), de ezek használata korlátozott, az eddigiekben leírtak szerint történik. A mobil adathordozók használatát kerülni kell! A már nem használt, megrongálódott vagy selejtezendő adathordozókat a felhasználók kötelesek leadni.

4.6.2. A szervereken tárolt adatok mentése

A központi szervereken tárolt elektronikus információvagyont a biztonsági káresemények ellen szintén mentéssel védi az üzemeltetői csoport. A rendszer egészéről a *B37 Mentési rend* című dokumentumban leírtaknak megfelelően teljes mentést kell készíteni. A mentéseket minden mentési rendet érintő (fizikai, logikai, vagy adminisztratív) változáskor, de legalább évente egyszer ellenőrizni kell aszerint, hogy visszatöltésük, helyreállításuk valóban működik-e. Az ellenőrzéseket dokumentálni kell a *B37 Mentési rend* dokumentumon.

A mentések rendjét, valamint az esetleges helyreállítási tervet a rendszerszintű leírásoknak, illetve *B37 Mentési rend*nek kell tartalmaznia.

4.7. Az elektronikus információs rendszer helyreállítása és újraindítása

A hivatal informatikusa a *B36 Informatikai Működésfolytonossági- és Katasztrófa Terv*ben leírtaknak megfelelően gondoskodik az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.

4.8. Karbantartás

4.8.1. Rendszer karbantartási eljárásrend

A hivatal...

- megfogalmazza, és a hivatalra érvényes követelmények szerint dokumentálja, valamint a hivatalon belül kihirdeti a rendszer karbantartási eljárásrendet (***B39 Karbantartási rend***), mely a rendszer karbantartási kezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
- a fizikai védelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a rendszer karbantartási eljárásrendet.
- kialakít egy folyamatot a karbantartók munkavégzési engedélyének kezelésére, és nyilvántartást vezet a karbantartó szervezetekről vagy személyekről;
- megköveteli a hozzáférési jogosultság igazolását az elektronikus információs rendszeren karbantartást végzőktől;
- felhatalmazást ad a hivatalhoz tartozó, a kívánt hozzáférési jogosultságokkal és műszaki szakértelemmel rendelkező személyeknek arra, hogy felügyeljék a kívánt jogosultságokkal nem rendelkező személyek karbantartási tevékenységeit.

4.8.2. Rendszeres karbantartás

A hivatal...

- a karbantartásokat és javításokat ütemezetten hajtja végre (B39 Karbantartási rend), dokumentálja és felülvizsgálja a karbantartásokról és javításokról készült feljegyzéseket (***B40 Karbantartási napló***) a gyártó vagy a forgalmazó specifikációinak és a hivatali követelményeknek megfelelően;

- jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban;
- az ezért felelős személyek jóváhagyásához köti az elektronikus információs rendszer vagy a rendszerelemek kiszállítását a hivatali létesítményből (*B22 IT eszköz kiviteli-behozatali engedélye*);
- az elszállítás előtt minden adatot és információt – mentést követően – töröl a berendezésről;
- ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat;
- csatolja a meghatározott, karbantartással kapcsolatos információkat a karbantartási nyilvántartáshoz (*B40 Karbantartási napló*);

5. RENDSZER- ÉS INFORMÁCIÓ SÉRTETLENSÉG

Ezeket a rendelkezéseket egy adott elektronikus információs rendszer tekintetében abban az esetben kell alkalmazni, ha az adott elektronikus információs rendszert a hivatal üzemelteti. Üzemeltetési szolgáltatási szerződés esetén szerződéses kötelemként kell az alábbiakat érvényesíteni, és azokat a szolgáltatónak kell biztosítania.

5.1. Rendszer- és információsértetlenségre vonatkozó eljárásrend

A hivatal...

- megfogalmazza, és a hivatalra érvényes követelmények szerint dokumentálja, valamint a hivatalon belül kihirdeti a rendszer- és információsértetlenségre vonatkozó eljárásrendet, mely a hivatal információbiztonsági szabályzatának részét képező, rendszer- és információsértetlenségre vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
- a rendszer- és információsértetlenségre vonatkozó eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a rendszer- és információsértetlenségre vonatkozó eljárásrendet.

5.2. Felügyelet

A biztonsági események olyan események, melyek eltérnek a megszokott ügymenettől, zavarokat okozhatnak és fenyegethetik az információk, illetve az információ feldolgozó eszközök bizalmasságát, sértetlenségét és rendelkezésre állását.

Az információbiztonsági incidensek az IBF vagy a hivatal vezetője által minősített olyan biztonsági események, melyek ténylegesen fenyegetik az információk, illetve az információfeldolgozó eszközök bizalmasságát, sértetlenségét és rendelkezésre állását.

Minősített incidens a hibás működés, mely a rendszerelemek (hardverek, szoftverek, adathordozók) rendeltetésszerű használata közben fellépő, normál működéstől eltérő viselkedését jelenti.

A védelem gyenge pontjai a rendszer, a folyamatok, illetve az abban részt vevő személyek olyan tulajdonságai, hiányosságai, melyek biztonsági incidensek kialakulásához vezethetnek.

Biztonsági eseményt, illetve a védelem gyenge pontjait a hivatal minden munkatársa, a rendszereket használó szerződött partnere és a projektekbe bevont harmadik felek észlelhetik, illetve annak létét feltételezhetik. Biztonsági eseményre utaló jelek lehetnek többek között:

- Adatok, információk, fájlok eltűnése, módosulása;
- Információ feldolgozó eszközök, adattárolók eltűnése, rongálódása;
- Információ feldolgozó eszközök megszokottól eltérő működése;
- Adatátvitel szokásostól eltérő lelassulása;
- Bizalmas információk nem ellenőrzött, külső csatornából történő visszahallása.

Elsődleges szabály, hogy az információbiztonsági incidensek gyanújának felmerülésekor (incidens észlelésekor) azonnal értesíteni kell az információbiztonsági felelőst (IBF) és az informatikust. TILOS az incidens körülményeit vizsgálni, illetve megkísérelni elhárítani azt!

5.2.1. Felügyeleti eszközök

A hivatal az információs rendszerei meghatározott alapvető attribútumainak (pl. merevlemez telítettség, CPU használat) gyűjtésére és elemzésére automata felügyeleti eszközöket alkalmaz. A gyűjtendő információkat az érintett rendszer dokumentációja tartalmazza. Az elektronikus információs rendszerben üzemelő aktív elemek üzemállapotának megfigyelése, forgalmának nyomon követése csak az informatikai vezető engedélye és az érvényes törvények betartása mellett lehetséges, az általa kijelölt hardver- és szoftvereszközökkel. A diagnosztikai megfigyelő tevékenységet csak az informatikai vezető által felhatalmazott személyek végezhetnek. Minden egyéb állapot-, illetve forgalomfigyelő tevékenység gyakorlása szigorúan tilos.

Az elektronikus információs rendszer felügyeleti információt az IBF havi vagy negyedéves rendszerességgel elemzi, igény esetén jelentést készít azokról. Fokozott kockázatra utaló jelek észlelése esetén javaslatokkal él ***(B41 Rendszerfelügyeleti információs jelentés)***.

5.2.2. Biztonsági riasztások és tájékoztatások

A hivatal...

- folyamatosan figyeli a Kormányzati Eseménykezelő Központ (GovCERT-Hungary) által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;
- folyamatosan figyelemmel kíséri a Nemzeti Elektronikus Információbiztonsági Hatóságtól (NEIH) érkező értesítéseket;
- szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki (***B46 IT biztonsági riasztási napló***)
- a belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez;
- kialakítja és működteti a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, és kapcsolatot tart az érintett, jogszabályban meghatározott szervekkel;
- megfelelő ellenintézkedéseket és válaszlépéseket tesz.

5.3. Incidensek kezelése

Az incidensek kezelése során a hivatal vezetője és az IBF döntenek a szükséges lépésekről, de döntésük során figyelembe kell venniük az alábbi főbb irányelveket. A döntésekről írásban értesítik az informatikust, aki felelősséggel tartozik azok haladéktalan végrehajtásáért.

A biztonsági incidensek érintett rendszerelemeit, a minősítést követően lokalizálni kell és megakadályozni az esetleges tovább terjedést (hálózatról leválasztani, internet kapcsolatot megszüntetni, hardverelemet kiemelni stb.).

Be kell gyűjteni az összes releváns adatot és bizonyítékot a biztonsági incidensről (naplóbejegyzések, okozott jelenségek stb.) és az okozott fennakadásokról, károkról.

Gondoskodni kell a károk enyhítéséről. Biztosítani kell a hivatali funkcionalitás minimálisan elvárt szintű (az érintett vezetők határozzák meg) visszaállítását (ha az sérült) a biztonsági incidens megismétlődését kizáró, vagy a megismétlődést elfogadható kockázatúra csökkentő módon.

Biztosítani kell a hivatali funkcionalitás teljes körű visszaállítását.

5.3.1. Tanulás az incidensekből

Az IBF az Incidens nyilvántartást *(B10 IT biztonsági események naplója)* minden évben a vezetőségi átvizsgálás előtt felülvizsgálja. Ezen felülvizsgálat során különös figyelmet fordít...

- az ismétlődő incidensek azonosítására;
- az incidensek megfelelő kezelésének vizsgálatára;
- az incidensek előfordulási valószínűségét csökkentő, átfogó, az elektronikus információs rendszert érintő fejlesztési lehetőségek azonosítására.

A felülvizsgálatokról jelentést készít a hivatal vezetésének, melyben értékeli az incidenseket és ha szükséges, megelőző, helyesbítő intézkedéseket kezdeményez ***(B42 Incidens-felülvizsgálati jelentés)***.

5.4. Naplózás

A hivatal informatikai rendszereinek tervezésekor rögzített naplózási szabályokat kell alkalmazni. Ennek során az alábbi alapelveknek kell megfelelni:

- A hivatal az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.
- Az egyedi elszámoltathatóság érdekében a naplózási funkciókat úgy kell beállítani, hogy a felhasználói tevékenységek személyre szólóan nyomon követhetők legyenek (***B45 Naplófájlok listája***).
- Az események és problémák azonosítása érdekében a napló tartalmazza a problémák megoldásához szükséges adatokat.
- A visszaélések felderítése érdekében a jogosult felhasználói tevékenységek és jogosulatlan tevékenységekre irányuló kísérletek naplózásra kerülnek.
- A hivatal minden rendszerében megbízható módon védeni kell az ott keletkezett naplóállományokat a jogosulatlan felfedés, módosítás és törlés ellen.
- A naplóállományok ellenőrzését az informatikus végzi. Az ellenőrzéseknek rendszeresen, legalább kéthetente kell megtörténnie. Az ellenőrzések hatékonyságának növelésére automata ellenőrzőszoftvert is lehet alkalmazni, amennyiben ez az adott rendszeren technológiailag lehetséges.
- Az Informatikuson túl a naplóállományok adattartalmába betekinthetnek:
  - IBF;
  - az informatikus vagy az IBF által írásban felhatalmazott szakember.

Az elektronikus információs rendszer:

- naplózási hiba esetén riasztást küld a meghatározott személyeknek vagy szerepköröknek;
- elvégzi a meghatározott végrehajtandó tevékenységeket, így például a rendszer leállítását, a legrégebbi naplóbejegyzések felülírását, a naplózási folyamat leállítását;
- belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához;
- időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz – úgynevezett UTC – vagy a Greenwichi középidőhöz – úgynevezett GMT – rendelhető módon, megfelelve a hivatal által meghatározott időmérési pontosságnak.

5.4.1. Naplózható események

A hivatal...

- meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét;
- egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő hivatali egységgel, hogy növelje a kölcsönös támogatást, és hogy iránymutatással segítse a naplózható események kiválasztását;
- megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

5.4.2. Naplóinformációk védelme

Az elektronikus információs rendszert úgy kell felépíteni, hogy az megvédje a naplóinformációkat és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

5.4.3. Napló tárkapacitás

A hivatal a naplózásra elegendő méretű tárkapacitást biztosít, a biztonsági osztályba sorolásból következő naplózási funkciók figyelembevételével.

5.4.4. Naplózási hiba kezelése

Az elektronikus információs rendszer...

- naplózási hiba esetén riasztást küld a meghatározott személyeknek vagy szerepköröknek;
- elvégzi a meghatározott végrehajtandó tevékenységeket, így például a rendszer leállítását, a legrégebbi naplóbejegyzések felülírását, a naplózási folyamat leállítását.

5.4.5. Naplóvizsgálat és jelentéskészítés

A hivatal...

- rendszeresen felülvizsgálja és elemzi a naplóbejegyzéseket (*B45 Naplófájlok listája*) nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából (***B43 Naplóelemzés-jelentés***);
- jelenti ezeket a meghatározott személyeknek vagy szerepköröknek.

5.5. Kártékony kódok elleni védelem

A lehetséges információbiztonsági fenyegetések közül igen jelentős kockázatot jelentenek a rosszindulatú programok és kódok, a levélszemetek (spam) és a káros Internet tartalmak. A felsorolt negatív elemek ellen számos technológiai eszközzel lehet védekezni, ilyenek a biztonságos átjárók, tűzfalak, vírusvédelmi eszközök, levélszemét szűrő szoftverek, IDS-ek és IPS-ek.

A hálózati határvédelem elsősorban a megelőzésre, másodsorban az elhárításra szolgál. A vírustámadások nagy része az internet, és a levelező rendszerek közreműködésével valósul meg.

A hivatal számítógépes hálózatát, szervereit és munkaállomásait folyamatosan, illetve egy adott számítástechnikai eszközt a felhasználó jelzése alapján vírusvédelmi szempontból figyelni kell. A vírusfertőzés ellenőrzéséről és annak eredményéről nyilvántartást kell vezetni (a legtöbb vírusvédelmi rendszer ezt magától megteszi).

A preventív vírusvédelmet, a tartalom- és spamszűrést és a hálózati határvédelmet hardvereszközök és szoftveres megoldások biztosítják. Ezek kiszűrik a vírusos üzeneteket és a kéretlen leveleket, valamint *letiltják meghatározott weblapok megnyitását*. A honlapok megnyitásának korlátozását elsősorban a Nemzeti Kibervédelmi Intézet (GovCERT-Hungary) által közzétett tiltólistákból, másodsorban helyi tiltólistákból kell előállítani.

A hálózati határvédelem eszközeinek működését folyamatosan ellenőrizni kell, a szoftverrendszer elemeinek (programok, szabályrendszerek, vírusdefiníciós adatbázisok, listák) frissítéséről automatizált módszerrel gondoskodni kell. A frissítések hiba nélküli megtörténtét ellenőrizni kell.

Valamennyi felhasználónak kötelessége minden tőle telhetőt megtenni annak érdekében, hogy olyan fájl (szoftver, dokumentum stb.), amely rosszindulatú kódot, tartalmat tartalmaz, ne kerüljön fel a felhasználók munkaállomásaira, hordozható számítógépeire (laptop), sem pedig a hálózati adattárolókra.

A fentiek miatt mind a munkaállomásokon, mind a szervereken védelmi szoftvereket kell alkalmazni. A hivatalban a hálózati határvédelmi illetve vírusvédelmi funkciókat a hivatal *B36 Informatikai működésfolytonossági- és katasztrófaterv*ben felsorolt szoftverek valósítják meg.

A határvédelem folyamatára az alábbi szabályok érvényesek:

- A határvédelmi programoknak folyamatosan kell működniük. A programoknak folyamatosan vizsgálniuk kell a bejövő és kimenő hálózati forgalmat (pl. levelezés, web).
- A vírusvédelemnek a klienseken rezidens módon kell futniuk, azaz a rendszer indulásakor automatikusan indul a program, illetve rendszeres időközönként vírusellenőrzést kell végrehajtani a klienseken, amely vizsgálatok eredményét ellenőrizni kell. A vírusvédelemnek a rendszer alábbi komponenseire kell kiterjednie: fájlok, rendszeradatok, hálózati web- és emailforgalom.
- A felhasználóknak a vírusvédelmi alkalmazások működését tilos leállítani!
- A felhasználónak tilos vírusirtót, személyes tűzfalat vagy egyéb biztonsági szoftvert telepíteni.
- A határvédelmi szoftverrendszer elemeinek (programok, szabályrendszerek, vírusdefiníciós adatbázisok) frissítéséről automatizált módszerrel kell gondoskodni. A frissítések hiba nélküli megtörténtét ellenőrizni kell.
- Külső helyekről származó adattárolókat csak hivatali okból szabad használni és a használat előtt vírusellenőrzésnek kell alávetni. Az adattárolók csak akkor használhatók, ha az ellenőrzés vírusfertőzést nem jelez.

- Vírusfertőzés gyanúja vagy nem üzemszerű működés esetén a felhasználóknak haladéktalanul értesíteni kell az informatikust, aki megvizsgálja az eseményt és hiba esetén elhárítja azt.
- Vírusfertőzés gyanúja esetén az informatikus és/vagy az IBF a fertőzött gépet lezárhatja, annak használatát a hiba elhárításáig felfüggesztheti.

5.6. Hibajavítás, biztonsági frissítések

A hivatal által használt szoftverek hibáinak napvilágra kerülése esetén számítani lehet arra, hogy az ártó szándékú támadók ezeket a biztonsági réseket kihasználva próbálnak az információs rendszerbe behatolni, ezért elengedhetetlen, hogy a szoftver gyártója által készített javítások (frissítések) a lehető leghamarabb telepítésre kerüljenek.

A hivatal informatikusa a fentiek megvalósulása érdekében...

- azonosítja, belső eljárásrendje alapján jelenti és kijavítja vagy kijavíttatja az elektronikus információs rendszer hibáit;
- telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket az érintett hivatali egység feladatellátásának hatékonysága, a szóba jöhető következmények szempontjából;
- a biztonságkritikus szoftvereket a frissítésük kiadását követően a lehető legrövidebb időn belül telepíti vagy telepítteti;
- beépíti a hibajavítást a konfigurációkezelési folyamatba.

6. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM

6.1. Rendszer- és kommunikációvédelmi eljárásrend

A hivatal...

- megfogalmazza, és a hivatalra érvényes követelmények szerint dokumentálja, valamint a hivatalon belüli szabályozásában meghatározott személyek vagy szerepkörök számára kihirdeti a rendszer- és kommunikációvédelmi eljárásrendet, mely a rendszer- és kommunikációvédelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
- a rendszer- és kommunikációvédelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a rendszer- és kommunikációvédelmére vonatkozó eljárásrendet.

6.2. Határok védelme

Az elektronikus információs rendszer felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt. A zónák közötti kommunikáció csak szabályozott formában, határvédelmi rendszer beiktatásával biztosítható. Jelen fejezetben rögzített szabályok betartása alapvető követelmény, megszegése súlyos biztonsági eseménynek tekintendő.

A hivatal belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki a vezeték nélküli technológiák kapcsán, valamint engedélyezési eljárást folytat le a vezeték nélküli hozzáférés feltételeként.

Alapvető szabályok:

- A különböző zónák (pl. intranet -> internet) közötti kommunikáció tűzfal által kontrollált.
- Ha egy kommunikációs csatorna nincs külön engedélyezve, az tiltott.
- Az egyes hálózati zónák közötti kapcsolat létrehozásakor az alábbiakat kell figyelembe venni:
  - a kapcsolat legyen megfelelő erősségű titkosítással biztosítva;
  - a kapcsolat legyen megfelelő erősségű azonosítási algoritmussal ellátva.
- A kapcsolat megvalósításához ajánlott technológiák (ebben a sorrendben):
  - VPN kapcsolat kiépítése
  - SSL/TLS kapcsolat kiépítése
  - egyedi, titkosított és azonosított kapcsolat kiépítése

Az alkalmazott tűzfal beállításainak meghatározása a rendszergazda hatáskörébe tartozik, melyet az IBF véleményezhet. A tűzfal-konfiguráció módosításának igényét, valamint annak jóváhagyását és végrehajtását dokumentálni kell. A módosítás végrehajtása a kijelölt rendszergazda feladata.

A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban kell elhelyezni, elkülönítve a belső hivatali hálózattól.

A hálózati határvédelem eszközeinek működését folyamatosan ellenőrizni kell, annak rendszeres frissítéséről kiemelt figyelemmel kell gondoskodni!

6.3. Kriptográfiai kulcsok előállítása és kezelése

Az elektronikus információs rendszer szabványos, a jogszabályokban biztonságosnak minősített kriptográfiai műveleteket valósít meg.

Az elektronikus információs rendszer meggátolja az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha a hivatal engedélyezte azt, és közvetlen jelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.

Az elektronikus információs rendszer elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára.

6.4. Hitelesítés szolgáltatók tanúsítványának elfogadása

Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság (NMHH) elektronikus aláírással kapcsolatos nyilvántartásában szereplőhitelesítés szolgáltatók által kibocsátott tanúsítványokat fogadhatja el a hivatalon kívüli felhasználók hitelesítéséhez.

Az elektronikus információs rendszer egy adott kriptográfiai modulhoz való hitelesítésre olyan mechanizmusokat használ, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának.

6.5. Biztonságos név/cím feloldó szolgáltatások

Az elektronikus információs rendszer a név/cím feloldási kérésekre a hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozó kiegészítő adatokat is biztosít, és ha egy elosztott, hierarchikus névtár részeként működik, akkor jelzi az utódtartományok biztonsági állapotát is,

és (ha azok támogatják a biztonságos feloldási szolgáltatásokat) hitelesíti az utód- és elődtartományok közötti bizalmi láncot.

Biztonságos név/cím feloldó szolgáltatás (úgynevezett rekurzív- vagy gyorsítótárat használó feloldás). Az elektronikus információs rendszer eredethitelesítést és adatsértetlenség ellenőrzést kér és hajt végre a hiteles forrásból származó név/cím feloldó válaszokra.

Architektúra és tartalékok név/cím feloldási szolgáltatás esetén azok az elektronikus információs rendszerek, amelyek együttesen biztosítanak név/cím feloldási szolgáltatást egy hivatal számára, hibatűrők és belső/külső szerepkör szétválasztást valósítanak meg.

6.6. Túlterheléses (szolgáltatás megtagadás alapú) támadás elleni védelem

Az elektronikus információs rendszer véd a túlterheléses (úgynevezett „szolgáltatás megtagadás") jellegű támadásokkal szemben, vagy korlátozza azok kihatásait a megtagadás jellegű támadások listája alapján, a meghatározott biztonsági intézkedések bevezetésével.