**Nagykamarás Község Önkormányzat**

# INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Érvényes: 2017. december hó 12-től

| Készítette: | Jóváhagyta: |
| --- | --- |
| _____ | _____ |
| rendszergazda | jegyző |

T A R T A L O M J E G Y Z É K

**DOKUMENTUM VÁLTOZÁSOK TÖRTÉNETE**

| Verzió | Dátum | Változás leírása | Módosította |
|---|---|---|---|
| 1.0 | 2017. december 12. | 1. verzió | PRO-IT Kft., Németh Attila Péter |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# 1. BEVEZETÉS

## 1.1. A szabályzat célja, terjedelme

A magyar Országgyűlés 2013. április 15-én fogadta el az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt (továbbiakban: Ibtv.)

Az Ibtv. előírja, hogy az önkormányzati szerveknek, ki kell dolgoznia saját információbiztonsági követelményrendszerét. Ezen követelményrendszert jelen Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ vagy Szabályzat) tartalmazza.

Az IBSZ célja a biztonsági követelményrendszer meghatározása a következő tartalommal:

- biztonsági irányelv, mely meghatározza az informatikai infrastruktúra teljes életciklusára (tervezésnél, beszerzésénél, fejlesztésénél, üzemeltetésénél és selejtezésénél) alkalmazandó általános biztonsági elvárásokat;

  biztonsági szabályzat, mely leírja a biztonsági intézkedéseket, azok dokumentálásának és ellenőrzésének feladatait, a végrehajtás felelősét és végrehajtás gyakoriságát vagy idejét;

  végrehajtási eljárásrendek, melyek részletesen leírják a szabályzatban meghatározott feladatok végrehajtásának, ellenőrzésének módját, folyamatát.

Az IBSZ az Ibtv.-ben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről kiadott 77/2013. (XII. 19.) NFM rendelete által meghatározott összes területre kiterjed, ugyanakkor egyes biztonsági témakörökkel kapcsolatban csak az általános elvárásokat fogalmazza meg, míg a részletes szabályozás további dokumentumokban találhatók meg.

## 1.2. A Szabályzat szervezeti hatálya

Jelen dokumentum szervezeti hatálya kiterjed a Hivatal valamennyi fő és részfoglalkozású dolgozójára, illetve az informatikai eljárásokban résztvevő más szervezetek dolgozóira. Az egyes intézkedések tekintetében a következő szervezeti egységekre:

- Jegyző: a személyi biztonság vonatkozásában, az informatikai vagyontárgyak kezelése, a fizikai és környezeti és adminisztratív biztonság tekintetében.
- Informatikai biztonsági felelős: az informatikai rendszerben kezelt adatok biztonsági osztályozása, a szabályzati rend végrehajtása és ellenőrzése vonatkozásában.

A fentieken túlmenően jelen Szabályzat szervezeti hatálya kiterjed még a Hivatallal szerződéses jogviszonyban álló azon természetes és jogi személyekre, akik bármilyen módon kapcsolatba kerülnek a Hivatal informatikai infrastruktúrájával, vagy bármely, az IBSZ hatálya alá tartozó, a megbízható működést vagy információ védelmet érintő eszközzel. Ezen személyek esetében a Szabályzat rendelkezéseit a velük kötött szerződésben és titoktartási nyilatkozatban kell érvényesíteni, melynek felelőse az Informatikai biztonsági felelős.

## 1.3. A Szabályzat tárgyi hatálya

Jelen dokumentum tárgyi hatálya kiterjed a Hivatalban található összes üzemelő, használatban lévő vagy a jövőben bevezetett, alkalmazott informatikai rendszerre, azok környezetét alkotó rendszerelemre teljes életciklusában a tervezéstől, elkészítéstől, a rendszerből történő teljes kivonásáig, vagy megsemmisítésig.

## 1.4. Kiadás dátuma, érvényessége

A Szabályzat a Hivatal Jegyzője által történő jóváhagyás pillanatában lép hatályba, és mindaddig érvényesnek tekintendő, amíg annak egy új változatát a jegyző jóvá nem hagyja.

## 1.5. Kötelező felülvizsgálat rendje

A Szabályzat, illetve mellékletei felülvizsgálatát rendszeresen, de legalább kétévente, illetve minden olyan esetben végre kell hajtani, amikor a Szabályzatban leírtakhoz képest jelentős változás történik. A mindenkori felülvizsgálat végrehajtása az IBSZ-ben meghatározott Informatikai biztonsági felelős feladata.

## 1.6. Figyelembe vett mértékadó dokumentumok

Jelen Szabályzat az alábbi, a módszertani leírásokat, előírásokat is tartalmazó hazai és nemzetközi mértékadó dokumentumokon alapul:

[1] ISO/IEC 27001:2006 informatikai biztonságtechnikai nemzetközi szabvány

[2] Ibtv.

[3] 77/2013 (XII. 19.) NFM rendelet az Ibtv-ben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről

[4]

## 1.7. A dokumentum felépítése

A Szabályzat felépítése a következő:

- Az információbiztonság szervezete
- Informatikai vagyontárgyak kezelése
- Személyi biztonság
- Fizikai és környezeti biztonság
- A kommunikáció és az üzemeltetés irányítása
- Hozzáférés-ellenőrzés
- Információs rendszerek beszerzése, fejlesztése és működtetése
- Informatikai biztonsági események kezelése
- ASP rendszercsatlakozás
- Mellékletek

1. sz. melléklet Biztonsági osztályok és biztonsági szint
2. sz. melléklet Fogalomtár
3. sz. melléklet Adathordozók selejtezési jegyzőkönyve

# 2. AZ INFORMÁCIÓBIZTONSÁG SZERVEZETE

## 2.1. Informatikai biztonsági felelős szerepkörének kiosztása

**Cél:** A biztonsági feladatok ellátására és ellenőrzésére azonosítható szerepkörök álljanak rendelkezésre.

**Szabályok**

***A vezetés elkötelezettsége az információbiztonság ügye iránt***

A Hivatal vezetésének világos iránymutatással, elkötelezettsége kinyilvánításával, az informatikai biztonsággal összefüggő felelősségi körök egyértelmű kijelölésével és elismertetésével aktív módon támogatnia kell az informatikai biztonságot a szervezeten belül.

Az információbiztonság elismertetése a vonatkozó szabályzatok hatályba léptetésével, és az érintettek körében végzett tudatosítás és képzés keretében valósul meg.

***Az információbiztonság koordinálása, felelősségi körök kijelölése***

A Hivatal vezetése jelen Szabályzatban meghatározza, és időszakosan felülvizsgálja az információbiztonsággal összefüggő felelősségi köröket. Az információbiztonsággal kapcsolatos felelősség megoszlik az Informatikai biztonsági felelős, az egyes szervezetek és a felhasználók között.

Az információbiztonsági tevékenység koordinálását az Informatikai biztonsági felelős (IBF) végzi, aki jelenleg a Hivatal Informatikusa (a továbbiakban együttesen: Informatikus/IBF). Az Informatikus/IBF tevékenységét a Hivatal Jegyzője közvetlenül felügyeli. Személyesen felel a biztonsági követelmények megvalósulásáért, és e feladatának ellátása körében nem utasítható.

A információbiztonsági szabályzatokban meghatározott biztonsági előírások végrehajtásáért és betartatásáért a Hivatal egyes szervezeti egységeinek vezetői, vagy az általuk bizonyos részfeladatokra kijelölt munkatársai a felelőseket.

## 2.2. Külső szolgáltatók igénybevétele

**Cél:** Az informatikai feladatok kiszervezése esetén fenntartani az informatikai biztonság szintjét.

**Szabályok**

***Az információbiztonság a szolgáltatási szerződésekben***

A külső szolgáltatók igénybevétele esetén a szolgáltatási megállapodásokban (szerződésekben) kell kikötni a szolgáltatásra érvényes biztonsági követelményeket és szabályozást. Biztosítani kell a feladatért felelős szervezet számára a mérés és ellenőrzés feltételeit.

Az informatikai rendszerek, eszközök bevezetése, üzemeltetése során harmadik felek különféle személyes, illetőleg bizalmas adatokhoz férnek hozzá. Ezen adatok védelméről gondoskodni kell.

A szolgáltatási megállapodásokban ki kell térni a külső szolgáltató titoktartási kötelezettségére a Hivatal rendszereinek üzemeltetésével, fejlesztésével kapcsolatos, illetve a rendszerekben tárolt, feldolgozott adatok, információk vonatkozásában.

***További szabályozás***

Az informatikai célrendszereket érintő biztonsági követelményeket és védelmi intézkedéseket az Üzemeltetési szabályzat részét képező Kockázatkezelési eljárásban kell rögzíteni, míg a külső ügyfelek hozzáférését a hivatali információkhoz, a rendszerekhez, illetve az informatikai infrastruktúrához az Üzemeltetési szabályzatban kell rendezni.

***Felelősség***

Külső szolgáltatók, harmadik felek igénybe vételével az informatikai biztonsággal kapcsolatos felelősség nem hárítható át, az a feladatért felelős szervezet első számú vezetőjét terheli.

Minden harmadik féllel kötött megállapodás esetében elvárásként kell megfogalmazni a jelen Szabályzatban foglaltak betartását. Ennek teljesítése érdekében informatikai tárgyú szerződést a Hivatal kizárólag az Informatikus/IBF jóváhagyásával köthet.

A folyamatban lévő megállapodások (pl. üzemeltetési, karbantartási szerződések) és az új szerződések információbiztonsági, titoktartási vonatkozásait, azok tartalmát és formáját az Informatikus/IBF ellenőrzi, és legalább évenként felülvizsgálja.

# 3. INFORMATIKAI VAGYONTÁRGYAK KEZELÉSE

## 3.1. Felelősség az informatikai vagyontárgyakért

**Cél:** Meg kell határozni, hogy a szervezetben ki és milyen módon viseli a felelősséget az informatikai vagyontárgyakért (materiális és immateriális vagyonelemekre egyaránt).

**Szabályok**

***Az informatikai vagyontárgyak nyilvántartása***

A Hivatal Informatikusa az alábbi informatikai vagyontárgyairól vezet nyilvántartást:

- Információs rendszerek
- felhasználói alkalmazások,
- rendszerszoftverek (operációs rendszerek, adatbázis-kezelők, egyéb szoftverek),
- hardver elemek (szerverek, asztali és hordozható számítógépek, monitorok, nyomtatók, hálózati és kommunikációs infrastruktúra, egyéb hardverek),

Ugyanakkor nem követelmény, hogy az alkatrészszintű adatokról külön nyilvántartás szülessen.

A nyilvántartás eltérő tartalmú a vagyontárgy típusának megfelelően, azonban alapvető elvárás, hogy az adott vagyontárgy a nyilvántartás alapján egyértelműen beazonosítható, jellemzői megállapíthatók legyenek.

A vagyontárgyak nyilvántartása az erre rendszeresített Törzslapon történik. 3. sz. melléklet Az informatikai vagyontárgyakról vezetett nyilvántartást naprakészen kell tartani a vagyontárgy beszerzésétől kezdve egészen annak leselejtezéséig.

## 3.2. Az informatikai rendszerben biztonsági osztályba sorolása

### 3.2.1. Osztályozási elvek kialakítása

**Cél:** Annak érdekében, hogy az Ibtv. hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket be kell sorolni egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából

**Szabályok**

***Osztályozási elvek meghatározása***

Az információs rendszerek biztonsági osztályba sorolását az Ibtv., és a 77/2013. (XII. 19.) NFM rendelet iránymutatásai alapján szükséges elvégezni.

A biztonsági osztályba sorolásnál - az érintett elektronikus információs rendszer vagy az általa kezelt adat bizalmasságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján - 1-től 5-ig számozott fokozatot kell alkalmazni, a számozás emelkedésével párhuzamosan szigorodó védelmi előírásokkal együtt.

A biztonsági osztályba sorolást a szervezet vezetője hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért.

Az elektronikus információs rendszer bizalmasság, sértetlenség és rendelkezésre állás szerinti biztonsági osztálya alapján kell megvalósítani az 77/2013. (XII. 19.) NFM rendeletben előírt védelmi intézkedéseket az információs rendszerek vonatkozásában.

***További szabályozás***

A Hivatal informatikai célrendszereinek kockázatfelmérésének, biztonsági osztályba sorolásának módszertana, a mindenkori Üzemeltetési szabályzatban és mellékleteiben található.

***Felelősség***

Az osztályozási elvek kialakításának és éves gyakoriságú felülvizsgálatának felelőse a Hivatal Informatikus/IBF-e.

A Hivatal információs rendszereinek biztonsági osztály besorolását az 1. számú melléklet tartalmazza.

A Hivatal biztonsági szintje a jelen Szabályzat érvényességi időpontjában a 2. szint.

## 3.2.2. Adatok jelölése és kezelése

**Cél:** A felhasználók az adatokat (elektronikus és papír alapú) biztonsági besorolásának megfelelően kezeljék.

**Szabályok**

***Az adatok osztályba sorolásának jelölése és a kezelésre vonatkozó eljárások***

Összhangban a **3.2.1.** sz. fejezetben meghatározott biztonsági osztályozási rendszerrel, az alábbi eljárások vonatkoznak az adatok (információhordozók) jelölésére és kezelésére.

Az adatok osztályba sorolását az informatikai célrendszerek kockázatkezelési folyamatába illesztve kell végrehajtani, mely a következő lépéseket jelenti:

1. **Kockázatfelmérés végrehajtása.** A kockázatfelmérés során meg kell határozni egy adott informatikai rendszerre, annak teljes élettartamára vonatkozóan a kockázat szintjét, és általa kezelt adatok körét. Ezek alapján, a bizalmasság, sértetlenség és a rendelkezésre állás biztonsági célok figyelembe vételével az informatika célrendszer és az általa kezelt adatok biztonsági osztályba sorolás megtörténhet.
2. **Kockázatok kezelése - informatikai biztonsági cselekvési terv kidolgozása.** Az informatikai célrendszert, illetve az általa kezelt adatok kockázatainak csökkentése során olyan költséghatékony módon megvalósítható biztonsági intézkedéseket kell beépíteni a rendszerbe, melyek megfelelnek a rendszer környezetének és segítik a szervezet feladatainak teljesítését, egyúttal hozzájárulnak a korábban meghatározott kockázatok csökkentéséhez.
3. **Értékelés és felülvizsgálat.** Az értékelés a rendszer biztonsági állapotának pontos feltérképezése a rendszer megvalósítási szakaszának végén, a felülvizsgálat pedig egy időszakos újraértékelés a rendszer üzemeltetési szakaszában.

***További szabályozás***

A Hivatal informatikai célrendszereinek kockázatfelmérésének, biztonsági osztályba sorolásának módszertana, a mindenkori Üzemeltetési szabályzatban és mellékleteiben található.

***Felelősség***

Az Üzemeltetési szabályzat és mellékletei (beleértve az egyes informatikai célrendszerekre és adatai vonatkozó kockázatfelmérést és biztonsági cselekvési tervet) kialakításának és éves gyakoriságú felülvizsgálatának felelőse a Hivatal Informatikus/IBF-e.

# 4. SZEMÉLYI BIZTONSÁG

## 4.1. Feladatok és felelősségi körök meghatározása

**Cél:** A biztonsági intézkedések végrehajtásával kapcsolatos feladatok, felelősségi és hatáskörök legyenek megfelelően rögzítettek.

**Szabályok**

***Munkakörök meghatározása***

Szabályzatokban, a munkakörökre vonatkozó feladat-leírásokban, a munkaköri leírásokban, kell rögzíteni az egyes munkakörökhöz tartozó feladatokat és felelősségi kört, a szükséges informatikai jogosultságokat. Minden munkakörhöz csak a munkához feltétlen szükséges jogosultságokat kell megadni.

***Munkahelyi informatikai környezet kialakítása***

Új munkatársak felvételekor a következő informatikai környezet kialakításáról kell gondoskodni a felelős szervezeti egységeknek:

| Feladat | Felelős |
|---|---|
| Telefonszám | Jegyző |
| Számítógép | Jegyző |
| Hozzáférési jogok beállítása (szerverekhez, alkalmazásokhoz) | Informatikus/IBF (alkalmazások esetében a jogosultságok beállítását az érintett szervezeti egység vezetője kezdeményezi) |
| e-mail cím kiosztása | Informatikus/IBF |
| Informatikai oktatások (általános és felhasználói) | Informatikus/IBF |
| Informatikai biztonsági oktatás | Informatikus/IBF |
| Személyügyi azonosító | Jegyző |
| Titoktartási nyilatkozat | Jegyző |

***Informatikai témájú oktatások***

A Hivatal az alábbi témájú oktatásokat követeli meg, illetve támogatja:

- Általános célú informatikai oktatás: célja az informatikai eszközök (pl. számítógép, billentyűzet, egérhasználat, hálózat), irodai szoftverek (pl. Word, Excel, Intéző, Internet Explorer) alapszintű oktatása.
- Biztonsági oktatás: célja a jelen Szabályzatban, illetve az egyéb szabályzatokban található elvárások megismertetése a munkatársakkal.

- Felhasználó rendszer oktatás: célja a felhasználó által a napi munka során használt alkalmazások (pl. szakigazgatási rendszer, ügyiratkezelő) felhasználói szintű oktatása.
- Szakmai tanfolyamok: célja az informatikai területen dolgozó munkatársak (pl. rendszergazda, üzemeltető, biztonsági felelős) szakmai felkészültségének szinten tartása, fejlesztése.

Az oktatásokon az egyes szervezeti egységek vezetőinek is részt kell venniük. Az oktatásokat követően értékelni kell, hogy

a munkatársak a tanagyagot milyen mértékben sajátították el, illetve

- mennyire találták hasznosnak az oktatást, voltak elégedettek az oktatás színvonalával. Az alkalmazást követően az érintett munkatársaknak az általános célú informatikai oktatáson, a biztonsági oktatáson, a felhasználó rendszer-oktatáson kell részt venniük.

A biztonsági oktatást frissítő jelleggel esetileg (pl. szabályzatok változása, új rendszer bevezetése esetén) is meg kell tartani minden munkatárs számára.

***További szabályozás***

A munkatársak felelősségi köreinek informatikai leképezését a felhasználó jogosultsági rendszere mutatja. Az ezzel kapcsolatos szabályozást a Üzemeltetési szabályzat tartalmazza.

Munka-, tűz- és balesetvédelmi oktatás anyagát a vonatkozó szabályzatok tartalmazzák.

***Felelősség***

Feladatok és felelősségi körök meghatározása, a belépőkkel kapcsolatos feladatok végrehajtásának felelőssége megoszlik a Személyügyi szervező, és az Informatikus/IBF között.

## 4.2. Személyi biztonság az alkalmazás megszűnése, illetve megváltozása esetén

**Cél:** A munkatársak jogállásának megváltozása esetén fenn kell tartani a biztonsági szintet.

**Szabályok**

***Eljárás az alkalmazás megszűnése, illetve megváltozása esetére***

A munkatársak kilépése, tartós távolléte, a munkakör változása esetére az informatikai jogosultságok, eszközök tekintetében a következő eljárás kell alkalmazni:

- Intézkedni kell az érintett munkatárs jogosultságainak visszavonásáról, felfüggesztéséről, vagy megváltoztatásáról.

  A munkatárs kilépése, tartós távolléte esetén a munkatársnak vissza kell szolgáltatni az informatikai vagyontárgyak nyilvántartásában a nevén szereplő vagyontárgyakat. A munkakör megváltozása esetén felül kell vizsgálni, hogy a munkatárs felelősségébe adott vagyontárgyak közül az új munkakör esetében mely vagyontárgyak megtartása indokolt. Egyben a felülvizsgálat alatt ellenőrizni kell a vagyontárgyak meglétét is. A munkatársak kilépéséről, tartós távollétéről, illetve a munkakör változásáról Személyügyi szervező köteles értesíteni az Informatikus/IBF-t.

***További szabályozás***

A felhasználói jogosultságokkal kapcsolatos feladatok az Üzemeltetési szabályzatban, illetve a Felhasználói informatikai biztonsági szabályzatban találhatók.

***Felelősség***

Az alkalmazás megszűnésével, megváltozásával kapcsolatos fenti feladatok végrehajtásának felelőse az Informatikus/IBF.

# 5. FIZIKAI ÉS KÖRNYEZETI BIZTONSÁG

## 5.1. Területek védelme, biztosítása

### 5.1.1. Fizikai biztonsági zónák kialakítása

**Cél:** A védett erőforrások fizikai védelmének kockázatarányos megvalósítása.

**Szabályok**

***Biztonsági zónák***

A szervezet helyiségeinek és információinak védelme, a jogosulatlan, illetéktelen fizikai behatolás, károkozás és zavarkeltés megakadályozása céljából a hivatali helyiségeket informatikai biztonsági szempontból kategóriákba kell sorolni, melyek a következők lehetnek:

- Zárt terület: információ biztonsági szempontból kritikus területek (pl. szerverszoba), melyek különleges fizikai védelmet, szabályozott beléptetést igényelnek.
- Kiemelt terület: információ biztonsági szempontból fontos területek (pl. raktárak, áramellátó helyiségek, hálózati elosztó helyiségek), melyek fizikai védelmet (pl. biztonsági ajtó), szabályozott beléptetést igényelnek.
- Ellenőrzött terület: különleges fizikai védelmet nem igénylő olyan hivatali helyiségek (pl. irodák, folyosók), melyekben idegenek csak ellenőrzött módon tartózkodhatnak.
- Nyilvános terület: az előzőekbe nem sorolt (pl. ügyfélszolgálati tér) hivatali helyiségek.

***Adminisztratív és műszaki védelmi intézkedéseket***

Gondoskodni kell arról is, hogy a helyiségek megfelelően el legyenek választva, az ajtók be legyenek csukva, a legutoljára távozó nyitott irodát nem hagyhat maga után.

Az egyes biztonsági zónák kapcsán a következő adminisztratív és műszaki védelmi intézkedéseket kell kialakítani:

| Kategória | Adminisztratív és védelmi intézkedéseket |
|---|---|
| Zárt terület | • Kártyás beléptető rendszer (ajánlott)<br>• Biztonsági ajtó<br>• Riasztó berendezés<br>• Több szerver számítógép esetén rackszekrény használata |
| Kiemelt terület | • Biztonsági ajtó<br>• Ablak esetén rács, illetve biztonsági fólia |
| Ellenőrzött terület | • Zárható ajtó |
| Nyilvános terület | • Különleges fizikai védelmet nem igényel |

***Helyiségek biztonsági besorolása***

A Hivatal az egyes helységeit a következő biztonsági kategóriákban sorolja be:

| Kategória | Helyiség | Funkció |
|---|---|---|
| Zárt terület | Földszint | Szerverszoba/Informatikus/IBF iroda |
| Ellenőrzött terület | Irodák | |
| Nyilvános terület | Az előzőekbe nem sorolható helyiségek | |

***Felelősség***

Területek védelmével, biztosításával kapcsolatos feladatok végrehajtásáért a hivatalvezető felel.

### 5.1.2. Belépés ellenőrzés

**Cél:** Az erőforrásokhoz való fizikai hozzáférési eljárás ellenőrzése.

**Szabályok**

***Adminisztratív és műszaki védelmi intézkedéseket***

A különböző biztonsági zónák közötti mozgást ellenőrizni kell. A biztonsági zónákhoz meghatározott követelményeknek megfelelő adminisztratív és műszaki eljárásokat kell alkalmazni.

Azokat a területeket, ahol külső személyek is tartózkodhatnak, nyilvános területként kell kezelni, és a hozzáférési pontokon és zónahatárokon az ennek megfelelő védelmet kell kialakítani.

A Hivatal munkatársai a Hivatal területén arcképes igazoló kártyájukat kötelesek viselni.

A Hivatalon belül zárt, kiemelt és ellenőrzött területen idegenek (pl. vendégek, ügyfelek) engedély nélkül nem közlekedhetnek. Ügyfélszolgálati időn kívül a Hivatal teljes területére kiterjed, hogy a belépő idegenek engedély nélkül nem közlekedhetnek.

Az engedélyt a portaszolgálaton keresztül az a munkatárs adhatja meg, akihez az idegen érkezett.

Az idegen személyek, valamint a saját munkatársak zárt területre történő belépéséről az Informatikus/IBF-nek nyilvántartást kell vezetni a következő adatok feljegyzésével:

- a belépő személy neve, munkahelye,
- a belépés ideje, a belépés célja,
  a kísérő személy neve, szervezeti egysége,
- a kilépés ideje.
- Eljárás a belépési rendszerek működtetésére és használatára

A belépési rendszer működtetése a jegyző feladata.

Zárt területre idegennek (pl. karbantartás, takarítás céljából) csak az Informatikus/IBF engedélyével és felügyeletével történhet. A zárt területre történő belépés a kísérő személy beléptető kártyájával lehetséges.

***Zárt és kiemelt területek kulcskezelési rendje***

Zárt és kiemelt területeken található helyiségek, elválasztó ajtók esetében biztosítani kell, hogy a kulcsok központilag legyenek tárolva, és azokat csak az arra illetékesek vehessék fel.

A kulcsok - beleértve a tartalék kulcsokat is - központi tárolásának helye:

- Informatikus/IBF
- Jegyző (tartalék kulcs)

A helyiségeket napközben nyitva és őrizetlenül hagyni nem szabad.

***Felelősség***

A belépés- és mozgásellenőrzéssel kapcsolatos feladatok végrehajtásáért az Informatikus/IBF felel.

## 5.2. Informatikai eszközök védelme

### 5.2.1. Berendezések elhelyezése és védelme

**Cél:** Biztosítani kell a berendezések működőképességét és védelmét az illetéktelen hozzáféréstől.

**Szabályok**

***Berendezések biztonsága***

A berendezéseket úgy kell elhelyezni, illetve védeni, hogy csökkenjen a környezeti fenyegetésekből és veszélyekből eredő kockázat, valamint a jogosulatlan hozzáférés lehetősége. A megfelelő védelem eléréséhez a berendezéseket az alábbi biztonsági kategóriákba kell besorolni:

| Kategória | Berendezések típusai |
|---|---|
| Kiemelt biztonság | • Szerver számítógépek<br>• Menedzselhető hálózati eszköz elemek (router, switch)<br>• Rendszerfelügyeleti eszközök |
| Fokozott biztonság | • Informatikus/IBF által használt személyi számítógépek<br>• Informatikus/IBF által használt személyi számítógép<br>• Különösen érzékeny és érzékeny adatokat tartalmazó személyi számítógépek<br>• Kábelelosztó szekrények |

| Kategória | Berendezések típusai |
|---|---|
| Normál biztonság | • Az előző kategóriákba nem sorolható informatikai berendezések |

***Berendezések elhelyezése***

A berendezéseket a biztonsági kategóriájuk alapján a következő biztonsági zónákba sorolt helyiségekbe kell elhelyezni:

| Kategória | Fizikai biztonsági zónák |
|---|---|
| Kiemelt biztonság | Zárt terület |
| Fokozott biztonság | Kiemelt terület |
| Normál biztonság | Ellenőrzött terület vagy Nyilvános terület |

Az egyes biztonsági zónákkal kapcsolatos védelmi fizikai, elektronikai védelmi intézkedések a jelen Szabályzat egyéb fejezeteiben kerülnek meghatározásra.

A biztonsági zónákon belül a berendezéseket úgy kell elhelyezni, hogy azokhoz karbantartás, hibajavítás miatt a hozzáférhetőség biztosított legyen.

***Felelősség***

Berendezések biztonsági besorolása az Informatikus/IBF feladata.

### 5.2.2. Közműszolgáltatások biztosítása

**Cél:** A berendezések védelme a közműszolgáltatások kiesésével, valamint működési rendellenességeivel szemben.

**Szabályok**

***Védelem áramkimaradás, illetve —ingadozás esetén***

Informatikai biztonsági szempontból a közműszolgáltatások közül az áramkimaradás, illetve ingadozás az egyetlen jelentős kockázatot jelentő fenyegetettség. Ennek megelőzése és kezelése érdekében a következő védelmi intézkedéseket kell alkalmazni az egyes fizikai biztonsági zónák esetében.

| Kategória | Fizikai védelmi intézkedéseket |
|---|---|
| Zárt terület | • Áramkimaradás és túlfeszültség elleni védelem, mely lehetővé teszi az eszközök legalább 20 percig történő működését. |
| Kiemelt terület | • Túlfeszültség ellen védő elosztók a munkatársak számítógépeihez. |
| Ellenőrzött terület | • Túlfeszültség ellen védő elosztókat kell elhelyezni a kritikus alkalmazásokat használó munkatársak számítógépeihez. |
| Nyilvános terület | • Túlfeszültség ellen védő elosztókat kell elhelyezni a kritikus alkalmazásokat használó munkatársak számítógépeihez. |

***Egyéb védelmi intézkedések***

- A hivatali épületek védelme a villámcsapás negatív következményeivel szemben.
- A telephelyek bejáratánál, az áramszolgáltató beállásoknál nehézvédelem kialakításra, míg az épületen belül a kapcsolószekrények elhelyezése (könnyűvédelem).

***Felelősség***

A berendezések védelmének megteremtése a közműszolgáltatások kiesése kapcsán az Informatikus/IBF feladata. A szükséges erőforrások biztosítása a Jegyző feladata.

### 5.2.3. Kábelezés biztonsága

**Cél:** Az informatikai erőforrások által használt kábelek védelme sérülésektől és lehallgatástól.

**Szabályok** ***Védelmi intézkedések***

Az épületeken belül a hálózati vezetékek kábelcsatornában kell vezetni. A kábelek elhelyezésekor, a használt anyagok kiválasztásakor figyelembe kell venni a kiszolgált informatikai erőforrások biztonsági besorolását. A kábeleket a várható fizikai igénybevételnek és a továbbított adatok kritikusságá-

nak megfelelően kell védeni, figyelembe véve az elektromágneses sugárzások be-, illetve kijutása (zavar, illetve információ) elleni védelmet is.

A belső hálózat kívülről történő elérése kizárólag engedélyezett módon, titkosított csatornán (pl. https/SSL, AES) keresztül lehetséges.

A kábelezéssel kapcsolatos megelőzési, javítási és karbantartási feladatokat csak az Informatikus/IBF előzetes engedélyével lehet végrehajtani.

***Felelősség***

A megfelelő kábelbiztonság kialakítása és fenntartása az Informatikus/IBF feladata.

### 5.2.4. Berendezések karbantartása

**Cél:** A berendezések megbízhatóságának biztosítása, a váratlan hibák elhárítására fordítandó erőforrások minimalizálása.

**Szabályok**

***Berendezések beszerzése***

A berendezések megtervezésekor, kiválasztásárakor és a beszerzése lebonyolításakor - összhangban a Hivatal hatályos szabályzataival, és az adott évre vonatkozó költségvetési tervével - a következő szempontokra kell figyelemmel lenni:

- technológiai elvárások (pl. biztonsági funkciók, terhelhetőség, skálázhatóság, kompatibilitás a meglévő infrastruktúrával, várható elavulás)
- funkcionális elvárások (jelenlegi felhasználói igények, jövőbeni növekedési szükségletek)
- installálás, üzembe-helyezés,
- bekerülési költség, elvárt haszon, üzemeltetési költség,
- garanciális, karbantartási és támogatási elvárások.

A szempontokat érvényesíteni kell - közbeszerzés esetén az ajánlati kiírásban és - a szállítóval kötött szerződésben is.

A beszerzések lebonyolításakor törekedni kell az azonos, a piacon magas technikai színvonalat és megbízhatóságot jelentő, ismert gyártótól származó berendezések megvásárlására, mivel ez megkönnyíti az eszközök üzembe-helyezését, karbantartását, és javítását.

Csak olyan berendezéseket szabad megvásárolni, melyek karbantartása - a garanciális idő lejártát követően is - megoldható. A Hivatal az egyes berendezés típusokra (pl. számítógépek, nyomtatók, hálózati elemek) karbantartási szerződést köthet, melyek garantálják, hogy a berendezés esetleges meghibásodása esetén azok javíthatósága biztosítható legyen.

***Berendezések meghibásodása***

A tervszerűen végzett karbantartás ellenére is megtörténhet, hogy a berendezések meghibásodnak. A javítást elsődlegesen az Informatikus/IBF-nek kell végrehajtania.

Amennyiben ez nem lehetséges (pl. idő, alkatrész vagy szakértelem hiányában) úgy

- a javításra - előzetes árajánlat kérést követően - külső cég kerül bevonásra, vagy
- az eszköz selejtezésre kerül (pl. az eszközt már nem lehet, vagy nem éri meg javítani, mert drága vagy elavult, ezért cseréje indokolt).

Amennyiben számítógépről van szó, úgy mindkét esetben gondoskodni kell arról, hogy annak merevlemezén ne maradjon kiolvasható információ.

A berendezések beszerzése, javítása, karbantartása alkalmából történő szállítása megfelelő óvatossággal, lehetőleg gyári védőcsomagolásban, ütés-, rázás-, és beázás mentesen végezendő el.

Amennyiben a berendezés javítását külső cég végezi, úgy a berendezés átadását és visszavételezését is szállítólevéllel, vagy a külső cég által átadott bizonylattal dokumentálni kell.

A berendezéseket a Hivatalból kivinni csak az Informatikus/IBF engedélyével lehet.

A visszavételezéskor, a bizonylat aláírását megelőzően, az Informatikus/IBF-nek a javítás eredményességéről meg kell győződnie.

***Felelősség***

A berendezések karbantartásával kapcsolatos feladatok végrehajtása az Informatikus/IBF feladata.

### 5.2.5. Berendezések biztonságos selejtezése és újrafelhasználása

**Cél:** Az adathordozókon tárolt információk ne kerülhessenek illetéktelen kezekbe.

**Szabályok**

***Selejtezhetőség***

A berendezések, azok elemei (pl. merevlemez) csak akkor selejtezhetők, ha a meghibásodott alkatrész gazdaságosan nem javítható vagy elöregedés, elavulás miatt az alkatrész cseréje szükséges, és azt máshol nem lehet felhasználni. A hibás és az elöregedett alkatrészeket egymástól egyértelműen elkülönítetten kell tárolni.

A Hivatal a leselejtezésre kerülő eszközöket először megpróbálja értékesíteni valamely külső szervezetnek, vagy amennyiben erre nincsen érdeklődés, úgy átadja egy megfelelő jogosítvánnyal rendelkező társaságnak, hogy annak környezetbarát megsemmisítése megtörténhessen.

***Selejtezési és megsemmisítési eljárások***

Selejtezési és megsemmisítési eljárások célja annak biztosítása, hogy a selejtezett eszközökön tárolt információk visszaállítása ne legyen lehetséges.

Ennek megfelelően valamennyi olyan berendezés esetében, amely tárolóeszközt foglal magába, az Informatikus/IBF az érzékeny adatok és engedélyezett szoftverek eltávolítása érdekében a selejtezést megelőzően a tárolóeszközt

- biztonságos módon felülírja (amennyiben lehetséges), illetve
- amennyiben az eszköz megsemmisítésre is kerül, úgy fizikailag használhatatlanná teszi (pl. a merevlemez megfúrásával).

***Selejtezés dokumentálása***

A selejtezésről a selejtezési bizottság jegyzőkönyvet vesz fel, melynek dokumentálása a Leltározási és selejtezési szabályzatban leírtaknak megfelelően történik.

A selejtezés megtörténtét az informatikai vagyontárgyak nyilvántartásában (ld. **3.1.** sz. fejezet) is át kell vezetni.

***További szabályozás***

A selejtezéssel kapcsolatban további információk találhatók a Hivatal Leltározási és Selejtezési szabályzataiban.

***Felelősség***

A berendezések biztonságos selejtezésével és újrafelhasználásával kapcsolatos feladatok végrehajtásának felelőse a jegyző.

# 6. A KOMMUNIKÁCIÓ ÉS AZ ÜZEMELTETÉS IRÁNYÍTÁSA

## 6.1. Üzemeltetési eljárások és felelősségi körök

### 6.1.1. Dokumentált üzemeltetési eljárások

**Cél:** Az üzemeltetési tevékenységek végrehajtásának és az ellenőrzés alapjának biztosítása. **Szabályok**

***Üzemeltetési szabályzat és - eljárások***

Az üzemeltetési feladatok határidőre történő, szabályozott végrehajtása érdekében üzemeltetési szabályzatot és üzemeltetési eljárásokat kell készíteni.

Az üzemeltetési szabályzatokban az üzemeltetéssel kapcsolatos feladatokat és felelősségeket kell meghatározni.

Az üzemeltetési eljárásokban az üzemeltetési feladatok végrehajtási eljárásait, műszaki leírásait kell meghatározni.

***További szabályozás***

Dokumentált üzemeltetési eljárások a Hivatal Üzemeltetési szabályzatában kerülnek rögzítésre.

***Felelősség***

A dokumentált üzemeltetési eljárásokkal kapcsolatos feladatok végrehajtása az Informatikus/IBF feladata.

### 6.1.2. Változáskezelési eljárások

**Cél:** Az informatikai rendszer konfigurációján csak előzetesen engedélyezett változások történhessenek.

**Szabályok**

***Változáskezelési eljárás***

A változások kezelésének szabványos folyamatát, mely az igényfelvetéstől az átadás-átvételig terjed, a változáskezelési eljárás tartalmazza az alábbiak szerint:

- változási igények fogadása, kezelése,
- kockázat elemzése, priorizálás,
- változás dokumentálása és implementálása.

***További szabályozás***

A változáskezelési eljárások a Hivatal Üzemeltetési szabályzatában kerülnek rögzítésre. ***Felelősség***

A változáskezelési eljárásokkal kapcsolatos feladatok végrehajtása az Informatikus/IBF feladata.

## 6.2. Harmadik felek tevékenységének irányítása

### 6.2.1. Szolgáltatásnyújtás

**Cél:** A külső szolgáltatótól igénybe vett szolgáltatások esetén is biztosítani kell a biztonsági követelmények teljesülését.

**Szabályok**

***Szerződéses elemek***

Meg kell határozni azokat a szerződéses elemeket és tevékenységeket, amelyeket érvényesíteni kell a harmadik felekkel kötött szolgáltatási szerződésekben. A szerződéses elemek eltérhetnek attól függően, hogy a szerződés tartalma szerint milyen szolgáltatás teljesítésére szól (alkalmazás bevezetése, karbantartása, vagy berendezés beszerzése, karbantartása). Az alábbi követelményeknek nem csak a szerződésekben, hanem azt megelőzően, az ajánlati kiírásokban is meg kell jelennie.

Az egyes szolgáltató szerződésekben legalább a következő biztonsági, vagy azt érintő követelményekről kell rendelkezni:

| Tevékenység | Biztonsági követelmény és ellenőrzése |
|---|---|
| Alkalmazás bevezetési módszertan | Alkalmazások bevezetéséhez a szállítónak kialakult módszertannal kell rendelkeznie. |
| Adatok átadása | Az üzemi rendszerből származó adatokat csak tesztelési célból és csak anonimizálva lehet átadni a szállítónak. |
| Felhasználói jogok | Szellemi termékek esetében tisztázni kell a szerzői jogok és a védjegyhasználat kérdéskörét. |
| Karbantartás, rendszerkövetés | Egyértelműen meg kell határozni, hogy a karbantartás, rendszerkövetés milyen feladatokat foglal magába a szállító részéről. |
| Berendezések karbantartása, üzemeltetése | Külső szolgáltató által végzett tevékenység esetében rögzíteni kell a szolgáltató rendelkezésre állásának feltételeit, a karbantartással kapcsolatos feladatait. |
| Helyszíni munkavégzés | A szerződésben egyértelműen tisztázni kell, hogy a helyszíni munkavégzés a Hivatal mely szervezeti egységeinél, mely erőforrásainak felhasználásával kik számára engedélyezett. |
| Jótállás, garancia, szavatosság | A szerződésekben rögzíteni kell, hogy a szállító milyen időtartamra és feltételek mellett vállal jótállást, garanciát az általa szállított berendezésekre, szoftverekre, hogyan javítja a felmerülő hibákat. |

| Tevékenység | Biztonsági követelmény és ellenőrzése |
|---|---|
| Titoktartás | Minden bizalmassági kérdésben érintett szereplővel titoktartási nyilatkozatot kell kitölteni, melynek aláírásával felvállalja, hogy a birtokában levő információval nem él vissza (ld. 2.2. sz. fejezet). |

A biztonsági követelményeknek az ajánlatkérésben, a szerződésben való megjelenéséért az Informatikai biztonsági felelős, míg annak ellenőrzéséért a Jegyzői Iroda a felelős.

***Biztonsági követelmények teljesülésének ellenőrzési eljárásai***

A szerződés biztonsági feltételei megvalósulásának, a követelményeknek való megfelelésnek a vizsgálata az Informatikai biztonsági felelős feladata. Ennek során történhet meg a szolgáltató munkavállalóinak helyszíni ellenőrzése, a rendszerek bevezetésének, az adatok átadásának, a berendezések telepítésének és karbantartásának felügyelete.

***Felelősség***

A harmadik felek tevékenységének információbiztonsági vonatkozású irányítása az Informatikus/IBF felelőssége.

### 6.2.2. Harmadik felek szolgáltatásainak figyelemmel kísérése és átvizsgálása

**Cél:** Ellenőrizni kell, hogy a külső féltől igénybe vett szolgáltatások esetén teljesül-e az elvárt szolgáltatási szint.

**Szabályok**

***Szerződéses elemek***

Különböző szabályozások tartalmazzák a szolgáltatási szintek leírásának, érvényesítésének, a teljesítés dokumentálásának, ellenőrzésének és a nem megfelelő teljesítés szankcionálásának eljárásait, melyeket a harmadik féllel kötött szerződésekben is rögzíteni kell.

***Felelősség***

A harmadik felek tevékenységének irányítási felelőse az Informatikus/IBF.

### 6.2.3. Harmadik felek szolgáltatásaival kapcsolatos változások kezelése

**6.2.4. Cél:** Biztosítani kell, hogy a változásokat csak a megfelelő jogosultságokkal lehessen kezdeményezni, és a végrehajtás ellenőrzött és dokumentált körülmények között történjen az igény felvetésétől az átadás-átvételig.

**Szabályok**

***Változáskezelési eljárások***

Különböző szabályozások tartalmazzák a változáskezelési eljárásokat a külső fél által nyújtott szolgáltatásokra, melyek a következőket biztosítják:

- a változások végrehajtása csak a megfelelő jóváhagyás után történjen,
- a végrehajtás során is érvényesüljenek a biztonsági követelmények,
- az átvétel során ellenőrzésre kerüljön a specifikációban/változási kérelemben leírtak teljesülése.

***Felelősség***

A harmadik felek tevékenységének irányítási felelőse az Informatikus/IBF.

## 6.3. Rendszertervezés és elfogadás

### 6.3.1. Kapacitás-menedzsment

**Cél:** A mindenkori erőforrás-igények hatékony kielégítése és a szűk keresztmetszetek kialakulásának elkerülése.

**Szabályok**

***Kapacitás-menedzsment tervezése***

A szervezet informatikai céljait és annak megvalósítását szolgáló akció- és feladattervet az Informatikai Stratégia hivatott tartalmazni. Az Informatikai Stratégiai célkitűzésekkel összhangban, a hivatali és jogszabályi elvárásoknak megfelelően, a rendelkezésre álló pénzügyi források és lehetőségek (pl. pályázatok) alapján kell megtervezni a következő évre vonatkozó informatikai költségvetést. Ennek összeállításához figyelemmel kell lenni az erőforrások (humán, IT alkalmazások és infrastruktúra) kihasználtságára, és annak elemzésével, az Informatikai Stratégiában meghatározott jövőbeli trendek súlyozásával kell megtervezni az erőforrások beszerzését.

***Felelősség***

A kapacitás-menedzsmenttel kapcsolatos felelősség megoszlik az Jegyző (források biztosítása) és az Informatikus/IBF (tervezés) között.

### 6.3.2. Rendszerek elfogadása, átvétele

**Cél:** Biztosítani kell, hogy az átvett rendszerek tegyenek eleget az elvárt minőségi, mennyiségi, biztonsági és funkcionális követelményeknek.

***Felelősség***

A rendszerek elfogadásának, átvételének felelőse az Informatikus/IBF.

## 6.4. Védelem a rosszindulatú és mobil kódok ellen

### 6.4.1. Rosszindulatú kód elleni védelem

**Cél:** Meg kell akadályozni, hogy a szervezet működésében zavart, adatvesztést vagy adatkiszivárgást okozzon bármilyen rosszindulatú kód (vírus, trójai stb.).

**Szabályok**

***Rosszindulatú kód elleni védelem***

Olyan adminisztratív és technikai intézkedéseket kell alkalmazni, amelyek megakadályozzák a rosszindulatú kódokat tartalmazó programok bejutását, alkalmazását.

***Felelősség***

A rosszindulatú kód elleni védelem felelőse az Informatikus/IBF.

### 6.4.2. Mobil kód elleni intézkedések

**Cél:** Meg kell akadályozni, hogy a szervezet működésében zavart, adatvesztést vagy adatkiszivárgást okozzon bármilyen rosszindulatú mobil kód.

**Szabályok**

Biztonságos böngésző beállítások

Le kell tiltani minden olyan kód futtatását, amelyek nem szükségesek a felhasználók munkájához.

***Felelősség***

A mobil kód elleni védelem felelőse az Informatikus/IBF.

## 6.5. Biztonsági mentés

### 6.5.1. Információk biztonsági mentése

**Cél:** Az elviselhetetlen mértékű adatvesztés megakadályozása, és az elvárt időn belüli visszaállítás biztosítása.

**Szabályok**

Az informatikában a legnagyobb értéket a számítógépen tárolt adatok jelentik. Ezek védelmében meghatározó jelentőségű a biztonsági másolatok készítése.

A mentések folyamata:

- A mentéseket naponta, külső adathordozóra kell végrehajtani.
- A mentésből a rendszerek, a szoftverkörnyezet beállításainak, valamit a tárolt adatoknak teljes körűen visszaállíthatónak kell lennie a mentés pillanatának állapotára.
- A szerverek esetében az adatokat legalább 2 példányban kell menteni, és egymástól fizikailag elkülönült helyiségben elzárt, a szerverterem tűzterétől elkülönülő térben, tűzbiztos helyen kell tárolni.
- A szerverek mentését hetente, illetve a hálózati aktív eszközökét a beállítás változtatásakor kell elvégezni.
- A mentett adatokhoz csak az arra jogosultak férhetnek hozzá.

A munkák során létrehozott word és excel és egyéb dokumentumok mentése az azt létrehozó munkatársak *(felhasználók)* feladata.

A személyi anyagok adatállományának mentését a pénzügyi és gazdálkodási ügyintéző havi gyakorisággal végzi el.

A főkönyvi könyvelés adatainak mentését a pénzügyi és gazdálkodási ügyintéző napi gyakorisággal végzi el. *(Automatikusan, NAS)*

A pénztár könyvelés adatainak mentését a pénzügyi és gazdálkodási ügyintéző napi gyakorisággal végzi el. *(Automatikusan, NAS)*

Az egyéb analitikus nyilvántartások adatainak mentését a pénzügyi és gazdálkodási ügyintéző heti gyakorisággal végzi el. *(Automatikusan, NAS)*

A file-szervereken és SQL-szervereken tárolt adatok, illetve adatbázisok mentése naponta történik *(Automatikusan, NAS)*

A levelezések mentését vagy a felhasználó, vagy kérésre a rendszergazda végzi el. Dokumentálni kell, hogy ki és mikor végezte el a mentést.

Az adatállományok file-védelme során gondoskodni kell arról, hogy azok ne károsodjanak.

***Felelősség***

A mentési és visszaállítási eljárások felelőse az Informatikus/IBF.

## 6.6. Hálózatbiztonság kezelése

### 6.6.1. Hálózatok védelme

**Cél:** A hálózatokon továbbított adatok biztonságának és a hálózat rendelkezésre állásának védelme.

**Szabályok**

***Hálózatbiztonsági intézkedések***

A hálózatok biztonsági érdekében a következő intézkedések megvalósítása javasolt:

- tűzfalas védelem (csomag-/alkalmazásszintű),
- vírusvédelmi eszközök,
- tartalomszűrés,
- titkosított adatvédelmi csatornák kialakítása.

A hálózati rendelkezésre állás érdekében a hálózati forgalmat rendszeresen mérni és értékelni kell, és biztosítani, hogy a szükséges sávszélesség kellő biztonsággal rendelkezésre álljon.

***További szabályozás***

A hálózatbiztonsági intézkedések szabályozása a Hivatal hatályos Üzemeltetési szabályzatában található.

***Felelősség***

A hálózatbiztonsági intézkedések végrehajtásának felelőse az Informatikus/IBF.

## 6.7. Adathordozók kezelése 6.7.1. Adathordozók kezelése

**Cél:** Biztosítani kell, hogy az adathordozók, illetve a rajtuk tárolt adatok a telephelyről kikerülve se sérülhessenek, módosulhassanak vagy kerülhessenek illetéktelen kezekbe.

**Szabályok**

***Az adathordozók kezelési szabályai***

Ki kell dolgozni valamennyi adathordozó kezelésének eljárásait, kiemelt figyelmet fordítva a telephelyen kívüli védelemre. A szabályzatnak ki kell terjednie a teljes élettartamra, a nyilvántartásra, a selejtezésre, a frissítésekre, több példány készítésére.

***További szabályozás***

Az adathordozókkal kapcsolatban további kezelési szabályok a **3.1.** sz. fejezetben találhatók. ***Felelősség***

Az adathordozók kezelésével kapcsolatos feladatok végrehajtásának felelőse az Informatikus/IBF.

## 6.7.2. Adathordozók selejtezése

**Cél:** Biztosítani kell, hogy a selejtezett adathordozókon tárolt információk se kerülhessenek illetéktelen kezekbe.

**Szabályok**

***Az adathordozók selejtezési szabályai***

Adathordozónak tekinthetők a következő eszközök: floppy, CD/DVD, egyéb hordozható háttértároló, pl. memóriakártya, USB drive, mobiltelefon.

Az adathordozók a legmagasabb biztonsági besorolásúak; esetükben a rajtuk tárolt adatok miatt selejtezés után sem kerülhetnek ellenőrizetlen körülmények közé, így azokat fizikailag is meg kell semmisíteni.

***Selejtezési és megsemmisítési eljárások***

Selejtezési és megsemmisítési eljárások célja annak biztosítása, hogy a selejtezett eszközökön tárolt információk visszaállítása ne legyen lehetséges.

Ennek megfelelően valamennyi adathordozó esetében az Informatikus/IBF a selejtezés részeként az adathordozót speciális iratmegsemmisítővel fizikailag megsemmisíti, vagy amennyiben az nem lehetséges (pl. USB drive), úgy biztonságos módon felülírja, majd átadja egy megfelelő jogosítvánnyal rendelkező társaságnak, hogy annak környezetbarát megsemmisítése megtörténhessen.

***Adathordozók újrafelhasználása***

Az adathordozókat alkalmazásuk megszűnésekor be kell gyűjteni, és erről átadás-átvételi bizonylatot (Munkalap) kell kitölteni. A még felhasználható, nem sérült adathordozókon olyan felszabadítást kell végezni, amely garantálja a tárolt adatok visszaállíthatatlanságát; ezt legalább - amennyiben lehetséges - véletlen tartalommal való felülírással, majd törléssel és formattálással lehet elérni. Az így felszabadított adathordozókról a korábbi jelöléseket el kell távolítani, és az informatikai vagyontárgyak nyilvántartásában (ld. **3.1.** sz. fejezet) a kiadható adathordozók közé kell ismételten felvenni.

***Selejtezés dokumentálása***

A selejtezés folyamatát dokumentálni kell a későbbi ellenőrizhetőség érdekében. Ennek érdekében a selejtezésről jegyzőkönyvet kell felvenni a következő adatokkal:

- selejtezett adathordozó azonosítója,
- selejtezés oka,
- selejtezést végző személy neve, és beosztása,
- selejtezést jóváhagyó személy neve, és beosztása,
- selejtezett alkatrész tárolási módja (raktár, vagy megsemmisítés).

A selejtezés megtörténtét az informatikai vagyontárgyak nyilvántartásában (ld. **3.1.** sz. fejezet) is át kell vezetni.

Az Adathordozók selejtezési jegyzőkönyv mintája a 4. sz. mellékletben található.

***További szabályozás***

A selejtezéssel kapcsolatban további információk találhatók a Leltározási és selejtezési szabályzatban.

***Felelősség***

Az adathordozók selejtezésével kapcsolatos feladatok végrehajtásának felelőse az Informatikus/IBF.

## 6.7.3. Rendszerdokumentáció védelme

**Cél:** A rendszerdokumentáció rendelkezésre állásának és adatbiztonságának védelme.

**Szabályok**

Az informatikai rendszerek felhasználói leírásai a belső intranet hálózaton, vagy nyomatott formában hozzáférhetők az összes munkatárs számára.

Az informatikai rendszerekkel kapcsolatos további rendszerdokumentációkat (pl. rendszertervek, üzemeltetési dokumentumok) egyetlen könyvtárban, rendszerenként különböző elnevezésű alkönyvtárakban kell tárolni.

Az egyes alkönyvtárakhoz - és így az adott rendszer dokumentációjához - kizárólag az Informatikus/IBF férhet hozzá.

A dokumentációk naprakészen tartásának, a változások átvezetésének felelőse az Informatikus/IBF, melybe bevonhatja a rendszer szállítóját, amennyiben a vele kötött szerződés ezt lehetővé teszi.

A rendszerdokumentáció aktualizálására évente egyszer, vagy a rendszert vagy környezetét érintő jelentősebb változás esetén kell végrehajtani.

***Felelősség***

A rendszerdokumentációk karbantartásának felelőse az Informatikus/IBF.

## 6.8. Ügyfeleknek biztosított szolgáltatások

### 6.8.1. On-line üzenetváltások (tranzakciók)

**Cél:** Biztosítani kell az on-line tranzakciók bizalmasságát, sértetlenségét, és meg kell akadályozni az adatvesztést.

**Szabályok**

***On-line tranzakciók biztonsági követelményei és biztonsági intézkedései***

Az on-line tranzakciókat bonyolító informatikai célrendszerek védelmére vonatkozó követelményeket, és a követelmények teljesítése érdekében végrehajtott technikai és adminisztratív intézkedéseket az informatikai célrendszer biztonsági tervében kell meghatározni.

### 6.8.2. Nyilvánosan hozzáférhető információk

**Cél:** Biztosítani kell a nyilvánosan hozzáférhető információk sértetlenségét.

**Szabályok**

***Nyilvánosan hozzáférhető információk kezelése***

A Hivatal a nyilvánosan hozzáférhető információkat a honlapján (www.nagykamaras.hu) teszi közzé. Ezen túlmenően a 305/2005. (XII. 25.) Korm. rendelet a közérdekű adatok elektronikus közzétételére, az egységes közadatkereső rendszerre, valamint a központi jegyzék adattartalmára, az adatintegrációra vonatkozó részletes szabályokról alapján a közérdekű adatokat átadja a közadatkereső számára is.

A nyilvánosan hozzáférhető információk, beleértve a közérdekű adatokat, sértetlensége érdekében adminisztratív és technikai intézkedéseket kell kidolgozni, melyben ki kell térni az információ változtatásának eljárásrendjére, új információ közzététele előtt követendő eljárásra és egyes információk törlésének eljárásaira is.

Ezen túlmenően a Hivatal honlapja, mint informatikai célrendszer védelme érdekében technikai intézkedéseket kell meghatározni.

## 6.9. Követés (monitoring)

### 6.9.1. Audit naplózás

**Cél:** A felhasználói tevékenység (jogosult és illetéktelen) figyelemmel kísérése, a támadási kísérletek mielőbbi felfedése érdekében biztosítani kell a naplófájlok biztonságát.

**Szabályok**

***Naplófájlok létrehozásának, kezelésének és felhasználásának szabályai***

Az erre felkészített célrendszerek esetében ki kell alakítani az alábbi felhasználói tevékenységek naplózását: be- és kilépések, adatok felvitele, módosítása, törlése, betöltése.

Az erre felkészített célrendszerek esetében - ilyen jellegű biztonsági követelmények esetén - a felhasználói tevékenységek naplózását ki kell terjeszteni az adatlekérések (listák, riportok) naplózására is.

A naplófájlok megtekintését az informatikai célrendszernek magának kell lehetővé tennie.

Új informatikai célrendszer bevezetése esetén a célrendszernek a fenti követelményeknek meg kell felelnie. A felhasználói tevékenységeket operációs rendszer szinten is naplózni kell az esetleges üzemzavarok és támadási kísérletek felfedése érdekében. A naplófájlokat szúrópróba-szerűen ellenőrizni kell. A vizsgálat részben automatizálható, amennyiben a naplófájlok mennyisége ezt indokolja.

***Felelősség***

A naplózási fájlok létrehozásának felelőse az Informatikus/IBF.

### 6.9.2. Rendszerhasználat figyelése

**Cél:** A rendszerek jogosulatlan használatának megakadályozása, és a hibás működés időben történő észlelése.

**Szabályok**

***Monitoring eljárások***

Az erre felkészített célrendszerek esetében - amennyiben az lehetséges - a rendszerhasználat figyeléséhez az adatgyűjtést magának a célrendszernek kell lehetővé tennie.

Új informatikai célrendszer bevezetése esetén a célrendszernek a fenti követelménynek meg kell felelnie. Az operációs rendszer szintű rendszerhasználat figyelése kapcsán az adatgyűjtést, elemzést, és az intézkedést az operációs rendszer biztonsági eszközei által kínált lehetőségek maximális kihasználása mellett automatizálva kell megoldani annak érdekében, hogy a rendellenességek időben feltárásra kerüljenek és kezelhetők legyenek. A beállítások során arra kell törekedni, hogy biztonsági esemény bekövetkezése esetén arról a rendszeradminisztrátor azonnal értesítést kapjon, hogy a szükséges intézkedéseket mielőbb megtehesse.

A biztonsági eseményeket naplózni kell, annak eredményeit legalább negyedévente át kell vizsgálni.

***Felelősség***

A rendszerhasználat figyelésének felelőse az Informatikus/IBF.

### 6.9.2. Időadatok szinkronizálása

**Cél:** Biztosítani kell, hogy a különböző rendszerekben rögzített adatok (tranzakciók, naplóbejegyzések, üzenetek) időadatai a lehető legteljesebb összhangban legyenek.

**Szabályok**

***Az órajelek szinkronizálási rendje***

A szervezeten belül, illetve adott biztonsági tartományban működő valamennyi érintett információ-feldolgozó rendszer órajelét szinkronizálni kell egy közösen megállapított pontos időforráshoz.

***Felelősség***

Az órajelek szinkronizálásáért az Informatikus/IBF felelős.

# 7. HOZZÁFÉRÉS-ELLENŐRZÉS

## 7.1. A hozzáférés-ellenőrzéshez fűződő működési követelmény

### 7.1.1. Hozzáférés-ellenőrzési szabályozás

**Cél:** A dokumentumokhoz, információkhoz, adatokhoz történő hozzáférés ellenőrzése.

**Szabályok**

***Az információ-hozzáférés szabályozása***

Jogosultság és hozzáférés kezelési szabályzat kialakítása, bevezetése, betartatása; a szabályzat periodikus felülvizsgálata és módosítása elengedhetetlen.

Dokumentált hozzáférés-ellenőrzési szabályzatot kell kialakítani és azt a hozzáférésre vonatkozó, működési és biztonsági követelmények alapján időszakosan felül kell vizsgálni. A szabályozás révén csökkenhet az információk kiszivárgásának és az illetéktelen hozzáférések kockázata.

Alapelv, hogy minden felhasználó csak azokhoz az erőforrásokhoz/információkhoz férhessen hozzá, amelyek a munkájához mindenképp szükségesek.

***További szabályozás***

Az információ-hozzáférés szabályozása a Hivatal Üzemeltetési szabályzatában található.

***Felelősség***

A szabályzat elkészítése és időszakos felülvizsgálata az Informatikai biztonsági felelős hatáskörébe tartozik.

### 7.1.2. Felhasználói hozzáférés irányítása

**Cél:** Az erőforrásokhoz és információkhoz való hozzáférési jogok megadásának és megvonásának szabályozása.

**Szabályok**

***A hozzáférési jogok kezelésének eljárásrendje***

Valamennyi információs rendszerhez és szolgáltatáshoz való hozzáférés megadására és visszavonására hivatalos felhasználó regisztrálási és regisztráció megszüntetési eljárást kell alkalmazni. A felhasználók hozzáférési jogait rendszeresen át kell tekinteni, hogy minden felhasználó csakis azokhoz az információkhoz férhessen hozzá, amelyek munkájához aktuálisan szükségesek.

***További szabályozás***

A hozzáférési jogok kezelésének eljárásrendje a Hivatal Üzemeltetési szabályzatában található.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

### 7.1.3. Speciális jogosultságok kezelése

**Cél:** A speciális jogosultságok megszerzésének és alkalmazásának korlátozása.

**Szabályok**

***A speciális jogosultságok kezelésének eljárásrendje***

Az általános összeférhetetlenségi szabályoktól való speciális eltérés kockázati tényező, ezért az ilyen jogosultságok kiadását mindenképp kerülni kell. Amennyiben valamilyen elkerülhetetlen ok miatt mégis létre kell hozni ilyent, akkor azt csak dokumentáltan, s csak a feltétlenül szükséges időtartamra szabad adni.

Az eljárásrend alkalmazásának hatására csökken annak a kockázata, hogy a speciális jogosultságok nem megfelelő menedzselése miatt a rendszer működésében hibák keletkeznek; vagy illetéktelen helyre kerülnek védendő adatok.

***További szabályozás***

A speciális jogosultságok kezelésének eljárásrendje a Hivatal Üzemeltetési szabályzatában található.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

### 7.1.4. Felhasználói jelszavak kezelése, gondozása

**Cél:** A jelszavak kezelésének biztonságos megvalósítása.

**Szabályok**

***A felhasználói jelszókezelés szabályozása***

A jelszavak felhasználói kezelését szabályozni kell, figyelve arra, hogy a felhasználók titokban tartsák, és megfelelő időközönként változtassák jelszavaikat. Emellett biztosítani kell, hogy a jelszavak kiosztásakor, illetve használatakor csakis a tulajdonos szerezzen tudomást a jelszóról.

***További szabályozás***

A felhasználói jelszókezelés szabályozása a Hivatal hatályos Üzemeltetési szabályzatában és a Felhasználói szabályzatában található.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

## 7.2. Felhasználói felelősségek

### 7.2.1. Jelszóhasználat

**Cél:** Megfelelő erősségű jelszavak használata.

**Szabályok**

***A jelszóhasználat szabályozása***

A felhasználók számára olyan használati rendet kell kialakítani, amely biztosítja megfelelő erősségű jelszavak használatát és ezen jelszavak megfelelő gyakoriságú cseréjét.

***További szabályozás***

A felhasználói jelszókezelés szabályozása a Hivatal Üzemeltetési szabályzatában és a Felhasználói szabályzatában található.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

### 7.2.2. Őrizetlenül hagyott felhasználói berendezések kezelése

**Cél:** Az őrizetlenül hagyott berendezéseken való jogosulatlan hozzáférések megelőzése.

**Szabályok**

***Felhasználói informatikai biztonsági követelmények***

A külső felhasználókat a kapcsolati alrendszerek megfelelő kialakításával, a belső felhasználókat (alkalmazottakat) szabályzatokkal kell kötelezni arra, ha őrizetlenül hagyják a berendezéseiket, akkor (akár logikailag, akár fizikailag) zárják le azokat.

A belső felhasználókat (alkalmazottakat) kötelezni kell arra, hogy csak az aktuális munkához szükséges dokumentumokat tartsák az asztalon/képernyőn, és ne hagyják ezeket a dokumentumokat, adatokat felügyelet nélküli hozzáférhető helyen.

***További szabályozás***

A felhasználói viselkedés szabályozása a Hivatal Felhasználói szabályzatában található.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

## 7.3. Hálózati szintű hozzáférés-ellenőrzés

### 7.3.1. Hálózati szolgáltatások használatára vonatkozó szabályzat

**Cél:** A hálózatra telepített szolgáltatások védelme.

**Szabályok**

***A hálózati szolgáltatások használatára vonatkozó szabályozás***

A hálózati szolgáltatások használatát szabályzatban kell rögzíteni, s azt be kell tartatni. A szabályzatnak tartalmazni kell, hogy milyen felhasználói kör milyen hálózati területhez férhet hozzá.

***További szabályozás***

A hálózati szolgáltatások használatára vonatkozó szabályozás a Hivatal Üzemeltetési szabályzatában található.

***Felelősség***

A szabályzat elkészítése és időszakos felülvizsgálata az Informatikus/IBF hatáskörébe tartozik.

### 7.3.2. Felhasználó hitelesítése külső hozzáférés esetén

**Cél:** A távoli felhasználók megbízható hitelesítése.

**Szabályok**

***Külső hozzáférés kezelése***

A külső összeköttetéseket csak a feltétlenül elérni szükséges rendszerekhez szabad engedélyezni, s kriptográfiai védelmi módszereket kell alkalmazni.

***További szabályozás***

A távoli felhasználókra vonatkozó szabályozás a Hivatal hatályos Üzemeltetési szabályzatában található.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

### 7.3.3. Távdiagnosztikai és konfigurációs portok védelme

**Cél:** A távdiagnosztikai és a konfigurációs portok védelmének biztosítása.

**Szabályok**

***A távdiagnosztikai és a konfigurációs portok védelme***

A távdiagnosztikai és a konfigurációs portokhoz való fizikai és logikai hozzáférést ellenőrizni, szabályozni kell. A hozzáféréshez a rendszerben alkalmazott legszigorúbb azonosítási eljárásokat és naplózási rendet kell használni.

***További szabályozás***

A távdiagnosztikai és a konfigurációs portok védelmére vonatkozó szabályozás a Hivatal Üzemeltetési szabályzatában található.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

## 7.4. Operációs rendszer szintű hozzáférés-ellenőrzés

### 7.4.1. Biztonságos bejelentkezési eljárások

**Cél:** Szabályzat az operációs rendszerek hozzáférési eljárásainak beállítására és használatára.

**Szabályok**

***Hozzáférés az operációs rendszerfunkciókhoz***

Az operációs rendszerekbe való bejelentkezési eljárásokat - a jogosulatlan hozzáférés, a szándékos károkozás elkerülése érdekében - szabályozni kell. Fontos a különböző szerepköröknek megfelelő hozzáférési jogosultság meghatározása és az ehhez tartozó jogok beállításának szabályozása (igénylés, engedélyezés, beállítás, visszavonás).

***További szabályozás***

Az operációs rendszer funkciókhoz való hozzáférés szabályozása a Hivatal Üzemeltetési szabályzatában található.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

### 7.4.2. Felhasználó azonosítása és hitelesítése

**Cél:** Az operációs rendszer szintű felhasználók azonosítása és hitelesítése.

**Szabályok**

***A felhasználók azonosításának és hitelesítésének szabályozása***

A felhasználók egyedi azonosítására, hitelesítésére megbízható módszert kell választani, annak használatát szabályzatban kell rögzíteni, használatát szigorúan meg kell követelni. A szabályzatnak ki kell terjednie az azonosítás és hitelesítés teljes életciklusára (igénylés, engedélyezés, beállítás, visszavonás).

Meg kell határozni a biztonságos jelszóra vonatkozó követelményeket, szabályozni kell a jelszavak létrehozására, módosítására, tárolására, használatára, visszavonására vonatkozó eljárásokat. A felhasználók a jelszóhasználattal kapcsolatos feladatait és kötelezettségeit szintén szabályzatba kell foglalni, és rendszeresen ellenőrizni kell annak betartását.

***További szabályozás***

A felhasználók azonosításának és hitelesítésének szabályozása a Hivatal Üzemeltetési szabályzatában található.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

### 7.4.3. Rendszer-segédprogramok használata

**Cél:** Átlátható, ellenőrzött, dokumentált, a biztonságot nem veszélyeztető rendszer- segédprogram használat megvalósítása.

**Szabályok**

***A rendszer-segédprogramok ellenőrzött, biztonságos használata***

A rendszer-segédprogramok használata lehetőségeket teremt nehezen ellenőrizhető manipulációkra, ezért ezek használatát különös figyelemmel kell szabályozni és a szabályzatban foglaltakat ellenőrizni. A fejlesztő eszközökhöz, az adatbázis közvetlen hozzáféréseket lehetővé tevő segédprogramokhoz való hozzáférés csak indokolt esetben engedélyezhető és a tevékenység végén az engedélyt vissza kell vonni, és lehetőleg ki kell zárni az ellenőrizhetetlen származású programok használatát.

***További szabályozás***

A rendszer-segédprogramok használatának szabályozása a Hivatal Üzemeltetési szabályzatában található.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

## 7.5. Alkalmazás és adat-szintű hozzáférés-ellenőrzés

### 7.5.1. Adat-hozzáférés korlátozása

**Cél:** A konkrét alkalmazás egyes funkciói elérésének, használatának korlátozása.

**Szabályok**

***Alkalmazás szintű adat-hozzáférés korlátozása***

Alkalmazás funkciónként, illetve egyes adatkörökre (adatminősítés, biztonsági szint, stb. szerint) vonatkozóan szükséges a hozzáférés szabályozása, a jogosulatlanok kizárása. Fontos az egyes manipulációk, jogosulatlan kísérletek naplózása, a naplóállomány rendszeres értékelése. A funkció, illetve adatkörre vonatkozó korlátozások lehetőségét az alkalmazás fejlesztésének időszakában kell megtervezni és az alkalmazást ennek megfelelően implementálni, mivel ez utólag már nehezen megvalósítható.

***További szabályozás***

Alkalmazás szintű adat-hozzáférés korlátozásával kapcsolatban további szabályozás található a Hivatal Üzemeltetési szabályzatában.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

## 7.6. Mobil számítógép használata és távmunka

### 7.6.1. Mobil számítógép használata és a vele történő kommunikáció

**Cél:** Mobil számítógép biztonságos használatának szabályozása.

**Szabályok**

***Távoli és helyi mobil számítógép használat szabályai***

A mobil számítógépek (notebook, okostelefon, tablet, stb.) biztonságos használatának érdekében szabályozni kell ezen eszközök esetében a hozzáférést, a logikai és fizikai biztonságot, az adatmentések megvalósítását, illetve a biztonságos környezeten kívüli munkavégzés szabályrendszerét.

***További szabályozás***

A biztonságos távoli és helyi mobil számítógép használat szabályozása a Hivatal Felhasználói szabályzatában találhatók.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

### 7.6.2. Távoli elérés

**Cél:** A biztonságos távoli elérés megvalósítása.

**Szabályok**

***Távoli elérés szabályai***

Szabályozni kell, hogy a biztonságos távoli hozzáférés, érdekében milyen tevékenységek és technikai feltételek szükségesek. Távoli hozzáférés csak indokolt esetben engedélyezhető, és a hozzáférés, adatcsere biztonsága érdekében külön eljárásokat kell meghatározni és megvalósítani (OpenVPN).

***További szabályozás***

A távoli elérés szabályozása a Hivatal Felhasználói Informatikai Biztonsági Szabályzatában található.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

# 8. INFORMÁCIÓS RENDSZEREK BESZERZÉSE, FEJLESZTÉSE ÉS MŰKÖDTETÉSE

## 8.1. Információs rendszerek biztonsági követelményei

### 8.1.1. Biztonsági követelmények elemzése és meghatározása

**Cél:** Annak biztosítása, hogy a biztonság az informatikai rendszerek szerves részét képezze.

**Szabályok**

***Biztonsági követelmények meghatározása***

A fejlesztés vagy beszerzés kezdete előtt, az információs rendszerekre vonatkozó biztonsági kockázatokat elemezni kell, ez alapján meg kell határozni a vonatkozó biztonsági intézkedéseket. A biztonsági elvárásokat rögzíteni kell az ajánlatkérési dokumentációban, teljesítésük módját, megfelelőségét pedig értékelési szempontként kell meghatározni.

***Felelősség***

A biztonsági követelmények elemzése és meghatározása a fejlesztés vagy beszerzés előtt az Informatikus/IBF feladata.

## 8.2. Helyes adatfeldolgozás az alkalmazásokban

### 8.2.1. Bemenő adatok érvényesítése

**Cél:** Az informatikai rendszerek helyes működéséhez szükséges bemenő adatok megfelelőségének biztosítása.

**Szabályok**

***Adatbeviteli ellenőrzési eljárások***

Az alkalmazások jogosultsági rendszerét úgy kell beállítani, hogy az adatfelviteli képernyőkhöz csak az illetékes, megfelelő szakértelemmel bíró és a felhasználói oktatásban részesült munkatársak férhessenek hozzá

Az alkalmazások tervezése során annak belső logikáját úgy kell kialakítani, hogy az képes legyen a különböző összefüggések vizsgálatára, tartalmi, és formai ellenőrzésére (pl. ellenőrző számok, adatok határértékei, kötelező adatok), a bemenő adatok érvényesítésére. A konkrét pénzmozgással járó banki terminál használatakor az utalások két személy engedélyével történhetnek (aláíró jelszó).

***Felelősség***

Az adatbeviteli ellenőrzési eljárások kialakításáért az egyes rendszerfejlesztések során az Informatikus/IBF és az érintett szervezeti egység vezetője felelősek.

### 8.2.2. Belső feldolgozás ellenőrzése

**Cél:** A belső feldolgozás során mind a szándékos, mind a véletlen károkozás kockázatának minimálisra csökkentése.

**Szabályok**

***Érvényességi ellenőrzések***

Az alkalmazásokba érvényességi ellenőrzéseket kell beépíteni, hogy észlelni lehessen az információk feldolgozási hibákból vagy akár a szándékos cselekedetekből adódó bármilyen sérülést.

Amennyiben ez nem lehetséges, úgy a fokozott és kiemelt biztonsági osztályba sorolt informatikai célrendszerek esetében időszakosan (pl. év végén), vagy bizonyos munkafázisok végrehajtását követően (pl. rendszerek közötti adatátadások alkalmával) egyezető listákat kell készíteni, melyek alapján a rendszeren belül az adatok konzisztenciája leellenőrizhető.

***Felelősség***

Az alkalmazás szintű érvényességi ellenőrzések megkövetelése a fejlesztés során az Informatikus/IBF, valamint az érintett szervezeti egység vezetője, míg a manuális ellenőrzés végrehajtása az érintett irodák feladata.

### 8.2.3. Üzenetek hitelessége és sértetlensége

**Cél:** Az alkalmazások közötti kommunikáció során a hitelesség és a sértetlenség biztosítása.

**Szabályok**

***Érvényességi ellenőrzések***

Még az egyes alkalmazások beszerzését megelőzően a Hivatalnak meg kell határoznia, hogy az alkalmazások közötti kommunikáció során milyen eszközökkel (például aszimmetrikus kulcsú digitális aláírás, szimmetrikus vagy aszimmetrikus titkosítás, időbélyegek alkalmazásával) lehet biztosítani a sértetlenséget és a hitelességet; illetve hogy ezen óvintézkedés mely üzenettípusok esetén szükséges.

Ezen biztonsági elvárásokat rögzíteni kell az ajánlatkérési dokumentációban, teljesítésük módját, megfelelőségét pedig értékelési szempontként kell meghatározni.

***Felelősség***

A biztonsági követelmények elemzése és meghatározása a fejlesztés vagy beszerzés előtt az Informatikus/IBF feladata.

### 8.2.4. Kimenő adatok ellenőrzése

**Cél:** A kimenő adatok érvényessége, a tárolt információk későbbi feldolgozása helyes és a körülményeknek megfelelő legyen.

**Szabályok**

***Kimenő' adatokat érvényesítése***

Biztosítani kell, hogy mind az automatikus, mind a manuális illesztő felületeken (interfészeken) a megfelelő időben, a megfelelő (szabályozott) struktúrában és adattartalommal jelenjen meg a kimenő információ. Ezt a követelményt a rendszerek megtervezésekor (követelmény-specifikáció) figyelembe kell venni, illetve a felhasználói teszteléskor le kell ellenőrizni.

Ezt követően az üzemi alkalmazásból kimenő adatok (pl. határozat, banki adatok) helyességéért az ügyintéző, illetve az irodavezető felel; ezek ellenőrzése az adatok átadásakor kell, hogy megtörténjen.

Utólagos rendszeres és eseti ellenőrzéseket belső (Belső ellenőr, intézményi ellenőr) és külső (Közigazgatási Hivatal, NAV, Állami Számvevőszék, stb.) szervezetek is végeznek.

***Felelősség***

A kimenő adatokra vonatkozó ellenőrzési eljárások kialakításáért az egyes rendszerfejlesztések során az Informatikus/IBF, valamint az érintett szervezeti egység vezetője felelősek.

## 8.3. Rendszerfájlok biztonsága

### 8.3.1. Üzemelő szoftverek ellenőrzése

**Cél:** Megbízható szoftverek használata.

**Szabályok**

***Megbízható szoftverek használata***

A Hivatal számítógépein, valamint alkalmazások futtatására alkalmas egyéb eszközein (pl. okostelefon, táblagép) kizárólag az Informatikus/IBF által telepített alkalmazások használhatók. Emellett a megbízható szoftverek használata, az információ kiszivárgási veszélyének csökkentése érdekében:

- szabályozni kell a szoftverek telepítésének és üzemeltetésének elvárt folyamatát,
- létre kell hozni a központi, illetve intézményi szoftverkatalógust, s csak az abban szereplő (előzetesen bevizsgált) szoftvereket szabad a számítógépekre telepíteni (ld. **3.1.** sz. fejezet törzslap), biztosítani kell, hogy a fejlesztők és karbantartók csak azokhoz a rendszerekhez férjenek hozzá, amelyekre munkájukhoz feltétlenül szükségük van.

***További szabályozás***

Megbízható szoftverek használatával kapcsolatban további szabályozás található a Hivatal Üzemeltetési szabályzatában és Felhasználói szabályzatában.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

### 8.3.2. Programok forráskódjához való hozzáférés ellenőrzése

**Cél:** A programok forráskódjához való hozzáférés szabályozása.

Szabályok

***A programok forráskódjához való hozzáférés korlátozása***

A programok forráskódjához való hozzáférést korlátozni kell.

A belső fejlesztések esetében a forráskód a fejlesztés ideje alatt a Fejlesztő gépén található, majd annak lezárulta után a szerveren egy külön könyvtárban, annak dokumentációjával együtt archiválásra kerül. A könyvtárhoz olvasási/írási joggal a rendszer fejlesztője, valamint az Informatikus/IBF férhet hozzá. A forráskódhoz való hozzáférést naplózni szükséges.

Külső fejlesztések esetében a forráskód a fejlesztő cég tulajdona marad, így azt az Hivatal nem kapja meg, ahhoz hozzáférése nincs. Ettől eltérő esetben a forráskóddal kapcsolatos eljárás megegyezik a belső fejlesztéseknél rögzített eljárással, azzal, hogy olvasási joggal csak az Informatikus/IBF rendelkezhet.

***További szabályozás***

A forráskóddal kapcsolatban további szabályozás található a Hivatal hatályos Üzemeltetési szabályzatában.

***Felelősség***

A forráskódok elhelyezésének felelőse az Informatikus/IBF.

## 8.4. Biztonság a fejlesztési és támogató folyamatokban

### 8.4.1. Változás-kezelés szabályozási eljárásai

**Cél:** A változtatások megvalósításának ellenőrzés alatt tartása. **Szabályok**

***A változás-kezelés szabályozása***

A változtatások végrehajtására változás-kezelési eljárásokat kell bevezetni, kidolgozni és betartatni. Biztosítani kell, hogy a fejlesztők és karbantartók csak azokhoz a rendszerekhez férjenek hozzá, amelyekre munkájukhoz feltétlenül szükségük van.

Az új rendszerek bevezetését projektszerű keretek között kell lebonyolítani, ahol a bevezetéssel kapcsolatos feladatok (specifikálás, dokumentálás, tesztelés, stb.) a projekt indításakor rögzítésre kerülnek.

A meglévő rendszerek változás-kezelésével kapcsolatban a karbantartási szerződésekben kell rögzíteni a vonatkozó előírásokat.

***További szabályozás***

A változás-kezelés szabályozása a Hivatal hatályos Üzemeltetési szabályzatában található. ***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

### 8.4.2. Alkalmazások műszaki átvizsgálása az üzemelő rendszerek megváltoztatását követően

**Cél:** A változtatás ne okozzon működési zavart a szervezetben és biztonságában. **Szabályok**

***Eljárás használatban lévő rendszerek változásakor***

A használatban levő rendszerek megváltozásakor meg kell vizsgálni, hogy (főleg a működés szempontjából kritikus) alkalmazások működésére az adott változtatás nincs-e káros hatással. Ennek érdekében meg kell követelni a sikeres vállalkozói tesztelés igazolását, illetve - lehetőség szerint - a Hivatalnak is el kell végeznie a felhasználói tesztelést.

***További szabályozás***

A rendszerek változáskezelésének szabályozása, beleértve a rendszerek tesztelését is, a Hivatal hatályos Üzemeltetési szabályzatában található.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF, illetve az érintett rendszert használó szervezeti egységek hatáskörébe tartozik.

### 8.4.3. Szoftvercsomagok változásának korlátozása

**Cél:** A szoftvercsomagok módosításának visszaszorítása a feltétlen szükséges esetekre.

**Szabályok**

***Szoftvercsomagok változás-kezelése***

A szoftvercsomagok (ideértve pl. az operációs rendszereket, adatbázis kezelőket, irodai szoftvereket, üzleti, hivatali alkalmazásokat) módosítását vissza kell szorítani, valamennyi változtatás szükségességét, indokoltságát ellenőrizni kell. A szoftvercsomagok esetén csak a szükséges változásokat (pl. hibajavítás, jogszabályi előírások) kell telepíteni, és azok hatását legalább a kritikus rendszerek esetében ellenőrizni kell.

Változtatás esetén az eredeti verziót meg kell őrizni, s a fejlesztést, változtatást egy másolaton kell végezni. Az új verziót alapos tesztelésnek kell alávetni, éles bevezetése csak ez után lehetséges.

***További szabályozás***

A rendszerek változáskezelésének szabályozása a Hivatal hatályos Üzemeltetési szabályzatában található.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

### 8.4.4. Veszélyes (forrás) kódok kiszűrése

**Cél:** Meg kell előzni az információk kiszivárgását.

**Szabályok**

***Veszélyes (forrás) kódok kiszűrése***

A Hivatal számítógépein, valamint alkalmazások futtatására alkalmas egyéb eszközein (pl. okostelefon, tablet) kizárólag az Informatikus/IBF által telepített alkalmazások, forráskódok használhatók.

Az információk kiszivárgásának elkerülése érdekében az Informatikus/IBF-nek minden rendelkezésre álló forráskódot le kell vizsgálni/vizsgáltatni használat előtt. Csak tiszta forrásból szabad programokat beszerezni. Csak ezen, vizsgálatok után lehet bármely programot a végleges rendszerbe engedni.

***További szabályozás***

Veszélyes (forrás) kódok kiszűrésével kapcsolatban további szabályozás található a Hivatal Üzemeltetési szabályzatában és Felhasználói szabályzatában.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

## 8.5. Műszaki sebezhetőség kezelése

### 8.5.1. A műszaki sebezhetőségek ellenőrzése

**Cél:** A műszaki sebezhetőség minimális szinten tartása.

**Szabályok**

***Külső szoftverfejlesztés ellenőrzése***

Fel kell mérni az informatikai célrendszerek sebezhető pontjait, s az ezekből fakadó kockázatot meg kell szüntetni (illetve minimalizálni a kockázattal arányosan) megfelelő védelmi intézkedések meghozásával.

***További szabályozás***

A Hivatal informatikai célrendszereinek kockázatfelmérésének, biztonsági osztályba sorolásának módszertana, illetve egyes informatikai célrendszerek besorolása, a védelmi intézkedése meghatározása a mindenkori Üzemeltetési szabályzatban és mellékleteiben található.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

# 9. INFORMATIKAI BIZTONSÁGI ESEMÉNYEK KEZELÉSE

## 9.1. Informatikai biztonsági események és sérülékenységek jelentése

**Cél:** A biztonsági sérülékenységek és események ismertek legyenek, azokra megfelelő választ adjon a szervezet.

**Szabályok**

***Biztonsági események osztályozása***

Biztonsági eseménynek minősül az informatikai rendszer védelmi állapotában beállt illetéktelen változás, melynek hatására az informatikai rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.

Biztonsági események például a vírus-, hacker-, spamtámadás, betörés, lopás, áramszünet, vagy a hozzáférés megsértése.

***Biztonsági események osztályozása***

Az informatikai erőforrások rendelkezésre állásának megszakadása alapján a biztonsági események a következő kategóriákba sorolhatók:

**I. Kategória:** az informatikai erőforrások az érintett központban nem állnak rendelkezésre, az ottani informatikai rendszer működése megszakad.

Ezt okozhatják például a tűz és a víz okozta katasztrófák. Jellegüknél fogva ezek nagy pusztításokat jelentenek a számítástechnikai eszközökben és/vagy a kiszolgáló infrastruktúrában. A helyreállítás időigényes és költséges.

**II. Kategória:** az érintett központban egyes erőforrások nem állnak rendelkezésre, és az ottani informatikai rendszer működése megszakad.

Ide tartozik pl. az energiaellátás kiesése. Jellegénél fogva a sérülés lokalizált, a helyreállítás kevésbé költséges és időigényes, mint az I. Kategóriába sorolt biztonsági események esetében.

A II. Kategóriát az igényeknek és a helyi adottságoknak megfelelően két alkategóriára bontjuk:

**II/a Kategória:** emberi vagy eszköz erőforrások megsemmisülése, illetve ezek olyan, hosszabb idejű üzem-, munkaképtelensége (kiesése), amely jelentős problémát okoz az informatikai rendszer működésében azáltal, hogy küldetéskritikus vagy lényeges rendszert érint.

**II/b Kategória:** emberi vagy eszköz erőforrások nem semmisülnek meg és hosszabb- rövidebb idejű üzem-, munkaképtelensége (kiesése) nem okoz jelentős problémát az informatikai rendszer működésében azáltal, hogy nem küldetéskritikus vagy lényeges rendszert érint.

**III. Kategória:** az érintett központban csak erőforráselem(ek) sérül(nek) meg, de az informatikai rendszer működése folyamatos.

A III. Kategória veszélyforrásai az Üzemeltetési szabályzat tárgykörébe esnek. A veszélyforrások képezte fenyegetés bekövetkezése az Üzemeltetési szabályzatban és mellékletében tárgyalt védelmi intézkedések alkalmazásával előzhetők meg, illetve bekövetkezés esetén ugyancsak ezen védelmi intézkedések alkalmasak a károk mértékének csökkentésére.

Informatikai katasztrófának minősülnek az I. és Il/a Kategóriába sorolható események. Informatikai veszélyhelyzetnek minősülnek a II/b Kategóriába sorolható események. Nem minősülnek katasztrófának a III. Kategóriába sorolt események.

***Biztonsági események jelentése***

A biztonsági eseményeket az észlelő (pl. felhasználó, rendszerüzemeltető) köteles bejelenteni az Informatikus/IBF-nek.

Az Informatikus/IBF haladéktalanul elvégzi a biztonsági esemény kategorizálását, majd I. vagy Il-es kategóriájú esetben intézkedéseket foganatosít a Katasztrófa elhárítási tervben foglaltaknak megfelelően.

***Felelősség***

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikus/IBF feladata.

## 9.2. Informatikai biztonsági események kezelése

**Cél:** Az informatikai biztonsági események gyors, hatékony kezelése.

**Szabályok**

***Biztonsági események kezelése***

A bejelentett biztonsági eseményekkel kapcsolatban az Informatikus a szükséges lépéseket gyorsan és hatékonyan köteles megtenni.

Az I. és Il/a. kategóriába sorolt biztonsági események esetén a Katasztrófa elhárítási tervben található releváns akcióterv szerint kell eljárni.

A II/b. és a III. kategóriába sorolt biztonsági események esetén azok kezelésére az Üzemeltetési szabályzatban leírtak az irányadók.

***Biztonsági események nyilvántartása és értékelése***

A feltárt és dokumentált eseményeket gyűjteni és rendszeresen értékelni kell. Ennek során az események okozta hibákat analizálva meg kell határozni a hibák okát, az események kezeléséhez bizonyítékokat kell gyűjteni, valamint a megtett intézkedéseket is dokumentálni kell annak érdekében, hogy később előforduló hasonló eseményeket már a kialakított módon lehessen kezelni vagy megelőzni.

***További szabályozás***

A biztonsági események kezelésével kapcsolatos eljárásrendet a Működés folytonosság és Katasztrófa elhárítási terv, valamint az Üzemeltetési szabályzat tartalmazzák.

***Felelősség***

A biztonsági események nyilvántartása, az elhárításban való részvétel, az események értékelése és javaslatok kidolgozása az Informatikus/IBF feladata.

## 9.3. Informatikai biztonsági problémakezelési eljárás kialakítása

**Cél:** Az informatikai biztonsági problémák megelőzése, illetve hatékony védekezés kialakítása.

**Szabályok**

***Probléma-kezelési eljárás kialakítása***

Az informatikai biztonsági problémák megállapítására és kezelésére vonatkozó eljárást, valamint a biztonsági eseményekkel kapcsolatban nyilvántartást az előző alfejezetek tartalmazzák.

A biztonsági események értékelését és a problémák megelőzését, detektálását, javítását szolgáló javaslatok megtételét az Informatikus/IBF köteles megtenni.

A működés-folytonossági akciótervet érintő biztonsági esemény esetén az értékelést a Működés folytonosság és Katasztrófa elhárítási terv alapján kell végrehajtani.

Ezen túlmenően az értékelés során Informatikus/IBF -nek el kell végeznie az érintett szabályzatok (pl. Katasztrófa elhárítási terv, Üzemeltetési szabályzat) felülvizsgálatát és szükség szerinti aktualizálását.

A problémák ellen védelmi intézkedéseket kell hozni, az általuk képviselt kockázatok arányában; ezt az alapelvet a problémák megelőzését, detektálását, javítását szolgáló javaslatok megtételekor szem előtt kell tartani.

***További szabályozás***

A biztonsági események kezelésével kapcsolatos eljárásrendet a Működés folytonosság és Katasztrófa elhárítási terv, valamint az Üzemeltetési szabályzat tartalmazzák.

***Felelősség***

A biztonsági események nyilvántartása, az elhárításban való részvétel, az események értékelése és javaslatok kidolgozása az Informatikus/IBF feladata.

# 10. MŰKÖDÉS FOLYTONOSSÁGÁNAK IRÁNYÍTÁSA

## 10.1. Az informatikai működés folyamatosságának biztosítása

**Cél:** Az informatikai működés folyamatosságának biztosítása. **Szabályok**

***A működés folytonosságának irányítása***

Eljárásokat kell kidolgozni és felelősöket kell megnevezni az informatikai működés folytonosság biztosítására, illetve ennek irányításának megszervezését kell elkészíteni. Dokumentumokban kell meghatározni, melyek a:

- kritikus informatikai szolgáltatások
- mekkora lehet az informatikai szolgáltatások megengedett kisesési ideje
- melyek a minimális szolgáltatási szintek
- melyek az átmeneti eljárások
- hogyan történik az informatikai szolgáltatások visszaállítása

Meg kell határozni azokat az informatikai, vagy más technikai infrastruktúrákat és szolgáltatásokat, amelyeknek működniük kell lokális események vagy katasztrófák esetén is, hogy informatikai támogatást lehessen nyújtani a bekövetkezett káresemények elhárításához. Ki kell alakítani a megfelelő redundáns tartalék rendszereket és szabályozni kell ezek működtetését és használatukat, valamint rendszeresen felül kell vizsgálni azok működőképességét.

***További szabályozás***

A működés folytonosság irányítására vonatkozó eljárásrendet a Működés folytonosság és Katasztrófa elhárítási terv, és annak mellékletei tartalmazzák.

***Felelősség***

A működés folytonosság irányítására, az abban való részvétel, az események értékelése és javaslatok kidolgozása az Informatikus/IBF feladata.

## 10.2. Informatikai katasztrófa-elhárítási terv

**Cél:** A kritikus informatikai erőforrások működésének visszaállítása

**Szabályok**

***Informatikai katasztrófa-elhárítási terv***

Az informatikai működés során sérülhet az informatikai erőforrás katasztrófa jellegű kiesése esetén. Ennek kezelésére katasztrófa-elhárítási tervet kell készíteni, mely kiterjed:

- a kritikus informatikai erőforrások azonosítására,
- az elviselhető kiesési időablak meghatározására
- az erőforrások pótlására /visszaállítására történő eljárások kialakítására az időablakon belül a felkészülés, a válasz és a visszaállítás feladatainak meghatározására, felelősök hozzárendelésére

Az eljárásokat tesztelni kell, és a dokumentumot évente, illetve a releváns változások alkalmával felül kell vizsgálni.

***További szabályozás***

A Működés folytonosság és Katasztrófa elhárítási terv és a hivatali akciótervek vonatkoznak az informatikai katasztrófa elhárításra.

***Felelősség***

Az informatikai katasztrófa elhárítás irányítása, az abban való részvétel, az események értékelése és javaslatok kidolgozása az Informatikus/IBF feladata.

# 11. KÖVETELMÉNYEKNEK VALÓ MEGFELELÉS

## 11.1. Jogi követelményeknek való megfelelés

**Cél:** Jogszerű informatikai működés és szolgáltatások **Szabályok**

***A jogszabályoknak megfelelő eljárások.***

Az informatikai működés során fenn kell tartani a jogszabályi megfelelőséget. Ennek érdekében be kell tartani a következő szabályokat:

- Az informatikai működésre hatással lévő jogszabályokat azonosítani kell.
- Az adott informatikai tevékenységre vonatkozó jogszabályok listáját az egyes szabályzatokban kell rögzíteni.
- A jogszabályoknak való megfelelés biztosítása és az időszakos (évenkénti) felülvizsgálat a Jegyző feladata.

***További szabályozás***

A jogszabályi előírásokban foglalt előírások, valamint az azokban meghatározott felülvizsgálati periódusok végrehajtása.

***Felelősség***

A jogi követelményeknek való megfelelés a Jegyző felelőssége.

## 11.2. Biztonsági szabályzatnak és szabványoknak való megfelelés és műszaki megfelelőség

**Cél:** Az informatikai működés megfelelőségének biztosítása érdekében a szabványokat is figyelembe vevő szabályzatok készítése

**Szabályok**

***Szabályzatok felülvizsgálati eljárása***

Az IBSZ és a további informatikai szabályzatok felülvizsgálatára, a szabványoknak való megfelelés ellenőrzésére évente egy alkalommal kell sort keríteni. Emellett szükséges a szabályzatok felülvizsgálata minden olyan esetben, amikor a szabályzatban leírtakhoz képest jelentős változás történik.

Ezek során ellenőrizni kell a biztonsági eljárások tartalmát és működését, figyelemmel kell lenni a szabványok követésére és a változások nyomán végrehajtandó teendőkre.

***Felelősség***

Biztonsági szabályzatnak és szabványoknak való megfelelés és műszaki megfelelőség ellenőrzése, értékelése és javaslatok kidolgozása az Informatikus/IBF feladata.

## 11.3. Auditálási szempontok

**Cél:** Biztosítani kell, hogy a védelmi intézkedések a szabályzatokban leírtak szerint megvalósuljanak

**Szabályok**

***A védelmi intézkedések rendszeres, módszeres felülvizsgálata, javító intézkedések.***

A védelmi intézkedések felülvizsgálatát az Üzemeltetési szabályzatban leírt módon és ütemezésben kell végrehajtani.

A kockázatok, fenyegetettségek kezelésére - a jogszabályi előírásoknak megfelelően - a Hivatalnak az informatikai célrendszerek informatikai biztonsági kockázatait legalább kétévente fel kell mérnie, ennek során javasolt külső, független szakértő bevonása az ellenőrzésbe.

***Felelősség***

Az auditálási szempontok meghatározása, az abban való részvétel, az események értékelése és javaslatok kidolgozása az Informatikus/IBF feladata.

# 12. ASP RENDSZERCSATLAKOZÁS

### 12.1.Az informatikai eszközök környezete, azok védelme

### 12.2. A szerver (szoba)

- a szervert a legbiztonságosabb, legvédettebb területre kell telepíteni,
- váratlan áramkimaradás esetén a szerver(eke)t intelligens UPS–sel kell ellátni (szünetmentes tápegység), mellyel az áramkimaradás folyamatosságát biztosítani lehet. (N+1 redundancia biztosítása, ha lehetséges)

### 12.3. Egyéb vagyonvédelmi előírások

- a szerver (szoba) helyiségeit biztonsági zárakkal kell felszerelni,
- csak az illetékes dolgozók tartózkodhatnak a gépteremben,
- munkaidőn túl a szerverhelyiségben csak engedéllyel lehet dolgozni,
- a számítógép monitorát úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
- az informatikai eszközöket csak a kijelölt dolgozók használhatják,
- az informatikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

### 12.4. A Hálózati központ kialakítása

- Fali rack szekrény
    - Földelő készlet a szekrényhez
    - Leszedhető oldallapok
    - Üvegezett (esetleg plexi), kilincses első ajtó
    - Szellőztetés perforációval biztosítva
- 1U Patch panel keline 24port gigabit
- 1U Kábelrendező
- 1U Easy webmanagement Switch
    - port-security
    - IEEE 802.1D Spanning Tree Protocol
    - 802.1x alapú linkvédelmi eljárás
    - MDIX
    - Multicast VLAN Registration
    - IPV4 / IPV6
    - SNMP v1, v2c, and v3.
- 2U 1000VA-es UPS
    - Online kettős konverziójú, 230 V 1/1 fázisú, 900 W teljesítményű

- VFI-topológia (online kettős konverzió)VFI SS 111 szerinti első osztályú besorolás
- Áthidalási idő > 5perc
- Auto reboot (lemerülés utáni visszakapcsolás)
- Hot-swap rendszerű akkumulátorcsere lehetősége elölről
- Grafikus kijelző (LCD, javaslat legalább 128x64 képpont felbontású)
- RS232 és USB keresztüli kommunikáció

- Router

**12.5 Passzív LAN hálózat**

- Moduláris, RJ45-ös portonként bővíthető 24 portos UTP patch panel
- Fésűs panel
- Moduláris,1x RJ45-ös UTP végponti csatlakozót tartalmazó szerelvény
- Cat5e RJ45-ös UTP modul
- 5m-es Cat5e UTP patch kábel
- Cat5e halogén mentes UTP fali kábel
    - 4x2xAWG24 réz kábel, Kategória 5E, 350 MHz, lehetővé teszi az összes nagysebességű protokoll átvitelét, beleértve az 1000BASE-T protokollt is.
    - Az alábbi szabványoknak felel meg:
        - ISO/IEC 11801 ed. 2.2
        - IEC 61156-5 2nd Ed
        - EN 50173-1
        - EN 50288-3-1
        - EIA/TIA 568-C.2

# 13. Mellékletek

## 13.1. 1. sz. melléklet: Biztonsági osztályok, és biztonsági szint

A Hivatal alapbiztonsági fokozatba tartozik, általános informatikai feldolgozást végez.

| **Adminisztratív védelmi intézkedések szintje** | **Fizikai védelmi intézkedések szint-je** | **Logikai védelmi intézkedések szintje** | | |
|---|---|---|---|---|
| 3 | 3 | *Bizalmasság* | *Sértetlenség* | *Rendelkezésre állás* |
| | | 3 | 3 | 3 |

| **A rendszer biztonsági osztálya** | | |
|---|---|---|
| *Bizalmasság* | *Sértetlenség* | *Rendelkezésre állás* |
| 3 | 3 | 3 |

## 13.2. 2. sz. melléklet: Fogalomtár

Jelen szabályzat fogalom meghatározásai az Ibtv. 1.§-ban megfogalmazottak szerint értendőek.

| | |
|---|---|
| **Adatbázis** | Tárolt adatok összessége. |
| **Adatgazda** | Az adat felett rendelkező szervezet. |
| **Adatkapcsolat** | Olyan interakció, amelynek keretében adatok átadása és átvétele történik nyilvántartók között. |
| **Adatvédelem** | Az adatkezelés során érintett személyek, azok személyiségi jogainak, adataival való önrendelkezési jogának védelme érdekében megvalósítandó/megvalósított, az adatkezelés módjára, formájára, tartalmára vonatkozó szabályozások és eljárások. |
| **ASP** | Application Service Providing, alkalmazásszolgáltatás |
| **Elektronikus irat** | Olyan elektronikus dokumentum, melynek funkciója szöveg betűkkel való közlése, és a szövegen kívül az olvasó számára érzékelhetően kizárólag olyan egyéb adatokat foglal magába, melyek a szöveggel szorosan összefüggenek, annak azonosítását (pl. fejléc), illetve könnyebb megértését (pl. ábra) szolgálják. |
| **Elektronikus ügyintézés** | Azok az eljárási cselekmények, amelyek során az ügyfél vagy az ügyintézést biztosító szerv elektronikus nyilatkozatot tesz, vagy az ügyintézést biztosító szerv az ügyfél vagy más ügyintézést biztosító szerv nem elektronikus nyilatkozatát elektronikus nyilatkozattá alakítja át és azt az eljárás során felhasználja. |
| **Hardver** | Fizikai eszközök rendszere. Hardver alatt a számítógép fizikailag megfogható részeinek összességét értjük. |
| **Informatikai biztonság** | Az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. |
| **Internet** | Technikai értelemben az a hálózattípus, amely a TCP/IP protokollt használja és mára kvázi standarddá vált. Az internet kifejezés nemzetközileg elterjedt szó, az angol eredetű internetwork szóból ered, ami magyarul leginkább hálózatok hálózata'-ként adható vissza, szó szerint hálózatok közötti-t jelent. Az internet az egész világot körülölelő számítógép-hálózat, hatalmas rendszer, amely kisebb számítógép-hálózatokat fog össze. Ennek eredménye egyfajta kibertér, amely a valódi világ mellett alternatív teret biztosít. Az internet a számítógépek összekötéséből jött létre, hogy az egymástól teljesen különböző hálózatok egymással átlátszó módon tudjanak elektronikus leveleket cserélni, állományokat továbbítani. |
| **Jogosultságellenőrzés** | Rendszerekhez történő hozzáférés validálása. |
| **Nyilvántartás** | A feladatok ellátásához szükséges információk feltárható módon való rendszerezése és rögzítése. |
| **Személyes adat** | Meghatározott természetes személlyel (az érintettel) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. |
| **Szoftver** | Programok, eljárások. A szoftver alatt a legszűkebb értelemben elektronikus adatfeldolgozó berendezések (például számítógépek) memóriájában elhelyezkedő, azokat működtető programokat értünk. |

## 13.4. 4. sz. melléklet: Adathordozók selejtezési jegyzőkönyve

Adathordozó selejtezési jegyzőkönyve

A Selejtezési Bizottság igazolja a kijelölt adathordozó selejtezésének/megsemmisítésének végrehajtását.

selejtezett adathordozó azonosítója: selejtezés oka:

selejtezést végző személy neve, és beosztása:

selejtezést jóváhagyó személy neve, és beosztása:

selejtezett alkatrész tárolási módja (raktár, vagy megsemmisítés):

Nagykamarás, _____év _____hónap _____nap

_____

Selejtezési Bizottság vezetője