

iAgency Szolgáltató Korlátolt Felelősségű Társaság

info@iagency.hu

Elfogadva: 2019.

Utolsó módosítás: 2019.
Hatályba lép: 2019.

INFORMÁCIÓ BIZTONSÁGI SZABÁLYZAT

Budapest Főváros XVI. kerületi Önkormányzat Gazdasági Működtető- Ellátó Szervezet számára

**DOKUMENTUMKONTROLL**

**DOKUMENTUM JELLEMZŐK**

|  |  |
| --- | --- |
| Dokumentum címe: | Informatikai Biztonsági Szabályzat |
| Verziószám: | v1p1 |
| Készítés dátuma: | 2019. szeptember 21. |
| Készítette: | iAgency Szolgáltató KFT |

**VERZIÓKÖVETÉS**

|  |  |  |  |
| --- | --- | --- | --- |
| **Verzió** | **Dátum** | **Módosította** | **Módosítások leírása** |
| v0p8 | 2019. május 28. | Hargitay Zoltán | Szabályzat kidolgozása |
| v0p9 | 2019. június 17 | Hargitay Zoltán | Kiegészítés eljárásrendekkel |
| v0p9p1 | 2019. június 19 | Hargitay Zoltán | XVI. ker. POHI. észrevételeinek bedolgozása |
| v1p0 | 2019. augusztus 6 | Kúsz Andrea | Intézményi véleményezésre kerülő verzió |
| v1p1 | 2019. szeptember 21 | Hargitay Zoltán | Rövidített változat. A helyszíni interjúk alapján |
|  |  |  |  |
|  |  |  |  |

**JÓVÁHAGYÓK**

|  |  |  |  |
| --- | --- | --- | --- |
| **Név** | **Szervezeti egység / Beosztás** | **Dátum** | Aláírás |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Tartalom

[1. Tartalom 3](#_Toc20668818)

[1. Általános rendelkezések 9](#_Toc20668819)

[1.1. A szabályozás célja 9](#_Toc20668820)

[1.2. A szabályzat hatálya 9](#_Toc20668821)

[1.2.1. A szabályzat szervezeti hatálya 9](#_Toc20668822)

[1.2.2. A szabályzat személyi hatálya 9](#_Toc20668823)

[1.2.3. A szabályzat tárgyi hatálya 9](#_Toc20668824)

[1.2.4. A szabályzat időbeni hatálya 9](#_Toc20668825)

[1.3. Vonatkozó jogszabályok 10](#_Toc20668826)

[1.4. A szabályzat elkészítése felülvizsgálata és módosítása 10](#_Toc20668827)

[1.4.1. Időszaki felülvizsgálat 10](#_Toc20668828)

[1.4.2. Rendkívüli felülvizsgálat 10](#_Toc20668829)

[1.5. A szabályzat elfogadása és kihirdetése 10](#_Toc20668830)

[1.6. A szabályzat betartásának ellenőrzése 10](#_Toc20668831)

[1.7. Kivételkezeléssel kapcsolatos feladatok 10](#_Toc20668832)

[1.8. A szabályozókban megjelölt Ibtv. kontrollpontok és biztonsági osztályok magyarázata 11](#_Toc20668833)

[1.9. Szabályozási rendszer szintjei 11](#_Toc20668834)

[1.9.1. Szabályzati szint 11](#_Toc20668835)

[1.9.2. Eljárásrendi szint 11](#_Toc20668836)

[1.9.3. Munkautasítások szintje 12](#_Toc20668837)

[2. Használt fogalmak 13](#_Toc20668838)

[3. Az informatikai biztonság szervezete 14](#_Toc20668839)

[3.1. Informatikai biztonsági szerepek és felelőségek 14](#_Toc20668840)

[3.1.1. Szervezet Vezetője (SZV) 14](#_Toc20668841)

[3.1.2. „Második számú vezető” (MSZV) Intézményvezető-helyettes 14](#_Toc20668842)

[3.1.3. „Informatikai Biztonsági Felelős (IBF)” 15](#_Toc20668843)

[3.1.4. Adatgazdák (AG) 16](#_Toc20668844)

[3.1.5. Humánpolitikai feladatok ellátásáért felelős munkatárs (HSZV) 16](#_Toc20668845)

[3.1.6. IT üzemeltetésért felelős vezető (IÜFV) 16](#_Toc20668846)

[3.1.7. Alkalmazás támogatásáért felelős vezető (ATFV) 17](#_Toc20668847)

[3.1.8. Fizikai védelemért felelős vezető (FVFV) 17](#_Toc20668848)

[3.1.9. Tűzvédelmi felelős (TVF) 17](#_Toc20668849)

[3.1.10. Munkavédelmi felelős (MVF) 17](#_Toc20668850)

[3.1.11. Rendszerüzemeltetést végző munkatársak (RGAZD) 17](#_Toc20668851)

[3.1.12. Szervezeten belüli vagy kívüli felhasználók (FELH) 17](#_Toc20668852)

[3.2. Kapcsolattartás a hatóságokkal 17](#_Toc20668853)

[4. A szervezet biztonsági szintje 19](#_Toc20668854)

[4.1. Biztosági szintbe és osztályba sorolás, informatikai biztonsági kockázatelemzés 19](#_Toc20668855)

[4.1.1. Biztonsági szintbe és osztályba sorolás 19](#_Toc20668856)

[4.1.2. Cselekvési terv készítése 20](#_Toc20668857)

[4.2. Informatikai biztonsági kockázatelemzés 20](#_Toc20668858)

[4.3. Informatikai biztonsági ellenőrzés 20](#_Toc20668859)

[5. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK 22](#_Toc20668860)

[5.1. Az elektronikus információs rendszerekkel kapcsolatos engedélyezés (3.3.6.2.2. [4]) 22](#_Toc20668861)

[5.1.1. Engedélyek kérelmezése és megadása (3.1.1.5. [1]) 22](#_Toc20668862)

[5.1.2. Engedélyek visszavonása/felfüggesztése (3.1.1.5. [1]) 22](#_Toc20668863)

[5.2. Az elektronikus információs rendszerek nyilvántartása (3.1.1.4. [1]) 22](#_Toc20668864)

[5.3. Kockázatkezelés, kockázatelemzés (3.1.2. [1]) 23](#_Toc20668865)

[5.3.1. A kockázat azonosítása 23](#_Toc20668866)

[5.3.2. A kockázatok értékelése 24](#_Toc20668867)

[5.3.3. Intézkedési terv készítése (3.1.1.3. [2]) 27](#_Toc20668868)

[5.3.4. A végrehajtás ellenőrzése, felülvizsgálat 28](#_Toc20668869)

[5.3.5. A kockázatkezelés lezárása 28](#_Toc20668870)

[5.4. Biztonsági osztályba sorolás (3.1.2.2. [1]) 28](#_Toc20668871)

[5.4.1. Adatbesorolás 29](#_Toc20668872)

[5.4.2. A rendszerrel kapcsolatos kockázatelemzés 30](#_Toc20668873)

[5.4.3. A rendszer elvárt biztonsági osztályának meghatározása 30](#_Toc20668874)

[5.4.4. A rendszer tényleges biztonsági osztályának meghatározása 30](#_Toc20668875)

[5.4.5. A biztonsági osztálybesorolás eredményének rögzítése a rendszer nyilvántartásban 30](#_Toc20668876)

[5.4.6. Kapcsolódás biztosítása más intézkedési tervek mérföldköveihez 30](#_Toc20668877)

[5.4.7. A NEIH értesítése az osztályba sorolásról 30](#_Toc20668878)

[5.4.8. A biztonsági osztályba sorolás felülvizsgálata 31](#_Toc20668879)

[5.5. Az informatikai rendszerek biztonsági követelményei 31](#_Toc20668880)

[5.5.1. A biztonsági követelmények elemzése és meghatározása 31](#_Toc20668881)

[5.5.2. Biztonság az alkalmazási rendszerekben 32](#_Toc20668882)

[5.5.3. A bemeneti adatok ellenőrzése 32](#_Toc20668883)

[5.5.4. Az adatfeldolgozás ellenőrzése 33](#_Toc20668884)

[5.5.5. Az üzenetek hitelesítése 33](#_Toc20668885)

[5.5.6. A kimenő adatok ellenőrzése 34](#_Toc20668886)

[5.6. Rendszer és Szolgáltatás beszerzés eljárásrendje (3.1.3.1. [3]) 34](#_Toc20668887)

[5.6.1. A rendszerre vonatkozó dokumentáció 34](#_Toc20668888)

[5.6.2. Külső információs rendszerek szolgáltatásai (3.2.3.6 [2]) 36](#_Toc20668889)

[5.7. Működés-(Ügymenet) folytonosság tervezés (3.1.4. [2], 3.1.4.2. [2]) 36](#_Toc20668890)

[5.7.1. A folyamatos működésre felkészítő képzés (3.1.4.3. [3]) 37](#_Toc20668891)

[5.7.2. Az elektronikus információs rendszer mentései (3.1.4.8.[3]) 37](#_Toc20668892)

[5.7.3. Minősített adatok, elektronikus dokumentumok tárolása 39](#_Toc20668893)

[5.8. Biztonsági események figyelése és kezelése (3.1.5.) 40](#_Toc20668894)

[5.8.1. Biztonsági események figyelése (3.1.5.4. [3], 3.1.7.1. [3]) 40](#_Toc20668895)

[5.8.2. Biztonsági események priorálása, reagálás a biztonsági eseményekre 40](#_Toc20668896)

[5.8.3. A biztonsági események kezelése (3.1.5) 41](#_Toc20668897)

[5.8.4. Képzés a biztonsági események kezelésére (3.1.5.9. [3]) 42](#_Toc20668898)

[5.8.5. Informatikai incidensek nyilvántartásba vétele (Segítségnyújtás a biztonsági események kezeléséhez) (3.1.5.7 [3]) 43](#_Toc20668899)

[5.9. Emberi tényezőket figyelembe vevő – személy – biztonság (3.1.6., 3.3.1.4. [2]) 43](#_Toc20668900)

[5.9.1. Munkakörök, feladatkörök biztonság alapú besorolása (3.1.6.2. [3]) 43](#_Toc20668901)

[5.9.2. Személyi biztonság a munkaerő felvételénél 43](#_Toc20668902)

[5.9.3. Adatvagyon kezelése, hozzáférése 44](#_Toc20668903)

[5.9.4. Jogosult felhasználók 44](#_Toc20668904)

[5.9.5. Informatikai biztonság a munkaköri leírásokban 44](#_Toc20668905)

[5.9.6. Személyi biztonság a jogviszony alatt (3.1.6.1. [3]) 45](#_Toc20668906)

[5.9.7. Viselkedési szabályok az interneten (3.1.6.9. [1]) 45](#_Toc20668907)

[5.9.8. E-mail használat 45](#_Toc20668908)

[5.9.9. A felhasználó feladatai a munkahely elhagyásakor (3.1.6.4. [1]) 46](#_Toc20668909)

[5.9.10. Tiszta asztal tiszta képernyő szabályok a munkavégzés közben 47](#_Toc20668910)

[5.9.11. A vezetők felelőssége 47](#_Toc20668911)

[5.9.12. Személyi biztonság a jogviszony megszűnésekor, megszüntetésekor vagy kinevezés módosítás esetén (3.1.6.4. [1]; 3.1.6.5. [3]) 47](#_Toc20668912)

[5.9.13. A jogviszony megszűnésének, megszüntetésnek biztonsági kérdései (3.1.6.4. [1]) 48](#_Toc20668913)

[5.9.14. Az eszközök visszaadása 48](#_Toc20668914)

[5.9.15. A hozzáférési jogok visszavonása 48](#_Toc20668915)

[5.9.16. Az informatikai biztonsági oktatás és képzés (3.1.7.) 49](#_Toc20668916)

[5.9.17. A biztonsági képzésre vonatkozó dokumentációk (3.1.7.6. [3]) 49](#_Toc20668917)

[5.9.18. Fegyelmi eljárás (3.1.6.7. [1]) 49](#_Toc20668918)

[5.9.19. Külső szervezetre vonatkozó követelmények (3.1.6.6. [3]) 49](#_Toc20668919)

[6. FIZIKAI VÉDELEMI INTÉZKEDÉSEK ELJÁRÁSRENDJE (3.2.1.2 [2]) 51](#_Toc20668920)

[6.1. Fizikai belépési engedélyek (3.2.1.3. [2]) 51](#_Toc20668921)

[6.2. A fizikai belépés ellenőrzése (3.2.1.4. [2]) 51](#_Toc20668922)

[6.3. Vészvilágítás (3.2.1.11. [3]) 52](#_Toc20668923)

[6.4. Tűzvédelem (3.2.1.12. [3]) 52](#_Toc20668924)

[6.5. Karbantartók (3.2.1.19 [3]) 52](#_Toc20668925)

[7. LOGIKAI VÉDELMI INTÉZKEDÉSEK 53](#_Toc20668926)

[7.1. Általános védelmi intézkedések (3.3.1.1.[R2]) 53](#_Toc20668927)

[7.1.1. Az elektronikus információs rendszer kapcsolódásai (3.3.1.3.[3]) 53](#_Toc20668928)

[7.2. Tervezés (3.3.2.) 53](#_Toc20668929)

[7.2.1. Felmérés 54](#_Toc20668930)

[7.2.2. Az elvárt biztonsági osztály meghatározása 54](#_Toc20668931)

[7.2.3. Követelményrendszer kidolgozása 54](#_Toc20668932)

[7.2.4. Cselekvési terv (3.3.2.3. [2]) 54](#_Toc20668933)

[7.2.5. Személyi biztonság (3.3.2.4. [2]) 54](#_Toc20668934)

[7.3. Rendszer és szolgáltatás beszerzés (3.3.3. [2]) 55](#_Toc20668935)

[7.3.1. A rendszer fejlesztési életciklusa (3.3.3.2. [2]) 55](#_Toc20668936)

[7.4. Konfigurációkezelés (3.3.6.) 55](#_Toc20668937)

[7.4.1. Konfigurációs eljárásrend és nyilvántartások (3.3.6.1. [2]) 55](#_Toc20668938)

[7.4.2. Alkalmazások konfigurációinak nyilvántartása 55](#_Toc20668939)

[7.4.3. Alapkonfiguráció (3.3.6.2. [2]) 56](#_Toc20668940)

[7.4.4. A konfigurációváltozások felügyelete (változáskezelés) (3.3.6.3. [3]) 56](#_Toc20668941)

[7.4.5. Változáskezelés alapvető szabályai 56](#_Toc20668942)

[7.4.6. Új konfiguráció éles üzembeállása 56](#_Toc20668943)

[7.4.7. A működő rendszer konfiguráció figyelése 56](#_Toc20668944)

[7.4.8. Legszűkebb funkcionalitás (3.3.6.7. [3]) 57](#_Toc20668945)

[7.4.9. Elektronikus információs rendszerelem leltár (3.3.6.8. [2]) 57](#_Toc20668946)

[7.4.10. A szoftverhasználat korlátozásai (3.3.6.10. [2]) 57](#_Toc20668947)

[7.4.11. A felhasználó által telepített szoftverek 57](#_Toc20668948)

[7.5. Karbantartás (3.3.7.) 58](#_Toc20668949)

[7.5.1. Karbantartók (3.2.1.19 [3]) 58](#_Toc20668950)

[7.6. Adathordozók védelme (3.3.8. [4]) 59](#_Toc20668951)

[7.6.1. Hozzáférés az adathordozókhoz (3.3.8.2. [2], 3.3.8.7. [2]) 59](#_Toc20668952)

[7.6.2. Adathordozók törlése (3.3.8.6. [2]) 60](#_Toc20668953)

[7.6.3. Adathordozók újrahasznosítása 60](#_Toc20668954)

[7.6.4. Adathordozók megsemmisítése 60](#_Toc20668955)

[7.7. Azonosítás és hitelesítés (3.3.9.) 60](#_Toc20668956)

[7.7.1. A felhasználók azonosítása (3.3.9.2. [2]) 60](#_Toc20668957)

[7.7.2. Felhasználók hitelesítése (3.3.9.2. [2]) 61](#_Toc20668958)

[7.7.3. Felhasználói fiókok kezelése (3.3.10.2.) 63](#_Toc20668959)

[7.7.4. Ellenőrzés 65](#_Toc20668960)

[7.7.5. A hitelesítésre szolgáló eszköz visszacsatolása (3.3.9.6. [2]) 65](#_Toc20668961)

[7.7.6. Azonosítás és hitelesítés (Szervezeten kívüli felhasználók) (3.3.9.8. [2]) 65](#_Toc20668962)

[7.7.7. Hitelesítés szolgáltatók tanúsítványának elfogadása (3.3.9.8.2. [2]) 65](#_Toc20668963)

[7.8. Hozzáférés az informatikai rendszerekhez (3.3.10., 3.3.10.1. [2]) 65](#_Toc20668964)

[7.8.1. Általános alapelvek 65](#_Toc20668965)

[7.8.2. Hozzáférés ellenőrzés eljárásrendje (3.3.10) 66](#_Toc20668966)

[7.8.3. Hálózati hozzáférés 67](#_Toc20668967)

[7.8.4. Biztonságos hitelesítő, bejelentkező eljárások (3.3.13.16. [3]) 67](#_Toc20668968)

[7.8.5. A rendszerhasználat jelzése (3.3.10.8. [3]) 68](#_Toc20668969)

[7.8.6. Mobil eszközök hozzáférés ellenőrzése (3.3.10.15. [3]) 68](#_Toc20668970)

[7.8.7. Vezeték nélküli hozzáférés (3.3.10.14. [3]) 68](#_Toc20668971)

[7.8.8. Külső elektronikus információs rendszerek használata (3.3.10.16. [2]) 68](#_Toc20668972)

[7.8.9. Nyilvánosan elérhető tartalom (3.3.10.18. [2]) 69](#_Toc20668973)

[7.9. Rendszer és információsértetlenség (3.3.11., 3.3.11.2. [2]) 69](#_Toc20668974)

[7.9.1. Hibajavítás (3.3.11.3.[S2]) 69](#_Toc20668975)

[7.9.2. Kártékony kódok elleni védelem (3.3.11.4. [2]) 70](#_Toc20668976)

[7.9.3. Az elektronikus információs rendszer felügyelete (3.3.11.5. [2]) 71](#_Toc20668977)

[7.9.4. A kimeneti információ kezelése és megőrzése (3.3.11.12. [2]) 71](#_Toc20668978)

[7.9.5. Használatból történő kivonás 71](#_Toc20668979)

[7.10. Naplózás és elszámoltathatóság (3.3.12., 3.3.12.1. [2]) 72](#_Toc20668980)

[7.10.1. Biztonsági események naplózása 72](#_Toc20668981)

[7.10.2. Ideiglenes naplózás 74](#_Toc20668982)

[7.10.3. Kockázati tényezők 74](#_Toc20668983)

[7.10.4. Naplózási információk védelme (3.3.12.9. [2]) 74](#_Toc20668984)

[7.10.5. Naplóinformációk figyelése, reagálás a napló információkra (3.3.12.6. [3]) 75](#_Toc20668985)

[7.10.6. Rendszer órajel szinkronizáció (3.3.12.8. [2]) 75](#_Toc20668986)

[7.10.7. A naplóbejegyzések megőrzése (3.3.12.11. [2]) 75](#_Toc20668987)

[7.10.8. Naplózó rendszer beállításainak módosítása 77](#_Toc20668988)

[7.10.9. Naplózási beállításokról nyilvántartás vezetése 77](#_Toc20668989)

[7.11. Rendszer és kommunikációvédelem (3.3.13., 3.3.13.1. [2]) 77](#_Toc20668990)

[7.11.1. A határok védelme (3.3.13.6. [2]) 77](#_Toc20668991)

[7.11.2. A hálózati szintű hozzáférések menedzsmentje 77](#_Toc20668992)

[7.11.3. Mobil informatikai tevékenység, távmunka (3.3.10.13. [3]) 78](#_Toc20668993)

[7.11.4. Kulcsmenedzsment (3.3.13.10. [2]) 80](#_Toc20668994)

[8. Jogszabályi háttér 81](#_Toc20668995)

[9. Megismerési nyilatkozat 82](#_Toc20668996)

# Általános rendelkezések

## A szabályozás célja

* Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) célja a Budapest Főváros XVI. kerületi Önkormányzat Gazdasági Működtető- Ellátó Szervezet (továbbiakban: **Szervezet**) által használt informatikai rendszer, alkalmazások és szolgáltatások, valamint az általuk kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának szabványos, szabályozott és egységes biztosítása, illetve a kapcsolódó jogszabályoknak (lásd: 1.4 Vonatkozó jogszabályok) való megfelelés. Az egységesítés érdekében jelen szabályzat keretjelleggel meghatározza mindazokat a normákat és magatartásformákat, amelyek megvalósítják a kockázatokkal arányos, folyamatos és komplex információvédelmet az informatikai rendszer fizikai, adminisztratív és logikai védelmi területén.
* Az IBSZ általános célja, hogy a **Szervezet** által használt informatikai rendszer biztonságát garantáló eljárásokat és előírásokat átlátható és nyomon követhető formában egységes keretbe foglalva rögzítse az informatikai biztonság magasabb fokú kialakításának további szabályozása érdekében.
* Az IBSZ kiadásának célja továbbá a **Szervezet** által használt informatikai rendszer alkalmazásának és felhasználásának biztonsági szempontból történő szabályozása.

## A szabályzat hatálya

### A szabályzat szervezeti hatálya

A szabályzat hatálya kiterjed a **Szervezet** valamennyi szervezeti egységére, akik feladataik teljesítése során vagy egyéb céllal, jogosultsággal, vagy annak hiányában felhatalmazással, az IBSZ tárgyi hatálya alá tartozó eszközöket, alkalmazásokat és szolgáltatásokat (továbbiakban együtt informatikai rendszert) használnak, adatokat vagy dokumentumokat, információkat hoznak létre, tárolnak, használnak vagy továbbítanak, valamint azokra, akik ilyen tevékenységekkel kapcsolatosan döntéseket hoznak.

A felhasználókkal kötendő valamennyi jogviszony vonatkozásában a jogviszonyra vonatkozó szerződésben rögzített hivatkozás mellett biztosítani kell az IBSZ rendelkezéseinek érvényesülését.

### A szabályzat személyi hatálya

A szabályzat hatálya kiterjed a **Szervezet** által foglalkoztatott valamennyi munkavállalóra, illetve munkavégzés céljából egyéb jogviszonyban álló jogi és természetes személyre.

### A szabályzat tárgyi hatálya

A szabályzat tárgyi hatálya kiterjed:

* a **Szervezetben** üzemelő számítógépes rendszer teljes konfigurációjára, az ahhoz tartozó rendszer- és felhasználói szoftverekre, valamint ezek dokumentációira;
* a számítógépes feldolgozásra szánt, feldolgozás alatt álló, és a feldolgozás után számítógépes adathordozókon tárolt, a feldolgozás eredményeként létrejött adatra;
* a számítástechnikai eszközök alkalmazásának teljes folyamatára, tevékenységeire;
* a számítástechnikai infrastruktúra elhelyezésére szolgáló helyiségekre.
* Az IBSZ rendelkezéseit alkalmazni kell a külső helyszínen történő munkavégzéshez használt eszközökre is, amennyiben azok az IBSZ tárgyi hatálya alá tartoznak.

### A szabályzat időbeni hatálya

A szabályzat érvényes a hatálybalépés napjától, visszavonásig.

## Vonatkozó jogszabályok

A védelmet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) és az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet szerinti (továbbiakban együttesen jogszabály), valamint az alkalmazott szabványi előírások alapján valósítja meg.

## A szabályzat elkészítése felülvizsgálata és módosítása

A szabályzat elkészítése, felülvizsgálata és szükség szerinti módosítása az **Informatikai Biztonsági Felelős** feladata és felelőssége, együttműködve a **Szervezet vezetőjé**vel. A szabályzat elkészítésében, felülvizsgálatában és módosításában közreműködnek az elektronikus információ-biztonsági feladatok ellátásában közreműködő személyek, szervezeti egységek, munkacsoportok, valamint az elektronikus információs rendszer üzemeltetéséért, fejlesztéséért felelős szervezeti egységek vezetői.

### Időszaki felülvizsgálat

Az Informatikai Biztonsági Szabályzatot legalább évenként felül kell vizsgálni és szükség esetén módosítani kell. A vizsgálat alapja az ellenőrzések, rendkívüli események naplói, valamint a kockázat elemzés és kezelés megállapításai.

### Rendkívüli felülvizsgálat

Az Informatikai Biztonsági Szabályzatot az időszakos felülvizsgálaton túl felül kell vizsgálni és szükség esetén módosítani kell:

* a szabályzatban hivatkozott **Szervezetnek** vagy munkakörök változása esetén;
* súlyos informatikai biztonsági események bekövetkezése esetén;
* az informatikai biztonság szabályozását érintő jogszabályváltozások esetén;
* Az informatikai rendszer nagy mértékű változása esetén.

A felülvizsgálatok eredményéről az **Informatikai biztonsági felelős** tájékoztatja a **Szervezet vezetőjét**.

## A szabályzat elfogadása és kihirdetése

A szabályzat elfogadása és kihirdetése a **Szervezet vezetőjé**nek feladata és felelősége. A kihirdetés normatív utasítással történik. A kihirdetés során a **Szervezet Vezetője** gondoskodik arról, hogy annak tartalma ne legyen módosítható, és az abban foglalt adatok csak az arra felhatalmazott személyek által legyen megismerhető.

## A szabályzat betartásának ellenőrzése

A szabályzat betartásának ellenőrzése az **Informatikai Biztonsági Felelős** feladata, melyben közreműködnek az elektronikus információ-biztonsági feladatok ellátásában közreműködő személyek, szervezeti egységek, munkacsoportok, valamint az elektronikus információs rendszer üzemeltetéséért, fejlesztéséért felelős szervezeti egységek vezetői.

## Kivételkezeléssel kapcsolatos feladatok

Kivétel alatt kell érteni minden olyan technológiai kontroll nem teljesülését, mely a jelen szabályozásban rögzített követelményeket nem tudja teljesíteni.

A Szabályzattól való kivételeket minden esetben az adott rendszer rendszerbiztonsági tervében kell dokumentálni. A kivételek engedélyezése a **Szervezet Vezetőjé**nek felelőssége.

A Szabályzatban és a függelékekben szereplő nyilvántartásokat elektronikusan kell vezetni, amennyiben ez nem biztosított, papír alapú nyilvántartással kell rendelkezni.

**A kivételkezelés irányelvei:**

* A kivételek megszüntetésére vonatkozóan tervben kell rögzíteni a hiányosságot (szabályzattól való eltérést) és annak tervezett kezelését (akcióterv).
* A kivétel megszüntetése érdekében javító intézkedéseket kell alkalmazni, melyek megfelelőségét és szükségességét a kockázatelemzés során meg kell vizsgálni. Ennek koordinálása az **Informatikai Biztonsági Felelős** feladata.
* A kivételek kezelésére hozott intézkedésekre vonatkozóan az *Informatikai biztonsági kockázatelemzési és kockázatkezelési eljárásrend* kockázatkezelési előírásait kell alkalmazni.
* Meg kell szervezni az információs rendszer törvénynek való megfelelését, a költséghatékonyság figyelembevételével, szükség esetén a rendszer kiváltásáról gondoskodni kell.
* Új, bevezetés alatt álló elektronikus információs rendszer esetén a szabályzati követelmények teljesülésére vonatkozó kivétel nem alkalmazható.

## A szabályozókban megjelölt Ibtv. kontrollpontok és biztonsági osztályok magyarázata

Egyes szabályozókban a fejezetek címében vagy bekezdéseiben zárójelben az Ibtv. végrehajtási rendelete szerinti kontrollpontok és a szögletes zárójelben a hozzá tartozó biztonsági osztályok (bizalmasság, sértetlenség és rendelkezésre állás szerinti) besorolása rögzítésre került. Az adott fejezetek, bekezdések a megjelölt osztálytól felfelé alkalmazandók az egyes elektronikus információs rendszerek osztályba sorolásától függően.

## Szabályozási rendszer szintjei

### Szabályzati szint

Szabályzatok szintje, mely a stratégiai szinten megfogalmazott elvek leképezésére, a követelmények meghatározására szolgáló szabályzatokat tartalmazza. A szabályzatok célja, hogy pontosan rögzítsék azokat a követelményeket, amelyek ahhoz szükségesek, hogy a legfelsőbb szinten meghatározott stratégiai célkitűzések érvényre tudjanak jutni:

### Eljárásrendi szint

Egységes irányelveket és etalon eljárásrendi mintákat fogalmaz meg. Az itt meghatározott eljárásrendi minták kerülnek kiadásra.

### Munkautasítások szintje

Munkautasítások szintjén szerepel mindazon rendszer specifikus dokumentáció, kézikönyv, útmutató, melyek az informatikai biztonság működtetéséhez szükséges, környezet és rendszer függő információkat tartalmaznak.

# Használt fogalmak

A használt fogalmak listáját az 1. számú melléklet (Használt fogalmak, értelmező rendelkezések.) tartalmazza.

# Az informatikai biztonság szervezete

## Informatikai biztonsági szerepek és felelőségek

###  Szervezet Vezetője (SZV)

#### Hatásköre:

A szabályzatok és eljárásrendek elfogadása és szervezeti szintű kihirdetése és az **Informatikai Biztonsági Felelős** (**IBF**) kinevezése, valamint a Cselekvési terv és az ahhoz kapcsolódó Költségvetési terv elfogadása.

#### Felelőssége:

Az informatikai biztonság személyi és tárgyi feltételeinek, valamint a jogszabályoknak megfelelő működéshez szükséges feltételek biztosítása.

#### Feladatai:

Mint a **Szervezet Vezetője**, köteles gondoskodni a jogszabályi megfelelésnek a következők szerint:

* biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
* biztosítja a **Szervezetre** irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,
* az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,
* meghatározza a **Szervezet** elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az **IBSZ**-t,
* jóváhagyja az *Informatikai Biztonsági Stratégiát (****IBS****)* és a hiányosságok megszüntetésének céljából készített *Cselekvési tervet*, valamint biztosítja az ezekben foglaltak végrehajtásához szükséges személyi és tárgyi feltételeket,
* gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a **Szervezet** munkatársai elektronikus információ-biztonsági ismereteinek szinten tartásáról,
* rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén biztosítja, hogy a **Szervezet** elektronikus információs rendszereinek biztonsága megfeleljen a jogszabályoknak és a kockázatoknak.
* gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
* biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,
* ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik a szerződéses kötelmek teljesüléséről,
* felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért.

### „Második számú vezető” (MSZV) Intézményvezető-helyettes

#### Hatásköre:

A **Szervezet** működését és személyi állományát érintő döntések meghozatala és a rá delegált munkáltatói jogok gyakorlása.

#### Felelőssége:

A **Szervezet** operatív működésének elősegítése és felügyelete, a rendelkezésre álló személyi és tárgyi erőforrások optimális kihasználásának biztosítása, valamint a jogszabályoknak megfelelő működés ellenőrzése.

#### Feladatai:

Mint a **Szervezet** második számú vezetője, köteles a **Szervezet** Vezetőjeje által részére delegált informatikai biztonsági feladatokat ellátni.

### „Informatikai Biztonsági Felelős (IBF)”

Az Ibtv. értelmében a **Szervezetnek** az elektronikus információs rendszer biztonságáért felelős személyt (**Informatikai Biztonsági Felelős**, a továbbiakban: **IBF**) kell kineveznie vagy megbíznia. Amennyiben ez az **IBF** kinevezési okmányában és munkaköri leírásában meghatározott szolgálati beosztással nem egyeztethető össze, úgy a munkaköri leírás mellé megbízólevelet szükséges kiadni az **IBF** részére, mely kifejezetten kitér az Ibtv. 13 § (1) – (7) bekezdése szerinti feladatok ellátását érintő személyes felelősségre.

Amennyiben a **Szervezet** elektronikus információs rendszereinek mérete vagy biztonsági igényei indokolják, a **Szervezeten** belül elektronikus információ-biztonsági szervezeti egység hozható létre, amelyet az elektronikus információs rendszer biztonságáért felelős személy vezet.

#### Hatásköre:

Jogosult bármely elektronikus információs rendszer tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködőtől a biztonsági követelményekről tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához jogosult bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot. Jogosult ezen bekért információk és dokumentumok véleményezésére, továbbá véleményezési joga van valamennyi elektronikus információbiztonságot érintő szabályzat tekintetében, továbbá minden olyan beszerzés esetében, amelynek közvetlen vagy közvetett hatása lehet az elektronikus információbiztonságra. Elektronikus információ-biztonsági szakmai kérdésekben döntéshozó. Feladatai ellátása során a **Szervezet** vezetőjének közvetlenül adhat tájékoztatást, jelentést.

#### Felelőssége:

A **Szervezet** elektronikus információbiztonságának fenntartása és folyamatos fejlesztése, az Informatikai Biztonsági Irányítási Rendszer (a továbbiakban: IBIR) eseti és rendszeres karbantartása, valamint a jogszabályban előírt adatszolgáltatási és jelentési kötelezettség teljesítése más szervezetek és szakmai csoportok irányába, illetve a folyamatos szakmai kapcsolat fenntartása az érdekeltekkel.

#### Feladatai:

Az elektronikus információs rendszer biztonságáért felelős személynek elsősorban, de nem kizárólagosan az alábbi feladatokat kell ellátnia:

* gondoskodik a **Szervezet** elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
* elvégzi vagy irányítja az előző pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
* előkészíti a **Szervezet** elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
* előkészíti a **Szervezet** elektronikus információs rendszereinek biztonsági osztályba sorolását és a **Szervezet** biztonsági szintbe történő besorolását,
* véleményezi az elektronikus információs rendszerek biztonsága szempontjából a **Szervezet** e tárgykört érintő szabályzatait és szerződéseit,
* kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.

Továbbá biztosítja az Ibtv.-ben meghatározott követelmények teljesülését:

* a **Szervezet** valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők tevékenysége során,
* ha a **Szervezet** az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők az Ibtv. hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

### Adatgazdák (AG)

### Humánpolitikai feladatok ellátásáért felelős munkatárs (HSZV)

### IT üzemeltetésért felelős vezető (IÜFV)

#### Hatásköre:

**Szervezeti** informatikai infrastruktúra kialakításával, üzemeltetésével és fejlesztésével kapcsolatban javaslattételi hatásköre van, illetve a kapcsolódó feladatok ellátása tekintetében döntési jogköre van, mely döntési jogköre az előzetesen jóváhagyott kereteken belül érvényes.

#### Felelőssége:

Felelős a **Szervezeten** belüli, illetve **Szervezeten** kívüli, vállalt szolgáltatási szintek, illetve az üzemmenet folytonosság elvárt szinten való fenntartásáért.

#### Feladatai:

**Szervezeti** informatikai infrastruktúra kialakításával, üzemeltetésével és fejlesztésével kapcsolatos feladatok tervezése, végrehajtása, javaslattétel a fejlesztésekre, erőforrástervezés az üzemeltetési, fejlesztési, illetve javítási feladatok tekintetében.

Az informatikai erőforrások teljesítményét és kapacitását folyamatosan figyelemmel kíséri, a kapcsolódó problémák kezelésére javaslatot ad.

Infrastruktúra elemek és kapcsolódó rendszer beszerzés és fejlesztés esetén a szükséges erőforrások felmérése, és igénylése.

Hibajelentések megfelelő kezelésének biztosítása.

Üzemmenet folytonossági feladatok szabályozása és tervezése az informatikai rendszerek (infrastruktúra) tekintetében.

Részt vesz az Informatikai biztonsági kockázatelemzési és kockázatkezelési eljárásrendnek megfelelő kockázatmenedzsment folyamatokban, elkészíti a hatáskörébe tartozó elemek (infrastruktúra) kockázatelemzését és kockázatkezelési tervére javaslatot ad.

Informatikai auditokon való részvétel.

### Alkalmazás támogatásáért felelős vezető /munkatárs/ (ATFV)

### Fizikai védelemért felelős vezető /munkatárs/ (FVFV)

### Tűzvédelmi felelős (TVF)

A **Szervezet** tűzvédelemre vonatkozó szabályzása alapján előírt feladatok végrehajtásában működik közre.

### Munkavédelmi felelős (MVF)

A **Szervezet** munkavédelemre vonatkozó szabályzása alapján előírt feladatok végrehajtásában működik közre.

### Rendszerüzemeltetést végző munkatársak (RGAZD)

#### Hatáskörük:

A közvetlen szakmai vezetőjük és/vagy az Informatikai feladatok ellátásáért felelős vezetőn keresztül szakmai véleményt és javaslatokat fogalmazhatnak meg a szabályozásokkal és eljárásrendekkel, valamint az alkalmazott technológiákkal kapcsolatban.

#### Felelősségük:

Minden információs eszköz vagy eszközcsoport, információs rendszer, informatikai szolgáltatás működtetésére informatikai referenst vagy alkalmazásgazdát (adminisztrátort) kell kijelölni, aki felelős a szabályzatokban és eljárásrendekben megfogalmazott követelmények szerinti üzembe helyezésért, üzemeltetésért, vagy kivonásért.

#### Feladataik:

A szervezeti előírásoknak és a gyártói ajánlásoknak megfelelően a folyamatos működéshez szükséges beállítások elvégzése, munkafolyamatok és ellenőrzések végrehajtása, a dokumentációk naprakészen tartása, a rendszerek felhasználóinak támogatása, valamint ezen tevékenységeik előírásszerű adminisztrálása.

### Szervezeten belüli vagy kívüli felhasználók (FELH)

#### Hatáskörük:

Jogosultak a munkavégzésükhöz szükséges és elégséges mértékű hozzáférést kapni az információs rendszerekhez, eszközökhöz, szolgáltatásokhoz.

#### Felelősségük:

Valamennyi felhasználó felelős az átvett informatikai eszközök előírásszerű használatáért, megőrzéséért, valamint a rájuk vonatkozó előírások és biztonsági követelmények betartásáért azon adatok és információs rendszerek tekintetében, amelyeket használnak, vagy amelyekkel bármilyen módon kapcsolatba kerülnek.

#### Feladataik:

Minden rendellenességet a szabályzatokban meghatározottak szerint haladéktalanul jelenteniük kell.

## Kapcsolattartás a hatóságokkal

A jogszabályokban meghatározott hatóságokat az **Informatikai Biztonsági Belelős** tájékoztatja az elektronikus információs rendszerek biztonsági eseményeiről és incidenseiről, valamint teljesíti a **Szervezet** jogszabályi előírásként megfogalmazott elektronikus információbiztonsággal összefüggő adatszolgáltatási kötelezettségeit is, továbbá a kapcsolatot tart fenn a Kormányzati Eseménykezelő Központtal és a Nemzeti Elektronikus Információ-biztonsági Hatósággal.

|  |  |  |  |
| --- | --- | --- | --- |
| Feladat | Felelős | Konzulens(ek) | Tájékoztatandó(k) |
| Kapcsolat a hatóságokkal | IBF | - | SZV |

3. táblázat Kapcsolattartás a hatóságokkal

A fenti tevékenységeiről az **Informatikai Biztonsági Felelős** a **Szervezet Vezetője** felé tartozik tájékoztatással, továbbá megosztja a tudomására jutott naprakész informatikai biztonsági – fenyegetésekre és sebezhetőségekre vonatkozó – információkat, eljárásokat és technikákat az érintett szervezeti egységekkel.

A Nemzeti Elektronikus Információ-biztonsági Hatóság és a Kormányzati Eseménykezelő Központ részére az **Informatikai Biztonsági Felelős**nek az Ibtv. alapján előírt adatait be kell jelentenie.

Az **Informatikai Biztonsági Felelős**nek folyamatosan figyelemmel kell kísérnie a jogszabályban kijelölt szervezetek által kiadott riasztásokat és gondoskodnia kell az egyes elektronikus információs rendszerekre vonatkozó megfelelő ellenintézkedésekről és válaszlépésekről.

# A szervezet biztonsági szintje

**A szervezet a jogszabály szerinti 2-as biztonsági szintbe sorolja magát.**

A **Szervezetnél** azonban üzemelnek 2-es biztonsági osztályba sorolt rendszerek, ezért kerültek feltüntetésre a 3-as szintű biztonsági követelmények is – ezen intézkedések jelölése: [3], melyeket csak a mellékletben jelölt, 3-as szintű rendszerek esetében kell figyelembe venni.

Indoklás: A 41/2015. (VII. 15) BM rendelet 2. számú mellékletében foglaltak szerint:

A **Szervezet** biztonsági szintje 2. „ha a **Szervezet** vagy szervezeti egység az 1. szinthez rendelt jellemzőkön túl elektronikus információs rendszert használ, amely személyes adatokat kezel, és a szervezet jogszabály alapján kijelölt szolgáltatót vesz igénybe.”

A **Szervezet** biztonsági szintje 3. „ha a **Szervezet** vagy szervezeti egység a 2. szinthez rendelt jellemzőkön túl szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt. A **Szervezet** kritikus, nem minősített, de nem közérdekű, vagy közérdekből nyilvános adatot kezel, központi üzemeltetésű, és több szervezetre érvényes biztonsági megoldásokkal védett elektronikus információs rendszerek vagy zárt célú elektronikus információs rendszer felhasználója, illetve feladatai támogatására más külső szolgáltatót vesz igénybe.”

## Biztosági szintbe és osztályba sorolás, informatikai biztonsági kockázatelemzés

A biztonsági szintbe és osztályba sorolást, valamint az informatikai biztonsági kockázatelemzést az **Informatikai Biztonsági Felelős** koordinálja a:

* Szervezeti egység vezetők / Adatgazdák,
* Informatikai biztonsági megbízott,
* Informatikai feladatok ellátásáért felelős vezető,

 (illetve az általuk kijelölt munkatársak) bevonásával.

A **Szervezetnél** az informatikai biztonság szinten tartása, valamint az elektronikus információs rendszerek biztonsági osztályba sorolása elvégzésének megalapozása érdekében az informatikai biztonsági kockázatelemzésre vonatkozó további részletes követelményeket és eljárásokat, továbbá szabályokat az *Informatikai biztonsági kockázatelemzési és kockázatkezelési eljárásrend* tartalmazza.

### Biztonsági szintbe és osztályba sorolás

A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében az elektronikus információs rendszereket – ideértve a rendszer által kezelt adatokat – biztonsági osztályba kell sorolni, a bizalmasságuk, a sértetlenségük, valamint a rendelkezésre állásuk szempontjából.

Az elektronikus információs rendszerek biztonsági osztályba sorolását az alábbi alapkövetelmények figyelembevételével kell végrehajtani:

* a biztonsági osztályokhoz tartozó védelmi követelményeket jogszabály rögzíti,
* a nemzeti adatvagyont kezelő rendszerek esetében a jogszabályi előírásoknak megfelelően,
* a biztonsági osztályokat a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából erősödő védelmi követelményeket meghatározó, 1-5 fokozatú skála szerint kell megállapítani.

A **Szervezetet**, valamint a jogszabályban meghatározott szervezeti egységeit az elektronikus információs rendszerek védelmére való felkészültségük alapján biztonsági szintekbe kell sorolni a jogszabályban meghatározott szempontok szerint.

A biztonsági szintbe és osztályba sorolást a **Szervezet** vagy az elektronikus információs rendszer – illetve az abban kezelt adatok – jelentős megváltozása esetén, de legalább 3 évente felül kell vizsgálni.

A **Szervezet**, szervezeti egységek elvárt biztonsági szintbe, valamint az elektronikus információs rendszerek elvárt biztonsági osztályba sorolását az *1. számú függelék* tartalmazza.

### Cselekvési terv készítése

Amennyiben a vizsgálat – vagy felülvizsgálat – alapján meghatározott biztonsági szint alacsonyabb, mint az adott **Szervezetre** vagy szervezeti egységre jogszabályban meghatározott biztonsági szint, vagy ha a **Szervezet** az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, akkor a vizsgálatot követő 90 napon belül cselekvési tervet kell készítenie a számára előírt biztonsági szint elérésére vagy hiányosságok megszüntetésére.

A cselekvési terv elkészítése és folyamatos nyomon követése az **Informatikai Biztonsági Felelős** (**IBF**) feladata, együttműködve az elektronikus információ-biztonsági feladatok ellátásában közreműködő személyekkel, szervezeti egységekkel és munkacsoportokkal. A cselekvési terv elfogadása az **Szervezet Vezetőjének** feladata

## Informatikai biztonsági kockázatelemzés

Az informatikai biztonsági kockázatelemzés célja azoknak az informatikai, fizikai és humán tényezőknek a feltárása, amelyek kockázatot hordoznak magukban, ezáltal veszélyeztetve a **Szervezet** megfelelő működését, illetve, hogy számszerűsíthető módszerekkel megbecsülje a fenyegető tényezők bekövetkezési gyakoriságát és hatását, majd a kockázatok összehasonlítása érdekében számszerűsítse a releváns kockázatokat.

A felmerült kockázatok kezelésére intézkedési terveket kell készítenie az **Informatikai Biztonsági Felelősnek**, melyek a feltárt kockázatok függvényében az alábbiakat kell, hogy tartalmazzák:

* a kockázatok csökkentésére tett javaslatokat a technikai eszközök megváltoztatására, vagy fejlesztésére (pl.: új védelmi eszközök alkalmazása, vagy a jelenlegi átkonfigurálása),
* a kockázatok csökkentésére tett javaslatokat az érvényben lévő szabályozás megváltoztatására,
* a kockázatok csökkentésére tett javaslatokat a személyi állományra vonatkozóan (pl.: motiváció, a fegyelmi eljárások szigorítása, oktatás stb.),
* a kockázatok tudatos felvállalására irányuló javaslatot, ha a védelmi intézkedés anyagi vonzata nagyobb, vagy közel azonos, mint a fenyegetettség által elszenvedhető anyagi kár.

## Informatikai biztonsági ellenőrzés

Az informatikai biztonsági ellenőrzések alapvető célja, hogy a kockázatok csökkentése és a rendkívüli események elkerülése érdekében objektív információkat szolgáltasson a felelős vezetők számára az informatikai biztonság helyzetéről.

Az informatikai biztonsági ellenőrzés célja, hogy rendszeresen vizsgálja:

* az informatikai rendszerek biztonsági megfelelését a **Szervezet** által elfogadott biztonsági követelményeknek;
* a **Szervezeti** és rendszerszintű biztonsági szabályozásokban foglaltak érvényesülését;
* az alkalmazott módszerek a jogszabályi előírásoknak való megfelelését;
* az informatikai rendszerek és az általuk nyújtott szolgáltatások biztonságát;
* a biztonsági alapelveket sértő események bekövetkezési valószínűségét, illetve bekövetkezését és kivizsgálását.

Az ellenőrzések során feltárt hiányosságok képezik azon védelmi intézkedések alapját, melyek biztosítják, hogy minimális legyen a védelmi képességek kívánt és valós szintje közötti távolság. A megállapításokat mindig írásos jelentésbe kell foglalni, a védelmi intézkedések megsértésével kapcsolatban adott esetben szankciókat is kell alkalmazni. Az ellenőrzések során tapasztalt hiányosságok megszüntetésére intézkedési tervet kell kidolgozni.

# ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

## Az elektronikus információs rendszerekkel kapcsolatos engedélyezés (3.3.6.2.2. [4])

A **Szervezet** az általa kezelt adatok, adatkezelő rendszerek információ-biztonsági céljait az információbiztonsággal kapcsolatos engedélyezési eljárásrenddel biztosítja.

### Engedélyek kérelmezése és megadása (3.1.1.5. [1])

Bármely, a **Szervezet** informatikai eszközeinek (hardverek, szoftverek, alkalmazások) használatával összefüggő engedélyezési eljárást a szervezeti egység vezetőinek kell kezdeményezniük e-mail-ben.

A kérelemben fel kell tüntetni:

* az engedély jogosultjának, nevét, beosztását;
* az engedélyezés időtartamát (kezdő és záró időpontot);
* a kért hozzáférések, elvégezhető műveletek leírását;
* a munkahelyi feladatokat, amelyekhez a kért jogosultság szükséges;
* az esetleges korlátozásokat.

A fiókok esetében a jogosultság megadásának kérelmét az **Informatikai vezető** jóváhagyja. A kérelem jóváhagyása során a következők alapján mérlegel:

* hatályos jogszabályok;
* hatályos utasítások;
* a kérelem indokoltsága;
* a rendelkezésre álló erőforrások.

Az **Informatikai Vezető** által engedélyezett jogosultságot el kell juttatni az illetékes rendszergazdához, aki az engedély bírtokában további mérlegelés nélkül beállítja az engedélyezett jogosultságot a fiókhoz.

### Engedélyek visszavonása/felfüggesztése (3.1.1.5. [1])

Bármely, a **Szervezet** informatikai eszközeinek (hardverek, szoftverek, alkalmazások) használatával összefüggő jogosultság visszavonását vagy felfüggesztését e-mail-ben

* az alkalmazott jogviszonyának megszűnése;
* a külső vállalkozó számára biztosított jogosultság okafogyottá válása;
* jogerős fegyelmi büntetés

esetén a **Szervezet** vezetőinek kell kezdeményezniük a jogosultság beállításának elvégzésében az **Informatikai vezető** jóváhagyásával az illetékes rendszergazdánál.

A jogosultságok megadásának és visszavonásának e-mail levelezését az utólagos ellenőrzés céljából 5 évig meg kell őrizni.

## Az elektronikus információs rendszerek nyilvántartása (3.1.1.4. [1])

A **Szervezet** az elektronikus információs rendszereiről nyilvántartást vezet. A nyilvántartást elektronikus formában vezeti, és gondoskodik azok naprakészségéről.

A nyilvántartásnak minden rendszerre nézve tartalmaznia kell:

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

A különböző adatokat nem szükségszerűen egy nyilvántartásban kell tárolni, hanem logikus módon szétválasztva is lehetséges, biztosítva az össze tartozó adatok összekapcsolásának lehetőségét.

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

## Kockázatkezelés, kockázatelemzés (3.1.2. [1])

### A kockázat azonosítása

A kockázati tényezők azonosításának célja annak megállapítása, hogy melyek a **Szervezet** informatikai biztonságának célkitűzéseit veszélyeztető fő kockázatok.

A kockázatok azonosítását az **Informatikai Biztonsági Felelős** végzi el. Az **Informatikai Biztonsági Felelős** kötelessége minden olyan kockázat azonosítása, amelyek potenciális hatással lehetnek a **Szervezet** informatikai biztonságának céljaira vagy működésére, függetlenül attól, hogy azok igazgatási, szabályozási, jogi, technológiai, szállítói, emberi erőforrás-jellegű, vagy működési szempontot érintenek.

A kockázatok a következők lehetnek:

* Informatikai: az alkalmazott IT rendszerek, az informatikai infrastruktúra hibái (rendszerhiba, rendszerleállás, korlátozott rendelkezésre állás).
* Ügyviteli: az üzleti folyamatok hiányosságai, nem megfelelő szervezettség, szabályozatlanság.
* Külső hatások: gazdasági, jogszabályi, környezeti, természeti csapások vagy a harmadik fél által okozott veszteség: árvíz, földrengés, villámcsapás, rablás, betörés vandalizmus, terrortámadás.
* Humán: a munkavállalók, vezetők által – akár szándékosan – elkövetett károkozás, információ és pénz jogosulatlan eltulajdonítása, üzleti és személyiségi jogokhoz kapcsolódó titok megszerzése, megvesztegetés, tévedés vagy szakmai hozzáértés hiánya miatti hibák.
* Egyéb: az előzőkbe nem sorolható kockázati tényező.

A kockázattal kapcsolatos érdemi információk megadása, összegyűjtése érdekében rögzíteni kell a **Kockázatmenedzsment Naplóban** (továbbiakban: **KMN**) az adott kockázat jellemző adatait, amelyek a következők:

* kockázat azonosítója;
* kockázat típusa;
* kockázat rövid leírása (Mi történhet, ami rossz, mikor következhet be);
* kockázat azonosításának dátuma;
* kockázat azonosítójának neve;
* kockázat azonosítójának szervezeti egysége.

Az **Informatikai Biztonsági Felelős** vagy annak megbízottja elemzi a **KMN**-ben újonnan rögzített kockázatot és:

* megállapítást tesz a bekövetkezési valószínűség és a lehetséges kár értékére;
* kijelöli a kockázat gazdát;
* meghatározza az adott kockázathoz tartozóan a:
	+ kockázat jellemzőket,
	+ bekövetkezhető kár osztályát (1-5),
	+ bekövetkezés valószínűségi osztályát (1-5),
	+ kockázati faktort,
	+ kockázati osztály (kritikus, magas, közepes….),
	+ kockázat gazda nevét,
	+ kockázat kezelésnek határidejét.

### A kockázatok értékelése

#### A kockázat bekövetkezéséből adódó lehetséges kár értékelése

Az egyes lehetséges kockázati események bekövetkezéséből adódó lehetséges károk nagyságait 1-től 5-ig terjedő skálán, kár osztályokba kell sorolni a következő szempontok alapján:

| Kár osztály | Bekövetkezhető kár |
| --- | --- |
| **1** | **Jelentéktelen káresemény következhet be, mivel:*** személyes adatok nem sérülhetnek;
* nincs bizalomvesztés, a probléma kisebb, a Szervezeten belül marad, és azon belül meg is oldható;
* a közvetlen és közvetett anyagi kár a Szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest jelentéktelen.
 |
| **2** | **Csekély káresemény következhet be, mivel:*** személyes adat sérülhet;
* az ügymenet szempontjából csekély értékű, és/vagy csak belső (Szervezeti) szabályozóval védett adat, vagy elektronikus információs rendszer sérülhet;
* a lehetséges társadalmi-politikai hatás a Szervezeten belül kezelhető;
* a közvetlen és közvetett anyagi kár a Szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest csekély.
 |
| **3** | **Közepes káresemény következhet be, mivel:*** különleges személyes adatok, vagy nagy tömegű személyes adatok sérülhetnek;
* az ügymenet szempontjából közepes értékű, vagy a Szervezet szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett adat sérülhet;
* lehetséges társadalmi-politikai hatás, bizalomvesztés állhat elő a Szervezeten belül, vagy Szervezeti szabályokban foglalt kötelezettségek sérülhetnek;
* a közvetlen és közvetett anyagi kár a Szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest közepes.
 |
| **4** | **Nagy káresemény következhet be, mivel:*** nagy tömegű különleges személyes adat sérülhet;
* személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket);
* az ügymenet szempontjából nagy értékű, üzleti titok, vagy a Szervezet szempontjából különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet;
* a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a Szervezeten belül, a Szervezet felső vezetésében, a Szervezet vezetésében személyi konzekvenciákat kell alkalmazni;
* a közvetlen és közvetett anyagi kár a Szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest jelentős.
 |
| **5** | **Kiemelkedően nagy káresemény következhet be, mivel:*** kiemelten nagy tömegű különleges, személyes adat sérül;
* emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be;
* a nemzeti adatvagyon helyreállíthatatlanul megsérülhet;
* az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;
* a lehetséges társadalmi-politikai hatás súlyos bizalomvesztés a Szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;
* a közvetlen és közvetett anyagi kár a Szervezet költségvetését, szellemi és anyagi erőforrásait meghaladó, különösen nagy értékű üzleti titok, a Szervezet szempontjából kiemelten érzékeny információt képező adat sérül.
 |

*5. táblázat - Kár osztályok és a bekövetkezhető kár*

#### A kockázati események bekövetkezésének valószínűsége

A **Szervezet** az egyes lehetséges kockázati eseményeket azok bekövetkezési valószínűségei szerint valószínűségi osztályokba sorolja.

|  |  |
| --- | --- |
| Valószínűségi osztály (lehetséges értékek) | A bekövetkezés valószínűsége |
| **1** | Rendkívül alacsony |
| **2** | Alacsony |
| **3** | Közepes |
| **4** | Magas |
| **5** | Rendkívül magas |

*6. táblázat - Kockázati események valószínűségi osztályai*

#### A kockázatok besorolása kockázati faktor szerint:

|  |  |
| --- | --- |
| Kockázati faktor | Kockázati osztály |
| **1-2** | 1 (Nagyon alacsony) |
| **3-5** | 2 (Alacsony) |
| **6-7** | 3 (Közepes) |
| **8-14** | 4 (Magas) |
| **15-20** | 5 (Kritikus) |

*7. táblázat - Kockázatok besorolása kockázati faktor szerint*

### Intézkedési terv készítése (3.1.1.3. [2])

A kockázati naplóban rögzített kockázatok kezelésével kapcsolatban intézkedési tervet kell készíteni. Az intézkedési tervet az **Informatikai Biztonsági Felelős** és az általa kijelölt kockázatgazda (a kockázat megszűntetésének vagy csökkentésének felelőse) közösen készíti el.

#### Az intézkedési terv tartalma

Az intézkedési tervnek tartalmaznia kell az alábbi információkat:

* az adott kockázat megnevezése, azonosítója a Kockázat Menedzsment Naplóban;
* a kockázat kezelésének célja;
* a kockázat kezelésének javasolt módja;
* a kockázat kezeléséhez szükséges feladatok, felelősök és határidők;
* a kockázat kezeléséhez szükséges eszköz/ szoftver beszerzések;
* a kockázat kezelése után megmaradó kockázatok;
* a kockázat kezelését koordináló felelős.

 A kockázatkezelési intézkedések lehetséges céljai a következők lehetnek:

* **Elkerülés**: a kockázat bekövetkezési valószínűségének vagy a kockázat bekövetkezés a **Szervezetre** való hatásának kiküszöbölése. (Jellemzően magas kockázati faktorú kockázatok esetén szokták kitűzni ezt a célt).
* **Áthárítás**: az Elkerülés egy speciális esete, amikor a kockázat hatásait egy másik félre hárítjuk, pl. szerződéses kötbér, biztosítás stb. segítségével.
* **Valószínűség** **csökkentés**: a kockázat bekövetkezési valószínűségének tolerálható szintre történő csökkentése.
* **Vészforgatókönyv:** a kockázat bekövetkezése esetén a negatív hatások csökkentésére irányuló terv.
* **Tolerálás**: A túlzottan jelentős ráfordítási igény miatt kockázattal történő együttélés.

#### Az intézkedési terv elkészítésének határidei

|  |  |  |  |
| --- | --- | --- | --- |
| Kockázati osztály | Intézkedési terv kidolgozása és elfogadása | Az intézkedési terv végrehajtásának végső határideje | Az intézkedési terv végrehajtásának ellenőrzése |
| **Kritikus** | A kockázat értékelését követő 15. munkanap | Az intézkedési tervben meghatározott ütemterv szerint | 2 hetenként |
| **Magas** | A kockázat értékelését követő 20. munkanap | Az intézkedési tervben meghatározott ütemterv szerint | 2 hetenként |
| **Közepes** | A kockázat értékelését követő 30. munkanap | Az intézkedési tervben meghatározott ütemterv szerint | havonként |
| **Kicsi** | A kockázat értékelését követő 30. munkanap | Az intézkedési tervben meghatározott ütemterv szerint | havonként |
| **Nagyon kicsi** | A kockázat értékelését követő 60. munkanap | Az intézkedési tervben meghatározott ütemterv szerint | 2 havonként |

*8. táblázat - Az intézkedési terv elkészítésének határidői*

#### Kockázatkezelő intézkedések végrehajtása

A kockázatgazda által beterjesztett/kidolgozott intézkedést a **kockázatgazda** vagy az **Informatikai Vezető** terjeszti a **Szervezet Vezetője** elé jóváhagyásra. A **Szervezet** **Vezetője** által jóváhagyott intézkedési tervet a kockázatgazda végrehajtja/végrehajttatja.

Abban az esetben, ha a kockázat kezelésre az azzal történő együttélés javasolt, a kockázat kezelését annak kiemelt figyelésével kell megvalósítani.

A kockázatkezelési intézkedés végrehajtása után a Kockázat Menedzsment Naplóban frissíteni kell a kockázat valószínűségének és hatásainak értékét.

### A végrehajtás ellenőrzése, felülvizsgálat

#### A kockázatkezelési feladatok nyomon követése

Az intézkedési terv végrehajtásának nyomon követése az **Informatikai Biztonsági Felelős** feladata.

A kockázatkezelés végrehajtásának ellenőrzése során:

* nyomon kell követni és dokumentálni kell az egyes kockázatkezeléssel kapcsolatban megfogalmazott feladatok végrehajtását;
* rendszeresen jelentést kell készíteni a vezetés számára az egyes kockázatkezelési feladatok végrehajtásának státuszáról.

#### Eszkaláció

A Kockázatgazda eszkalálni köteles, ha:

* a kockázati faktor megnövekszik;
* a kockázatkezelés kitűzött céljának elérése olyan akadályba ütközik, hogy az csak vezetői szinten kezelhető.

### A kockázatkezelés lezárása

A kockázatkezelés lezárását a kockázatgazda kezdeményezésére az **Informatikai Biztonsági Felelős** hagyja jóvá és adminisztrálja a Kockázat Menedzsment Naplóban.

## Biztonsági osztályba sorolás (3.1.2.2. [1])

A 2013. évi L. törvény 7. §-ának (1) bekezdése, illetve a 9. §-ának (1) bekezdése alapján a **Szervezet** elektronikus információs rendszereit a kockázatarányos, költséghatékony védelem megvalósítása érdekében biztonsági osztályokba kell sorolni.

Az osztályba sorolást az elektronikus információs rendszereket 1-5-ig terjedő skálán az elektronikus információs rendszerben kezelt adatok bizalmassága, a sértetlensége és a rendelkezésre állása, illetve az elektronikus információs rendszer sértetlensége és rendelkezésre állása elvesztéséből fakadó jogi, társadalmi-politikai, közvetlen, illetve közvetett anyagi kár vagy hatás szempontjából külön-külön kell elvégezni.

A biztonsági osztályba sorolást minden új rendszer implementációja esetén el kell végezni, illetve minden olyan esetben, amikor változás áll be az elektronikus információs rendszerben vagy annak működési környezetében, továbbá olyan körülmények esetén, amelyek befolyásolják az elektronikus információs rendszer biztonsági követelményeit vagy állapotát.

A biztonsági osztályok megállapítása során a következő feladatokat kell elvégezni:

* adatbesorolás;
* a rendszerrel kapcsolatos kockázatelemzés;
* a rendszer elvárt biztonsági osztályának meghatározása;
* a rendszer tényleges biztonsági osztályának meghatározása;
* a biztonsági osztálybesorolás eredményének rögzítése a **Szervezet** rendszereinek nyilvántartásában;
* kapcsolódás biztosítása a 41/2015. (VII. 15.) BM rendelet szerinti 3.1.1.3 pontban foglalt intézkedési terv mérföldköveihez;
* a NEIH értesítése az osztályba sorolásról.

### Adatbesorolás

A **Szervezetben** használt egyes adatokat, adatköröket adatvédelmi szempontok alapján osztályozni kell. Az adatok besorolását bizalmasság, sértetlenség és rendelkezésre állás szerint kell elvégezni.

#### Az adatok osztályozása bizalmasság szerint

|  |  |
| --- | --- |
| Biztonsági osztályok | Jogszabállyal, belső szabályozóval szabályozott, vagy védett adat |
| **1.****(Nyilvános)** | * Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény szerint közérdekű vagy közérdekből nyilvános adatok
* Egyéb, a Szervezet által nyilvánosnak besorolt adat.
 |
| **2.****(Belső)** | * Napi operatív munkavégzéshez szükséges, vagy annak során keletkezett belső használatú adatok.
 |
| **3.****(Fokozott biztonságú)** | * Szervezet egyéb belső szabályozásban hozzáférés korlátozás alá eső adatok (pl. egyes feladatok végrehajtása érdekében keletkezett bizalmas adatok)
* Az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény szerinti személyes adatok
* Egyéb, jogszabállyal védett titok (kivétel üzleti titok, minősített adat.)
 |
| **4****(Kiemelt bizalmasságú)** | * Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény szerinti különleges adatok
* Üzleti titkok, tömeges személyes adat.
 |
| **5.****(Minősített adat)** | A minősített adat védelméről szóló 2009. évi CLV. törvény hatálya alá tartozó:* Korlátozott terjesztésű;
* Bizalmas;
* Szigorúan titkos;

minősítésű adatok. |

9. táblázat Az adatok osztályozása bizalmasság szerint

#### Az adatok osztályozása sértetlenség és rendelkezésreállás szerint

Az adatok osztályozása sértetlenség és rendelkezésre állás szerint megegyezik az adatintegritás vagy rendelkezésre állás sérülés kockázati osztályba sorolásával (6.3.2 A kockázatok értékelése).

### A rendszerrel kapcsolatos kockázatelemzés

Elemezni kell az egyes informatikai rendszerek kockázatait:

* bizalmasság;
* sértetlenség;
* rendelkezésreállás

szerint külön-külön.

### A rendszer elvárt biztonsági osztályának meghatározása

A **Szervezet** az elektronikus információs rendszere biztonsági osztályba sorolásakor az elektronikus információs rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit a rendszer funkcióira tekintettel, és azokhoz igazodó súllyal érvényesíti;

* a nemzeti adatvagyont kezelő rendszerek esetében a sértetlenség követelményét emeli ki;
* a létfontosságú információs rendszerelemek esetében a rendelkezésre állást követeli meg elsődlegesen;
* a különleges személyes adatokkal kapcsolatban alapvető igényként fogalmazza meg a bizalmasság fenntartását.

Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást, amelyet a **Szervezet Vezetője** hagy jóvá, kockázatelemzés alapján kell elvégezni.

### A rendszer tényleges biztonsági osztályának meghatározása

A rendszer tényleges biztonsági osztályának meghatározását a NEIH által kiadott táblázat alapján kell elvégezni. A táblázat letölthető a NEIH oldaláról: <http://neih.gov.hu/urlapok> ([NEIH-OVI] Osztályba sorolás és védelmi intézkedés űrlap)

### A biztonsági osztálybesorolás eredményének rögzítése a rendszer nyilvántartásban

Minden egyes osztályba sorolást követően a változást át kell vezetni az informatikai rendszerek nyilvántartásán.

### Kapcsolódás biztosítása más intézkedési tervek mérföldköveihez

Abban az esetben, ha egy informatikai rendszer nem felel meg az elvárt biztonsági osztályának megfelelő biztonsági előírásoknak, az előírások teljesülésének érdekében intézkedési tervet kell készíteni, amelynek illeszkednie kell a **Szervezet** kockázatkezelésekkel kapcsolatos intézkedési terveihez.

### A NEIH értesítése az osztályba sorolásról

Az egyes rendszerek biztonsági osztályba sorolásának eredményéről 10 munkanapon belül az Informatikai Biztonsági Felelősnek értesítést kell küldenie a NEIH számára. A rendszerek biztonsági osztályba sorolásának és állapotfelmérésének eredményét rendszerenként a NEIH által közzétett segédlet kitöltött formájában kell feltölteni. A táblázat letölthető a NEIH oldaláról: <http://neih.gov.hu/urlapok> ([NEIH-OVI] Osztályba sorolás és védelmi intézkedés űrlap)

### A biztonsági osztályba sorolás felülvizsgálata

A rendszerek kockázatelemzését és biztonsági osztályba sorolását az Informatikai Biztonsági Felelősnek dokumentált módon legalább évente, de a következő esetekben soron kívül felül kell vizsgálni:

* amennyiben változik az elektronikus információs rendszer biztonságát érintő jogszabály;
* új elektronikus információs rendszer bevezetése esetén;
* ha bármely audit során szükségessé válik kockázatelemzés elvégzése;
* a **Szervezet** státuszában változás áll be;
* a **Szervezet** által kezelt vagy feldolgozott adatok vonatkozásában változás következik be.

## Az informatikai rendszerek biztonsági követelményei

Az informatikai rendszerek integrált biztonságának kialakítása a biztonságpolitika által meghatározott szempontok szerint kell, hogy történjen. A biztonság alapvető feltétele az alkalmazást vagy szolgáltatást támogató szervezeti munkafolyamat megtervezése és megvalósítása. Az informatikai rendszerek beszerzése / üzembe állítása előtt szükség van a biztonsági követelmények meghatározására és egyeztetésére.

Informatikai projekt követelményeinek megfogalmazása során meg kell határozni az összes biztonsági követelményt. A követelményeket és szükséges megoldásokat az informatikai rendszer fejlesztésének részeként kell megindokolni, egyeztetni és dokumentálni.

### A biztonsági követelmények elemzése és meghatározása

Az informatikai beruházások előkészítési, tervezési fázisában figyelemmel kell kísérni a következő biztonsági szempontok érvényesítését:

* az informatikai rendszer által kezelendő adatoknak az információvédelem és a megbízható működés szempontjából történő elemzése és a védelmi célkitűzések meghatározása;
* az informatikai rendszer várható informatikai biztonsági osztályba sorolása az információvédelem és a megbízható működés területén;
* a jogszabályokból és a belső szabályozásból eredő kötelezettségek (felsorolása) bemutatása;
* a fizikai és a logikai védelem rendszerszintű felsorolása (bemutatása);
* a megvalósításhoz szükséges feltételrendszer meghatározása;
* a biztonsági rendszer teljes költségének becslése, ennek összehasonlítása a lehetséges kockázatokkal, károkkal;
* az informatikai biztonsági fejezetnek a tervezési dokumentumokba történő beállításáért a projektvezető, annak kijelöléséig, vagy hiánya esetén az illetékes vezető (előterjesztő) a felelős;
* a **Szervezet** minden informatikai projektje előterjesztésének tartalmaznia kell a létrehozandó (beszerzendő, fejlesztendő, átalakítandó) informatikai rendszer fizikai, logikai és adminisztratív védelmi rendszerének – a projekt keretében történő – tervezési és megvalósítási lépéseit, költségeit, felelőseit;
* az informatikai projekt jóváhagyott költségvetésében szerepelnie kell a biztonsági rendszer tervezési és megvalósítási költségeinek;
* az informatikai rendszerek részére szállított termékek esetében alapkövetelmény, hogy kiértékelt, tanúsított legyen, vagy tanúsítási eljárás alatt álljon egy elismert nemzeti tanúsító szervezetnél;
* az alkalmazott operációs rendszer meg kell feleljen minimum az ISO/IEC 15408 (Common Criteria) EAL3-as szintjének;
* az előző pontokban megfogalmazott feltételek hiánya az informatikai projektek esetében jelentősen megnöveli az információ-biztonsági kockázatokat, valamint a későbbi kiadásokat, mivel a tervezési szakaszban bevezetett intézkedések lényegesen olcsóbban foganatosíthatók, mint azok, amelyeket a bevezetés alatt vagy után valósítanak meg. Amennyiben szükséges (pl. a költségek vagy a projekt nagysága miatt) a **Szervezet** **Vezetése** megkövetelheti a független kiértékelt és tanúsított termékek használatát.

### Biztonság az alkalmazási rendszerekben

A felhasználói rendszerek integrált biztonsága kiterjed a rendszerekben tárolt felhasználói adatok illetéktelen hozzáférésének, módosításának, törlésének, nem megfelelő felhasználásának stb. megelőzésére. A rendszertervek összeállítása során mérlegelni kell a rendszerbe beépítendő automatikus ellenőrző eszközök, valamint a biztonságot támogató manuális ellenőrző eszközök szükségességét.

A felhasználói rendszerek biztonságát a következő intézkedések szavatolják:

* A felhasználói rendszerekben meg kell tervezni a megfelelő ellenőrző eszközöket és eseménynaplókat, valamint a tevékenységek naplózását. Ezeknek tartalmazniuk kell a bemenő adatok, a belső adatfeldolgozás és a kimenő adatok ellenőrzését.
* Az érzékeny, értékes vagy kritikus adatok feldolgozását végző, vagy ilyen adatokat befolyásoló rendszereknél további ellenőrző eszközökre lehet szükség. Ezeket az ellenőrző eszközöket a biztonsági követelmények és a kockázatelemzés alapján kell kiválasztani.
* Az előző két pontban meghatározott biztonsági intézkedéseket pontosan, minden részletre kiterjedően dokumentálni kell.

### A bemeneti adatok ellenőrzése

Az adatfeldolgozó rendszerekbe bevitt adatokat a lehetséges kockázatok mértékének, a rendelkezésre álló lehetőségek és a feldolgozás jellegének figyelembevételével ellenőrizni kell. A bemenő adatok ellenőrzésének eszközei a következők lehetnek:

* az ismételt adatbevitel és az ebből származó adatkarbantartási anomáliák elkerülésére írt eljárások;
* időszakos adatmező és -állomány vizsgálat, valamint a felvitt adatok hitelességének, integritásának ellenőrzése és igazolása;
* az adatbevitel alapját képező nyomtatott input dokumentumok ellenőrzése, illetve ezek engedély nélküli módosításának megakadályozása, valamint az engedélyezés kikényszerítésére írt eljárások;
* adat ellenőrzési hibák kiküszöbölését elősegítő eljárások;
* adatbevitel során, a mezőtípus kompatibilitást biztosító, illetve adattartalom helyességét ellenőrző és kikényszerítő eljárások, függvények;
* az alkalmazáshoz történő hozzáférés naplózása;
* a feldolgozásban résztvevő alkalmazottak feladatkörének és felelősségének rögzítése a munkaköri leírásokban.

### Az adatfeldolgozás ellenőrzése

A felvitt adatok pontosságát, hiánytalanságát, és integritását a feldolgozás ideje alatt a lehetséges kockázatok mértékének, a rendelkezésre álló lehetőségek és a szoftver jellegének figyelembevételével a következő intézkedésekkel kell elősegíteni:

* Az adatfeldolgozás rendszerébe ellenőrzési, hitelesítési pontokat kell beépíteni, különös tekintettel az adatmódosító-, törlő funkciók helyére.
* Adatfeldolgozási hibák esetén hibadetektáló, és a további rendszerfutást leállító eljárások beépítése a rendszerbe.
* Korrekciós programok alkalmazása a feldolgozás során felmerülő hibák korrigálására.

A folyamatba épített ellenőrzés ellátásáért a **Szervezet Vezető**je által kijelölt személy a felelős.

#### A sértetlenség biztosítása

A helyesen rögzített adatok is elromolhatnak akár a feldolgozás hibáitól, akár szándékos tevékenységektől. A rendszerekben az ilyen meghibásodások felismerése érdekében a lehetséges kockázatok mértékének, a rendelkezésre álló lehetőségek és a szoftver jellegének figyelembevételével érvényesítő ellenőrzéseket kell beépíteni. Az alkalmazások tervezésével lehetőség szerint gondoskodni kell arról, hogy a korlátozások megvalósítása valóban minimalizálja a sértetlenség elvesztésére vezető feldolgozási hibák kockázatát. Biztonsági szempontok alapján a lehetséges kockázatok mértékének, a rendelkezésre álló lehetőségek és a szoftver jellegének figyelembevételével meg kell tervezni:

* az adatváltoztatást megvalósító hozzáadó és leválasztó funkciók helyét és használatát a végrehajtó programokban;
* azokat az eljárásokat, amelyek megakadályozzák, hogy a programok rossz sorrendben, vagy korábbi feldolgozásban előállt meghibásodás után lefussanak;
* a helyes programok használatát a meghibásodás utáni visszatérésre annak érdekében, hogy az adatokat helyesen/pontosan dolgozzuk fel.

#### Vezérlő és ellenőrző eljárások

A szükséges intézkedések attól függenek, hogy milyen az alkalmazás természete, és hogy a **Szervezet** tevékenységére a hibás adat milyen hatással lehet. Esettől függően a következő ellenőrzések felvételét kell mérlegelni:

* eseményenkénti ellenőrzéseket;
* az állományfrissítések ellenőrző összegeit;
* program(futás)onkénti ellenőrzéseket;
* a rendszer által keltett adatok érvényesítését;
* a központi és a távoli számítógépek között a feltöltött vagy letöltött adatok vagy szoftverek ellenőrzéseit;
* az ellenőrzéseket, amelyek szavatolják, hogy az alkalmazási programokat időben lefuttatták;
* az ellenőrzéseket, amelyek szavatolják, hogy az alkalmazási programokat a helyes sorrendben futtatták le, és hogy a programokat meghibásodáskor félbeszakították, amíg a felmerült nehézséget meg nem oldották.

### Az üzenetek hitelesítése

Az üzenethitelesítés alkalmazása esetén észlelhető a továbbított elektronikus üzenet integritásának megváltozása.

Alkalmas módként kriptográfiai módszereket alkalmazhatóak az üzenethitelesítés megvalósítására. Elvárások az üzenethitelesítés, valamint az elektronikus aláírás kialakítása kapcsán:

* az azonosítás és hitelesítés keretében a hozzáférést ellenőrizni kell;
* a hitelesítést a felhasználó és a rendszer között egy, a felhasználó által megnyitott, védett csatornán keresztül kell biztosítani.

### A kimenő adatok ellenőrzése

Az adatfeldolgozás rendszerében ellenőrizni kell a kimenő adatokat. A kimenő adatok biztonsága érdekében a következő védelmi eljárásokat kell alkalmazni:

* integritás ellenőrzés;
* adattartalom meglétének, értékének ellenőrzése;
* a megfelelő minősítés meglétének ellenőrzése;
* a kimenő adatok értékelésében és ellenőrzésében résztvevők feladatainak és felelősségének meghatározása

## Rendszer és Szolgáltatás beszerzés eljárásrendje (3.1.3.1. [3])

Az eljárásrend célja, hogy a **Szervezet** ezt az eljárásrendet alkalmazza minden olyan esetben, amelyben informatikai szolgáltatást vagy eszközöket szerez be vagy, ha rendszerfejlesztési tevékenységet végez vagy végeztet. Az eljárásrend a beszerzést szabályozó utasítások folyamatait figyelembe véve írja elő a biztonsági feladatokat az elektronikus információs rendszerek beszerzésére, figyelembe véve azok biztonsági osztályba való sorolási szintjét.

Az eljárásrendben kerülnek rögzítésre mindazok a követelmények, amelyeket be kell tartani a beszerzés során, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.), és az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet alapján.

### A rendszerre vonatkozó dokumentáció

Az alkalmazás fejlesztés során a fejlesztőtől – függetlenül attól, hogy külső, vagy belső fejlesztő – a következő dokumentumokat kell megkövetelni:

* fizikai és logikai rendszerterv;
* rendszerbiztonsági terv;
* felhasználói kézikönyv;
* üzemeltetési kézikönyv;
* működés-folytonossági terv (BCP);
* topológiai ábra
* mentési utasítás
* az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentáció, amely tartalmazza:
	+ a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését,
	+ a biztonsági funkciók hatékony alkalmazását és fenntartását,
	+ a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket.

Meg kell követelni az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amelynek tartalmaznia kell:

* a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját;
* a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit;
* a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához;
* katasztrófahelyzet kezelési terv (DRP - akár közös dokumentumban a BCP-vel).

Az infrastrukturális rendszerfejlesztések alkalmával az alábbi dokumentációkat kell elkészíteni:

* rendszerterv;
* rendszerbiztonsági terv;
* üzemeltetési utasítás;
* az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely tartalmazza:
	+ a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését,
	+ a biztonsági funkciók hatékony alkalmazását és fenntartását,
	+ a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket.

Meg kell követelni az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amelynek tartalmaznia kell:

* a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját;
* a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit;
* a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához.

Szerződéses követelményként meg kell határozni, hogy a fejlesztő, szállító hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések terv- és megvalósítási dokumentációit, köztük a biztonsággal kapcsolatos külső rendszer interfészek leírását, a magas, és alacsony szintű biztonsági tervet, - amennyiben azzal a szállító rendelkezik - a forráskódot, fejlesztési kézikönyvet és futtatókörnyezetet.

A szerződésekben kötelezni kell a szállítókat arra, hogy már a fejlesztési életciklus korai szakaszában meghatározzák a használatra tervezett funkciókat, protokollokat és szolgáltatásokat.

Az **IBF**-nek véleményezési joga van minden olyan beszerzés esetében, amelynek közvetlen vagy közvetett hatása lehet az informatikai biztonságra.

#### Külső elektronikus információs rendszerek szolgáltatásai (3.1.3.6. [2])

A szolgáltatási szerződésekben ki kell kötni, hogy a szolgáltatási szerződés alapján igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek a **Szervezet** elektronikus információ-biztonsági követelményeinek.

A **Szervezetnek** külső és belső ellenőrzési eszközökkel ellenőriznie kell, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket. Az ellenőrzést az **IBF** végzi szúrópróba-szerűen.

### Külső információs rendszerek szolgáltatásai (3.2.3.6 [2])

A szolgáltatási szerződésesekben ki kell kötni, hogy a szolgáltatási szerződés alapján igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek a **Szervezet** elektronikus információ-biztonsági követelményeinek.

Külső és belső ellenőrzési eszközökkel ellenőrizni kell, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

Kötelezni kell a szolgáltatót arra, hogy meghatározza a szolgáltatások igénybevételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat.

## Működés-(Ügymenet) folytonosság tervezés (3.1.4. [2], 3.1.4.2. [2])

A **Szervezet** működés-folytonossági tervet készít, amely segítséget nyújt abban, hogy kritikus üzleti folyamatok sérülése vagy leállása esetén a lehető legkisebb kieséssel lehessen megvalósítani a visszaállást. A működés folytonossági tervének az alábbi esetekre kell kiterjednie:

* nem tervezett szolgáltatás leállás;
* hosszan tartó szolgáltatás leállás;
* olyan leállás, amit a normális probléma menedzsment eljárásokon belül nem lehet megoldani;
* olyan leállás, amely komoly károkat vagy veszteségeket okoz.

A működés folytonosság tervben a következő információknak kell szerepelniük:

* eljárások és erőforrások listája, amit a visszaállítás során fel kell használni;
* részletes leírás, amit a felelősök végre tudnak hajtani;
* azon partnerek azonosítása, akik bevonása indokolt lehet a visszaállítás során;
* a zavar elkerülését segítő részletes útmutatók és a tesztelési eljárások;
* a visszaállításhoz szükséges információk listája;
* a tartalék helyen történő működés szabályai, ha az elsődleges hely nem elérhető;
* az elsődleges helyre való visszatérés eljárásai.
* kritikus, az elektronikus információs rendszer alapfunkcióit támogató rendszerelemek meghatározása;
* alapfunkciók újrakezdésének időpontját a működés-folytonossági terv aktiválását követően;
* hogyan tartja fenn a **Szervezet** az előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is.

A működés folytonossági tervet évenként tesztelni kell. A tesztelés eredményét értékelni kell és az értékelés eredményeképpen el kell végezni a szükséges módosításokat. Az **Informatikai Biztonsági Felelős** fél évenként ellenőrzi, hogy az informatikai tartalékok folyamatosan működőképes állapotban álljanak rendelkezésre.

A működés folytonossági tervet legalább évente felül kell vizsgálni és aktualizálni kell. Aktualizálni kell továbbá minden olyan esetben, amikor a személyi információs rendszerben olyan változás következik be a **Szervezet** életében, amely változásokat tesz szükségessé.

### A folyamatos működésre felkészítő képzés (3.1.4.3. [3])

A **Szervezet** az elektronikus információs rendszer folyamatos működésére felkészítő képzést tart a felhasználóknak, szerepkörüknek és felelősségüknek megfelelően:

* szerepkörbe vagy felelősségbe kerülésüket követő meghatározott időn belül;
* A folyamatos működésre felkészítő képzésben szimulált eseményeket kell bemutatni, hogy elősegítse a személyzet hatékony reagálását a kritikus helyzetekben.
* a képzéseket évente el kell végezni az elektronikus információs rendszer mindenkori állapotának megfelelően.

### Az elektronikus információs rendszer mentései (3.1.4.8.[3])

Az elektronikus információs rendszer mentéseinek szabályait rendszerenként kell meghatározni az alábbiak figyelembevételével.

A mentési és visszaállítási eljárásokat úgy kell kialakítani, hogy a **Szervezet** rendszerei előre nem látható esemény bekövetkezte után szükség esetén helyreállíthatók legyenek, ezáltal ne sérüljenek az információk, adatok, rendszerek rendelkezésre állásának kritériumai.

Az adatmentésnek és archiválásnak mindig a lehető legfrissebbnek kell lennie. A mentés gyakoriságát ennek megfelelően kell meghatározni. Rögzíteni kell a mentések végrehajtásának idejét, módját és felelősét. Minimálisan a következő mentéseket kell elvégezni:

* a szervereken tárolt adatokról automatikus napi inkrementális mentést kell készíteni;
* A mentésekért felelős rendszergazdának a központi szerverek adattartalmáról napi heti és havi inkrementális, mentéseket és három havonta teljes, (ún. 3 generációs) mentést kell készítenie.
* A tranzakció alapú rendszerek esetén tranzakció alapú mentést kell készíteni, ami lehetővé teszi a tranzakció helyreállítást

A felelős informatikus köteles esetenként a mentések elvégzését és megbízhatóságát ellenőrizni.

A **Szervezet** meghatározott gyakorisággal mentést végez az elektronikus információs rendszerben tárolt felhasználószintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.

Meghatározott gyakorisággal elmenti az elektronikus információs rendszerben tárolt rendszerszintű információkat, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.

Meghatározott gyakorisággal elmenti az elektronikus információs rendszer dokumentációját, köztük a biztonságra vonatkozókat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.

Megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen.

#### Mentési eszközök

Biztosítani kell, hogy a mentett adatok mindig vissza olvashatóak legyenek. Ezért a mentéseket olyan eszközökkel kell elvégezni, amelyek garantálják a mentett adatok visszaolvashatóságát. Időnként (minimum évenként) próba visszatöltést kell megvalósítani az alkalmazott eszközök és módszerek megbízhatóságának ellenőrzése céljából.

A mentések elvégzéséhez biztosítani kell a megfelelő számú adathordozó egységet. Folyamatosan figyelemmel kell kísérni a mentendő adatmennyiség változását, és ennek megfelelően kezdeményezni új adathordozók beszerzését. Minden médiatípus esetén legalább 10 % tartalékot szükséges tartani.

A mentéshez használt mentési médiák használati idejét a gyártó által megadott élettartam figyelembevételével, 10 %-os biztonsági tartalékkal javasolt meghatározni. Az élettartamot figyelembe kell venni mind a többszöri felhasználásnál, mind pedig a hosszú távon megőrzendő adatok tárolásánál. Az élettartamok figyelését a mentésért felelős munkatársaknak kell elvégezniük. Amennyiben egy média élettartama meghaladta a használati időt, a mentésért felelős munkatársnak kell kezdeményeznie a média selejtezését, és az új média beszerzését.

#### A mentett adatok tárolása

A mentéseket mindig biztonságos helyen kell tárolni. Biztosítani kell, hogy a mentett állományok csőtörés, tűz vagy lopás során ne semmisülhessenek meg. Ezért a biztonsági mentéseket tűzbiztos páncélszekrényben kell tárolni.

A biztonsági mentéseket és archiválásokat tartalmazó adathordozókat minden esetben a szervertől elkülönített helyiségben elzárva kell őrizni.

Tekintettel arra, hogy a **Szervezet** rendszereinek mentései olyan adatokat tartalmazhatnak, amelyek jogszabályi előírás alapján adatvédelmi szempontból érzékenyek szükséges, hogy a mentés során ezek az adatok titkosítva vagy illetéktelenek számára elérhetetlenül kerüljenek tárolásra.

Javasolt, hogy az adathordozók számmal és vonalkóddal is azonosíthatók legyenek. Az adathordozókkal végzett tevékenységeket az azonosító számhoz kötve ajánlatos dokumentálni. Amennyiben nem áll rendelkezésre olyan technika, amellyel a mentési média címkézése a fent említett módon megtehető, kiemelt figyelmet kell fordítani az egyes mentési elemek egyedi azonosítására.

#### Visszatöltési eljárások

Abban az esetben, ha visszatöltésről nem készül elektronikus naplóállomány, a visszatöltési tesztekről vagy az üzemelő rendszerbe történő visszatöltésről Jegyzőkönyvet kell készíteni a következő tartalommal:

* visszatöltött rendszerek;
* visszatöltés időpontja;
* visszatöltést végző neve;
* visszatöltött adatmennyiség, amennyiben ez ismert;
* visszatöltési idő (kezdés/vég időpont);
* visszatöltés során szerzett tapasztalatok, észrevételek.

A visszatöltési tapasztalat alapján, szükség esetén elvégzendő a visszatöltéshez kapcsolódó dokumentációk frissítése is. A visszatöltési idő összehasonlítandó a korábbi tesztek eredményével, hogy a visszatöltési időben bekövetkező kedvezőtlen trendek időben észlelhetők legyenek.

#### Mentési feladatok

A mentési tevékenységgel megbízott felelőst vagy alvállalkozót az Informatikai Vezető jelöli ki. A mentésért felelős személy/alvállalkozó feladata:

* mentések ütemezése;
* mentési job-ok beállítása (honnan - hova és mit mentsen);
* mentések elvégzése;
* mentési média ellenőrzése és rendelkezésre állás biztosítása;
* mentés folyamatának ellenőrzése;
* mentés eredményének ellenőrzése.

A mentéseket lehetőleg úgy kell elvégezni, hogy azzal a felhasználók munkáját ne akadályozzák. Online rendszerek esetén „hideg” mentést ajánlott alkalmazni.

A rendszergazda feladata ellenőrizni, hogy a meghatározott mentési rend alapján az adatminősítésnek megfelelően a visszaállítási eljárások során is csak az arra jogosult személyek férhessenek hozzá a visszaállítandó adatokhoz.

#### Mentési naplók

A mentések végrehajtásáról naplót kell vezetni, amelynek a következőket kell tartalmaznia:

* a mentés tartalmát;
* a mentés időpontját;
* mentés jellegét (teljes mentés, inkrementális kumulatív, inkrementális differenciált stb.);
* a mentés eredményét (sikeres / sikertelen, hiba oka).

Amennyiben a mentést mentőrendszerrel végzik, a mentési naplót a mentőrendszer automatikusan generálja. A mentési naplókat ebben az esetben is, - a mentőrendszer nélkül is - olvasható formátumban kell tárolni, a mentésekkel azonos biztonsági körülmények között.

Amennyiben a mentésről az adott rendszer nem készít automatikus mentési naplót, a mentés tételes dokumentálása a mentésért felelős személy feladata és felelőssége. A tárolásra, valamint kezelésére vonatkozó előírások ebben az esetben is érvényesek.

A biztonsági eseménynaplókat ajánlott 1 évre visszamenőleg, a napi mentéseket minimum 1 hétig, az egyedi mentéseket pedig a mentést elrendelő **Szervezet** Vezetője utasításának megfelelő ideig őrizni. Ha az előírt mentéseket valamely okból nem lehet megvalósítani, már meglévő korábbi mentéseket nem szabad törölni.

Az **IT Üzemeltetésért Felelős (Vezető)** a mentési média gyártóinak ajánlását figyelembe véve kialakítja az ellenőrzési rendet, amely alapján a mentéseket ellenőrizni kell sértetlenségükkel kapcsolatban. Ez magába foglalja az adathordozókat, melyeken a mentett anyagokat tárolják. Ezeket megbízhatósági szempontok alapján szintén ellenőrzés alá kell vonni.

### Minősített adatok, elektronikus dokumentumok tárolása

Biztosítani kell, hogy a tárolóeszközökön levő programok, és adatállományok listája mindig az érvényes állapotot tükrözze vissza. Ezt a dokumentumot a biztonsághoz kapcsolódó többi dokumentummal együtt, azokkal azonos biztonsági szinten kell őrizni.

Minősített adatokat az adathordozókon rejtjelezve kell tárolni és szükség esetén továbbítani, amennyiben az adathordozók védelme máshogy nem oldható meg.

Az elektronikus dokumentumokat oly módon kell megőrizni, amely kizárja az utólagos módosítás lehetőségét, a törlési határnapig folyamatosan biztosítja a jogosultak által a hozzáférhetőséget, valamint az elektronikus dokumentumok értelmezhetőségét (olvashatóságát). Az elektronikus dokumentumokat védeni kell a jogosulatlan hozzáférés, módosítás, törlés vagy megsemmisítés ellen.

Dokumentumba kell foglalni, hogy mely adatállományok és programok nem változtathatók meg, illetve, ha erre sor kerül, akkor az, hogy kinek az engedélyével (Informatikai Vezető és/vagy területi vezető) és ki által (rendszeradminisztrátor, rendszergazda) végezhető el. A változtatást lehetőleg a tárolóeszközön kialakítható fizikai írásvédelemmel kell megakadályozni.

Ha az utólagos módosítás lehetőségének kizárása úgy történik, hogy az elektronikus dokumentumot fokozott biztonságú elektronikus aláírással vagy minősített elektronikus aláírással látják el, és a megőrzésre kötelezett személy a megőrzési kötelezettségének maga tesz eleget, úgy köteles az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény alapján a Nemzeti Média- és Hírközlési Hatóság által határozatban közzétett mindenkori biztonságos kriptográfiai algoritmussal ellátott időbélyegzőt elhelyeztetni az elektronikus dokumentumon olyan szolgáltatóval, amely e szolgáltatást minősített szolgáltatóként nyújtja.

## Biztonsági események figyelése és kezelése (3.1.5.)

### Biztonsági események figyelése (3.1.5.4. [3], 3.1.7.1. [3])

A **Szervezet** minden informatikai eszközén, folyamatosan figyelni kell a rendszerek esetleges hibaüzeneteit. A felhasználóknak figyelemmel kell kísérni a működési zavar tüneteit, a képernyőn megjelenő üzeneteket. A hiba elhárítására szükség esetén a felhasználó vegye fel a kapcsolatot az illetékes informatikai munkatárssal.

Minden az informatikai rendszereket érintő vagy az informatikai rendszerekkel összefüggésbe hozható biztonságot veszélyeztető eseményt vagy annak gyanúját haladéktalanul jelenteni kell az Informatikai Vezetőnek és az érintett informatikusnak, illetve mindent meg kell tenni a szükséges bizonyítékok összegyűjtésére.

### Biztonsági események priorálása, reagálás a biztonsági eseményekre

A biztonsági incidenseket a következők szerint kell priorálni és reagálni:

Az **1. prioritású** incidensek kivizsgálását és elhárítását munkaidőben az észlelést követően azonnal, munkaidőn túl 4 órán belül meg kell kezdeni:

* határsértés és illegális tevékenység észlelése (behatolás),
* vírus-vészhelyzet (tömeges fertőzés), vagy központi vírusvédelmi eszköz kiesése,
* adminisztrátori jogosultságok sérülése,
* rendelkezésre állás szerint 3-as vagy ennél magasabb biztonsági osztályba sorolt rendszer, vagy rendszer elemek teljes kiesése,
* Informatikával összefüggésbe hozható bűncselekmények.

A **2. prioritású** incidens elhárítását munkaidőben az észlelést követően azonnal, munkaidőn kívül 6 órán belül meg kell kezdeni, ha az 1. prioritású incidens elhárítását nem akadályozza:

* ismétlődő vírusfertőzés, vagy vírusdefiníciós állomány nem frissülése,
* felhasználói jogosultságok sérülése,
* rendelkezésre állás szerint 2-es biztonsági osztályba sorolt rendszer, vagy rendszer elemek kiesése,
* „Titkos” információk bizalmasságának, sértetlenségének elvesztése,
* vétségek.

A **3. prioritású** incidensek kivizsgálását munkaidőben az észlelést követően kettő órán belül, munkaidőn kívül 8 órán belül meg kell kezdeni. Ilyen például a/az:

* egyszeri vírusfertőzés, vagy helyi vírusvédelmi eszköz kiesése,
* rendelkezésre állás szerint 1-es biztonsági osztályba sorolt rendszer, vagy rendszer elem kiesése
* „Szolgálati használatra” minősítésű információk bizalmasságának, sértetlenségének elvesztése,
* kisebb jogosultsági incidensek (felhasználó elfelejtette a jelszavát, vagy az lejárt stb.),
* törvényi szabálysértések.

A **4. prioritású** incidensek kivizsgálását kezelését a folyamatban levő magasabb prioritású incidensektől függően kell megkezdeni. Ilyen például a:

* vírusvédelmi menedzsment eszközök kiesése,
* felügyeleti és menedzsment eszközök,
* munkaállomás működésével kapcsolatos működési hibák,
* belső szabály- és eljárássértések,
* felhasználói hibák.

Az incidensek priorálása az **Informatikai Vezető** vagy az **Informatikai Biztonsági Felelős** feladata.

### A biztonsági események kezelése (3.1.5)

#### Általános alapelvek

Informatikai biztonsági incidens előfordulása esetén az abban érintett alkalmazottaknak és külső vállalkozónak törekedni kell arra, hogy a biztonsági események, zavarok okozta károk minimálisak legyenek, valamint a biztonsági események folyamatosan nyomon legyenek követve, és a megfelelő következtetéseket az illetékesek levonják. Mérsékelni kell a biztonságot befolyásoló események és működési zavarok következményeit, nyomon kell követni az eseményeket, biztosítani kell a mielőbbi normális üzemre való visszaállást és a tapasztalatokat írásban kell megfogalmazni.

**Amennyiben a rendszerhibát vélhetően külső, illetéktelen beavatkozás, vagy vírustámadás okozta, az érintett munkaállomást, számítógépet / alhálózatot le kell választani a hálózatról, szükség esetén ki kell kapcsolni.** Ilyen esetekben fokozottan figyelni kell a hordozható adathordozókra is, melyeket az illetékes informatikai munkatársnak vizsgálat céljára át kell adni.

A meghibásodott számítógépben használt adathordozók kizárólag a biztonsági ellenőrzést követően használhatók más számítógépekben.

A biztonsági eseményekről tájékoztatást kell küldeni:

* 1-es és 2-es prioritás esetében az Informatikai Vezető észrevételeivel kiegészítve a **Szervezet** vezetésének;
* 3. és 4. prioritás esetében az Informatikai Vezető számára;
* 1-es és 2-es prioritás esetében a Belügyminisztérium Nemzeti Elektronikus Információ-biztonsági Hatóság számára.

#### Az incidenskezelés folyamata (3.1.5.1 [3])

Annak érdekében, hogy az informatikai biztonság folyamatosan, minden területen a kívánt biztonsági szinten működjön, a következőket kell érvényesíteni a napi munka során:

* A biztonsági incidenseket észleléskor – egykapus rend kialakításával – jelenteni kell az Informatikára a (hibabejelento@xxxx.hu) e-mail-en, vagy a HELPDESK-en. Ha a hiba jellegéből adódón e-mailben nem lehetséges - telefonon kell megtenni.
* A bejelentés fogadása után, ha az informatika önálló hatáskörben nem tudja kezelni a felmerült problémát értesíti az illetékes support munkatársat vagy alvállalkozót.
* Amennyiben probléma megoldható e-mailben nyújtott válaszadással is, a leírt lépéseket a felhasználónak pontról-pontra kell végrehajtania. Amennyiben a felhasználónak küldött problémamegoldó e-mailre 2 napon belül nem érkezett válasz, akkor a problémát lezártnak kell tekinteni.
* Ha a hiba nem oldható meg távolról, a hiba elhárításával megbízott munkatárs/alvállakozó felkeresi a kezdeményező felet, és a helyszínen hárítja el a hibát. Ha a hiba nem hárítható el a helyszínen, a munkatárs/alvállakozó az eszközt dokumentáltan átveszi, és elszállítja hibaelhárításra.
* Távoli segítségnyújtás során a probléma elhárítását végző a felhasználó számítógépe felett, a felhasználó engedélyével ideiglenesen átveheti az irányítást, illetve megtekintheti annak tartalmát. Ilyenkor a felhasználó képernyőjére, aktuális folyamataira az adott munkatársnak/alvállalkozónak teljes rálátása és irányítási lehetősége van.
* A biztonsági incidenseket dokumentálni szükséges (IBF) a következők figyelembevételével:
	+ a rögzített incidensekből statisztikai adatként ki lehessen nyerni az egyes fenyegetettségek bekövetkezési valószínűségét (a kockázatelemzéshez szükséges),
	+ felhasználói incidensekből statisztikailag ki lehessen nyerni az elkövetési magatartást,
	+ üzemeltetési incidensek esetén statisztikailag ki lehessen nyerni az szolgáltatásokra vonatkozó incidensek számosságát,
	+ a biztonsági incidensekből folyamatosan levont tapasztalatokat vissza lehessen csatolni a védelmi rendszer tervezése, szervezése folyamataira.
* A szerver oldali és hálózati hibák a felhasználók nagy többségét érintik. Ezen hibaelhárítás a végfelhasználói prioritással szemben előnyt élvez, ezért szükség esetén a végfelhasználói hibaelhárítási folyamat az Informatikai Vezető döntésére felfüggesztendő.
* Az incidensek priorálása az Informatika feladata, az Informatika munkatársainak ezen irányú képzéséért az **Informatikai Biztonsági Felelős** felel. Abban az esetben, ha az incidenst az adott területen illetékes rendszergazda észleli és jelenti be, az incidens priorálása az ő feladata. Ebben az esetben bejelentés alkalmával az Informatika felé megadja az incidens prioritását is.

### Képzés a biztonsági események kezelésére (3.1.5.9. [3])

A **Szervezet** biztonsági eseménykezelési képzést biztosít az elektronikus információs rendszer felhasználóinak a számukra kijelölt szerepkörökkel és felelősségekkel összhangban;

a képzést a biztonsági eseménykezelési szerepkör vagy felelősség kijelölését követő, meghatározott időtartamon belül, vagy amikor ezt az elektronikus információs rendszer változásai megkívánják, vagy meghatározott gyakorisággal (legalább évente) tartja.

### Informatikai incidensek nyilvántartásba vétele (Segítségnyújtás a biztonsági események kezeléséhez) (3.1.5.7 [3])

Az informatikai incidenseket nyilvántartásba kell venni. A nyilvántartást úgy kell vezetni, hogy abból statisztikai információkat lehessen kinyerni az egyes fenyegetettségekre, illetve a következő rendszerelemekre vonatkozóan: bekövetkezési gyakoriság, éves rendelkezésre állási idő, kiesési idő.

A statisztikákat évente elemezni kell, és az Informatikai Vezetőnek meg kell állapítania, hogy:

* melyek az adott incidensek bekövetkezési tendenciái;
* elfogadható mértékű-e (gyakoriságú) az incidens;
* szükséges-e a kontrollokon változtatni, szigorítani, hogy az adott incidens bekövetkezési valószínűsége csökkenjen.

Az incidensek bejelentésével és kezelésével kapcsolatban a felhasználók számára segítséget és tájékoztatást a Polgármesteri Kabinet informatikai munkatársai, valamint az intézményben bevezetett automatizált támogató eszközök/mechanizmusok adnak.

## Emberi tényezőket figyelembe vevő – személy – biztonság (3.1.6., 3.3.1.4. [2])

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

### Munkakörök, feladatkörök biztonság alapú besorolása (3.1.6.2. [3])

Minden **Szervezetbeni** munkakört, vagy **Szervezethez** kapcsolódó feladatot be kell sorolni biztonsági szempontok alapján a következő kategóriákba:

* **ALAP BIZTONSÁGI OSZTÁLY** (Nem vezető beosztású, nem bizalmas adatokkal történik a feladat(ok) végrehajtása, kritikus rendszerekhez hozzáférés nem szükséges.)
* **FOKOZOTT BIZTONSÁGI OSZTÁLY** (Nem vezető beosztású, nem bizalmas adatokkal történik a feladat(ok) végrehajtása, kritikus rendszerekhez hozzáférés szükséges.)
* **KIEMELT BIZTONSÁGI OSZTÁLY** (Vezető beosztású, bizalmas adatokkal történik a feladat(ok) végrehajtása.)

A munkaköri és feladat besorolásokat rendszeresen felül kell vizsgálni és szükség esetén megfelelően módosítani kell.

### Személyi biztonság a munkaerő felvételénél

Az emberi hibák, lopás, csalárd magatartás vagy a létesítmények és az eszközök nem megfelelő használata során fellépő, az előírások szándékos vagy véletlen megsértéséből eredő biztonsági kockázatokat mérsékelni kell, a következők szerint:

* A biztonsági követelményeket a munkaerő-felvételnél, a munkaszerződésekben, valamint a munkaerő foglalkoztatása során egyaránt érvényesíteni kell.
* A munkaerő-felvételi eljárás során – törvényes keretek között – olyan vizsgálatokat kell lefolytatni, melyek egyértelmű képet adnak a jelentkező informatikai biztonság oldaláról tekintett alkalmasságáról. Ez különösen fontos az informatikai biztonság szempontjából kiemelt fontosságú munkakörök esetén.

### Adatvagyon kezelése, hozzáférése

Az adatok kezelésével, illetve a számítógépes rendszer üzemeltetésével kapcsolatos feladatok ellátására felhatalmazott munkavállalók az adatokhoz csak a feladatuk ellátásához szükséges mértékben férhetnek hozzá.

A **Szervezet** belső szervezeti egység vezetője az adott szervezeti egységnél keletkező valamennyi adathoz korlátozás nélkül hozzáférhet.

Az adatvagyon felhasználása, elérése, módosítása, másolása, törlése kizárólag a felhasználónak személyre szabottan biztosított jogosultságnak megfelelően történhet.

Minden felhasználó az adatvagyont köteles úgy kezelni, hogy az teljes mértékben megfeleljen az általa ellátott feladatok jellegének, illetve célkitűzéseknek.

### Jogosult felhasználók

Az adatvagyont kizárólag a **Szervezet** felhasználói érhetik el. A felhasználók azonosítóit a **Szervezet** használatában lévő szervereken kialakított címtárban kell elhelyezni, és azonosítani.

A **Szervezet** belső szervezeti egységének vezetője új dolgozó munkába lépését megelőzően írásban köteles a szervezeti egységhez tartozó munkavállalóra vonatkozóan a hozzáférési jogosultság mértékét meghatározni. Amennyiben a hozzáférési jogosultság mértékét utólag módosítani szükséges, fenti kötelezettségnek a módosításra okot adó körülmény felmerülésétől számított 5 munkanapon belül kell eleget tenni.

A jogosultsági szintekről az munkatársak javaslata alapján a **Szervezet** Vezetője rendelkezik.

Ha az adatkezelés folyamata több belső szervezeti egységet is érint, akkor a hozzáférési jogosultság mértékének meghatározása a **Szervezet Vezetőjé**nek hatáskörébe tartozik.

A munkavállaló köteles munkája során gondoskodni az adatok illetéktelen hozzáférése, nyilvánosságra hozatala megakadályozásáról.

### Informatikai biztonság a munkaköri leírásokban

A munkaköri leírásnak tartalmaznia kell az adott feladatkörre vonatkozó, az informatikai biztonsággal kapcsolatos követelményeket is, a felelősség egyértelmű megjelölésével.

* A rendszerek funkcionalitásait úgy kell meghatározni, hogy azok teljes terjedelmükben hozzárendelhetők legyenek a munkakörökhöz, és ezáltal el lehessen azokat határolni egymástól, hogy minden felhasználó csak a szigorúan rá vonatkozó feladatot hajtsa végre.
* Az informatikai biztonság szempontjából elengedhetetlen a humánerőforrás-gazdálkodási és a biztonsági szakterületek folyamatos együttműködése a be- és kiléptetési folyamatokkal kapcsolatban. A be- és kilépéskor a hozzáférési jogosultságokat is meg kell határozni, és azokat a kellő időben érvényesíteni kell.

### Személyi biztonság a jogviszony alatt (3.1.6.1. [3])

A jogviszony fennállása alatt folyamatosan gondoskodni kell arról, hogy a felhasználók tudatában legyenek az informatikai biztonság fenyegetéseinek, és motiválva legyenek a **Szervezet** információvédelmi szabályzatainak és intézkedéseinek a betartására. A felhasználók legyenek felkészítve a biztonsági eljárásokról és az adatfeldolgozó eszközök helyes használatáról a lehetséges biztonsági kockázatok minimalizálása érdekében.

Amennyiben a **Szervezet** elektronikus információs rendszereivel kapcsolatba kerülő személy nem a **Szervezet** tagja, akkor a munkatársakkal szembeni elvárásokat a tevékenység alapját képező jogviszonyt megalapozó szerződésben kell rögzíteni vagy hivatkozni.

### Viselkedési szabályok az interneten (3.1.6.9. [1])

A **Szervezet** internet használati jogokkal rendelkező felhasználói a munkájukkal kapcsolatban használhatják a **Szervezet** által biztosított internet szolgáltatást. Az internet szolgáltatásait azonban erre vonatkozó különleges engedély hiányában csak munkahelyi eszközökön és csak a munkahelyi feladatok ellátására szabad igénybe venni.

A felhasználók a **Szervezet** nevében csak előzetes engedéllyel tölthetnek fel internetre adatokat, anyagokat.

A **Szervezet** tulajdonát képező adatbázisok tartalmának interneten keresztül történő hozzáférésének lehetővé tétele csak az erre felhatalmazott felelős (adatgazda) írásos engedélyével megengedett. Az engedély megadása ilyen esetben vonatkozhat egyedi esetre vagy egyes rendszerekkel kapcsolatos feladatok elvégzésére az arra felhatalmazott munkatársak részére.

Az internet magán célú használata kizárólag **Szervezet Vezetőjének** előzetes engedélyezése alapján lehetséges. Ebben az esetben az alábbi szabályokat kell betartani:

* tilos a pornográf, online játék, fogadási oldalak, csevegő oldalak, letöltő oldalak és törvénybe ütköző tartalmakat szolgáltató oldalak látogatása.
* Az internetről magán céllal tilos fájlokat letölteni.
* Informatikai biztonsági megfontolásokból tilos a **Szervezetben** a csevegő és azonnali üzentküldő programok használata. Ezen programok rezidens futtatása tilos. Kivétel ez alól a **Szervezet** által esetlegesen biztosított hasonló szolgáltatást nyújtó szoftver **Szervezeten** belüli használata.

### E-mail használat

A belső hálózaton hozzáférhető levelezőrendszer munkaeszköznek minősül, adattartalmának ellenőrzésére a munkáltató jogosult. A levelezőrendszer magáncélú használata korlátozott keretek között biztosított az alábbiakban foglaltak szerint.

A Szervezeti levelezőrendszer magáncélú levelezésre nem használható. A magáncélú használatot is érintő, szükségképpen megvalósuló adatkezelés (informatikai rendszerben történő tárolás, törlés stb.) során fokozottan érvényesíteni kell a célhoz kötöttség elvét és a levéltitok védelmét. A nem kívánatos adatkezelés elkerülése érdekében a felhasználó köteles magáncélú leveleit – különösen a beérkező leveleket - 48 órán belül törölni/eltávolítani, ennek elmaradása esetén azok adattartalma indokolt esetben (informatikai üzemzavar, hibakeresés stb.) vizsgálható.

A felhasználóknak az elektronikus levelező szolgáltatás használatának folyamán az alábbi szabályokat kell betartaniuk:

* A levelek nem képviselhetnek a hatályos magyar jogba ütköző magatartásformát (pl.: tiltott tartalmak – pornográfia, szerzői jogok megsértése. stb.).
* Tilos kéretlen levelek (spam), lánclevelek, hoax-ok, adathalászati célú levelek (phising) illetve bármilyen „nem hasznos” üzenetek akár belső, akár külső e-mail címek felé küldése, továbbítása. (lásd. előzőekben)
* Tilos a felhasználóknak a Szervezeti e-mail címüket nem feladatuk ellátásához köthetően használni (pl.: regisztráció letöltési weboldalak, online játék oldalak stb.).
* Levelet küldeni csak a levél tartalmában érintett személy(ek) részére szabad.
* Tilos a levelek fejlécének megváltoztatása, hamis levelek küldése.
* Ismeretlen feladótól érkező, gyanús, csatolt fájlt tartalmazó, vagy ismeretlen linket ajánló (pl.: idegen nyelvű, láthatóan reklámcélú, olyan dokumentumra hivatkozó, amiről a címzett nem tud) elektronikus üzenetek csatolmányait, illetve a kapott linkeket nem szabad megnyitni, e leveleket törölni kell.

Informatikai biztonsági vizsgálat, auditálás, illetve hibakeresés céljából a **Szervezet** informatikai rendszereinek teljes hálózati forgalma megfigyelhető és rögzíthető. A felhasználó az IBSZ ismeretéről és elfogadásáról szóló nyilatkozatával elfogadja, hogy a rendszer használata egyben a felhasználó beleegyezését is jelenti az adatkezelésbe. Elektronikus levelek esetén a vizsgálat, illetve megfigyelés nem szükségképpen terjed ki a levelek tartalmára, de kivételesen indokolt esetben (pl. hibaelhárítás) a levelek megnyitására az **Informatikai Biztonsági Felelős** vagy a **Szervezet Vezetőjének** utasítása alapján sor kerülhet. Időszakos, illetve rendszeres biztonsági vizsgálat, avagy auditálás során a levelek az alábbi technikai tulajdonságok alapján kerülnek vizsgálatra:

* kéretlen levelek;
* vírusokat tartalmazó levelek;
* informatikai támadásokat megvalósító üzenetek;
* adathalászatot megkísérlő üzenetek.

A **Szervezetben** az e-mail címeket a következő konvenció szerint kell képezni:

vezetéknév.keresztnév@gamesz16.hu

### A felhasználó feladatai a munkahely elhagyásakor (3.1.6.4. [1])

A munkavállaló a munkavégzés befejezése után köteles a számítógépet és a hozzá kapcsolódó eszközöket kikapcsolni. A munkaidő lejártát követően az irodát utoljára elhagyó munkavállaló köteles ellenőrizni, hogy minden számítástechnikai eszközt kikapcsoltak-e.

A munkavállaló amennyiben szünetelteti munkavégzését és felügyelet nélkül hagyja számítógépét, úgy azt zárolni köteles.

A munkaidő lejártát követően az irodát utoljára elhagyó munkavállaló köteles ellenőrizni, hogy az iroda minden helyisége, ablakai, ajtói zártak legyenek, és - ahol van – a biztonsági berendezések (pl. riasztó) élesítve legyenek.

### Tiszta asztal tiszta képernyő szabályok a munkavégzés közben

A munkavállaló mindig csak a munkával kapcsolatos dokumentumok tarthatja elérhetően az íróasztalon és a képernyőn. Az érzékeny adatokat tartalmazó dokumentumokat, IT adathordozókat, mobil eszközöket a munka végeztével, illetve hosszabb távollét esetén munkanap közben is megfelelően el kell zárni.

Számítógép és mobil eszközök képernyő asztalaira egyidejűleg minimális, csak a munkával kapcsolatosan szükséges adatokat, illetve dokumentumokat helyezzük ki. Az eszközök fizikai elhagyása esetén megfelelő eljárással (zárolás, jelszavas képernyővédelem alkalmazásával) gondoskodni kell arról, hogy kívülállók ne tudjanak betekinteni a rendszerbe, ne férjenek hozzá a rendszerhez.

A munkavégzés során keletkező jegyzeteket, vázlatokat, illetve példányokat meg kell semmisíteni amennyiben már nincs szükség rájuk.

Prezentációk során oda kell figyelni, hogy mi kerül kivetítésre. Megbeszélések után a tárgyalókból minden dokumentumot, tábla tartalmat el kell távolítani.

### A vezetők felelőssége

A vezető felelőssége, hogy megkövetelje az alkalmazottól és alvállalkozóktól, hogy a biztonsági intézkedéseket a meghatározott szervezeti szabályzatokkal és eljárásokkal összhangban alkalmazzák. A vezetőknek biztosítaniuk kell, hogy az alkalmazottak és alvállalkozók:

* ismerjék biztonsági felelősségüket, a biztonsági eljárások alkalmazását és az adatfeldolgozó lehetőségek korrekt használatát, mielőtt az érzékeny információkhoz vagy információs rendszerekhez hozzáférnek, hogy ezzel is a minimálisra csökkentsék a lehetséges biztonsági kockázatokat;
* vegyenek részt biztonsági oktatásokban;
* legyenek ösztönözve, hogy a **Szervezet** biztonsági szabályzatait teljesítsék;
* alkalmazkodjanak a foglalkoztatás feltételeihez, tartsák be az ide vonatkozó biztonsági szabályzatokat, a biztonságot érintő kérdésekben megfelelő, naprakész jártasságuk legyen.

A felhasználói oktatás a biztonsági elképzeléseket is figyelembe vevő képzési terven kell, hogy alapuljon. Az informatika biztonságpolitikai elveknek, valamint a saját hatáskörben meghatározott képzési elveknek megfelelően ki kell dolgozni a képzési tervet.

### Személyi biztonság a jogviszony megszűnésekor, megszüntetésekor vagy kinevezés módosítás esetén (3.1.6.4. [1]; 3.1.6.5. [3])

A jogviszony megszűnése, megszüntetése, illetve a módosítása megközelítőleg azonos biztonsági kategória, mivel mindhárom az éppen használt adatfeldolgozó eszközök és jogosultságok leadásával jár. A felhasználók feladatainak elhatárolása alapvető biztonsági követelmény, éppen ezért a jogosultságok megvonása teljes mértékben indokolt. A **Szervezeten** belül másik szervezeti egységhez átirányított alkalmazottat vagy alvállalkozót ilyen szempontok alapján gyakorlatilag azonosan kell kezelni a kilépő alkalmazottal vagy alvállalkozóval.

### A jogviszony megszűnésének, megszüntetésnek biztonsági kérdései (3.1.6.4. [1])

A jogviszony megszűnése, megszüntetésekor a **Szervezet** szempontjából biztonsági alapkövetelmény, hogy az alkalmazottak és alvállalkozók szabályozott módon hagyják el a **Szervezetet**. A jogviszony megszüntetésnek folyamatát úgy kell kialakítani, hogy a használatra átadott eszközök visszaadása, és minden hozzáférési jog visszavonása időben befejeződjön.

A jogviszony megszűnése utáni felelősségek közlésének tartalmaznia kell a folyamatos biztonsági követelményeket és jogi felelősségeket, amelyek még vonatkoznak a kilépő alkalmazottra egy meghatározott időszakon át a jogviszony megszűnése után is. A jogviszony megszűnése után még érvényes felelősségek és kötelezettségek szerepeljenek a felhasználó személyi anyagában, írásos formában.

### Az eszközök visszaadása

Alapvető biztonsági cél, hogy minden jogviszony megszűnése után a **Szervezet** minden vagyontárgyát a használó szolgáltassa vissza, beleértve a szoftvereket, dokumentumokat, az informatikai eszközöket, hitelkártyákat, beléptető kártyákat, illetve különféle elektronikus adathordozón tárolt információkat.

A raktárban valamennyi, újra felhasználásra kerülő eszközt – biztonságos törlés után - alapszoftverekkel újratelepítve kell tárolni. Használatból kivonáskor – szintén biztonságos törlés után - az eszközök gyári beállításait kell visszaállítani, a felhasználó szervezetre utaló információktól, adatoktól meg kell fosztani.

### A hozzáférési jogok visszavonása

A távozó személy fokozott biztonsági kockázatot jelent a **Szervezet** számára. Távozók esetén biztonsági alapkövetelmény, hogy minden az informatikai rendszert érintő hozzáférési jog visszavonása legkésőbb az utolsó munkában töltött napon megvonásra kerüljön.

Fontos, hogy az informatikai jogosultságokon kívül visszavonásra kerülő vagy átalakítandó hozzáférési jogok közé tartoznak a fizikai vagy logikai hozzáférések, azonosító, beléptető kártyák, előfizetések. Amennyiben a kilépő alkalmazottnak vagy alvállalkozónak ismert jelszavai vannak aktív számlákhoz, ezeket le kell adnia az esetleges munkakör módosulás, illetve szolgálati jogviszony megszűnésekor. A kilépő által használt fiókokat zárolni kell, ettől csak a **Szervezet Vezetőjének** írásbeli engedélyével lehet eltekinteni.

Biztonsági szempontból szükséges, hogy a felelős vezetők informálják az üzemeltetőt személyi változásokról, és kezdeményezzék a távozók jogosultságainak (pl. belépési engedélyek, távoli hozzáférések) teljes körű visszavonását. Az adatfeldolgozó eszközök hozzáférési jogait minősített esetben akár még a felmentési idő alatt is ajánlatos csökkenteni vagy megszüntetni.

Az ilyen intézkedést csak különféle kockázati tényezők elemzése után lehet meghozni, amelyek a következők:

* ki kezdeményezte a jogviszony megszüntetését és mi a megszűnés oka;
* milyen mértékű az alkalmazott felelőssége;
* mennyi a pillanatnyilag számára hozzáférhető vagyontárgyak értéke.

### Az informatikai biztonsági oktatás és képzés (3.1.7.)

A **Szervezet** valamennyi alkalmazottját – feladatának és jogkörének figyelembevételével - megfelelő képzésben kell részesíteni a **Szervezet** biztonsági szabályairól és eljárásairól. Ezeket az ismereteket rendszeresen naprakész ismeretek közlésével fel kell újítani. A képzés foglalja magába:

* a biztonsági követelményeket;
* a jogi felelősséget;
* a **Szervezet** óvintézkedéseit;
* az informatikai eszközök helyes használatát, például a bejelentkezési eljárást, a szoftverek használatát.
* általános biztonság tudatossági ismereteket

Az általános képzést azelőtt kell lefolytatni, mielőtt a belépők megkapnák a hozzáférési jogot (jogosultság) az informatikai rendszerekhez, vagy az adatokhoz.

Az általános biztonságtudatosítási képzés mellett, melynek mindenkire vonatkoznia kell a **Szervezetben**, különleges biztonsági képzés is szükséges az informatikai biztonsággal foglalkozók számára. A biztonsági képzés mélységének a **Szervezeten** belüli általános fontosságához kell igazodnia, és az adott szerep biztonsági követelményeinek megfelelően kell változnia. Amennyiben szükséges, sokkal kiterjedtebb oktatást is biztosítani kell. Informatikai biztonsági képzési programot kell kialakítani az összes biztonsághoz kapcsolódó igény lefedésére. A képzési eljárásrendet rendszeresen felül kell vizsgálni és körülmények, rendszer változásával frissíteni.

Minden esetben ellenőrizni kell, hogy a tevékenységekhez szükséges-e különleges biztonsági képzés.

### A biztonsági képzésre vonatkozó dokumentációk (3.1.7.6. [3])

Az információ-biztonsági képzésen történő részvételt alá kell íratni a résztvevőkkel. Az aláírt dokumentumokat / online képzés naplóit 3 évig meg kell őrizni.

### Fegyelmi eljárás (3.1.6.7. [1])

Azokkal szemben, akik a **Szervezet** informatikai biztonsági szabályait és eljárásait vétkesen megszegték, fegyelmi eljárást kell kezdeményezni és lefolytatni. A fegyelmi, felelősségi, kártérítési eljárást a Munka Törvénykönyvében foglaltak alapján kell lebonyolítani.

### Külső szervezetre vonatkozó követelmények (3.1.6.6. [3])

A **Szervezet** a külső szervezettel kötött megállapodásban, szerződésben megköveteli, hogy:

* a külső szervezet határozza meg a **Szervezettel** kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat;
* a szerződő fél feleljen meg a **Szervezet** által meghatározott személybiztonsági követelményeknek;
* a szerződő fél a **Szervezett** érintő biztonsági auditokban közreműködjön;
* a szerződő fél dokumentálja és tartassa be a személybiztonsági követelményeket, beleértve azt az esetet, amikor a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik a **Szervezet** elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést a **Szervezet**nek;

Az **IBF** folyamatosan, de legalább 90 naponta ellenőrzi a szerződő féltől személybiztonsági követelményeknek való megfelelését.

# FIZIKAI VÉDELEMI INTÉZKEDÉSEK ELJÁRÁSRENDJE (3.2.1.2 [2])

Az infrastruktúrát és az információt meg kell védeni a jogosulatlan hozzáféréstől, a sérüléstől, valamint az illetéktelen beavatkozástól.

Gondoskodni kell az illetéktelen behatolást, hozzáférést, károkozást és beavatkozást megakadályozó fizikai-mechanikai, elektronikai és személyi védelem szükséges méretű – együttes – alkalmazásáról.

## Fizikai belépési engedélyek (3.2.1.3. [2])

Az illetéktelen hozzáférés, a károkozás és a **Szervezet** helyiségeibe való behatolás, valamint az adatok jogtalan elérésének megakadályozása érdekében a lehetséges kockázatokat fel kell mérni és ennek megfelelően biztonsági területeket kell kijelölni.

A zónákba való belépési jogosultságokat úgy kell meghatározni, hogy az egyes személyeket az informatikai rendszerben betöltött szerepük alapján kell hozzá rendelni a helyiségekhez vagy helyiség csoportokhoz.

Az informatikai eszközök fizikai védelme érdekében a **Szervezet** helyiségeit alap esetben a következő biztonsági zónákba kell sorolni:

* publikus zóna: vendégek által is szabadon megközelíthető
* **I-es zóna**, közösen használt helyiségben lévő informatikai végberendezések (folyosók, termek, tárgyalók);
* **II-es zóna**, felhasználói irodák;
* **III-as zóna**, vezető, helyettes, adatgazdák irodája (fokozott biztonsági zóna);
* **IV-es zóna**, szerverterem (kiemelt biztonsági zóna).

A **Szervezet** informatikai helyiségeinek megfelelő kategóriába besorolása az **Informatikai Vezető** feladata. Az **Informatikai Vezető**nek a besorolás során figyelembe kell vennie az adott helyiségben elhelyezésre kerülő informatikai eszközöket, tárolt adatokat. Ezért az **Informatikai Vezető** az informatikai zónák kialakítása során egyes helyiségek számára a fenti alap besorolásnál magasabb biztonsági fokozatú zónát is meghatározhat.

A zónákba való beléptetésnek az alábbi módon kell teljesülnie:

* publikus zóna: a **Szervezet** nem végez beléptetést
* **I-es zóna:** kulcsos beléptetés
* **II-es zóna:** csak a belépésre jogosult személyek kulcsos beléptetése
* **III-es zóna:** csak a belépésre jogosult személyek (személyesen kiadott kulcs)

## A fizikai belépés ellenőrzése (3.2.1.4. [2])

Az egyes biztonsági zónákba való belépést ellenőrizni kell.

* A fokozott vagy a kiemelt biztonsági osztályba sorolt zónák esetén az állandó belépési jogosultsággal rendelkező személyek be- és kilépését is naplózni kell.
* A támogató feladatot ellátó munkatársak hozzáférését korlátozni kell a fokozott vagy kiemelt biztonsági osztályba sorolt zónákon belül. Ha a hozzáférés indokolt és engedélyezett, akkor is figyelemmel kell őket kísérni. A biztonsági területekhez való hozzáférési jogokat – akár a rendszeres jogosultság felülvizsgálat során - rendszeresen át kell vizsgálni, frissíteni, illetve, ha már nem szükséges, akkor vissza kell vonni.
* Az **Informatikai Biztonsági Felelős** az éves ellenőrzési tervének keretein belül szúrópróba szerűen jogosult a belépési naplókat, az eseménynaplókat ellenőrizni, valamint a kiosztott kártyák és az elektronikus információs rendszerben engedélyezett belépések egyezőségét vizsgálni.

## Vészvilágítás (3.2.1.11. [3])

Áramszünet esetén automatikus vészvilágítás kell, hogy aktiválódjon, amely biztosítja a vészkijáratokat és menekülési útvonalakat.

## Tűzvédelem (3.2.1.12. [3])

A **Szervezet** az elektronikus információs rendszerek számára független áramellátással támogatott észlelő, az informatikai eszközökhöz megfelelő tűzelfojtó berendezéseket alkalmaz, és tart karban.

A helyiségek tűzvédelmét teljes körű tűzriasztó rendszerrel, valamint az adott helyiség kialakítási módjának megfelelő, automatikus tűzoltó rendszerrel és a helyiség tűzvédelmi besorolásának megfelelő kézi tűzoltó eszközökkel kell biztosítani. A helyiségeket tűzzáró ajtóval kell elválasztani az épület többi részétől.

## Karbantartók (3.2.1.19 [3])

A **Szervezet** az alábbi kialakított folyamat mentén kezeli a karbantartók munkavégzési engedélyeit:

* nyilvántartást vezet a karbantartó szervezetekről vagy személyekről;
* megköveteli a hozzáférési jogosultság igazolását az elektronikus információs rendszeren karbantartást végzőktől;
* felhatalmazást ad a **Szervezethez** tartozó, a kívánt hozzáférési jogosultságokkal és műszaki szakértelemmel rendelkező személyeknek arra, hogy felügyeljék a kívánt jogosultságokkal nem rendelkező személyek karbantartási tevékenységeit.

# LOGIKAI VÉDELMI INTÉZKEDÉSEK

## Általános védelmi intézkedések (3.3.1.1.[R2])

A **Szervezet** megfogalmazza, és a **Szervezetre** érvényes követelmények szerint dokumentálja, valamint a **Szervezeten** belül kihirdeti:

* az elektronikus információbiztonsággal kapcsolatos (ideértve a rendszer- és felhasználói, külső és belső hozzáférési) engedélyezési eljárási folyamatokat;
* felügyeli az elektronikus információs rendszer és környezet biztonsági állapotát;
* meghatározza az információbiztonsággal összefüggő szerepköröket és felelősségi köröket;
* kijelöli az ezeket betöltő személyeket;
* integrálja az elektronikus információ-biztonsági engedélyezési folyamatokat a szervezeti szintű kockázatkezelési eljárásba, összhangban az informatikai biztonsági szabályzattal.

Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, az érintett szervezet hatókörébe tartozó:

* emberi, fizikai és logikai erőforrásra;
* eljárási és védelmi szintre és folyamatra.

### Az elektronikus információs rendszer kapcsolódásai (3.3.1.3.[3])

A **Szervezet** szabályozza, és belső engedélyhez kötheti az elektronikus információs rendszerének kapcsolódását más elektronikus információs rendszerekhez. Dokumentálja az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.

#### Belső rendszerkapcsolatok (3.3.1.3.2.[3])

A **Szervezet** az **Informatikai Vezető** és az **Informatikai Biztonsági Felelős (IBF)** írásos engedélyéhez köti az elektronikus információs rendszereinek összekapcsolását.

#### Külső kapcsolódásokra vonatkozó korlátozások (3.3.1.3.3.[3])

A **Szervezet** a külső elektronikus információs rendszerekhez való kapcsolódásokhoz során a „minden tiltása, kivételek engedélyezése” elvet követi, amely mindennemű kapcsolat tiltásával kezdve az **Informatikai Vezető** és az **Informatikai Biztonsági Felelős (IBF)** által írásban jóváhagyott bejövő forgalom kivétel alapú engedélyezését jelenti.

## Tervezés (3.3.2.)

Biztonságtervezést kell végezni mindegyik olyan rendszerfejlesztés, továbbfejlesztés alkalmával, amely hatással lehet a **Szervezet** információbiztonságára nézve. A biztonságtervezéssel kapcsolatos feladatokat az egyes rendszerek teljes életciklusa során el kell látni.

A biztonságtervezési eljárás egyes fázisai a következők:

* felmérés;
* az elvárt biztonsági osztály meghatározása;
* követelményrendszer kidolgozása;
* rendszerbiztonsági terv készítése;
* rendszerbiztonsági terv ellenőrzése.

### Felmérés

A felmérés során meg kell határozni, hogy a rendszer milyen fizikai, személyi és szoftver környezetben fog üzemelni. Fel kell mérni és rögzíteni kell:

* a rendszer hatókörét, alapfeladatait, biztosítandó szolgáltatásait;
* a rendszer működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait;
* a rendszerben kezelendő adatok érzékenységét (megjelölve azokat az adatköröket, amelyek esetében a rendszer osztályba sorolásánál magasabb szintű védelemre van szükség.);
* a rendszerrel kapcsolatos kockázatokat, fenyegetéseket és gyenge pontokat.

### Az elvárt biztonsági osztály meghatározása

A felmérésben rögzített információkra alapozva meg kell határozni a rendszer elvárt biztonsági osztályát.

### Követelményrendszer kidolgozása

Ki kell dolgozni a rendszerrel kapcsolatos információ-biztonsági követelmények rendszerét. Ennek során a helyzetfelmérésre alapozva meg kell határozni a rendszer fejlesztői számára a fizikai, logikai és adminisztratív védelmi követelményeket.

### Cselekvési terv (3.3.2.3. [2])

#### Cselekvési terv készítése

Abban az esetben, ha egy adott elektronikus információs rendszerre vonatkozó biztonsági osztálynak való megfelelés vizsgálatánál hiányosság kerül megállapításra, cselekvési tervet kell készíteni a hiányosságok kiküszöbölésére. A cselekvési tervben dokumentálni kell a megállapított hiányosságok javítására, valamint a rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésre irányuló tervezett tevékenységeket, valamint az egyes tevékenységek felelőseit és határidőit.

#### Cselekvési terv frissítése

A cselekvési terv végrehajtását 2 évente felül kell vizsgálni és a vizsgálat eredményeképpen az adott helyzetnek megfelelően frissíteni kell.

### Személyi biztonság (3.3.2.4. [2])

#### A felhasználókkal szemben támasztott elvárások megfogalmazása

A hozzáférési jogosultságot igénylő felhasználóval szembeni elvárásokat, a rá vonatkozó szabályokat, felelősségüket az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységeket a felhasználó munkaköri leírásának, egyéb számára kiadott utasításnak, valamint az adott rendszer felhasználói dokumentációjának kell tartalmaznia.

#### A rendszer használattal kapcsolatos információk biztosítása

A hozzáférés engedélyezése előtt a hozzáférési jogosultságot igénylő személynek (belső munkatárs vagy külsős vállalkozó) írásbeli nyilatkozatott kell tennie arról, hogy az érintett rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja.

*(A felhasználó az Információ Biztonsági Szabályzatot és a Felhasználói szabályozást elolvasta megértette és magára nézve kötelező érvényűnek tartja és ezt az aláírt nyilatkozatával elismeri.)*

#### A felhasználókkal szemben támasztott elvárások felülvizsgálata

Kétévente felül kell vizsgálni a rendszerek használatával kapcsolatban a felhasználókkal szemben támasztott elvárásokat. A felülvizsgálatot a rendszergazdáknak kell elvégezniük. Abban az esetben, ha a rendszeres felülvizsgálat során vagy azon kívül megállapítást nyer, hogy a rendszer szolgáltatásai, funkcionalitása, hatóköre megváltozott vagy más okból következően az elvárásokban változás állt be, az illetékes rendszergazdának haladéktalanul jelentenie kell ezt az **Informatikai Biztonsági Felelős**nek és tájékoztatnia kell a rendszer felhasználóit.

A tájékoztatás történhet e-mail-ben vagy nagyobb változás esetén erre a célra megszervezett oktatáson. E-mail tájékoztatás esetén az egyes felhasználóknak vissza kell jelezniük, hogy a tájékoztatást megértették és a jövőben annak alapján járnak el.

## Rendszer és szolgáltatás beszerzés (3.3.3. [2])

### A rendszer fejlesztési életciklusa (3.3.3.2. [2])

A **Szervezet** az elektronikus információs rendszereinek teljes életútján, azok minden életciklusában figyelemmel kíséri informatikai biztonsági helyzetüket.

## Konfigurációkezelés (3.3.6.)

### Konfigurációs eljárásrend és nyilvántartások (3.3.6.1. [2])

A **Szervezet** birtokában lévő informatikai konfigurációs elemek teljes köréről naprakész nyilvántartást kell vezetni. A nyilvántartás és visszakereshetőség biztosítása céljából konfigurációs adatbázist kell létrehozni. A nyilvántartásban kötelezően kell szerepeltetni a következő konfigurációs elemeket:

* hardver elemek;
* szoftver elemek;

A nyilvántartásnak minden eszközre az alábbi adatokat kell tartalmaznia:

* A vagyonelem felelőse.
* Az eszköz logikailag milyen csoportba tartozik, illetve hol található.
* Az eszköz megnevezése, meghatározása.
* Azonosító, amennyiben az eszköz egyértelmű azonosításához arra szükség van, egyértelmű azonosítót kell hozzárendelni (a mező kitöltése tehát nem minden esetben kötelező).

### Alkalmazások konfigurációinak nyilvántartása

A **Szervezet** által használt alkalmazások konfigurációinak teljes köréről nyilvántartást kell vezetni. A nyilvántartásban kötelezően kell szerepeltetni a következő elemeket:

* az alkalmazási rendszer megnevezése;
* az alkalmazási rendszer konfigurációs elemei.

### Alapkonfiguráció (3.3.6.2. [2])

A **Szervezet** rendszerenként rögzített alapkonfigurációi kiindulási alapként szolgálhatnak a tovább fejlesztéseknél, illetve sikertelen változtatásoknál visszatérési pontként szolgálhatnak. Az alapkonfigurációs jelszóval védett központi tárolón kerülnek megőrzésre.

### A konfigurációváltozások felügyelete (változáskezelés) (3.3.6.3. [3])

A **Szervezetnél** a következő tevékenységek tartoznak a változáskezelés hatálya alá:

* fejlesztések, verzióváltások;
* a rendszerelemek cseréje;
* a rendszerműködés módosításai.

### Változáskezelés alapvető szabályai

A változáskezelést külön rendszer beavatkozási szabályzatként kell kiadni, melynek meg kell felelnie az alábbiakban felsorolt előírásoknak.

A rendszerkonfiguráció változásokat az alábbiak figyelembevételével lehet elvégezni:

* Új konfiguráció implementálását engedélyeztetni kell. Az implementációt kizárólag a szükséges engedély birtokában lehet megkezdeni. A változás megkezdése előtt az **Informatikai Vezető** engedélyezi a megvalósítandó hardver és szoftver konfigurációt. Az engedélyezett változtatásokat a szolgáltatás üzemeltetője az üzemeltetési leírásban foglaltak alapján végrehajtja, sikeres végrehajtás esetén a rendszerleírásban dokumentálja.
* Minden változtatással kapcsolatos bejelentést, véleményezést, döntést és kivitelezést dokumentálni kell.
* Bármely, az egyes konfigurációkat megváltoztató művelethez az **Informatikai Vezető** engedélye szükséges.
* Új konfigurációra történő áttérést kizárólag úgy lehet elvégezni, hogy vissza lehessen állni a megelőző konfigurációra.
* A fejlesztési, tesztelési és üzemeltetési környezeteket logikailag egymástól külön kell választani.
* A változáskezelési előírások betartását és a változáskezelési folyamatot az **Informatikai Biztonsági Felelős** az éves ellenőrzési tervében foglaltak szerint ellenőrzi.

### Új konfiguráció éles üzembeállása

Új konfiguráció éles üzembeállása során a következőket kell betartani:

* Csak adminisztrátori jogosultsággal lehet elvégezni a változtatásokat.
* Ellenőrizni kell, hogy mindegyik konfigurációs lépés megtörtént-e.
* Ellenőrizni kell, hogy jogosulatlan elemek nem kerülnek-e telepítésre. A jogosulatlan elemek észlelése esetén le kell tiltani és törölni azokat.

### A működő rendszer konfiguráció figyelése

A **Szervezet** megbízott munkatársának legalább havonta ellenőriznie kell, hogy a jogosulatlan hardver-, szoftver elemek nem kerültek-e telepítésre. Minősített adatok kezelését végző rendszerek esetében az ellenőrzést legalább hetente el kell végezni.

A jogosulatlan elemek észlelése esetén le kell tiltani, majd törölni azokat, valamint értesíteni az **Informatikai Vezető**t.

Folyamatosan figyelnie kell, hogy illetéktelen behatolás következményeképpen nem lett-e megváltoztatva a konfiguráció.

### Legszűkebb funkcionalitás (3.3.6.7. [3])

A **Szervezet** az egyes konfigurációkat csakis a feladatainak ellátására használt legszűkebb funkcionalitással implementálja és használja.

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

### Elektronikus információs rendszerelem leltár (3.3.6.8. [2])

A **Szervezet** leltárt készít az elektronikus információs rendszer elemeiről.

Gondoskodik arról, hogy a leltár:

* pontosan tükrözze az elektronikus információs rendszer aktuális állapotát,
* az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet tartalmazza;
* legyen kellően részletes a nyomkövetéshez és a jelentéskészítéshez.

#### Frissítés

A **Szervezet** évente felülvizsgálja és frissíti az elektronikus információs rendszerelem leltárt;

* a **Szervezet** rendszeresen, de legalább évente felülvizsgálja és frissíti az elektronikus információs rendszerelem leltárt;

### A szoftverhasználat korlátozásai (3.3.6.10. [2])

Az elektronikus információs rendszerrel kapcsolatban a következő szoftverhasználati korlátozásokat kell figyelembe venni:

* A **Szervezet**nél kizárólag az **Informatikai Vezető** által jóváhagyott hardver és szoftver elemek használhatók.
* A **Szervezet** kizárólag jogtiszta szoftvereket használ.
* A **Szervezet** kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak.
* A másolatok, megosztások ellenőrzésére nyomon követi a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát.
* A **Szervezet** ellenőrzi az állomány megosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.

### A felhasználó által telepített szoftverek

A **Szervezet** felhasználói nem telepíthetnek szoftvereket a **Szervezet** eszközeire.

## Karbantartás (3.3.7.)

Az informatikai eszközök karbantartását folyamatos rendelkezésre állásuk és sértetlenségük érdekében a gyártó útmutatása alapján, előírás-szerűen el kell végezni. A karbantartási ciklus kialakításáért, partnerek szerződtetéséért az **Informatikai Vezető** a felelős, aki:

* A karbantartások ütemezését és módját éves karbantartási tervben rögzíti, az informatikai eszközök karbantartásának konkrét időpontját 1 héttel előre meghatározza;
* Írásban engedélyezi a tervezett karbantartásokat;
* Kihirdeti a karbantartott eszközök felhasználói számára a karbantartások várható időpontjait;
* Jóváhagyja, nyilvántartja és ellenőrzi az elektronikus információs rendszer karbantartására használt eszközöket

A karbantartás során:

* Az eszközöket csak jóváhagyást követően lehet leállítani;
* Az elvégzett munkákat jegyzőkönyvezni kell, valamint a karbantartás tényét karbantartási nyilvántartásban kell dokumentálni, illetve nyilvántartani;
* Amennyiben az adatot tartalmazó adathordozó kiszállítása válik szükségessé, akkor gondoskodni kell annak titkosításáról. A kiszállítást az **Informatikai Vezető** engedélyezi.

A karbantartás során a **Szervezet** ellenőrzi a diagnosztikai és teszt programokat tartalmazó adathordozókat a kártékony kódok tekintetében, mielőtt azt az elektronikus információs rendszerben használnák.

### Karbantartók (3.2.1.19 [3])

Abban az esetben, ha saját erőből a karbantartás nem végezhető el, akkor az **Informatikai Vezető** kezdeményezi a **Szervezet** vezetőjénél külső fél megbízását.

Karbantartási tevékenységet csak olyan külső fél végezhet, aki érvényes szerződéssel rendelkezik, a titoktartási nyilatkozatot aláírta és dokumentált formában megismerte a **Szervezet** vonatkozó információ-biztonsági előírásait.

* A karbantartást végző külső felekről nyilvántartás kell vezetni, melynek minimálisan a következőket tartalmaznia:
* szervezet megnevezése;
* szerződésszám;
* szerződés időtartama;
* szerződéses kapcsolattartó neve, elérhetősége;
* szerződés tárgya, hatálya.

Külső munkavégzése esetén az informatikai terület vezetőjének ki kell jelölnie azokat a személyeket, akiknek folyamatos felügyeletet kell biztosítani a karbantartás során.

A külső féllel kötött szerződébe kell foglalni, hogy a karbantartást felügyelők jogosultak kérni a karbantartást végző személy személyazonosságának igazolását, illetve, hogy a karbantartást végző személynek kötelessége a felszólításra a szükséges iratokat bemutatni.

## Adathordozók védelme (3.3.8. [4])

Biztosítani kell az adathordozók fizikai védelmét annak érdekében, hogy a dokumentumok, a számítógépek adathordozói, a bemenet/kimenet adatai és a rendszer dokumentációi a jogosulatlan megszerzésétől, módosítástól, eltávolítástól és rombolástól megfelelően védve legyenek.

Az adathordozók kezelésének legfontosabb biztonsági követelményei:

* Gondoskodni kell az adathordozók ellenőrzéséről és fizikai védelméről.
* Meg kell előzni a dokumentumok, a számítástechnikai adathordozók, az input/output adatok és a rendszerdokumentációk károsodását, eltulajdonítását.
* Biztosítani kell, hogy az adathordozók kezelése – a vonatkozó iratkezelési szabályok szellemében, – a tartalmazott adatok szempontjából egyenértékű papír dokumentumokkal egyenértékű módon történjen.
* Minden adathordozót újra alkalmazás előtt, illetve selejtezés után az adatok megsemmisítését eredményező megfelelő eljárással törölni kell, melynek módszerét Törlési Üzemeltetési Utasítás tartalmazza. Ha ez nem valósítható meg, akkor az adathordozót fizikailag kell működésképtelenné tenni olyan módon, hogy a rajta lévő információ ne legyen visszanyerhető.
* Biztosítani kell az adatok sértetlen és hiteles állapotának megőrzését.
* Minden adathordozót biztonságos környezetben, a gyártó előírásainak megfelelően kell tárolni.

### Hozzáférés az adathordozókhoz (3.3.8.2. [2], 3.3.8.7. [2])

A **Szervezet** elektronikus információs rendszerében a következő táblázat szerint használhatók és hozzáférhetők az adathordozók:

| Adathordozó | Feltétel | Felhasználói kör |
| --- | --- | --- |
| **Beépített adathordozók** | Mindennapi munkavégzés során, beszerelve | Felhasználók |
| **Beépített adathordozók** | Kiszerelés, mozgatás | IÜFV, RGAZD |
| **Optikai adathordozók** | Komponensek telepítése | IÜFV, RGAZD |
| **Külső, hordozható adathordozók** | Komponensek telepítése,Mentések kezelése | IÜFV, RGAZD |
| **Mágneses szalagok** | Mentések kezelése | IÜFV, RGAZD |
| **Papír alapú adathordozók** | Iratkezelési szabályok szerint | Iratkezelési szabályok szerint |

11. táblázat Hozzáférés az adathordozókhoz

A táblázatban nem szerepelő felhasználási esetek tiltottak, ennek általános bővítése az **Informatikai Vezető** feladata, de írásos engedélyével egyedi kivétel adható.

### Adathordozók törlése (3.3.8.6. [2])

Biztonságos törlés az írható és olvasható adathordozók többszörös felülírásával valósul meg, mely során az adatok törlését Gutmann (35 menetes) vagy a Schneier (7 menetes) törlési eljárásokkal vagy ezekkel egyenértékű, az adatok helyreállíthatatlanságát biztosító szoftverrel kell elvégezni. A szoftver a fájlok törlését követően véletlenszerű algoritmus alapján előállított adatokkal írja felül azok fizikai és logikai helyét az adathordozón.

### Adathordozók újrahasznosítása

Védett informatikai rendszerben használt adathordozót olyan szabályozott módszerek alkalmazásával kell törölni, hogy az adatok a későbbiekben ne legyenek helyreállíthatók melynek módszerét a Törlési Üzemeltetési Utasítás tartalmazza.

### Adathordozók megsemmisítése

Az adathordozók típusának és fizikai megvalósulásának megfelelő módszert kell választani a megsemmisítéséhez, melynek módszerét a Törlési Üzemeltetési Utasítás tartalmazza

Az adathordozók megsemmisítése a következő módszerekkel engedélyezett:

## Azonosítás és hitelesítés (3.3.9.)

### A felhasználók azonosítása (3.3.9.2. [2])

#### Felhasználói azonosítókkal szemben támasztott követelmények

A felhasználó azonosító az informatikai rendszert használó identitásának egyedi, jellemző, ellenőrizhető és hitelesítésre alkalmas megjelenítése kell, hogy legyen az informatikai rendszerben. A felhasználók közé sorolandók a természetes személyek, folyamatok, vagy egyéb eszközök egyaránt. Az egyedi felhasználói azonosítót a hozzáférés szabályozására, az adatok és az információk védelmére, valamint a hitelesítés támogatására kell felhasználni. Biztosítani kell, hogy a felhasználó azonosítója az egyes erőforrásokhoz, folyamatokhoz, adatokhoz való hozzáférést megfelelően szabályozza (korlátozza) és követhető, ugyanakkor a biztonsági funkciók működése során ellenőrizhető legyen a biztonsági rendszer számára.

#### A felhasználói azonosítók képzésének és kezelésének szabályai

* A felhasználó-azonosítónak minden esetben egyedinek kell lennie, (azaz semmilyen körülmények között sem adható ki különböző felhasználók részére megegyező azonosító). Azonosítási problémák elkerülése végett, csoportazonosítók kiadása tilos, minden esetben egyértelműen meg kell tudni határozni a felhasználó személyét. Kivételt képeznek azok az azonosítók (technikai felhasználók), ahol azokra működési vagy üzemeltetési okokból feltétlenül szükség van, ezek legyenek szakmailag megindokolva, vezető által jóváhagyva és dokumentálva;
* A felhasználói azonosítók képzését központi névkonvenciós szabályozás alapján kell végezni az alábbiak alapján:

felhasználói azonosító: vezeteknev és keresztnev. Névegyezőség esetén postfixelhető.

* Tilos akár csak átmeneti jelleggel is, más azonosítójának használata. A kapott felhasználói azonosítót haladéktalanul érvényesíteni kell.
* A **Szervezet** alkalmazottjainak felhasználói azonosítóját jogviszonyuk megszűnésével haladéktalanul le kell tiltani. A megszűnt munkajogviszonyú alkalmazott a rendszer szolgáltatásait nem veheti igénybe és erőforrásait nem használhatja.
* A közszolgálati jogviszonyukat huzamosabb ideig szüneteltető, illetve a tartósan más okból távollévő alkalmazottak felhasználói azonosítóját le kell tiltani, illetve munkába állásukkal egy időben ismét engedélyezni kell.
* Az alkalmazottak áthelyezése kapcsán felmerülő változásokat az áthelyezéssel egyidőben, haladéktalanul át kell vezetni.
* Harmadik személyek, akik valamilyen okból igénybe vehetik a **Szervezet** bármelyik rendszerének szolgáltatásait, csak meghatározott időre, és korlátozott lehetőségeket biztosító felhasználói azonosítót kaphatnak. A részükre kiadott azonosító szerkezetileg feleljen meg a **Szervezet**en belüli alkalmazottak azonosítójával, de legyen egyértelműen és könnyen megállapítható, hogy az adott felhasználói azonosító egy harmadik (külső) személyé.
* Ha egy felhasználó azonosító 30 napot meghaladóan inaktívnak bizonyul, azonosítóját le kell tiltani és erről a munkahelyi vezetőjét haladéktalanul értesíteni szükséges, megjelölve az érvénytelenítés okát.
* A felhasználókkal alá kell íratni egy nyilatkozatot, amely dokumentálja, hogy megértették a hozzáférés feltételeit, felelősségeit.
* Azonnal zárolni kell az olyan felhasználói azonosítót, amely nem köthető alkalmazotti státuszhoz.
* Azonnal zárolni kell az olyan felhasználó azonosítókat, amelyek valószínűleg kompromittálódnak.
* A lezárt felhasználói neveket nem lehet más személynek kiadni, egyezés esetén úgy kell eljárni, mintha a lezárt felhasználói név is használatban lenne. (postfix)

#### Felhasználói azonosítók nyilvántartása

A felhasználói azonosítókat nyilván kell tartani és mindennemű változást naplózni kell.

### Felhasználók hitelesítése (3.3.9.2. [2])

#### A hitelesítők képzéseinek és használatuknak szabályai

A **Szervezet** informatikai rendszereiben a felhasználók hitelesítésének alapvető módja a jelszó megadása. A felhasználói jelszavak kezelésére a következő szabályokat kell alkalmazni:

* A felhasználónak kötelezően alá kell írnia egy nyilatkozatot, melyben felelősséget vállal jelszavai bizalmas kezelésére.
* Belépéskor megkapott ideiglenes jelszó átadása csak biztonságos csatornán történhet, a felhasználó előzetes azonosítása után. Az ideiglenes jelszavak csak 1 napig lehetnek érvényesek, megváltoztatásuk kötelező.
* Technikai felhasználók, valamint beépített (privilegizált) felhasználók jelszavait oly módon kell tárolni, hogy csak arra felhatalmazottak férhessenek hozzá, illetve a hozzáférések naplózottak legyenek.
* Amennyiben egy technikai felhasználói fiókhoz többen is hozzáférnek és a hozzáféréshez jogosultak listája változik, a csoport felhasználói fiókokhoz tartozó hitelesítő eszközöket vagy adatokat újra ki kell bocsátani.
* Jelszó alapú hitelesítő rendszer használata esetén a jelszavakat cserélni kell minden esetben ha kompromittálódnak, vagy illetéktelen személy birtokába jutnak.

#### A hitelesítés kezelése az informatikai rendszerekben (3.3.9.5.2 [4])

A hitelesítésre szolgáló eszközök kiosztásakor ellenőrizni kell az eszközt átvevő egyén vagy eszköz jogosultságát, az átadás tényét dokumentálni kell.

* A jelszavaknak minden felhasználó számára szabadon megváltoztathatónak kell lennie.
* A **felhasználói** jelszavak minőségére vonatkozóan az alábbi szabályokat kell alkalmazni:
	+ A jelszó hossza legalább 8 karakter legyen, tartalmazzon kis és nagybetű szám vagy speciális karakter közül legalább 2 félét
	+ A jelszó maximális élettartama 3 hónap, minimális pedig 2 nap
	+ Az utolsó 3 jelszó nem használható
	+ Első bejelentkezéskor a kötelező jelszó cseréje: 1 nap
	+ Az **adminisztrátori** jelszavak minőségére vonatkozóan az alábbi szabályokat kell alkalmazni:
	+ A jelszó hossza legalább 10 karakter legyen, tartalmazzon kis és nagybetűt, számot és speciális karaktert
	+ A jelszó maximális élettartama 12 hónap, minimális pedig 2 nap
	+ Az utolsó 10 jelszó nem használható
	+ Első bejelentkezéskor a kötelező jelszó cseréje: 1 nap
* Az **technikai** jelszavak minőségére vonatkozóan az alábbi szabályokat kell alkalmazni:
	+ A jelszó hossza legalább 30 karakter legyen, tartalmazzon kis és nagybetűt, számot és speciális karaktert
	+ A jelszó maximális élettartama 12 hónap, minimális pedig 2 nap
	+ Az utolsó 10 jelszó nem használható
* A jelszavak titkosítatlan formában való tárolása a **Szervezet** rendszereiben szigorúan tilos! (Ez alól kivételt csak a technikai és beépített rendszergazdai jelszavak papíralapú, lezárt borítékban és páncélszekrényben történő tárolása jelenthet.)
* A jelszavakat vagy a jelszófájlokat a hálózaton nyílt, olvasható formában továbbítani tilos.

#### Felhasználói tanúsítványhordozó eszközök nyilvántartása

A kiadott tanúsítványhordozó eszközről naprakész nyilvántartást kell vezetni.

#### Speciális felhasználókhoz tartozó jelszavak kezelése

* Beépített adminisztrátori fiókok, technikai felhasználók jelszavait lezárt borítékban az **Informatikai Vezető** páncélszekrényében kell őrizni, vagy olyan jelszókezelő alkalmazásban, mely a hozzá féréseket naplózza.
* A speciális felhasználók jelszavához csak különösen indokolt esetben lehet hozzáférni.
* A boríték felbontásáról minden esetben jegyzőkönyvet kell készíteni megjelölve a speciális felhasználó igénybevételének pontos okát és a felbontók személyét,
* Jelszókezelő alkalmazásban naplózni kell a hozzáféréseket,
* Gondoskodni kell arról, hogy a szükséges műveletek elvégzése után a speciális felhasználó számára új jelszó kerüljön kiadásra és azt haladéktalanul, lezárt borítékban ismét az **Informatikai Vezető** páncélszekrényébe kell helyezni, vagy fel kell vezetni a jelszó kezelő alkalmazásban.

#### Jelszó (tudás) alapú hitelesítés (3.3.9.5.2. [4])

A **Szervezet** a jelszóra a következő elvárásokat érvényesíti:

* kis- és nagybetűk megkülönböztetése; a karakterek számának meghatározása; a kisbetűk, nagybetűk, számok és speciális karakterek, és minimális jelszóhosszúság;
* meghatározott számú karakterváltozást kényszerít ki új jelszó létrehozásakor;
* a jelszavakat nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hasító érték tárolást) és nem továbbítja;
* a jelszavakra minimális és maximális élettartam korlátozást juttat érvényre úgy, hogy meghatározott számú új jelszóig megtiltja a jelszavak ismételt felhasználását, és a rendszerbe első lépést lehetővé tevő ideiglenes jelszó lecserélésére kötelez.

#### Birtoklás alapú hitelesítés (3.3.9.5.3. [4])

* Az elektronikus információs rendszer hardver token alapú hitelesítése esetén olyan mechanizmusokat alkalmaz, amely megfelel a **Szervezet** által meghatározott minőségi követelményeknek, vagy
* Az elektronikus információs rendszer nyilvános kulcsú infrastruktúra alapú hitelesítés esetén:
* ellenőrzi a tanúsítványokat egy elfogadott megbízható pontig tartó tanúsítványlánc felépítésével és ellenőrzésével, beleértve a tanúsítvány állapot információ ellenőrzését is;
* kikényszeríti a megfelelő magánkulcshoz való jogosult hozzáférést;
* összekapcsolja a hitelesített azonosságot az egyéni fiókkal;
* megvalósítja a visszavonási adatok helyi tárolását a tanúsítványlánc felépítésének és ellenőrzésének támogatására arra az esetre, amikor a visszavonási információk a hálózaton keresztül nem elérhetők.
* A felhasználók a **Szervezettől** kapott fizikai hitelesítő eszköz (token) esetében elszámolási kötelezettséggel bírnak. Az adott eszközt más személynek nem adható át. Az eszköz elvesztését vagy bármilyen kompromitálódását haladéktalanul jelezni kell a ticketing rendszerben és az Információ Biztonsági Felelősnek is.

### Felhasználói fiókok kezelése (3.3.10.2.)

A **Szervezet** elektronikus információs rendszerei központi címtárat használnak, amelyek karbantartása a rendszergazdák feladata az **Informatikai Biztonsági Felelős** és az **Informatikai Vezető** felügyeletével. Felhasználói fiókok létrehozására, módosítására csak a felhasználó felettesének (**Szervezeti Egység Vezető**), az **Informatikai Biztonsági Felelős** és az **Informatikai Vezető** jóváhagyásával ellátott írásos igény után kerülhet sor. (Ez alól kivételt az incidenskezelésben és a működés-folytonossági tervben meghatározott beavatkozások jelenthetnek.)

Az elektronikus információs rendszer fióktípusai:

| *Fióktípus* | *Felhasználói kör* | *Megjegyzés* |
| --- | --- | --- |
| Rendszergazda | Rendszergazdák | Csak privilegizált műveletek végrehajtásához. A csoport tagjai az informatikai osztály munkatársai, fiók kiadása az Informatikai Vezető egyedi jóváhagyásával. |
| Felhasználó | Rendszergazdák | Mindennapi munkához, a csoport tagjai a rendszergazdai jogokkal is rendelkező felhasználók. |
| Felhasználó | Felhasználók | Mindennapi munkához, a csoport tagjai az elektronikus információs rendszerhez érvényes hozzáférési engedéllyel rendelkező alkalmazottak. |
| ………………… | ………………… | ………………… |

*12. táblázat: Fióktípusok*

A rendszergazdák feladata a felhasználói fiókok 90 naponta történő felülvizsgálata, mely során ellenőrizni kell a fiókkezelési követelményekkel való összhangot.

Az elektronikus információs rendszernek automatizált mechanizmusokat kell alkalmaznia az elektronikus információs rendszer fiókjainak kezeléséhez, különösen:

* automatikusan eltávolítja, vagy letiltja az ideiglenes vagy kényszerhelyzetben létrehozott felhasználói fiókokat, ha azokat 30 napig nem használták.
* automatikusan letiltja az inaktív fiókokat 30 nap letelte után.
* a felhasználói fiókok használatának ellenőrzésére (szokatlan viselkedési minták keresése)

A **Szervezeti Egység Vezető** felelőssége a fiókkezelésben értesíteni a rendszergazdákat, ha

* egy felhasználói fiókokra már nincsen szükség;
* egy felhasználó kilép vagy áthelyezésre kerül;
* valamint az **Informatikai Biztonsági Felelős** és ATFV segítségével meghatározza a szervezeti egységhez tartozó elektronikus információs rendszer jogosult felhasználóit, a csoport- és szerepkör tagságot és a hozzáférési jogosultságokat, valamint (szükség esetén) az egyes felhasználói fiókok további jellemzőit (alapfeladatok és -funkciók, tervezett rendszerhasználat);
* a szervezeti egységhez tartozó elektronikus információs rendszer használata, vagy használatához szükséges feltételek megváltoznak

#### Személyes vagy megbízható harmadik fél általi regisztráció (3.3.9.5.5. [4])

A **Szervezet** meghatározott hitelesítő eszköz átvételéhez megkövetel egy olyan regisztrációs eljárást, melyet meghatározott regisztrációs szervezet folytat le a **Szervezet** által meghatározott személyek vagy szerepkörök jóváhagyása mellett.

A jelenleg támogatott hitelesítési eszközök:

| Hitelesítő eszköz | Regisztrációs szervezet | Jóváhagyó |
| --- | --- | --- |
| Jelszó | Informatika | IBF, SZEV |
| Kétfaktoros authentikációhoz használt hardver | Informatika | IBF, SZEV |

*13. táblázat: Hitelesítő eszközök regisztrációja*

### Ellenőrzés

Az **Informatikai Biztonsági Felelős**nek ellenőriznie kell az azonosítás és hitelesítéssel kapcsolatos előírások maradéktalan betartását.

### A hitelesítésre szolgáló eszköz visszacsatolása (3.3.9.6. [2])

Az elektronikus információs rendszerben csak olyan rendszerelemek használatók fel, amelyek fedett visszacsatolást biztosítanak a hitelesítési folyamat során.

### Azonosítás és hitelesítés (Szervezeten kívüli felhasználók) (3.3.9.8. [2])

Harmadik személy csak meghatározott időre, és korlátozott lehetőségeket biztosító személyes felhasználói azonosítót kaphatnak. Ilyen jogosultságot csak különösen indokolt esetben, vezetői kérésre, az **Informatikai Vezető** jóváhagyása esetén lehet kiadni.

### Hitelesítés szolgáltatók tanúsítványának elfogadása (3.3.9.8.2. [2])

Az azonosításhoz és a hitelesítéshez felhasznált tanúsítványok csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő a szolgáltatók által kibocsátott tanúsítványok lehetnek.

## Hozzáférés az informatikai rendszerekhez (3.3.10., 3.3.10.1. [2])

A **Szervezet** elektronikus információs rendszereinek ki kell kényszerítenie az azonosítást, ezekben tilos azonosítás vagy hitelesítés nélküli tevékenységeket végezni.

### Általános alapelvek

Az információs rendszerek illetéktelen elérésének megakadályozása érdekében megfelelő hozzáférés védelmi rendszert kell kialakítani. Hozzáférés iránti, illetve jogosultság módosítására, hozzáférés törlésére vonatkozó igény csak írásban kérhető. A beérkezett igényeket nyilvántartásba kell venni. A kiadott engedélyek listáját naprakészen kell tartani.

* A jogosultságok megadásának alapvető biztonsági intézkedései:
* Azonosítani kell, a hozzáférést kérő személyét, a kívánt és adható jogokat, valamint az érintett rendszert
* A felhasználók hozzáférési jogosultságait a minimálisan szükséges jogok alapján kell megadni
* A jogosultságok kiosztásának dokumentáltnak és engedélyezettnek kell lenniük,
* A rendszergazdai és egyéb előjogokat a rendes működési használattól eltérő használói azonosítóhoz kell kötni.
* Kerülni kell a rendszeradminisztráció előjogainak nem megfelelő alkalmazását.

Minimálisan a következő jogokat kell megkülönböztetni:

* olvasási jog (betekintés);
* létrehozási jog;
* módosítási jog;
* törlési jog.

Az adminisztrációs és naplózási jogoknak el kell különülni a felhasználói jogoktól.

A rendszereknek alkalmasnak kell lenniük a hozzáférési jogok egyedi vagy csoport szinten való megkülönböztetésére és szabályozására. A hasonló szerepű személyek csoportjai munkájának támogatására hozzáférési jogosultsági csoportokat kell kialakítani.

### Hozzáférés ellenőrzés eljárásrendje (3.3.10)

A **Szervezetnél** csak olyan elektronikus információs rendszer használható, amely képes a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

#### Ellenőrzés informatikai rendszerekben

Az informatikai rendszerekben biztosítani kell, hogy a felhasználók tényleges hozzáférési jogosultsága a szerepkörüknek megfelelő legyen. Ennek érdekében:

* A jogosultságokat rendszeres időközönként felül kell vizsgálni.
* Az általános felhasználók esetében: 12 havonta,
* kiemelt jogosultsággal rendelkező felhasználók esetében legalább 6 havonta
* Rendszeresen ellenőrizni kell, hogy privilegizált jogokkal csak egyedileg azonosítható felhasználók és eszközök rendelkezhessenek.
* A szerepkörök változásakor a hozzáférési jogosultságokat felül kell vizsgálni és az új szerepkörnek megfelelően módosítani kell.
* Az ellenőrzést a szervezeti egység vezetője által kijelölt személy végzi el.

#### Az operációs rendszerhez való hozzáférés ellenőrzése

Az informatikai eszközök illetéktelen elérésének megakadályozása érdekében az operációs rendszer szintjén rendelkezésre álló biztonsági lehetőségeket is fel kell használni a számítástechnikai erőforrásokhoz való hozzáférés korlátozásához. Ezeknek a következőket kell lehetővé tenniük:

* Az engedéllyel rendelkező felhasználó személyének azonosítása és hitelesítése, szükség esetén a terminál vagy hely azonosítása.
* A sikeres és az eredménytelen hozzáférési kísérletek rögzítése.
* Megfelelő hitelesítési eszközök és – jelszókezelő rendszer használata esetén – minőségi jelszavak biztosítása.
* Különleges rendszergazdai jogosultságok használatának naplózása (Pl. rendszergazda jogosultsággal rendelkező felhasználók esetében).
* Adott esetben a felhasználók csatlakozási idejének korlátozása.
* Amennyiben a kockázatok alapján ez indokolt, más hozzáférést vezérlő módszereket (például ujjlenyomat, chipkártya, kérdés-felelet) is használni kell.

#### Legkisebb jogosultság elve (3.3.10.6.1. [4])

Az elektronikus információs rendszer a legkisebb jogosultság elvét alkalmazza, azaz a felhasználók - vagy a felhasználók tevékenysége - számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezi.

#### A felelősségek szétválasztása (3.3.10.5. [4])

A **Szervezet** szétválasztja az egyéni felelősségeket.

Dokumentálja az egyéni felelősségek szétválasztását;

A **Szervezet** meghatározza az elektronikus információs rendszer hozzáférés jogosultságait az egyéni felelősségek szétválasztása érdekében.

### Hálózati hozzáférés

#### Távoli hozzáférés (3.3.10.13. [3])

Távoli hozzáférés esetén is gondoskodni kell a biztonsági követelmények és előírások betartásáról, a megfelelő és rendszeres ellenőrzésről.

* A távolról csak a kijelölt csatlakozási (hozzáférési) pontokon keresztül szabad csatlakozni a **Szervezet** hálózatába. Az **Informatikai Vezető** határozza meg ezeket a belépési pontokat.
* A távoli hozzáférés munkaszakaszok bizalmasságának és sértetlenségének a védelmére kriptográfiai mechanizmusokat kell alkalmazni.
* A **Szervezet** informatikai rendszeréhez kapcsolódni csak VPN csatornán keresztül lehet.
* A VPN használatához a szabályzatban meghatározott erősségű authentikáció és authorizáció szükséges. (felhasználónév, jelszó, e-token, stb.)
* A távoli hozzáférés biztosítsa során két faktoros authentikációt kell alkalmazni.
* A távoli hozzáféréseket automatizált módon figyelni és felügyelni kell.

#### Privilegizált parancsok elérése (3.3.10.13.5. [4])

A **Szervezet** privilegizált parancsok végrehajtásához és biztonságkritikus információk eléréséhez távoli hozzáférést csak meghatározott és elfogadott igény esetén engedélyez, dokumentálja és indokolja a hozzáféréseket a rendszerbiztonsági tervben.

### Biztonságos hitelesítő, bejelentkező eljárások (3.3.13.16. [3])

#### Munkaállomások automatikus azonosítása, hitelesítése

* A munkaállomás automatikus azonosítása kötelező, ha fontos és indokolt, hogy egy munkát, vagy tranzakciót csak egy adott terminálról lehessen kezdeményezni.
* Technikailag biztosítani kell, hogy csak a központilag nyilvántartott munkaállomásokról, címekről lehessen a rendszerekbe belépni.
* Egységes munkaállomás névhasználatot kell kialakítani.
* A LAN hálózatban biztosítani kell az idegen gép felismerését és az erőforrásokhoz történő hozzáférésének megakadályozását (pl. port security address összerendeléssel)

#### Biztonságos bejelentkezési eljárások

A számítógéprendszerbe való bejelentkezési folyamatnak minimumra kell csökkentenie az illetéktelen hozzáférés lehetőségét.

* Ennek során csak a bejelentkezés eredményes befejezése után jelenhet meg a használni kívánt rendszerre vonatkozó adat, azonosító, stb..
* A bejelentkezés elfogadására vagy elvetésére csupán az összes szükséges adat megadása után kerülhet sor, sikertelenség esetén nem jelölheti meg a hibás, elrontott azonosítót, jelszót.
* Korlátozni kell az eredménytelen bejelentkezési kísérletek számát. Rögzíteni kell az eredménytelen kísérleteket, próbálkozásonként egyre nagyobb késleltetést kell alkalmazni, mielőtt további bejelentkezési kísérletet engednek meg. Időtúllépés esetén meg kell szüntetni az adatátviteli kapcsolatot.
* Minősített esetben vészjelzést kell küldeni a rendszer-kezelőpulthoz, ha elérték a legnagyobb számú bejelentkezési kísérletet.
* A jelszóval való visszaélések és az ehhez kapcsolódó biztonsági események könnyebb felderíthetősége érdekében belépés után a rendszer jelezze ki a következőket:
	+ az előző sikeres bejelentkezés dátumát és időpontját;
	+ az utolsó sikeres bejelentkezés óta végzett sikertelen bejelentkezési kísérletek részletes adatait.

A fentiek segítségével, maga a felhasználó is nyomon tudja követni, hogy valaki más megpróbált-e visszaélni az ő jogosultságaival.

### A rendszerhasználat jelzése (3.3.10.8. [3])

A **Szervezet** meghatározott rendszer használatra vonatkozó figyelmeztető üzenetet vagy jelzést küldhet a felhasználó számára a rendszerhez való hozzáférés engedélyezése előtt, mely jelezheti, hogy:

* a felhasználó a **Szervezet** elektronikus információs rendszerét használja;
* a rendszer használatot figyelhetik, rögzíthetik, naplózhatják;
* a rendszer jogosulatlan használata tilos, és büntetőjogi vagy polgárjogi felelősségre vonással jár;
* a rendszer használata egyben a felhasználó előbbiekbe történő beleegyezését is jelenti.

### Mobil eszközök hozzáférés ellenőrzése (3.3.10.15. [3])

* Amennyiben az eszközön helyileg is találhatóak adatok, illetve a **Szervezet** informatikai rendszeréből lokális adathordozóra történő adatáthelyezésre van jogosultsága, akkor az eszközt teljes eszköztitkosítással, tároló alapú titkosítással, vagy más technológiai eljárással kell ellátni az eszközökön tárolt információk bizalmasságának és sértetlenségének a védelmére.
* Az eszköz – bekapcsolt állapotban, zárolás nélkül – soha nem maradhat felügyelet nélkül.
* A gyártó előírásait mindig be kell tartani az eszköz védelme érdekében.

Alkalmazni kell az azonosítás hitelesítésénél megadott szabályokat.

### Vezeték nélküli hozzáférés (3.3.10.14. [3])

A **Szervezet** rendszereihez közvetlen vezeték nélküli hozzáférés nem alakítható ki. A vezetéknélküli hozzáférési pontok bekötése az elektronikus információs rendszertől elkülönített biztonsági zónába történhet, amelyből a távmunka fejezetben meghatározott feltételek mellett lehet eszközöket csatlakoztatni a **Szervezet** belső rendszereihez.

A vezeték nélküli hozzáférést

* minden esetben az Informatikai Vezetőnek kell írásban indokolnia és engedélyeznie;
* a biztonsági architektúra tervben fel kell tüntetni és a kriptográfiával szembeni elvárásoknak megfelelően kell konfigurálni;
* azonosítást kell megkövetelnie -amely, ha jelszó alapú- azt 30 naponta meg kell változtatni mind a munkavállaók, mind a vendégek számára biztosított vezeték nélküli hálózaton.

### Külső elektronikus információs rendszerek használata (3.3.10.16. [2])

A **Szervezet** rendszereihez külső elektronikus információs rendszert csak az **Informatikai Vezető** engedélyével lehet csatlakoztatni. A csatlakoztatást megelőzően az **IBF** kockázatelemzést végez a csatlakozás lehetséges kockázataival kapcsolatban és meghatározza a csatlakozás módját. Ebben rögzíteni kell, hogy milyen feltételek és szabályok betartása mellett jogosult a felhasználó egy külső rendszerből hozzáférni a **Szervezet** rendszereihez, valamint meg kell határozni, hogy külső elektronikus információs rendszerek segítségével hogyan jogosult a felhasználó feldolgozni, tárolni vagy továbbítani a **Szervezet** által ellenőrzött információkat.

#### Hordozható adattároló eszközök (3.3.10.16.3. [4])

Külső elektronikus információs rendszer felhasználásának vonatkozásában a hordozható adattároló eszközök használatát minden esetben az **Informatikai Vezető** egyedi elbírálással, írásban engedélyezi.

### Nyilvánosan elérhető tartalom (3.3.10.18. [2])

A **Szervezet** nyilvánosan hozzáférhető rendszerként definiálja a **Szervezet** publikus weboldalát.

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

## Rendszer és információsértetlenség (3.3.11., 3.3.11.2. [2])

Az egyes alkalmazásokhoz és hálózati mappákhoz (könyvtárakhoz) való hozzáférés (jogosultságok) dokumentált engedélyeztetése útján gondoskodni kell arról, hogy jogosulatlan felhasználó azokat ne módosíthassa, és ne törölhesse.

A mentések és archívumok tárolása és őrzése során biztosítani kell az adatok sérthetetlenségét.

Számítógépes adatvesztés vagy adatsérülés esetén az adatfeldolgozást az adatokat tartalmazó rendszernél azonnal fel kell függeszteni és a kijelölt informatikust azonnal értesíteni kell. Az értesítés történhet e-mail, telefon vagy személyes bejelentés útján. A felmerült probléma tisztázása után a kijelölt informatikus útmutatása szerint lehet csak folytatni a további munkát.

Az integritás sérülésének gyanúja esetén azonnal meg kell kezdeni a körülmények, az okozott kár és a felelősség kivizsgálását. Ez alól kivételt képez, ha az integritássérülésnek következményeképpen várható kár mértéke alacsony és az integritás helyreállítása az adott rendszer eszközeivel megfelelően naplózott módon megoldható (pl. egy téves adatbevitel).

### Hibajavítás (3.3.11.3.[S2])

A **Szervezet** azonosítja, belső eljárásrendje alapján jelenti és kijavítja vagy kijavíttatja az elektronikus információs rendszer hibáit.

Telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket az érintett szervezet feladatellátásának hatékonysága, a szóba jöhető következmények szempontjából.

A **Szervezet** a biztonságkritikus szoftvereket a frissítésük kiadását követő meghatározott időtartamon belül telepíti vagy telepítteti, beépíti a hibajavítást a konfigurációkezelési folyamatba.

### Kártékony kódok elleni védelem (3.3.11.4. [2])

A **Szervezet** informatikai rendszereit védeni kell a kártékony kódok ellen. Ennek érdekében a következőket kell betartani:

* A határvédelmi programoknak a szervereken folyamatosan kell működniük. A programoknak folyamatosan vizsgálniuk kell a bejövő hálózati forgalmat (levelezés, web).
* A határvédelmi szoftverrendszer elemeinek (programok, szabályrendszerek, vírusdefiníciós adatbázisok) frissítéséről automatizált módszerrel gondoskodni kell. A frissítések hiba nélküli megtörténtét ellenőrizni kell.
* Hálózati munkaállomások az internethez kizárólag a **Szervezet** internet kijáratán (központi tűzfalán) keresztül csatlakozhatnak.
* Vírusvédelem nélkül sem hálózati, sem önálló munkaállomás nem üzemeltethető.
* A vírusvédelemnek a klienseken, rezidens módon kell futniuk, azaz, a rendszer indulásakor automatikusan indul a program, illetve folyamatosan vírusellenőrzést kell végrehajtani a klienseken, amely vizsgálatok eredményét ellenőrizni kell. A vírusvédelemnek a rendszer következő komponenseire kell kiterjednie: fájlok, rendszeradatok, webes és e-mail hálózati forgalom.
* A munkaállomásokon valós idejű ellenőrzést (azonnali riasztást) biztosító vírusvédelmet kell használni.
* A felhasználónak tilos vírusirtót, személyes tűzfalat, vagy egyéb biztonsági szoftvert telepítenie.
* Külső helyekről származó adattárolókat (Szervezeti okból történő) használat előtt vírusellenőrzésnek kell alávetni és csak akkor lehet használni, ha az adathordozó a vizsgálaton megfelel.
* Vírusfertőzés gyanúja vagy nem üzemszerű működés esetén a felhasználóknak haladéktalanul értesítenie kell az kijelölt informatikust, hogy a szakértők megvizsgálják az eseményt, és hiba esetén gondoskodjanak annak elhárításáról.
* Vírusfertőzés gyanúja esetén a **Szervezet** informatikusai a fertőzött gépet lezárhatják, annak használatát a hiba elhárításáig felfüggeszthetik.
* Az a felhasználó, aki az adatait és adathordozóit a vírus ellenőrzés vagy vírusvédelmi intézkedés (vírusirtás) alól bármilyen indokkal kivonja, az abból eredő károkért teljes felelősséggel tartozik.
* A vírusfigyelmeztetésekkel (vírus hoax) foglalkozó felelősök (rendszergazdák), feladata, hogy figyelemmel kísérjék a legfrissebb vírusok megjelenésével kapcsolatos híreket.
* Vírusfigyelmeztetéssel kapcsolatos levelet csak a rendszergazdák küldhetnek.

#### Vírustámadás elleni védekezés

A kijelölt informatikus feladata, hogy a felhasználói munkaállomásokra, illetve a mobil gépekre telepített vírusvédelmi rendszerek karbantartásáról gondoskodjon, a felhasználóknak támogatást nyújtson, továbbá a vírusdefiníciós állományok és a keresőmotorok szükséges frissítéseiről gondoskodjon.

#### Vírusvédelmi szoftverek használata

A vírusvédelmi rendszerek kiválasztását az Informatikai Vezetőnek a rendszergazdák javaslata alapján jóvá kell hagynia. A vírusvédelmi rendszer kiválasztásakor figyelembe kell venni a következő szempontokat:

* Nem megfelelő vírusvédelmi rendszer alkalmazásával a **Szervezet** vírusvédelme nem lesz kielégítő.
* A nem megfelelő vírusvédelmi szoftver lassítja a műveleteket és túlzott erőforrás igényt támaszthat. A rendszerek lassulása növeli a sebezhetőséget is.
* A vírusvédelmi szoftverek vírusdefiníciós állomány állományainak frissítési gyakoriságát.

### Az elektronikus információs rendszer felügyelete (3.3.11.5. [2])

A **Szervezet** rendszereinek napi üzemeltetéséhez tartozik azok működésének felügyelete, a mentések elvégzése, illetve hiba esetén az eszközök javítását végzők bevonása.

A **Szervezet** rendszereinek felügyelete az alkalmazások, az adatbázisok, a kiszolgálók és az alapszoftverek, az informatikai hálózat és a munkaállomások működésének folyamatos figyelemmel kísérését kívánja meg. Ennek érdekében:

* Meg kell ismerni a **Szervezet** rendszereszközeinek, elektronikus információs rendszereinek működését, azok figyelmeztető és hibaüzeneteit, amelyekre alkalmazni kell tudni a szükséges reagálásokat tartalmazó leírásokat.
* Rendszeresen el kell végezni azokat a tevékenységeket, amelyek alapján meg lehet győződni arról, hogy a felügyelt rendszer üzemszerűen működik.
* Automatizált eszközöket kell alkalmazni az események közel valós idejű vizsgálatának támogatására.
* Az elektronikus információs rendszer felügyelje a beérkező és kimenő adatforgalmat a szokatlan vagy jogosulatlan tevékenységekre, vagy körülményre tekintettel.
* Az elektronikus információs rendszer riassza a **Szervezet** illetékes személyeit, csoportjait, amikor veszélyeztetés vagy lehetséges veszélyeztetés előre meghatározott jeleit észleli.

### A kimeneti információ kezelése és megőrzése (3.3.11.12. [2])

Kimeneti információk a **Szervezet** által külső fél számára és belső használatra készített beszámolók, tájékoztatók, bizonylatok, nyilatkozatok, megrendelők, tranzakciók.

A kimeneti információk kezelésével és szétosztásával kapcsolatban a következők az előírások:

* Gondoskodni kell a kimeneti információ tartalmi ellenőrzéséről.
* Gondoskodni kell arról, hogy a kimeneti információhoz történő fizikai és logikai hozzáférés csak az arra jogosított személyekre korlátozódjon.
* Gondoskodni kell arról, hogy a jogosult személyek időben megkapják az elkészült kimeneti információkat.
* Biztosítani kell, hogy a megsemmisítési eljárások során a kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.
* A rendszer kimenő információit (pl.: számla) a vonatkozó jogszabályok, szabályzatok szerint kell megőrizni.

### Használatból történő kivonás

Szoftver használatból történő kivonására akkor kerül sor, ha az adott feladat végrehajtása szükségtelenné válik, vagy a végrehajtásra új eljárás került kifejlesztésre, vagy új program került beszerzésre.

A selejtezendő szoftver által kezelt adatokat át kell alakítani az új eljárás szerinti formátumra, de meghatározott ideig, általában egy hónapig a két eljárást párhuzamosan kell használni, hogy a folyamatos működés ne szenvedjen fennakadást. Ezt az időszakot követően a szoftvert selejtezni kell, ami azt jelenti, hogy az adott szoftvert a gépekből törölni kell, és az adathordozókat, ha már biztosan nem kellenek- meg kell semmisíteni, egyéb esetben az élesben használt szoftverektől elkülönítve kell tárolni azokat.

## Naplózás és elszámoltathatóság (3.3.12., 3.3.12.1. [2])

A **Szervezetnek** az elektronikus információs rendszereiben automatikus naplót és különleges esetekben ideiglenes naplót kell vezetnie az informatikai rendszer biztonsági szempontból lényeges tevékenységeiről.

Olyan naplózási architektúrát kell kialakítani, amely azt biztosítja, hogy ahol technikailag lehetséges, a naplózás szerveroldalon és a lehető legkevesebb számú naplóállomány használatával történjen.

A naplóállományokat központi napló gyűjtőrendszerben kell összegyűjteni és tárolni. A különböző naplóállományok összefésülését, feldolgozását és elemzését automatizált megoldásoknak kell támogatniuk.

A naplóban személyes adat nem lehet.

A **Szervezet** a személyes adatok kezelésével kapcsolatban az elektronikus naplóban rögzíti a naplózandó eseményeken felül:

* az adatkezelési művelettel érintett személyes adatok körének meghatározását;
* az adatkezelési művelet célját és indokát;
* az adatkezelési művelet elvégzésének pontos időpontját;
* az adatkezelési műveletet végrehajtó személy megjelölését;
* a személyes adatok továbbítása esetén az adattovábbítás címzettjét.

### Biztonsági események naplózása

A kivételes és a biztonságot fenyegető eseményeket eseménynaplóba kell bejegyezni, és azt a hozzáférés nyomon követhetősége érdekében meg kell őrizni. Az elszámoltathatóság és auditálhatóság biztosítása érdekében a regisztrálási és a naplózási rendszert (biztonsági napló) úgy kell kialakítani, hogy abból utólag megállapíthatók legyenek az informatikai rendszerben bekövetkezett fontosabb események, különös tekintettel azokra, amelyek a rendszer biztonságát érintik. Ezáltal ellenőrizni lehet a hozzáférések jogosultságát, meg lehet állapítani a felelősséget, valamint az illetéktelen hozzáférés megtörténtét vagy kísérletét.

#### Naplózandó események (3.3.12.2. [2])

A naplózási rendszernek alkalmasnak kell lennie mindegyik felhasználó vagy felhasználói csoport által végzett művelet szelektív regisztrálására. A következő eseményeket (sikeres/sikertelen) feltétlenül naplózni kell:

* rendszerindítások, -leállítások;
* rendszeróra állítások;
* be- és kijelentkezések;
* az azonosítási és a hitelesítési mechanizmus használata;
* hozzáférési jog érvényesítése azonosítóval ellátott erőforráshoz;
* azonosítóval ellátott erőforrás létrehozása vagy törlése;
* felhatalmazott személy műveletei, amelyek a rendszer biztonságát érintik.
* rendszerhibák és korrekciós intézkedések;
* programindítások és -leállások, leállítások;
* az adatállományok és kimeneti adatok kezelésének visszaigazolása.

Az elektronikus információs rendszernek lehetővé kell továbbá tennie, hogy a jogosult személyek vagy szerepkörök kiválasszák, mely naplózható események legyenek naplózva az egyes komponensekre, illetve alrendszerekre.

#### A napló adattartalma (3.3.12.3. [2], 3.3.12.3.2 [4])

A biztonsági naplóban az egyes eseményekhez kapcsolódóan a következő adatokat is rögzíteni kell:

a felhasználó azonosítása és hitelesítése esetén:

* dátum;
* időpont;
* a felhasználó azonosítója;
* az eszköz (például terminál) azonosítója, amelyről az azonosítási és hitelesítési művelet kezdeményezése történt;
* a hozzáférési művelet eredményessége vagy sikertelensége.

az olyan erőforráson kezdeményezett hozzáférési művelet esetén, amelynél a hozzáférési jogok ellenőrzése kötelező:

* dátum;
* időpont;
* a felhasználó azonosítója;
* az erőforrás azonosítója;
* a hozzáférési kezdeményezés típusa;
* a hozzáférés eredményessége vagy sikertelensége.

az olyan erőforrás létrehozása vagy törlése esetén, amelynél az ehhez fűződő jogok ellenőrzése kötelező:

* dátum;
* időpont;
* a felhasználó azonosítója;
* az erőforrás azonosítója;
* a kezdeményezés típusa;
* a művelet eredményessége vagy sikertelensége.

a felhatalmazott felhasználók (például rendszeradminisztrátorok) olyan műveletei esetén, amelyek a rendszer biztonságát érintik:

* dátum;
* időpont;
* a műveletet végző azonosítója;
* az erőforrás azonosítója, amelyre a művelet vonatkozik;
* a művelet eredményessége vagy sikertelensége.

#### Alapvető naplózási követelmények

* Kerüljön naplózásra a biztonságot érintő összes tevékenység.
* A naplófájlok tartalmát megadott időintervallum alapján képernyőn és nyomtatón is meg lehessen jeleníteni.
* A naplóállományokat tilos megsemmisíteni, felülírni, módosítani, azokat archiválni kell.
* A naplóállományok kódoltak, ellenőrző összeggel ellátottak legyenek.
* A fokozott és kiemelt biztonsági osztályba sorolt rendszerek biztonsági naplóit egy másik számítógépen is tárolni kell (annak érdekében, hogy védve legyenek a törlés és illetéktelen hozzáférés ellen). Ennek megvalósításáért az **Informatikai Vezető** felelős.
* Rögzíteni kell a hibás bejelentkezési kísérletek számát.
* A biztonsági napló adatait rendszeresen, de legalább havonta egy alkalommal ellenőrizni és archiválni kell.
* A biztonsági napló értékelése során meg kell határozni, hogy mely eseményeket kell Jegyzőkönyvezni, melyek azok az események, amelyek szankciókat vonnak maguk után, és mik ezek a szankciók.
* A biztonsági naplók alapján felvett Jegyzőkönyveket archiválni kell, és ennek során a megőrzési határidőket meg kell határozni.
* A biztonsági eseménynapló (naplófájl) és a Jegyzőkönyvek adatait védeni kell az illetéktelen hozzáféréstől.
* A biztonsági eseménynapló fájlok vizsgálatához és karbantartásához a rendszernek megfelelő eszközökkel és ezek dokumentációjával kell rendelkeznie. Ezen eszközök állapotának regisztrálhatónak és dokumentálhatónak kell lennie.
* A rendszerben a biztonsági eseménynapló fájlok auditálásához szükséges eszközöknek lehetővé kell tenniük egy vagy több felhasználó tevékenységének szelektív vizsgálatát.

A biztonsági naplót a létrehozástól folyamatosan karban kell tartani, valamint védeni kell az illetéktelen módosítástól és törléstől, ezért ember számára olvasható formában is el kell tárolni.

### Ideiglenes naplózás

Ideiglenes naplózást rendelhet el a naplózandó esemény és a naplózás időtartamának és céljának pontos megjelölésével, írásban:

* az **Informatikai Vezető**;
* az **Informatikai Biztonsági Felelős**.

### Kockázati tényezők

A naplózási és ellenőrzési tevékenységek eredményeit rendszeresen felül kell vizsgálni. A felülvizsgálat gyakoriságának az érintett kockázattól kell függenie. A figyelembe veendő kockázati tényezők a következők:

* az alkalmazási folyamatok kritikussága;
* az érintett információ értéke, érzékenysége és kritikussága;
* a rendszerbe való beszivárgásról és a rendszerrel való visszaélésről szóló korábbi tapasztalatok;
* a rendszerkapcsolatok kiterjedtsége (különös tekintettel a nyilvános hálózatokra).

### Naplózási információk védelme (3.3.12.9. [2])

Különös figyelmet kell fordítani a naplózó eszközök biztonságára, mert ha meghamisítják, hamis biztonságérzetet kelthetnek. Óvintézkedéseket kell alkalmazni azért, hogy a **Szervezet** meg legyen védve az olyan illetéktelen változtatásoktól és üzemeltetési problémáktól, mint:

* naplózási rendszer, amelyet kiiktattak;
* üzenetfajták, amelyeket rögzítés után módosítottak;
* naplófájlok, amelyeket átszerkesztettek vagy töröltek;
* naplófájlok adathordozói, amelyek kimerültek és ennek következtében vagy nem lehet már velük az eseményekről feljegyzést készíteni, vagy önmagukat írják felül.

A biztonsági naplókat archiválni kell, mint a rendszerhasználat bizonyítékait, annak érdekében, hogy ezek az információk (bizonyítékok) későbbi vizsgálatokhoz is felhasználhatók legyenek.

A naplóinformációk védelme érdekében a következőket kell betartani:

* A naplóban rögzített információkat megváltoztatni, törölni tilos.
* a naplók tartalmának megváltoztatásának megakadályozása érekében lehetőség szerint kriptográfiai mechanizmusokat kell alkalmazni.
* A napló mentéseket, archív állományokat elkülönítetten, elzárva vagy hozzáférhetetlenül kell tartani.

### Naplóinformációk figyelése, reagálás a napló információkra (3.3.12.6. [3])

Folyamatosan figyelemmel kell kísérni a naplóállományok bejegyzései alapján generált riasztásokat.

Informatikai biztonsági esemény bekövetkeztekor, vagy ennek alapos gyanúja esetén automatikusan információ-biztonsági eseménykezelési eljárást kell indítani a **Szervezet** informatikai biztonsági eseménykezelési eljárásrendjében foglaltak szerint.

### Rendszer órajel szinkronizáció (3.3.12.8. [2])

A **Szervezeten** belül, illetve adott biztonsági tartományban működő valamennyi érintett információ-feldolgozó rendszer órajelét szinkronizálni kell egy közösen megállapított pontos időforráshoz. Az órajelek szinkronizációjával kapcsolatos beállításokat jegyzőkönyvezni kell. A jegyzőkönyvben fel kell tüntetni:

* az elvégzett művelet időpontját;
* a beállítást elvégzős munkatárs nevét;
* az elvégzett beállítás leírását.

### A naplóbejegyzések megőrzése (3.3.12.11. [2])

A **Szervezet** a naplóbejegyzéseket meghatározott - a jogszabályi és a **Szervezet**en belüli információ megőrzési követelményeknek megfelelő - időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében."

#### Naplóállomány mentése

A naplók tárolását a következő szempontok figyelembevételével kell megoldani:

* A naplóadatoknak sértetlenül rendelkezésre kell állniuk az esetleges elévülési időn belül.
* biztosítani kell, hogy az adatokban keletkezésük után változtatást már ne lehessen végrehajtani.
* Az információk bizalmasságára tekintettel, az adatok nem juthatnak illetéktelenek kezébe.

Az általános alkalmazás naplókat minimálisan 1 évig meg kell őrizni, kivéve, ha kapcsolódó jogszabály vagy belső szabályozó ennél többet kíván meg.

A biztonsági (security) naplóbejegyzéseket a biztonsági események utólagos kivizsgálásának biztosítása érdekében – amennyiben a jogszabályi követelmények másképp nem rendelkeznek – legalább a következő időtartamig meg kell őrizni:

* folyamatirányítási rendszerek esetén 3 év;
* szerver operációs rendszerek esetén 3 év;
* végponti operációs rendszerek esetén 1 év;
* biztonsági alkalmazások esetén 2 év;
* vagyonvédelmi rendszerek esetén 3 év;
* ügyviteli rendszerek esetén 2 év;
* IPS-es, IDS-ek esetén 2 év;
* hálózati eszközök esetén 2 év;
* minden egyéb rendszer esetén 2 év.

#### Naplóállomány külön mentése

Abban az esetben, ha a naplóállomány külön, az egyes adatbázisoktól elkülönítve kerül mentésre, nyilvántartást kell vezetni, hogy az egyes naplómentések, mely adattárolókon helyezkednek el. A nyilvántartásban fel kell tüntetni:

* a mentési eszköz azonosítóját;
* a mentési eszköz tárolási helyét;
* a mentés időpontját;
* a mentett naplóállomány nevét.

#### Naplóállományok rendszeres mentéseinek felülvizsgálata

Gondoskodni kell a naplóállományok rendszeres mentéseinek felülvizsgálatáról. A naplóállományok mentéseinek felülvizsgálatáról Jegyzőkönyvet kell készíteni, amelynek tartalmaznia kell az alábbi információkat:

* az elvégzett felülvizsgálat időpontja;
* a felülvizsgálatot elvégző munkatárs neve;
* az elvégzett felülvizsgálat mely naplóállományokra terjedt ki;
* a felülvizsgálat megállapításai;
* javaslat a felmerült problémák kezelésére.

#### Biztonsági naplók archiválása

A biztonsági naplókat archiválni kell, mint a rendszerhasználat bizonyítékait, hogy ezek az információk (bizonyítékok) későbbi vizsgálatokhoz is felhasználhatóak legyenek.

A biztonsági napló adatait rendszeresen, de legalább havonta egy alkalommal kell archiválni. Az archiválásról Jegyzőkönyvet kell készíteni. Az archiválási Jegyzőkönyvben a következő adatokat kell rögzíteni:

* az archiválás időpontja;
* az archiválást elvégző munkatárs neve;
* az archív állomány elérhetősége;
* az archivált állomány neve;
* az archiválás során alkalmazott szűrési feltételek.

A biztonsági naplók archiválásáról felvett Jegyzőkönyveket meg kell őrizni. A biztonsági naplók archiválásáról készített Jegyzőkönyvek megőrzési ideje 5 év.

### Naplózó rendszer beállításainak módosítása

A naplózó rendszer beállításainak megváltoztatást az erre vonatkozó egy alkalomra szóló engedély birtokában lehet csak elvégezni, melyet a **Szervezet** jogosultság kezelési folyamata szerint kell kérvényezni és kiadni. A naplózó rendszer módosításáról jegyzőkönyvet kell készíteni (vagy a konfiguráció kezelő rendszerben hitelt érdemlően rögzíteni), amelynek a következő adatokat kell tartalmaznia:

* a módosítást engedélyező neve;
* a módosítás indoka;
* a módosítás engedély megadásának időpontja;
* az elvégzett beállítás módosítás időpontja;
* a módosítást elvégző munkatárs neve;
* az elvégzett módosítás leírásai.

### Naplózási beállításokról nyilvántartás vezetése

Az egyes rendszerek naplózási beállításairól naprakész nyilvántartást kell vezetni, amelyet minden változtatást követően haladéktalanul aktualizálni kell.

## Rendszer és kommunikációvédelem (3.3.13., 3.3.13.1. [2])

### A határok védelme (3.3.13.6. [2])

Az elektronikus információs rendszer felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt:

* a nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól;
* csak a **Szervezet** biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez;
* a **Szervezet** korlátozza az elektronikus információs rendszer külső hálózati kapcsolatainak a számát a működéshez szükséges minimumra;
* az elektronikus információs rendszer a felügyelt kapcsolódási pontjain tilt, és csak kivételként engedélyez hálózati forgalmat;

### A hálózati szintű hozzáférések menedzsmentje

A **Szervezet** informatikai rendszerének elemeit adminisztrációs célból az internet felől elérni csak titkosított kapcsolaton keresztül (VPN), kétfaktoros authentikáció után lehetséges. Az ilyen kapcsolat kiépítésére az **Informatikai Vezető** adhat engedélyt. Minden adminisztrációs tevékenységnek egyértelműen személyhez köthetőnek kell lennie.

#### Kötelező elérési útvonal

Külső hálózatról az informatikai rendszerek csak az erre a célra dedikált védelmi rendszeren (tűzfal, zónák VPN koncentrátor stb.) keresztül lehetnek elérhetőek.

#### Hálózati részek elválasztása

Az internet és a **Szervezet** rendszerei között határvédelmi eszköznek kell biztosítani az elválasztást.

#### Hálózati eszközök, munkaállomások azonosítása és hitelesítése

* A távoli rendszerekhez történő automatikus csatlakozás lehetősége egy **Szervezeti** alkalmazáshoz való illetéktelen hozzáférést tehet lehetővé, ezért az informatikai rendszerekhez távolról való összes csatlakozást azonosítani és hitelesíteni kell. Ez különösen fontos akkor, ha a csatlakozás egy olyan hálózatot használ, amely kívül esik a **Szervezet** biztonsági rendszerének hatókörén.
* Technikailag biztosítani kell, hogy csak a központilag nyilvántartott munkaállomásról lehessen a rendszerekbe belépni.
* Egységes munkaállomás névhasználatot kell kialakítani, a hálózatban lévő munkaállomások pontos azonosítása érdekében.

#### A hálózatra történő csatlakozás ellenőrzése

Az osztott hálózati munka, különösen a több szervezet által használt hálózat biztonsága szükségessé teszi bizonyos ellenőrző eszközök alkalmazását a felhasználók csatlakozási lehetőségeinek korlátozására. (Ezeket a forgalomszűrő, ellenőrző lehetőségeket, amennyiben szükséges, a gateway és operációs rendszer beállításánál alkalmazni kell.)

Az alábbi esetekben különösen fontos a korlátozások alkalmazása:

* Elektronikus levelezés.
* Egyirányú adatállomány mozgatás (például mentési rendszerek esetében).
* Adatállomány mozgatása mindkét irányban.
* Meghatározott időponthoz kötött hálózati hozzáférés.

### Mobil informatikai tevékenység, távmunka (3.3.10.13. [3])

A mobil informatikai eszközön, illetve a távoli hozzáféréssel végzett munka esetén is meg kell teremteni az informatikai biztonságot. A szükséges védelemnek összhangban kell lennie ennek a speciális munkavégzésnek a kockázataival. Mobil számítástechnikai eszközök használata során mérlegelni kell egyrészt a nem védett környezetben való munkavégzés kockázatait, másrészt a védekezés szükséges módját és eszközeit. A mobil számítástechnikai eszközökön az **Informatikai Vezető**nek gondoskodni kell a rejtjelezett adattárolásról és adatátvitelről. Távmunka (távoli hozzáférés) esetén a **Szervezet** érintett szervezeti egységeinek gondoskodniuk kell a biztonságos adatkapcsolat létrehozásáról, a kapcsolatot tartó hely és eszköz védelméről.

#### Mobil informatikai tevékenység (3.3.10.15. [3])

A mobil eszközök (laptopok, notebook-ok, otthoni munkaállomások, tabletek, mobil telefonok használóinak mind a fizikai biztonság, mind a logikai védelem területén a jelen IBSZ-ben foglaltakat kell figyelembe venniük. Ezek közül a legfontosabbak:

* A távmunka során is be kell tartani a **Szervezet** szabályzataiban foglaltakat.
* A mobil eszközök nem hagyhatók felügyelet nélkül, amennyiben nem biztosítható azok előírt védelme.
* Ki kell alakítani a mobil informatikai eszközök megfelelő fizikai védelmét.
* A kommunikációhoz védett csatornáról kell gondoskodni.
* Vírus- és behatolás védelmi eszközöket kell biztosítani a mobil eszközökre.
* A mobil eszközökön tárolt adatok bizalmasságának védelmére fokozott figyelmet kell fordítani.
* A távoli elérésre vonatkozó szabályokat kell alkalmazni.
* A mobil számítástechnikai berendezéseket nyilvános helyeken használóknak ügyelni kell arra, hogy elkerüljék a jogosulatlan személyek általi betekintés kockázatát.
* Kényes üzemeltetési információkat hordozó eszközt nem szabad felügyelet nélkül hagyni, és ha lehetséges, fizikailag el kell zárni vagy különleges zárat kell alkalmazni a berendezés biztosítására.
* A felhasználók részére oktatást kell tartani, hogy növeljék a biztonsági tudatosságot az ilyen jellegű munkavégzésből származó többletkockázattal szemben és a bevezetendő intézkedések elfogadtatásával kapcsolatban.
* A hordozható informatikai eszközök gazdája felelős az eszköz teljes biztonságáért és annak ellenőrzéséért. Ha az eszközt egy csoport használja, ugyanúgy szükséges a biztonsági átvilágítás és a szükséges tudás elve (need-to-know). Ilyen esetekben a csoport egyik tagját kell kijelölni, aki felelős az eszköz biztonságáért.
* A **Szervezetnek** folyamatosan frissített listát kell tárolnia a rendszerben definiált, jogokkal felruházott felhasználókról.
* Szükséges a kiváltságos account-ok használata. (Pl. rendszer, biztonsági adminisztrátor.) Az összes, jogosultsággal rendelkező felhasználó biztonsági beállításait, egyedileg kell karbantartani.
* A kiváltságos (magas jogosultságokat biztosító, – pl. rendszergazdai –) account-ok jelszavait – védetten (pl. lepecsételt borítékban) meg kell őrizni erre alkalmas biztonsági konténerben, hogy vészhelyzet esetén is biztosított legyen a rendszerhozzáférés.
* Használaton kívül, a hitelesítési tokent az eszköztől szeparáltan kell tárolni.
* Az **Informatikai Biztonsági Felelős**nek és a rendszergazdának meg kell határozniuk azokat a rendszer eseményeket, ahol a felhasználóknak újra kell azonosítania magát.
* A rendszer csak limitált visszacsatolási információt szolgáltathat a felhasználónak a hitelesítési eljárás alatt, így megakadályozza a felhasználót abban, hogy ismerteket szerezzen a hitelesítési folyamatról.
* Lehetővé kell tenni az interaktív kapcsolatok zárolását. Egy előre meghatározott felhasználót 15 perc inaktivitás után felül kell írni, vagy törölni kell a kijelzőeszközöket (képernyőket). Az aktuális képernyőtartalmat olvashatatlanná kell tenni, le kell tiltani minden felhasználói tevékenységet, a hozzáférést / kijelzőket és zárolni kell a munkameneteket.
* Meg kell engedni, hogy a felhasználó zárolhassa saját interaktív kapcsolatait (alkalmazásait, munkameneteit), felül kell írnia, vagy törölnie kell a kijelző eszközöket (képernyőket), az aktuális képernyőtartalmat olvashatatlanná kell tennie, le kell tiltania minden felhasználói tevékenységet, a hozzáférést / kijelzőket és zárolnia kell a munkameneteket.
* Ahol hordozható számítógépen tárolnak, vagy dolgoznak fel minősített információt, azt az eszközt úgy kell kezelni, mint egy minősített dokumentumot (iratot).
* A hordozható informatikai eszközökön, diszkrét címkével kell jelezni azt, hogy az eszközön magas minősítésű adat tárolása, vagy feldolgozása történik.
* Minősített feldolgozást hordozható számítógépen csak minősített adatok feldolgozására alkalmas, kijelölt területen lehet végezni. Ha az eszköz nincs használatban, magas minősítésű dokumentumok számára engedélyezett biztonsági konténerben kell tárolni.
* Amikor az adathordozó a mobil informatikai eszközzel együtt elhagyja a biztonsági területet, továbbra is védeni kell a hozzáférés-védelmi intézkedésekben megfogalmazott szabályok szerint. Hordozható informatikai eszközre csak ellenőrzött környezetben csatlakoztatható nyomtató.
* A törölt adatok (maradék információ) védelmi mechanizmusának gondoskodnia kell arról, hogy a törölt információ többé már ne legyen vagy (ne túl hosszú ideig) legyen hozzáférhető, és ezekre vonatkozó információkat az újonnan létrehozott objektumok (fájlok) ne tartalmazzanak. Ez a védelem szükséges a logikailag már törölt de fizikailag még elérhető adatok esetében.

#### A távmunka (3.3.10.13. [3])

Távmunka esetén is gondoskodni kell a biztonsági követelmények és előírások betartásáról, a megfelelő és rendszeres ellenőrzésről.

A távmunkát végző csak a kijelölt csatlakozási pontokon keresztül csatlakozhat a **Szervezet** hálózatához. Az **Informatikai Vezető** határozza meg ezeket a belépési pontokat. A munkaállomásokon egyidejűleg modem és hálózati kártya (engedély nélkül) nem lehet.

### Kulcsmenedzsment (3.3.13.10. [2])

A kulcsmenedzsmentet kötelező jelleggel ki kell alakítani minden elektronikus aláírással, rejtjelezéssel rendelkező rendszerben. A kulcsmenedzsment kialakítása során a hatályos jogi szabályozást, és a PKI-ra vonatkozó nemzetközi szabályozást kell figyelembe venni.

#### A kriptográfiai kulcsok védelme

A rendszerben használt kriptográfiai kulcsok védelme:

* A kriptográfiai kulcsok fizikai, valamint speciális, illetve fokozott biztonságot igénylő esetben rejtjelezéssel megvalósított logikai védelméről is gondoskodni kell.
* Szükség esetén a kulcs-felek megosztásával kell biztosítani a rejtjelkulcsok védelmét.

A kulcshamisítás kockázatának csökkentése érdekében, előzetesen meg kell határozni a kulcsok aktiválásának és visszavonásának dátumait. A kulcs élettartama függ a vélelmezett kockázat mértékétől.

A nyilvános kulcsokkal való esetleges visszaélések kockázatának csökkentése érdekében, csak hitelesített nyilvános kulcsok használhatók a rendszerben. A kriptográfiai szolgáltatók külső szállítóival, például egy hitelesítő hatósággal kötött, a szolgáltatás mértékét meghatározó megállapodásoknak vagy szerződéseknek szabályozniuk kell a felelősség kérdését.

# Jogszabályi háttér

* 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)
* 41/2015. (VII.15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.
* 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenység vizsgálat lefolytatásának szabályairól
* 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról.
* 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről.
* 38/2011. (III. 22.) Korm. Rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról.
* 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információ-biztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

# Megismerési nyilatkozat

**Megismerési nyilatkozat**

A szabályzatban foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

|  |  |  |  |
| --- | --- | --- | --- |
| **Név** | **Beosztás** | **Kelt** | **Aláírás** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |