

# Jászszentandrási Közös Önkormányzati Hivatal

## B07 Informatikai Biztonsági Szabályzata (IBSZ)

### v2.0



<b>Készült:</b>	<b>2017. november 02.</b>
<b>Utolsó módosítás:</b>	<b>2017. november 02.</b>
<b>Módosította:</b>	Vékás Sándor
<b>Azonosító:</b>	IBSZ v1.0
<b>Oldalak száma:</b>	45





1.	ÁLTALÁNOS RENDELKEZÉSEK.....	5
1.1.	A Szabályozás célja .....	5
1.2.	A Szabályozás hatálya .....	5
1.2.1.	Az IBSZ személyi hatálya .....	5
1.2.2.	Az IBSZ időbeli hatálya .....	6
1.3.	Az IBSZ alapelvei .....	6
1.4.	Szerepkörök, tevékenységek, felelősségek .....	7
1.4.1.	A Szervezet vezetője .....	8
1.4.2.	Az elektronikus információs rendszerek biztonságáért felelős személy .....	8
1.4.3.	Egyéb szerepkörök.....	9
1.4.3.1.	Honlap tartalom kezelő) .....	9
1.4.4.	Üzemeltetői csoport/üzemeltetők, informatikus .....	9
1.4.5.	Felhasználók.....	10
1.5.	A vezetőség elkötelezettsége, a pénzügyi erőforrások biztosítása .....	10
1.6.	Az IBSZ jogi háttere .....	11
1.7.	Kapcsolódó szabályozások.....	11
2.	ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK .....	11
2.1.	Informatikai biztonságpolitika .....	11
2.2.	Informatikai biztonsági stratégia .....	11
2.3.	Az elektronikus információs rendszerek nyilvántartása .....	12
2.3.1.	Elektronikus információs rendszerelem leltár .....	12
2.4.	Biztonsági osztályba sorolás .....	12
2.5.	Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás.....	12
2.6.	Biztonságtervezési eljárásrend .....	13
2.7.	Rendszerbiztonsági terv.....	14
2.8.	Személyi biztonság.....	14
2.9.	Rendszer és szolgáltatás beszerzés.....	15
2.9.1.	Beszerzési eljárásrend .....	15
2.9.2.	A rendszer fejlesztési életciklusa .....	15
3.	ADATOK ÉS IT RENDSZEREK VÉDELME, BIZTONSÁGA.....	15
3.1.	Fizikai védelmi intézkedések.....	15
3.1.1.	Fizikai védelmi eljárásrend.....	15
3.1.2.	Fizikai belépés ellenőrzése, belépési engedélyek.....	16



3.2.	Szervezeti és személyzeti szabályok .....	17
3.2.1.	Felvételi eljárás során követendő szabályok, személyes követelmények .....	17
3.2.2.	Képzési eljárásrend .....	18
3.2.3.	Biztonság tudatosság képzés .....	18
3.2.4.	Fegyelmi intézkedések.....	18
3.2.5.	Eljárás a jogviszony megszűnésekor .....	20
3.3.	Azonosítás és hitelesítés.....	20
3.3.1.	Azonosítási és hitelesítési eljárásrend .....	20
3.3.2.	Azonosításra, hitelesítésre szolgáló eszközök kezelése.....	22
3.3.3.	Szervezeten kívüli felhasználók azonosítása és hitelesítése.....	23
3.4.	Hozzáférés védelem, jogosultság kezelés.....	23
3.4.1.	Hozzáférés ellenőrzési eljárásrend .....	23
3.4.2.	Felhasználói fiókok kezelése .....	24
3.4.3.	Külső rendszerekből történő hozzáférés szabályozása .....	26
3.4.4.	Azonosítás és hitelesítés nélkül engedélyezett tevékenységek .....	26
3.4.5.	Nyilvánosan elérhető tartalom.....	26
3.5.	Viselkedési szabályok az interneten .....	26
3.5.1.	Elektronikus levelezés (e-mail) .....	28
4.	AZ INFORMATIKAI RENDSZEREK ÜZEMELTETÉSE .....	30
4.1.	Általános rendelkezések .....	30
4.2.	Konfigurációkezelés .....	31
4.2.1.	Konfigurációkezelési eljárásrend .....	31
4.2.2.	Alapkonfiguráció.....	31
4.3.	Szoftverhasználat korlátozásai .....	31
4.3.1.	Felhasználó által telepíthető szoftverek.....	32
4.4.	Adathordozók védelme .....	32
4.4.1.	Adathordozók védelmére vonatkozó eljárásrend .....	32
4.4.2.	Adathordozók használata, hozzáférés az adathordozókhoz .....	32
4.4.3.	Adathordozók újrahasználása, leselejtezése, megsemmisítése .....	33
4.5.	Felkészülés a rendkívüli helyzetekre, katasztrófákra .....	33
4.5.1.	Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre.....	34
4.6.	Az elektronikus információs rendszer mentései.....	34
4.6.1.	A felhasználók adatainak mentése .....	35



4.6.2.	A szervereken tárolt adatok mentése.....	35
4.7.	Az elektronikus információs rendszer helyreállítása és újraindítása.....	36
4.8.	Karbantartás .....	36
4.8.1.	Rendszer karbantartási eljárásrend .....	36
4.8.2.	Rendszeres karbantartás .....	36
5.	RENDSZER ÉS INFORMÁCIÓ SÉRTETLENSÉG.....	36
5.1.	Rendszer- és információsértetlenségre vonatkozó eljárásrend .....	37
5.2.	Felügyelet .....	37
5.2.1.	Felügyeleti eszközök .....	37
5.3.	Incidensek kezelése .....	38
5.3.1.	Tanulás az incidensekből .....	38
5.4.	Naplózás.....	38
5.4.1.	Naplózható események .....	39
5.4.2.	Naplóinformációk védelme.....	39
5.5.	Kártékony kódok elleni védelem .....	39
5.6.	Hibajavítás, biztonsági frissítések .....	40
6.	RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM .....	41
6.1.	Rendszer- és kommunikációvédelmi eljárásrend .....	41
6.2.	Határok védelme .....	41
6.3.	Kriptográfiai kulcsok előállítás és kezelése .....	42
7.	EGYÉB RENDELKEZÉSEK .....	<b>Hiba! A könyvjelző nem létezik.</b>
8.	MELLÉKLETEK.....	42
8.1.	IBSZ 1. számú melléklet - Biztonsági osztályba sorolás .....	42



# 1. ÁLTALÁNOS RENDELKEZÉSEK

## 1.1. A Szabályozás célja

Jászszentandrás Közös Önkormányzati Hivatal (a továbbiakban: Hivatal vagy Szervezet) Informatikai Biztonsági Szabályzatának (a továbbiakban: IBSZ) célja, hogy a vonatkozó jogszabályokkal (2013. évi L. törvény, 41/2015. (VII. 15.) BM rendelet, 257/2016. (VIII. 31.) Kormányrendelet), a Szervezet belső rendelkezéseivel összhangban meghatározza a Szervezet informatikai rendszerei által kezelt információvagyron bizalmassága, hitelessége, sértetlensége, valamint rendelkezésre állásának biztosítása, funkcionalitása és üzembiztonsága megőrzése érdekében betartandó elveket. Az IBSZ meghatározza a vezető és a biztonságért felelős személy feladatait, valamint az információs rendszer működtetői és felhasználói számára kötelező szabályokat. Az IBSZ kiemelt célja, hogy a Szervezet 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 Szervezet valamennyi teljes vagy részmunkaidős, valamint szerződéses dolgozójára kiterjed. Az IBSZ hatálya kiterjed a Szervezet 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 nem informatika célú munkavégzése kapcsán bármilyen informatikai eszközzel a Szervezet informatikai infrastruktúrájához csatlakozik, illetve azt – Szervezeti érdekből – igénybe veszi.

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 Szervezet tulajdonában lévő, illetve az általa bérelt, vagy használt valamennyi informatikai berendezésre (számítógépekre, azok tartozékaira és perifériáira);
- a különböző adathordozókra;
- a Szervezet 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.: 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;
- továbbá tulajdonviszonytól függetlenül (tulajdonolt, bérelt, stb.) a Szervezet területén (állandóan vagy ideiglenes jelleggel) telepített informatikai eszközökre, az azokkal kapcsolatos tevékenységekre.

Az IBSZ az érvényességi idejében 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/beszerezési szakasz: a rendszer fejlesztése, programozása, létrehozása;
- megvalósítási szakasz: a rendszer tesztelése, telepítése, testre szabása;
- üzemeltetés/karbantartás: a rendszer üzemelése, üzemeltetése, hardver, szoftver módosítások, karbantartás, események kezelése;
- visszavonás/selejtezés/megsemmisítés szakasz: információk, hardver, szoftver visszavonása az üzemelésből, törlése, megsemmisítése vagy hosszabb távú megőrzésre való felkészítése.

### 1.2.2. Az IBSZ időbeli hatálya

Az Informatikai Biztonsági Szabályzatot évente, vagy jelentősebb infrastrukturális változás, illetve jogszabály változás esetén időközben felül kell vizsgálni és szükség esetén módosítani kell, mind Szervezeti, mind informatikai szakmai szempontok szerint. *(IBSZ módosítások fejezet)*

### 1.3. Az IBSZ alapelvei

A Szervezet 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 Szervezet és szervezetei által kezelt, felhasznált adatokhoz való hozzáférés tekintetében, elsősorban a szervereken és a felhasználói munkahelyeken történő adathozzáférések és az adatkezeléseknél felhasznált adathordozók tekintetében, valamint a kommunikáció során.

Az egyedi elszámoltathatóságot a Szervezeti 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 rendszer technikailag ezt lehetővé teszi. A naplókat védeni kell a jogosulatlan hozzáférés, módosítás és törlés ellen.



Az információ és a rendszerek rendelkezésre állása érdekében a Szervezeti 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 Szervezeti rendszerekben, amelyek biztosítják, hogy a rendszer működésének megszakadása után minimális veszteséggel álljon vissza biztonságos állapotba a rendszer.

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 Szervezeti fejlesztési erőforrások alkalmazása esetén az adott rendszer fejlesztését, kialakítását végző szervezeti egységnek kell elkészítenie. Külső fejlesztő közreműködése esetén, a fejlesztést végző külső munkatárs készíti el, együttműködve a fejlesztésért felelős szervezeti egységgel.

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 Szervezet belső kapcsolataiban a kommunikáló felek, szervezeti 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 Szervezeti rendszerekben a felhasználó csak azonosítás és hitelesítés után férjen hozzá a rendszer-szolgáltatásokhoz.

Az információtartalom sértetlenségét biztosítani kell a Szervezet 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, törölhetőnek. Biztosítani kell, hogy a jogosultak a pontos és helyes információkat dolgozzák fel tevékenységük során.

A rendszer életciklus szakaszaiba épített biztonság elvének teljesítése céljából a rendszer teljes életciklusában érvényesülnie kell az informatika biztonsági 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 Szervezet informatikai rendszereinek adminisztrálása és biztonsági ellenőrzése.

#### **1.4. Szerepkörök, tevékenységek, felelőségek**

Az informatikai biztonsággal kapcsolatos feladatok szerepkörökhöz rendelték. 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 Szervezet vezetője

A Szervezet vezetője a Jegyző (továbbiakban: a szervezet 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 szervezetre és információs rendszerre vonatkozóan is.
- Biztonságért felelős személyt nevez ki (*B04 IT Biztonsági Felelős megbízása*), erről hatóságok felé tájékoztatást nyújt.
- Informatikai biztonsági stratégia (*B05 Információbiztonsági Stratégia*) és biztonságpolitika (*B06 Információbiztonsági Politika*) kiadása.
- Meghatározza a szervezet elektronikus információs rendszerei felhasználóira vonatkozó szabályokat (*B07 Információbiztonsági Szabályzat*).
- Meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira, és az ehhez szükséges hatáskörre vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot (*B07 Információbiztonsági Szabályzat*).
- Gondoskodik oktatásról, 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 *szereződéses kötelemként gondoskodik a törvényben foglaltak teljesüléséről*. A szervezet 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 szervezet vezetője nevezi ki (*B04 IT Biztonsági Felelős megbízása*). Az IBF felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:

- A szervezet vezetőjének közvetlen adhat tájékoztatást, jelentést.
- Gondoskodik a szervezet 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 szervezet elektronikus információs rendszereire vonatkozó Informatikai Biztonsági Szabályzatot (IBSZ, azaz ez a szabályzat).
- Meghatározza a rendszerek biztonsági beállításaival kapcsolatos elvárásokat, jogokat, feladatokat.
- Véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e 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 e törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről köteles tájékoztatni a Szervezet vezetőjét és a jogszabályban meghatározott szervezetet.

Az elektronikus információs rendszer biztonságáért felelős személy szervezeti vezetői támogatással biztosítja az e szabályzatban meghatározott követelmények teljesülését. A szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködik.

Ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, akkor az elektronikus információs rendszer biztonságáért felelős személy jogosult a közreműködőtől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelés alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatot, 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 nem átruházható.

### **1.4.3. Egyéb szerepkörök**

#### **1.4.3.1. Honlap tartalom kezelő**

JÁSZSZENTANDRÁS település honlapjának tartalomkezelését a Polgármesteri Kabinet végzi.

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

#### **1.4.4. Üzemeltetői csoport/üzemeltetők, informatikus**

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

- felelős a szerverek és a rajtuk futó alapszoftverek, operációs rendszerek, szolgáltatások, adatbázis-kezelők, fájl- és nyomtatószerverek működtetéséért
- felelős a Szervezet mentési rendjében foglaltak szerint az adatmentések elvégzéséért, a mentett adatok biztonságos tárolásáért, a szükséges visszaállításokért



- felelős a standard felhasználói alkalmazáskörnyezet és az általa nyújtott szolgáltatások és segédalkalmazások, továbbá a ráépülő általános irodai alkalmazások komponensei, továbbá a Szervezet felhasználói környezetében már megszokott általános alkalmazások és felhasználói segédprogramok, valamint a hálózati nyomtatók működtetéséért
- felelős az aktív és passzív hálózati eszközök működtetéséért, rendelkezésre állásáért
- felelős az adatbázisban tárolt adatok és szoftverek rendelkezésre állásáért, a hozzáférők adminisztrálásért.

#### 1.4.5. Felhasználók

A Szervezeti rendszerek nem Üzemeltetői csoportban lévő felhasználói.

- Ismerniük kell az Informatikai Biztonsági Szabályzatban szereplő előírásokat, illetve azokat maradéktalanul be kell tartani.
- Rendelkezniük kell az általuk üzemeltetett berendezésekre és szoftverekre vonatkozó előírásokkal, illetve ismerniük kell azok tartalmát.
- Tevékenységük megkezdésekor ellenőrizni kell, hogy az általuk használt eszközök üzemképesek-e és azok beállítása az előírásoknak megfelelő-e.
- Kötelesek figyelemmel kísérni az általuk használt berendezések és szoftverek állapotát és az esetleges meghibásodást vagy helytelen működést azonnal jelezni kell a közvetlen vezetőnek.
- Munkájuk során figyelni kell arra, hogy illetéktelen személyek lehetőleg ne tartózkodjanak az adat/információ feldolgozása során a helyiségben.
- Tevékenységük befejezésekor a használt programokból szabályszerűen ki kell lépni.
- Hálózati információ igénybevételét követően a hálózatról szabályosan ki kell lépni.
- A berendezést szükség esetén az előírásoknak megfelelően le kell állítani, illetve áramellátását meg kell szüntetni.
- A helyiségből utolsóként való távozáskor meg kell győződni a helyiség biztonságos lezárásáról.

### 1.5. A vezetőség elkötelezettsége, a pénzügyi erőforrások biztosítása

A Szervezet vezetősége elkötelezett az információbiztonság menedzselése iránt. Ennek megfelelően

- Az információbiztonság ügyének szükséges mértékű publicitást biztosít a Szervezet keretein belül, s gondoskodik a munkatársak megfelelő felvilágosításáról, tájékoztatásáról, oktatásáról;
- A szükséges anyagi, humán és technikai erőforrásokat biztosítja;
- Beruházások, beszerzések során tervezi az informatikai biztonsági 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 szereplők betartásáról, auditot folytat le (*B11 IT Biztonsági auditjelentés*) és be nem tartás esetére szankciókat határoz meg illetve foganatosít a köztisztviselőkre vonatkozó törvények (2011. évi CXCV. tv. a közszolgálati tisztviselőkről, 31/2012 (III. 7.) Korm. rendelet a közszolgálati tisztviselőkkal szembeni fegyelmi eljárásról) szerint;
- Támogatja az üzemeltető és a fejlesztő irányú törekvéseket.

Mivel a Szervezeti információvagyon biztonsága nem kizárólag az annak kezelésével megbízott személyek feladata és felelőssége, ezért a vezetőség elvárja, hogy a Szervezet minden dolgozója és



szerződéses partnere sajátjának tekintse az információ biztonságának ügyét, s 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
- 2015/41. 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

## 1.7. Kapcsolódó szabályozások

Nincsenek.

## 2. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

### 2.1. Informatikai biztonságpolitika

A Szervezet megfogalmazza és kihirdeti az informatikai biztonságpolitikát (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 esetén, illetve jogszabály változás esetén esedékes.

Felelős: a Szervezet vezetője

### 2.2. Informatikai biztonsági stratégia

A Szervezet megfogalmazza és kihirdeti az informatikai biztonsági stratégiát (a továbbiakban IBS), *(B05 Információbiztonsági Stratégia)* amely meghatározza a biztonságpolitikai célok megvalósításának módszerét, eszközrendszerét, ütemezését. Az IBS illeszkedik a Szervezet más stratégiáihoz, így különösen a költségvetési és humán erőforrás 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 Szervezet vezetője



### 2.3. Az elektronikus információs rendszerek nyilvántartása

A Szervezet az elektronikus információs rendszereiről nyilvántartást vezet *(B12 IT leltár)*. A nyilvántartást elektronikus formában vezeti, és gondoskodik azok naprakészségéről.

A nyilvántartásnak minden rendszerre nézve tartalmaznia kell:

- annak alapfeladatait;
- a rendszerek által biztosítandó szolgáltatásokat;
- az érintett rendszerekhez tartozó licenc számot (amennyiben azok a Szervezet kezelésében vannak);
- a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;
- a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.

A különböző adatokat nem szükségszerűen egy nyilvántartásban kell tárolni, hanem logikus módon szétválaszthatóak. 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 Szervezet az elektronikus információs rendszerének elemeiről elektronikus formában vezetett nyilvántartást vezet, mely az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet tartalmaz. 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 Szervezet 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 Informatikai Biztonsági Szabályzatban is. *(B12 IT leltár)*

A besorolást minimum 2 évente, vagy az elektronikus információs rendszereket érintő változások után, illetve jogszabály változás esetén felül kell vizsgálni és szükség esetén ismételt 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 szervezet vezetőjével. Amennyiben a szervezet 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 jogosultságokat beállítania. A beállítások megfelelőségét szűrőpróbaszerűen az IBF ellenőrizheti.

Amennyiben az információ biztonsági szabályozásban, feladat és 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 Szervezet 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 Szervezet 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 Szervezet:

- megfogalmazza, a Szervezetre 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 Szervezet 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 Szervezet az információs rendszerek valamennyi életciklusára vonatkozóan szem előtt tartja a *B06 Információbiztonsági Politika* megfogalmazott célokat és követelményeket, valamint a gyártói és iparági előírásokat, ajánlásokat.

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



## 2.7. Rendszerbiztonsági terv

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

- összhangban áll szervezeti felépítésével vagy szervezeti 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, vagy a jog, szabályozási, üzemeltetési körülmények nem teszik lehetővé a Szervezet 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, felelősségüket 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* 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 Szervezet:

- megfogalmazza, és a szervezetre érvényes követelmények szerint dokumentálja, valamint a szervezeten belül kihirdeti a beszerzési eljárásrendet (*B18 Beszerzési eljárásrend*), mely a szervezet 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 életrajza

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

A Szervezet az elektronikus információs rendszereinek teljes életútján, azok minden életrajzában figyelemmel kíséri informatikai biztonsági helyzetüket. Fejlesztés esetén már a rendszer tervezésénél fokozottan figyelembe kell venni az informatikai biztonsági előírásokat, ajánlásokat. A Szervezet a fejlesztési életrajz egészére meghatározza és dokumentálja az információbiztonsági szerepköröket és felelőségeket, valamint a szervezetre érvényes szabályok szerint kijelöli az ezen szerepköröket betöltő, felelős személyeket.

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

## 3. ADATOK ÉS IT RENDSZEREK VÉDELME, BIZTONSÁGA

*Jelen fejezet alkalmazása során figyelemmel kell lenni a más jogszabályban meghatározott tűz-, 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

#### 3.1.1. Fizikai védelmi eljárásrend

A fizikai és környezeti biztonságra vonatkozó óvintézkedések a Szervezeti rendszereknek helyet adó létesítmények, a rendszer erőforrások és a működést biztosító alapszolgáltatások védelmével kapcsolatban fogalmazzák meg szabályokat annak érdekében, hogy a számítástechnikai szolgáltatások megszakadását, eszközök ellopását, a fizikai károkozást, az információk jogosulatlan felfedését, a rendszer sértetlenségének elvesztését megakadályozzák (*B19 Fizikai védelmi eljárásrend*).





A Szervezeti számítógépeket és adathordozókat lopás, rongálás, megsemmisülés ellen értékarányos módszerekkel és eljárásokkal védeni kell (élőerős védelem és fizikai védelem – rácsok, ajtók, riasztóberendezés).

A hardverek és adatok részleges vagy teljes megsemmisülésével fenyegető tüzek megelőzése és elhárítása a *B20 Tűzvédelmi Szabályzat* rendelkezései szerint történik.

Az infrastrukturális gyengeségek és hiányosságok kivédése érdekében az egyes rendszerek rendelkezésre állási 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 Szervezet informatikai rendszeréhez nem a Szervezeti infrastruktúrájához tartozó (pl.: magántulajdonú) számítástechnikai, kommunikációs vagy multimédiás berendezést vagy adathordozót kapcsolni tilos! Amennyiben Szervezeti érdekből szükséges ilyen eszköz használata, úgy a feladat csak a Szervezet vezetőjének, vagy az IBF-nek az engedélye alapján, az Üzemeltetői csoport bevonásával, dokumentálási kötelezettség mellett végezhető el (*B21 Idegen eszköz használatának engedélyezése*).

A Szervezet tulajdonában lévő, vagy bérelt behozni/kivinni szándékozott számítástechnikai berendezések mozgatása (Szervezetbe behozatala, kivitele, pl.: javítás céljából, mobil egységek, laptop) Szervezeti céllal lehetséges, amelyet az IBF vagy a Szervezet 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.: Szervezeti laptopok, telefonok, stb.) (*B28 IT eszközök használatba adása és visszavétele*).

A javítás céljából a Szervezetből kikerülő eszközök esetében biztosítani kell, hogy a Szervezet által kezelt adatok ne kerüljenek ki. Olyan meghibásodott eszközök (pc, mobil eszközök, szerverek, stb.), amelyekben az adathordozók védendő adatokat tartalmazhatnak nem kivihetőek az adathordozó alkatrészsel. Ebben az esetben az adathordozót (merevlemez, statikus memória egység, stb.) a javítás idejére cserealkatrészsel 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 Szervezetből. 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 Szervezet székhelyén 3 biztonsági zóna van elkülönítve:

- 1. zóna: folyosó, lépcsőház – portaszolgálat védi (a bejutás ellenőrzötten lehetséges)
- 2. zóna: irodák, tárgyalók – az 1. zónán belül helyezkedik el (a bejutás kulccsal lehetséges)
- 3. zóna: szerverszoba – a 2. zónán belül helyezkedik el (a bejutás kulccsal, csak ideiglenesen lehetséges)

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



Az új belépő munkatársak kulcsokat és kártyákat csak a belépéskori oktatás (*B08 IT biztonsági oktatási terv és napló*), 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 Szervezet vezetőjével.

A jóváhagyott formanyomtatvány továbbításra kerül a kulcsok/azonosító kártyák kiosztásának felelőse felé, akinek felelőssége, hogy csak a vezetőség által jóváhagyott jogosultságokat állítsa be, csak a megfelelő kulcsokat adja ki. Amennyiben felmerül a jóváhagyás hiteltelenségének gyanúja, úgy azt köteles a kulcskiadás előtt igazolni a vezetőség megkérdezésével.

Azon helyiségek kijelölése, illetve kialakítása során, amelyekben a Szervezet 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 *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 személy veheti fel, mivel a szerver sértetlensége, rendelkezésre állása az ő felelősségük. A felvétel tényét minden esetben nyilván kell tartania (*B25 Szerverszoba belépési nyilvántartás*). Munkaidőn kívül a kulcsokat elzártan kell tartani. A helyiségben idegen személy felügyelet nélkül nem tartózkodhat. A belépések rögzítési történhet elektronikus rendszer segítségével is.

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.

## **3.2. Szervezeti és személyzeti szabályok**

Minden, a személybiztonsággal kapcsolatos eljárás, vagy elvárás kiterjed a Szervezet teljes személyi állományára, valamint minden olyan természetes személyre, aki a Szervezet elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem a Szervezet 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 Szervezet 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 informatika 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 naprakészen képezni kell új rendszerek bevezetésekor. A Szervezetben alkalmazott új dolgozót - vezetője kérése alapján- soron kívül ki 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, a jövőben elvárt kompetenciákat.

Az előzőeken túlmenően a Szervezet 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 Szervezet hosszú távú stratégiájával.

Az oktatás mellett a teljes felhasználói állománnyal ismertetni kell az IBSZ előírásait. 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 Szervezet 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*);
- amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;
- illetve a felhasználói személyi állományt legalább évente informatikai és IT-biztonsági képzésben, ismeret-felfrissítésben kell részesíteni (*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, és a Szervezet 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 Szervezet vezetője a kezdeményezést elbírálja, melyről értesítést küld a kezdeményezőnek és az IBF-nek. Kitézi 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 Szervezet 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 Szervezet vezetője meghív.

A feltáró megbeszélést a Szervezet 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 esemény 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 Szervezet 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 Szervezet

A záró megbeszélésen részt vesznek:

- A Szervezet vezetője
- Az eljárást kezdeményező
- Az eljárásban érintett személy
- Az IBF, amennyiben biztonságot érintő fegyelmi vétségről van szó
- Azok, akiket erre a megbeszélésre a Szervezet 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 Szervezet vezetője állásfoglalását a fentiekben részletezett kérdésekben.

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

### **Fegyelmi eljárás érvényesítése**

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

Amennyiben az elektronikus információbiztonsági szabályokat nem a Szervezet személyi állományába tartozó személy sérti meg, úgy a Szervezet érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések fennállásának lehetőségét, szükség szerint bevezeti ezeket az 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 Szervezet a kilépő számára igazolja, hogy a hozzáférési jogokat törölte, illetve a felhasználó a Szervezet felé elszámolt. A kilépőt továbbá tájékoztatni kell az esetleg rá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről *(B28 IT eszközök használatba adása és visszavétele)*.

A Szervezet meghatározott ideig megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz.

## **3.3. Azonosítás és hitelesítés**

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

### **3.3.1. Azonosítási és hitelesítési eljárásrend**

A Szervezetben 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 Szervezet 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 Szervezet 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 Szervezet kijelölt informatikusainak az azonosítási adatokat naprakészen kell tartani, az új felhasználókat be kell vezetni a rendszerbe, a Szervezetből, szervezeti egységből, munkakörből stb. eltávozott munkatársak jogait pedig vissza kell vonni.
- A hitelesítő eszközök személyre szólóan kerülnek kiadásra és nyilvántartásra, így kezelésükért, használatukért és tárolásukért a felhasználók felelnek.
- A Szervezet 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 az esetre 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 és nem csak kisbetűket tartalmaz
  - nem szótári szó, illetve annak egyszerű kiegészítése, pl.: anna78
  - nem egyszerű sorozat (pl.: 123456, abcdef, asdfgh)
  - tartalmaz számokat, kis- és nagybetűket
- Amennyiben egy Szervezeti munkaállomáson több felhasználó is jogosult dolgozni, úgy a feladat elvégzése után (mielőtt másik felhasználó a géphez hozzáférne) a rendszerből 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 6 havonta 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 Szervezet kijelölt munkatársa lehetővé teszi a következő módon:

- rendszergazdai hozzáféréssel megváltoztatja a felhasználó jelszavát



- majd a felhasználó hozzáféréseivel 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 szervezet:

- 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 eszköz típusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket
- dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a 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.

A felhasználói azonosítók/jelszavak elvesztését/elfelejtését, illetve vélelmezett kompromittálódását azonnal jelezni kell a Szervezet vezetője vagy az IBF felé. Elfelejtett jelszó esetében a rendszergazda új kezdeti jelszót állít be, amelyet az első bejelentkezéskor meg kell változtatni. Azonosító kompromittálódás esetén a kompromittált azonosítóhoz tartozó jogokat azonnal le kell tiltani, ebben az esetben 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, 2 db külön adathordozóra mentve, megfelelő titkosítású jelszótároló programban rögzítetten, szerepkörönként külön adatbázisban, melynek mester kulcsát (jelszavát) az adathordozó mellett, szerepkörönként egy lezárt, lepecsételt és legalább két jogosult személy által aláírt borítékban kell tárolni.
- A borítékba az adatokat úgy kell elhelyezni, hogy azok ne legyenek „átvilágíthatóak”, felbontás nélkül ne legyenek olvashatóak. A borítékokra kívül rá kell írni az utolsó módosítás dátumát és a megbontás okát (pl. audit, vagy pl. jogosult távolléte miatti vezetői bontás), ilyen eseteket követően a szerepköri jogosultaknak célszerű a jelszavakat lecserélni.



- A jelszótárolóban a korábbi jelszavak a History alatt, időmegjelöléssel megtalálhatóak. A változtatást végző jogosult köteles a hasonló szerepkörűeknek jelezni a változtatás tényét, adattartalmát. Ha a szerepkörhöz rendelt jogosult végez szabályzatban előírt kötelező jelszóváltást (3 havonta) a tárolt adatokban, akkor nincs szükség borítékbontásra.
- A borítékot zárt biztonsági szekrényben kell tárolni, az illetéktelen hozzáférést megakadályozandó.

### 3.3.3. Szervezeten kívüli felhasználók azonosítása és hitelesítése

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

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

## 3.4. Hozzáférés védelem, jogosultság kezelés

### 3.4.1. Hozzáférés ellenőrzési eljárásrend

A Szervezet 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 jogosultság-kezelési rendszer ellenőrzése mellett kell menedzselni az egyedi elszámoltathatóság elvének érvényre juttatásával. A hozzáférés-védelmi követelmények a Szervezet 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 Szervezet munkafolyamatain, szervezeti struktúráján, a hierarchikus és funkcionális kapcsolatokon alapul.

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

A Szervezet 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; hálózati nyomtató esetén: hozzáférés) hozzáférési módot. A jogosultságok beállítását az informatikai rendszerben az Üzemeltetői csoport végzi el.

A munkaállomásokon és a szervergépeken technikailag is korlátozni kell az úgynevezett alternatív bootolási lehetőségeket (pl.: CD, DVD, USB, Ethernet, stb.). Ezekre az eszközöket csak üzemeltetési / karbantartási / 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 automatikusan felhatalmazott, alapértelmezett jelszóval működő hozzáférések használatát!

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

A felhasználó jogviszonyának megszűnése esetén az Üzemeltetői csoport 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 évenként 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/munkaállomások kaphatnak jogot az erőforrások elérésére, amelyeknek ez a munkájukhoz valóban szükséges.

A Szervezet minden szobájában 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
- programok ill. adatok elérésének biztosítása

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

- olvasási jog
- írási jog
- törlési jog

A Szervezeti 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 Szervezeti 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, anyagaikhoz történő bármilyen illetéktelen hozzáférés vagy annak kísérlete.

A hozzáférés-védelmi és jogosultság-kezelési 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,
- csoport felhasználói fiókok esetén, ha a csoport tagjai megváltoznak,
- 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*).

További feladatok: a Szervezet...

- 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

Külső cégek folyamatos üzemeltetési feladatainak ellátása érdekében (pl.: szerverek karbantartása, 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 Szervezet azon munkatársai, akik a Szervezet által biztosított, távoli munkavégzésre alkalmas eszközzel rendelkeznek.

A távoli hozzáféréshez használt azonosítókat, jogosultságokat a Szervezet Üzemeltetői csoportja dokumentáltan adja ki (*B15 Hozzáférések igénylése és letiltása*), az azonosítóért felelős személy pontos meghatározásával. Az azonosító átvételét az azonosítóért felelős személy aláírásával igazolja.

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

A Szervezet 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 belépés nem lehetséges, így az elektronikus információs rendszeren belül semmilyen tevékenységre nincs lehetőség.

### 3.4.5. Nyilvánosan elérhető tartalom

Nyilvánosan hozzáférhető rendszerként definiálja a Szervezet a publikus weboldalát.

Az oldal üzemeltetéséért felelős szervezeti egység vezetőjének gondoskodni kell az azon publikált információk törvényi megfelelőségéről és valóságáról, sértetlenségéről. Tilos hatályos törvénybe, jogszabályba ütköző, vagy a jó ízlést és közérkölcset sértő tartalmat közzétenni. A felkerülő tartalmakat minden esetben ellenőriznie kell a szervezeti egység vezetőjének és csak a jóváhagyása után publikálhatóak az információk. A publikus weboldalnak gondosan szegmentálnak kell lennie a Szervezet belső hálózatától arra alkalmas eszközzel. Gondoskodni kell a weboldal jogosult használata közben kieszközölhető jogosulatlan elérések megakadályozásáról.

## 3.5. Viselkedési szabályok az interneten

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



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

Az Internet szolgáltatás magán célú használata nem megengedett! Az Internet forgalom automatikusan szoftveres alapon szűrésre kerül, így bizonyos tartalmak nem látogathatók, technológiai eszközzel is tiltásra kerültek. A technikai szűréstől függetlenül a felhasználóknak az internetes elérés szolgáltatás használatának folyamán a következő szabályokat kell betartaniuk.

- Az interneten csak a Szervezeti munkával kapcsolatos oldalakat lehet látogatni. Tilos a pornográf, online játék, fogadási oldalak, csevegő oldalak, letöltő oldalak 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 Üzemeltetői csoport vezetője, előzetes bevizsgálás után engedélyezheti az ilyen programok letöltését és futtatását. A bevizsgálás során ellenőrizni kell:
  - a letölteni kívánt program vírusmentességét,
  - a letölteni kívánt program képes-e működni abban a környezetben, amelybe a letöltést tervezik,
  - hogy a letöltés nem sért-e szerzői jogot.
- Informatikai biztonsági megfontolásokból tilos a Szervezetben a csevegő programok használata (pl.: Skype, msn, gtalk, irc, icq, stb. ). Ezen programok rezidens futtatása tilos! Ezen programok Szervezeti érdekből történő használatára (pl.: skype – kommunikációs költségek csökkentése) a Szervezet 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 bizalmas vagy annál magasabb minőségű, védett információt kizárólag az Interneten keresztül azonosított feleknek továbbítani mindaddig, amíg a másik fél megbízható, az Internettől független azonosítása meg nem történik.
- Tilos a Szervezettel kapcsolatos belső információk nyilvános oldalakon való bármilyen közzététele.
- Tilos a munkavégzéssel kapcsolatos adatok tárolására nem magyarországi illetőségű felhőszolgáltatás igénybe vétele. (pl. Dropbox)

Informatikai biztonsági vizsgálat, auditálás illetve hibakeresés céljából a Szervezet 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 vizsgálat illetve 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 Internet használata a munkája elvégzésének rovására megy (pl.: Szervezeti munkához nem kapcsolódó vagy nagy hálózati terhelést okozó tevékenységet folytat vagy biztonsági fenyegetést jelentő oldalakat látogat), az Üzemeltetői csoport vezetője jelzi a dolgozó közvetlen vezetőjének, aki



megteszi a szükséges intézkedéseket. Amennyiben az intézkedés eredménytelen marad, az érintett munkatárs vezetője utasítására a felhasználó Internet-hozzáférést az Üzemeltetői csoport részlegesen, vagy teljesen letiltja.

Az Internet-kapcsolatok üzemeltetéséért felelős vezetőknek joga van az Internet-hozzáférés 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 Szervezet által a felhasználók részére a Szervezeti elektronikus levelezés céljaira biztosított eszköz. Az e-mail rendszer, valamint a rendszerben előállított, elküldött és megkapott levél is a Szervezet felügyelete alá tartozik.

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

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

A Szervezet nevében folytatott elektronikus levelezésre kizárólag az erre a célra biztosított elektronikus levelezési cím, a rendszeresített levelező (kliens) program, illetve ezen csak az Üzemeltetői csoport vezetője által engedélyezett levelezési szolgáltatás használható. A beállítások (működési paraméterek) meghatározásáért és beállításáért az Üzemeltetői csoport a 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 munkakezdekor 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 Szervezeti e-mail címüket nem hivatalos minőségben használni (pl.: regisztráció letöltési weboldalak, online játék oldalak, stb.);
- a levelek fejlécének megváltoztatása, hamis levelek küldése;
- olyan üzenetek, illetve csatolt fájlok küldése, továbbítása, amelyek törvénytelenégeket vagy arra való felhívást tartalmaznak, fenyegetők, összességében sértik a Szervezet jó hírét, általánosan elfogadott erkölcsi szabályba vagy jogszabályba ütköznek;
- a tévesen címzett, másnak szóló levelek felhasználása;
- a Szervezet által biztosított e-mail címre érkező üzenetek átirányítása külső (nem a Szervezet 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 Szervezet érdekeit.

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

- Csoportos levelező, elosztási lista (pl. „mindenki”, „x osztály”, „Szervezeti 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”: Blind Carbon Copy) kategóriáját kell alkalmazni a címzés során.

Csoportos levelező, elosztási lista létrehozása iránti igényt a szervezeti 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 üzemeltetői csoport feladata. Ennek elvégzéséhez a lista összeállítását kezdeményező szervezeti egység, illetve a Szervezet munkavállalóinak változása esetén a munkaügyi vezető köteles az üzemeltetői csoport számára adatokat biztosítani.

A Szervezet a levelező rendszer működését akadályozó mennyiségű és méretű adat elektronikus levélként való továbbítását korlátozza.

A postaládára vonatkozó korlátozások:

Az e-mail felhasználó postaládájának mérete korlátos, melynek méretét az Üzemeltetői csoport határozza meg a technikai lehetőségek figyelembe vételével. A meghatározottnál nagyobb postaládára vonatkozó igényt a szervezeti egység vezetőjének jóváhagyásával az Üzemeltetői csoporthoz kell eljuttatni, amely a szükséges vizsgálatok, egyeztetések elvégzését követően dönt az igény kielégítéséről és intézkedik annak beállítása érdekében.

Amennyiben a Szervezeti levelezésben – pontos címzés mellett – az elektronikus levelező rendszertől a kézbesítés során kézbesíthetlenségre utaló hibajelzés érkezik, akkor a felhasználónak – szükség szerint az Üzemeltetői csoport megkeresésével – fel kell tárnia ennek okát annak érdekében, hogy üzenete ne veszessen el.

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



## 4. AZ INFORMATIKAI RENDSZEREK ÜZEMELTETÉSE

### 4.1. Általános rendelkezések

Az Üzemeltetői csoport feladata a felhasználók informatikai támogatása, a szolgáltatások folyamatos, Szervezeti 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 Üzemeltetői csoport munkatársa:

- felelősek az informatikai rendszer és a hálózat működőképességéért,
- felelősek a hálózati szolgáltatások, csatlakozások üzembiztonságáért, koordinálásáért.
- gondoskodnak az informatikai eszközök tervszerű megelőző karbantartásáról.
- A folyamatos, Szervezeti 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 Szervezet 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 Üzemeltetői csoport engedélyezte. Amennyiben valaki számítógépet vagy egyéb számítástechnikai berendezést önhatalmúlag csatlakoztat a hálózatra, úgy az Üzemeltetői csoport köteles a berendezést azonnali hatállyal a hálózatról lekötöni, és az illetéktelen eszköz-csatlakoztatást 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 Üzemeltetői csoport és az eszköznilyántartással foglalkozó szervezeti 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 Üzemeltetői csoport vezetője 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 Üzemeltetői csoport által végzendő karbantartási, szoftver frissítési munkák időtartamában az Üzemeltetői csoport 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 Szervezet:

- megfogalmazza, és a szervezetre érvényes követelmények szerint dokumentálja, valamint a szervezeten 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.

### 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 Szervezet:

- az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa;
- meghatározza a tiltott vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatát.

A Szervezet:

- 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 szervezet belső szabályzataival és eljárásaival összhangban.

## 4.3. Szoftverhasználat korlátozásai

A Szervezet bármely informatikai rendszerére csak az Üzemeltetői csoport munkatársai telepíthetnek szoftvert, *a felhasználónak szoftvertelepítésre és bizonyos beállítások módosítására nincs sem joga, sem lehetősége*. A Szervezet informatikai eszközeire TILOS illegális és/vagy nem jogtiszt szoftvert telepíteni! A Szervezet informatikai infrastruktúrájában a feladatok végrehajtására kizárólag a Szervezet 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 és az Üzemeltetői csoportvezető engedélyével az Üzemeltetői csoport munkatársa végzi el.





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

A telepítést megelőzően a Szervezetben 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 Szervezet infrastruktúrájában található eszközökre idegen program, adat másolása tilos!

#### **4.3.1. Felhasználó által telepíthető szoftverek**

A felhasználók az informatikai eszközöket Szervezeti 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 Szervezet informatikai infrastruktúráját magán célú használatra igénybe venni TILOS!

Ettől eltérni csak a szervezet vezetője vagy az Információbiztonsági Felelős (IBF) 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 tűzfalal leválasztott nyilvános részek (pl. free „vendég” wifi) kivételével (6.2. pont 4. bekezdés) - nem használja a szervezet belső informatikai struktúráját (B34 IT eszköz kivonási kérelem). Ebben az esetben a felhasználót a kockázatokról tájékoztatni kell, aki a nyilatkozat tételével lemond a szervezet nem nyilvános hálózatának bármilyen használati lehetőségéről és a kivont eszköz hardver és szoftver karbantartását is átvállalja. Karbantartási kötelezettsége nem terjed ki garanciális javítás ügyintézésére, azt továbbra is az informatikai üzemeltetésért felelős szervezeti egység feladata.

### **4.4. Adathordozók védelme**

#### **4.4.1. Adathordozók védelmére vonatkozó eljárásrend**

A Szervezet által használt hordozható külső adattárolókat (flash diskek, USB pendrive-ok, memóriakártyák, hordozható hdd-k és ssd-k) egyedi azonosítóval kell ellátni, kivételt képeznek ez alól az optikai adathordozók (CD, DVD) és a floppy lemezek, 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 csak azok az adathordozók lehetnek, amelyek a munkavégzéshez szükségesek.

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

#### **4.4.2. Adathordozók használata, hozzáférés az adathordozókhoz**

A Szervezeti informatikai rendszerekben kezelt adatok, dokumentumok bizalmosságát, hitelességét, sértetlenségét és rendelkezésre állását biztosítani kell, ezért a Szervezet nyilvántartást vezet az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek köréről, valamint jogosítványuk



tartalmáról. A nyilvántartást rendszeres időközönként felülvizsgálja, aktualizálja (*B35 Mobil adattárolók nyilvántartása*).

Minden munkatártnak kötelessége az adattárolók rendeltetésszerű használata. A Szervezet adathordozói csak a munkavégzéshez szükséges adatok és szoftverek tárolására hivatottak. A Szervezet tulajdonában lévő hordozható külső adattárolók (flash diskek, USB pendrive-ok, memóriakártyák, hordozható hdd-k és ssd-k). Szervezeten kívüli használata csak kivételes esetben, vezetői engedéllyel lehetséges.

A felhasználók saját tulajdonú adathordozóit az informatikai hálózatra csak az informatikus engedélyével, vírusszűrés után csatlakoztathatják.

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 Szervezet területéről, ha arról minden adat visszaállíthatatlan módon törlésre került.

#### **4.4.3. Adathordozók újrahhasználása, leselejtezése, megsemmisítése**

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

Amennyiben adathordozó eszközök (flash diskek, USB pendrive-ok, memóriakártyák, hordozható hdd-k és ssd-k) újra felhasználásra 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. A tárolók tartalmát, hogy az adathordozó törlése sikeres volt-e, a törlést végző minden esetben ellenőrzi. Azokat az adathordozókat, amelyeket nem lehet engedélyezett módon törölni, újrafelhasználni tilos, az ilyen eszközöket meg kell semmisíteni.

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

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: Floppy, CD, DVD pendrive-ok, statikus memóriák esetén az erre alkalmas adatmegsemmisítő eszközzel be kell zúzni azokat. Merevlemezeken pedig a mágneslemezt el kell távolítani az eszközből, majd a CD, DVD lemezek esetén is használatos adatmegsemmisítő eszközzel be kell zúzni azt.

#### **4.5. Felkészülés a rendkívüli helyzetekre, katasztrófákra**

A Szervezet teljes informatikai rendszerére *B36 Informatikai Működésfolytonossági- és Katasztrófa Terv* készül, amely megfogalmazza, hogyan lehet a Szervezet kritikus funkcióit üzemben tartani vagy



biztonságos üzemet minél hamarabb visszaállítani kisebb-nagyobb problémák bekövetkezése esetén.

#### 4.5.1. Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

A *B36 Informatikai Működésfolytonossági- és Katasztrófa 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, valamint a Szervezeti adatvagyon mentési- archiválási- és helyreállítási rendjét. Rendelkezik továbbá a helyreállítási feladatokról, prioritásokról és mértékekről, fenntartja a szervezet 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 kidolgozott stratégiák (előkészületek, eljárások dokumentálása, oktatás) megvalósításához a *B36 Informatikai Működésfolytonossági Tervben* 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 szervezeti egységeket minden esetben tájékoztatni kell.

#### 4.6. Az elektronikus információs rendszer mentései

A Szervezeti 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 Szervezet 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.

Az Üzemeltetői csoport feladata a felhasználói rendszerekben leírtakon felüli *rendszeres és időszakos biztonsági mentések elvégzése*. A mentéseket úgy kell végezni, hogy az adatbázisok konzisztenciájára 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 Üzemeltetői csoport felelős.

A szoftverekről változtatás előtt biztonsági mentést kell készíteni. Ezért a rendszergazda felel.

A mentést követően az adathordozót a szerver szobától eltérő helyiségben (ajánlott 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, mágnesség, stb.).

A biztonsági mentéseket hibajelzés-mentesen, visszatölthető módon kell elkészíteni. Ennek érdekében a mentések felhasználhatóságát, amennyiben technikailag lehetséges, szűrőpróbaszerűen 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.

#### 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 felhasználók az adataikat a szerverre menthetik. A mentés nem kötelező, de a szerverre nem mentett adatok helyreállításának hibáiért, vagy ennek lehetetlenségéért a felhasználó a felelős. A Szervezet által kiadott notebook-ok adatainak mentését az Üzemeltetői csoport kérésre elvégzi, a felhasználókkal történt előzetes egyeztetés után. A felhasználók adatainak DVD-re írását, - ha az iroda nem rendelkezik saját DVD-íróval, - kérésre az Üzemeltetői csoport végzi. A felhasználók által írt adathordozókon található adatok jogtisztaságáért a felhasználó a felelős.

A munkaállomások a felhasználó munkakörétől és jogosultságtól függően tartalmazhatnak adat be/kiviteli eszközöket (floppy, CD/író, DVD/író, USB), de ezek használata korlátozott, az eddigiekben leírtak szerint történik. A mobil adathordozók használatát kerülni kell! A már nem használt mobil adathordozót le kell adni.

A felhasználók kötelesek a megrongálódott vagy selejtezendő adathordozókat leadni.

#### 4.6.2. A szervereken tárolt adatok mentése

A központi szervereken tárolt elektronikus információvagyon 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 mentéseket a szerverektől elkülönítve, legalább külön helyiségben kell tárolni, védve mind a különböző fizikai káreseményektől (tűz, csőtörés-vízbetörés, stb.), mind az illetéktelen hozzáféréstől (lopás, illegális másolás).

A mentések rendjét, valamint az esetleges helyreállítási tervet a rendszerszintű leírásoknak, illetve *B37 Mentési rend*nek kell tartalmaznia. E dokumentumok elkészítésért a Szervezet vezetője a felelős.



#### 4.7. Az elektronikus információs rendszer helyreállítása és újraindítása

A Szervezet Üzemeltetői csoportja a *B36 Informatikai Működésfolytonossági- és Katasztrófa Tervben* 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 Szervezet:

- megfogalmazza, és a szervezetre érvényes követelmények szerint dokumentálja, valamint a szervezeten belül kihirdeti a rendszer karbantartási eljárásrendet, 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.

##### 4.8.2. Rendszeres karbantartás

A Szervezet:

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

- megfogalmazza, és a szervezetre érvényes követelmények szerint dokumentálja, valamint a szervezeten belül kihirdeti a rendszer- és információsértetlenségre vonatkozó eljárásrendet, mely a szervezet informatikai biztonsági 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 Szervezet vezetője által minősített olyan biztonsági események, melyek ténylegesen fenyegetik az információk, illetve az információ feldolgozó eszközök bizalmasságát, sértetlenségét és rendelkezésre állását.

Minősített incidens a hibás működés, mely a rendszerelemek (hardverek, szoftverek, adathordozók) rendeltetésszerű használata közben fellépő, normál működéstől eltérő működését 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 Szervezet 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 a jelentési kötelezettségnél meghatározott felelőst. TILOS az incidens körülményeit vizsgálni illetve megkísérelni, elhárítani azt!

### 5.2.1. Felügyeleti eszközök

A Szervezet 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 mellett és az érvényes törvények betartása mellett lehetséges,



az általa kijelölt hardver és szoftver eszközökkel, az általa felhatalmazott személyek végezhetnek ilyen tevékenységet. 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*).

### 5.3. Incidensek kezelése

Az incidensek kezelése során a Szervezet vezetője és az IBF döntenek a szükséges lépésekről, de döntésük során figyelembe kell venniük az alábbi főbb irányelveket:

- A biztonsági incidensek érintett rendszerelemeit, a minősítést követően lokalizálni kell és megakadályozni az esetleges tovább terjedést (hálózatról leválasztani, internet kapcsolatot megszüntetni, hardverelemet kiemelni...).
- Be kell gyűjteni az összes releváns adatot és bizonyítékot a biztonsági incidensről (naplóbejegyzések, okozott jelenségek...) és az okozott fennakadásokról, károkról.
- Gondoskodni kell a károk enyhítéséről. Biztosítani kell a Szervezeti funkcionalitás minimálisan elvárt szintű (az érintett vezetők határozzák meg) visszaállítását (ha az sérült) a biztonsági incidens megismétlődését kizáró, vagy a megismétlődést elfogadható kockázatra csökkentő módon.
- Biztosítani kell a Szervezeti 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 Szervezet vezetésének, melyben értékeli az incidenseket és ha szükséges, megelőző, helyesbítő intézkedéseket kezdeményez (*B42 Incidens-felülvizsgálati jelentés*).

### 5.4. Naplózás

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

- A Szervezet 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.
- 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 Szervezet 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.
- informatikuson túl a naplóállományok adattartalmába betekinhetnek:
  - IBF
  - informatikus vagy IBF valamelyike által írásban felhatalmazott (akár külsős) szakember.

Az elektronikus információs rendszer:

- belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához,
- időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz – úgynevezett UTC – vagy a Greenwichi középidejűhöz – úgynevezett GMT – rendelhető módon, megfelelő a szervezet által meghatározott időmérési pontosságnak.

#### 5.4.1. Naplózható események

A Szervezet:

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

#### 5.4.2. Naplóinformációk védelme

Az elektronikus információs rendszert úgy kell felépíteni, hogy az megvédi a naplóinformációt és a napló-kezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

### 5.5. Kártékony kódok elleni védelem

A lehetséges informatikai biztonsági 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 Szervezet számítógépes hálózatát, szervereit és munkaállomásait folyamatosan, illetve az adott számítástechnikai eszközt a felhasználó jelzése alapján vírusvédelmi szempontból figyelni kell. A vírushatás ellenőrzéséről és annak eredményéről nyilvántartást kell vezetni (a legtöbb vírusvédelmi rendszer ezt magától megteszi).





A preventív vírusvédelmet, a tartalom és spam szűrést és a hálózati határvédelmet hardver és eszközök és szoftver megoldások biztosítják. Ezek kiszűrik a vírusos üzeneteket és a kéretlen leveleket, valamint *letiltják meghatározott weblapok megnyitását*. A honlapok megnyitásának korlátozását elsősorban általános 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 sem 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 Szervezetben a hálózati határvédelmi illetve vírusvédelmi funkciókat a Szervezet *B36 Informatikai működésfolytonossági- és katasztrófatervben* felsorolt szoftverek valósítják meg.

A határvédelem folyamatára az alábbi szabályok érvényesek:

- A határvédelmi programoknak a szervereken 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 folyamatosan vírusellenőrzést kell végrehajtani a klienseken, amely vizsgálatok eredményét ellenőrizni kell. A vírusvédelemnek a rendszer alábbi komponenseire kell kiterjednie: fájlok, rendszeradatok, webes és email hálózati forgalom.
- A felhasználóknak a vírusvédelmi alkalmazások működését tilos leállítani!
- A felhasználóknak tilos vírusirtót, személyes tűzfalat, vagy egyéb biztonsági szoftvert telepítenie.
- A határvédelmi szoftverrendszer elemeinek (programok, szabályrendszerek, vírusdefiníciós adatbázisok) frissítéséről automatizált módszerrel gondoskodni kell. A frissítések hiba nélküli megtörténtét ellenőrizni kell.
- Külső helyekről származó adattárolókat (Szervezeti okból történő) használat előtt vírusellenőrzésnek kell alávetni és csak akkor lehet használni, ha az adathordozó a vizsgálaton megfelel.
- Vírusfertőzés gyanúja vagy nem üzemszerű működés esetén a felhasználóknak haladéktalanul értesítenie kell az Üzemeltetői csoportot, ahol megvizsgálják az eseményt, és hiba esetén elhárítják azt.
- Vírusfertőzés gyanúja esetén az informatikus és/vagy az IT biztonságért felelős munkatárs a fertőzött gépet lezárhatják, annak használatát a hiba elhárításáig felfüggeszthetik.

## 5.6. Hibajavítás, biztonsági frissítések

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



A Szervezet Üzemeltetői csoportja 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 szervezeti egység feladatellátásának hatékonysága, a szóba jöhető következmények szempontjából
- a biztonságkritikus szoftvereket a frissítésük kiadását követő meghatározott időtartamon belül telepíti vagy telepítteti
- beépíti a hibajavítást a konfigurációkezelési folyamatba.

## 6. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM

### 6.1. Rendszer- és kommunikációvédelmi eljárásrend

A Szervezet:

- megfogalmazza, és a szervezetre érvényes követelmények szerint dokumentálja, valamint a szervezeten 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.

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. (B45 Naplófájlok listája).



A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban kell elhelyezni, elkülönítve a belső szervezeti 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, egyéb 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 szervezet engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszközknél.

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

## 7. MELLÉKLETEK

### 7.1. IBSZ 1. számú melléklet - Biztonsági osztályba sorolás

Adatbiztonság szempontjából a Szervezet 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 Informatikai Biztonsági Szabályzatban is.

**A Jászszentandrás Közös Önkormányzati Hivatal besorolása: 3. biztonsági osztály**

**A Jászszentandrás Közös Önkormányzati Hivatal besorolása: 3. biztonsági szint**

A besorolást minimum 2 évente, vagy az elektronikus információs rendszereket érintő változások után felül kell vizsgálni és szükség esetén ismételt el kell végezni.

Jászszentandrás, 2017. november 2.

**Márkus Erika**  
Megbízó - Jegyző

**Vékás Sándor**  
Megbízott, IBF

