Ügyszám: VE/72/00554-1/2025.

A Veszprém Vármegyei Kormányhivatal vezetője

7/2025. (VII. 9.) utasítása

az Információbiztonsági Szabályzatáról

ELSŐ RÉSZ
Általános rendelkezések

I. Fejezet
Információbiztonsági politika

1. § (1) A Veszprém Vármegyei Kormányhivatal (a továbbiakban: kormányhivatal) elkötelezi magát az információbiztonság erősítése mellett.
(2) A kormányhivatal elektronikus információs rendszereiben a kezelt adatok védelme az Európai Unió és Magyarország hatályos jogszabályaival összhangban, a bizalmasság, sértetlenség, rendelkezésre állás szempontjából úgy kerül kialakításra, hogy a védelem az elektronikus információs rendszerre és környezetére nézve teljes körű, zárt és a kockázatokkal arányos legyen, illetve a megvalósított védelmi képességek a rendszer teljes életciklusában folytonosan működjenek.
(3) A fentiekkel összhangban a kormányhivatal

a) az elektronikus információs rendszerekben az ügyfelek adatait a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjainak megfelelően biztonságosan kezeli;
b) betartja a kezelt adatokra vonatkozó jogszabályi előírásokat, követi ezek változásait, a szükséges intézkedéseket beépíti a folyamataiba és rendszereibe;
c) azonosítja és értékeli az információbiztonságot veszélyeztető kockázatokat és azok arányában meghatározza a kockázatok kezeléséhez szükséges intézkedéseket;
d) gondoskodik az elektronikus információs rendszerek biztonságának fenntartásáról, az incidensek kezeléséről, az üzletmenet folytonosság biztosításáról;
e) folyamatosan fejleszti a foglalkoztatottak információbiztonsággal kapcsolatos tudatosságát és elkötelezettségét.

(4) A fentiek megvalósítása érdekében a kormányhivatal gondoskodik a szükséges feltételek teljes körű biztosításáról.

II. Fejezet
Információbiztonsági irányítási rendszer

1. Az Információbiztonsági irányítási rendszer alapelvei

2. § (1) A kormányhivatal Információbiztonsági Irányítási Rendszert működtet (a továbbiakban: IBIR) az Információbiztonsági politika által meghatározott célok elérése érdekében. Az IBIR meghatározza a szabályozási rendszer kereteit, szabályzó elemeit, egyéb területekhez való kapcsolódásának módját, működtetéséhez szükséges alapelveket úgy, hogy a kormányhivatal információbiztonságának folyamatos működtetése és fejlesztése, egységes keretek és célok mentén valósuljon meg.
(2) Az IBIR meghatározza a kormányhivatalban használt szabályozó dokumentumok struktúráját, azok kötelező tartalmát, kezelésük, módosításuk, kiadásuk módját. Az IBIR-ben megjelölt dokumentumok alkotják a kormányhivatal szabályozó dokumentumainak struktúráját és azon belül elfoglalt helyét.

2. Irányítási struktúra

3. § (1) A kormányhivatal információbiztonságának egységes irányítási rendszerét az Információbiztonsági Munkacsoport (a továbbiakban: munkacsoport) biztosítja.
(2) A munkacsoport a kormányhivatalt érintő információbiztonsági kérdésekben javaslatokat fogalmaz meg, központi koordinációs tevékenységet lát el, a kormányhivatal információbiztonság feladataival kapcsolatosan a költségvetésére vonatkozó irányelveket és javaslatokat fogalmaz meg.

(3) A munkacsoport állandó tagjai az információbiztonságban érintett szerepkörök listájában (1. számú függelék) megjelölt személyek. A szerepkörökhöz rendelt személyek mindenkor aktuális listáját jelen szabályzat mellékleteként közzé kell tenni a NOE Egységes Kormányhivatali Informatikai Rendszer Csoportmunka (https://vibe.kh.gov.hu) erre a célra kialakított tárhelyén.
(4) A munkacsoport nem állandó tagjai a munkacsoport által meghívott, az érintett témában szakértő egyéb személyek.
(5) A munkacsoport rendszeres vagy eseti megbeszéléseket tart, a megvitatásra kerülő témától függően. A munkacsoport maga határozza meg, mely témákat kell rendszeres időközönként és melyeket eseti megbeszélések keretében megvitatni.
(6) A megvitatásra kerülő téma, illetve feladat jellegétől függően vesznek részt az állandó tagok és az esetleges meghívott tagok a megbeszéléseken.

3. Kontrollpontok jelölése az egyes szabályozó dokumentumokban

4. § A szabályozó dokumentumok fejezet címeiben vagy bekezdéseiben zárójelben a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet (a továbbiakban: rendelet) szerinti kontrollpontok, szögletes zárójelben pedig a hozzá tartozó biztonsági osztály besorolás kerülhet rögzítésre. Az adott fejezetek, bekezdések a megjelölt osztálytól felfelé alkalmazandók az egyes elektronikus információs rendszerek osztályba sorolásától függően. A jelölés technikai segítséget biztosít a kontrollpontoknak történő megfeleltetés vonatkozásában.

4. Szabályozó dokumentumok

5. § (1) A kormányhivatal a szabályozó dokumentumai tekintetében
a) szabályzat,
b) eljárásrendek és
c) munkautasítások
szintjeit határozza meg.
(2) A szabályzat szintjén az Információbiztonsági Szabályzat (a továbbiakban: IBSZ) kerül megfogalmazásra.
(3) A kormányhivatal a rendeletben meghatározott szabályzatokat (valamennyi szabályzat esetében) az IBSZ kapcsolódó részében fogalmazza meg.
(4) A kormányhivatal a 2. számú mellékletben megjelölt eljárásrendek kiadását határozza meg.
(5) Az eljárásrendeket az IBF készíti elő az IÜFV vezető közreműködésével, az elkészítésért az IFEFV felel.
(6) Az eljárásrendeket az IFEFV adja ki a Főispán jóváhagyásával.
(7) Az eljárásrendek egy dokumentumban kerülnek kiadásra Információbiztonsági eljárásrendek címen.

III. Fejezet
Programmenedzsment

5. A szabályzat célja[1]

6. § (1) A szabályzat elkészítésének célja, hogy a kormányhivatal rendelkezésében lévő elektronikus információs rendszerek (a továbbiakban: EIR) teljes életciklusában biztosítsa

[1] Módosította a 1/2026. (I. 19.) főispáni utasítás 1. §-a. Hatályos 2026.01.20-tól

a) az EIR-ben kezelt adatok, információk és az EIR által nyújtott vagy azon keresztül elérhető szolgáltatások bizalmassága, sértetlensége és rendelkezésre állása, valamint
b) az EIR elemeinek sértetlensége és rendelkezésre állása

vonatkozásában a zárt, teljes körű, folytonos és kockázatokkal arányos védelmet.

(2) Az EIR védelme keretében a kormányhivatal, az adatkezelő vagy az adatfeldolgozó által, adott cél érdekében

a) az adatok, információk kezelésére használt eszközök, ideértve a környezeti infrastruktúrát, a hardvert, a hálózatot és az adathordozókat,
b) az adatok, információk kezelésére használt eljárások, ideértve a szabályozást, a szoftvert és a kapcsolódó folyamatokat, valamint
c) az a) és b) pontban foglaltakat kezelő személyek

együttesének védelmét is biztosítja.

(3) A szabályzat átfogóan szabályozza a kormányhivatal információbiztonsági követelményeit, leírja a kormányhivatalra érvényes biztonsági szabályokat és követelményeket, amelyek az egész szervezeten belül kötelező érvényűek.

6. A szabályzat hatálya

7. § (1) A szabályzat hatálya kiterjed a kormányhivatal valamennyi szervezeti egységénél kormányzati szolgálati jogviszonyban, munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban állókra (a továbbiakban együtt: foglalkoztatott), azzal, hogy a kormányhivatal által használt elektronikus információs rendszerek külső üzemeltetőire, fejlesztőire, szerződéses úton történő egyéb alkalmazóira az eljárásrend rendelkezéseinek megtartását szerződésben, vagy egyéb megállapodásban rögzíteni kell.

(2) A szabályzat hatálya kiterjed a kormányhivatal székhelyére, minden telephelyére, továbbá mindazon objektumokra és helyiségekre, ahol a kormányhivatal elektronikus információs rendszereinek erőforrásai találhatók, illetve felhasználásuk zajlik.

(3) A szabályzat hatálya kiterjed a kormányhivatal elektronikus információs rendszereinek minden erőforrására (infrastruktúra, technológia, szoftverelemek, hardverelemek, adathordozók, adatok).

(4) Amennyiben a kormányhivatal szervezeti egységei vonatkozásában az érintett szakmai központi irányító a jelen szabályzattól eltérő, magasabb szintű biztonsági előírásokat állapít meg, úgy a szakmai központi irányító által előállított információbiztonsági szabályozókat és eljárásrendeket kell alkalmazni a helyi sajátosságok figyelembevétele mellett.

7. A szabályzat kezelése

8. § (1) A szabályzat elkészítése, felülvizsgálata és szükség szerinti módosítása az IBF feladata, együttműködve az IÜFV, illetve az általa kijelölt Informatikai infrastruktúra üzemeltetési rendszergazdák. A szabályzat elkészítéséért felelős az IFEFV. A felülvizsgálat eredményéről az IBF tájékoztatja a Főispánt.

(2) A kormányhivatalt, illetve környezetét érintő információbiztonsági vagy szervezetet érintő változások esetén soron kívül szükséges a szabályzat eseti felülvizsgálata.

(3) A szabályzatot a kormányhivatal a személyi hatályban meghatározott személyek részére elérhető felületre helyezi ki úgy, hogy annak tartalma ne legyen módosítható, illetve csak az arra jogosultak érhessék el.

(4) A szabályzat tartalmának megismerését, a felhasználók normakövetésének fejlesztését, erősítését célzó kurzust alakít ki az IBF a kormányhivatal oktatási felületén, mely tananyag és teszt részből áll. Valamennyi új belépő foglalkoztatott részére a fenti kurzus elvégzése a munkakezdését követő 30 napon belül kötelező.

(5) A szabályzat betartásának ellenőrzése az IBF feladata. Az ellenőrzés során közreműködnek az érintett személy vagy szervezeti egység vonatkozásában a kormányhivatal szervezeti egységeinek vezetői, az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt

vevő szervezeti egységek foglalkoztatottjai, vezetői, valamint az informatikai fejlesztésben, üzemeltetésben, illetve a kormányhivatali ingó és ingatlan üzemeltetéséért felelős vezetők és foglalkoztatottjaik.

8. Értelmező rendelkezések

9. § A szabályzatban használt alapfogalmakat a kiberbiztonsági törvény tartalmazza.

9. Elektronikus információs rendszerek

10. § (1) A kormányhivatal rendelkezésében lévő elektronikus információs rendszerek felsorolását a 3. számú melléklet tartalmazza.
(2) A kormányhivatal az általa használt központi rendszerek listáját a 4. számú melléklet szerinti tartalommal tartja nyilván és a mindenkor aktuális listát jelen szabályzat mellékleteként közzéteszi a NOE Egységes Kormányhivatali Informatikai Rendszer Csoportmunka (https://vibe.kh.gov.hu) erre a célra kialakított tárhelyén.
(3) A kormányhivatal által igénybe vett, központi szolgáltató által biztosított szolgáltatások és támogató rendszerek listáját az 5. számú melléklet szerinti tartalommal tartja nyilván és a mindenkor aktuális listát jelen szabályzat mellékleteként közzéteszi a NOE Egységes Kormányhivatali Informatikai Rendszer Csoportmunka (https://vibe.kh.gov.hu) erre a célra kialakított tárhelyén.
(4) A kormányhivatal rendelkezésében lévő vagy a kormányhivatal által használt egyéb támogató rendszerek listáját az 6. számú melléklet tartalmazza.

MÁSODIK RÉSZ
Informatikai védelmi intézkedések

IV. Fejezet
Hozzáférés-felügyelet

10. A hozzáférés felügyelet alapelvei

11. § (1) Az információbiztonsági hozzáférés-felügyelet alapvető célja, hogy biztosítsa, csak az arra jogosult felhasználók, rendszerek vagy folyamatok férhessenek hozzá bizonyos erőforrásokhoz (adatokhoz, rendszerekhez, hálózatokhoz). Ez az egyik legfontosabb pillére a kiberbiztonságnak, és a CIA-modell (Confidentiality, Integrity, Availability – Bizalmasság, Sérthetetlenség, Elérhetőség) mindhárom aspektusát támogatja.
(2) A fentieken felül a legfontosabb alkalmazandó alapelvek:
a) minimális jogosultság elve (Principle of Least Privilege - PoLP),
b) felelősségi körök szétválasztása (Separation of Duties - SoD),
c) központosított hozzáférés-felügyelet (Centralized Access Control),
d) hozzáférés naplózása és auditálása (Logging and Auditing),
e) hozzáférés rendszeres felülvizsgálata (Regular Access Reviews).
(3) A további részletszabályokat a Hozzáférés-felügyeleti eljárásrend tartalmazza.

11. Az információbiztonság szervezete

12. § (1) A kormányhivatal vezetője a Főispán, aki legtöbb esetben a kormányhivatal érintő kérdésekben, ügyekben a hatáskör címzettje.
(2) A kormányhivatalban az EIR-ek biztonsága megteremtésének, fenntartásának kiemelt szereplője az IBF. Az IBF elérhetőségeit a 7. számú melléklet tartalmazza.
(3) A kormányhivatalban az információbiztonság megteremtésében az Információbiztonsági Munkacsoport tagjai vesznek részt.
13. § A kormányhivatalban az elektronikus információbiztonság megteremtése kapcsán releváns szerepeket betöltő személyek listáját az 1. számú melléklet tartalmazza.
14. § A kormányhivatal az információbiztonságot, kibervédelem kérdéseit érintő kérdésekben konzultációs jelleggel, és hatósági vizsgálat esetén hatósági vizsgálat keretei között kapcsolatot tart az IBF-en keresztül a Nemzeti Kibervédelmi Intézettel.

12. Fiókok, fióktípusok meghatározása

15. § (1) A kormányhivatalban valamennyi felhasználó rendelkezik egy címtárobjektummal, mely alapja a felhasználói fióknak. A felhasználói fiókot szintetikai szempontból megkülönböztetjük külső és belső felhasználóra. A külső felhasználó részére kiosztandó jogosultságok köre korlátozott.
(2) A természetes személyekhez kapcsolódó felhasználói fiókokon kívül a kormányhivatal technikai fiókokat kezel, ezek jellemzően szervezeti egységhez rendelt szervezeti postafiókok, tesztelés, nyomatelőállító eszközök riportolásához kialakított fiók stb.

13. Fiókkezelés, fiók életciklus

16. § (1) A kormányhivatal a központi címtárhoz kapcsolódó jogosultságok tekintetében a jogosultságmenedzsment és a humánpolitikai szakrendszer alkalmazásával együttesen biztosítja a teljes felhasználói életciklus kezelését.
(2) A központi címtáron kívül kezelt (szakági rendszerek saját jogosultságkezelő rendszerében) rendszerek vonatkozásában az felhasználói fiók életciklus eseményeit (létrehozás, változás kezelés, kivétel kezelés, kiléptetés) a szakrendszeren belül, az érintett szervezeti egység vezetője által benyújtott igény alapján a szakági jogosultságmenedzsment feladatokat ellátó szervezet (IFEFV vagy kormányhivatalon kívüli központi feladatellátó szerv) rögzíti.
17. § (1) A személyi biztonsági feltételek meglétét követően

a) a humánpolitikai rendszerben a megfelelő paraméterekkel felvételre kerül a felhasználó,
b) az ott rögzített adatok ütemezett, automatikus adatszinkron útján az IDM-be kerülnek és ott létrejön egy inicializálandó felhasználói objektum,
c) a kormányhivatal IDM adminisztrátorai kapnak egy üzenetet arról, hogy van új inicializálandó felhasználó, és elvégzik az inicializálást,
d) az inicializáció során az IDM adminisztrátor beállítja a felhasználó szervezeti egységéhez kapcsolódó paramétereket, kiosztásra kerül a felhasználó e-mail címe.

(2) az inicializálás befejezésével létrehozásra kerül a felhasználó a címtárban, a létrejött felhasználó közvetlen vezetője értesítést kap a felhasználói inicializálás tényéről, melyet követően elindítható részéről a jogosultság igénylés.
18. § (1) A kormányhivatali címtárhoz kapcsolódó, IDM-ben kezelt jogosultságok vonatkozásában a jogosultság igénylési eljárás:

a) a felhasználó felettes vezetője megigényli az IDM rendszerben a felhasználó számára a munkához szükséges jogosultságokat;
b) az IDM rendszerben a jogosultságigényhez definiált jóváhagyásokat követően az igényelt jogosultság a felhasználóhoz kerül hozzárendelésre;

c) a felhasználó a feladatellátásához szükséges eszközöket megkapja, melyet a folyamat során hozzá rendelt jogosultságok birtokában tudja használatba venni.

(2) A kormányhivatal címtár alapú jogosultságain kívül a jogosultságigénylés a (3)-(5) bekezdésben kerül meghatározásra.

(3) A kormányhivatal kezelésében lévő szakmai rendszereken belüli jogosultságkezelés esetében az érintett szervezeti egység vezetője a kormányhivatal bejelentő felületre elküldi a Jogosultság igénylési, módosítási és megszüntetési űrlapot (8. számú melléklet), vagy az alábbi adatokat minimálisan tartalmazó igényt:

a) felhasználó neve és adatai (szervezeti egység, címtárazonosító),
b) igényelt erőforrásobjektumok megnevezése, jogosultság, szerepkör meghatározása,
c) igényelt jogosultság kezdeti dátuma, végdátuma.

(4) Központi (kormányhivatalon kívüli jogosultságmenedzsmenttel rendelkező) jogosultságkezelés esetében az érintett szervezeti egység vezetője a központi szerv által biztosított bejelentő felületen elküldi a jogosultság igénylést, ami minimálisan a következő adatokat tartalmazza:

a) felhasználó adott központi rendszerben kurrens vagy kialakítandó azonosító adatai,
b) igényelt erőforrásobjektumok megnevezése, jogosultság, szerepkör meghatározása,
c) igényelt jogosultság kezdeti dátuma, végdátuma.

(5) KAÜ azonosítást és hitelesítést használó központi alkalmazások jogosultságkezelése esetében az érintett szervezeti egység vezetője a központi szerv által biztosított bejelentő felületen elküldi a jogosultság igénylést, ami minimálisan a következő adatokat tartalmazza:

a) felhasználó azonosító adatai (4T adatok, illetve adott központi rendszerben kurrens vagy kialakítandó azonosító adatai,
b) igényelt erőforrásobjektumok megnevezése, jogosultság, szerepkör meghatározása,
c) igényelt jogosultság kezdeti dátuma, végdátuma.

19. § (1) A kormányhivatali címtárhoz kapcsolódó, IDM-ben kezelt jogosultságok vonatkozásában a jogosultság módosítási eljárás:

a) a felhasználó felettes vezetője megigényli az IDM rendszerben a felhasználó részére korábban kiosztott jogosultság(ok)hoz kapcsolódó módosítási igényeit;
b) az IDM rendszerben a jogosultságigényhez definiált jóváhagyásokat követően az igényelt jogosultság a felhasználóhoz kerül hozzárendelésre.

(2) A kormányhivatal címtár alapú jogosultságain kívül a jogosultságigénylés a (3)-(5) bekezdésben kerül meghatározásra.

(3) a kormányhivatal kezelésében lévő szakmai rendszereken belüli jogosultságkezelés esetén az érintett szervezeti egység vezetője a kormányhivatal bejelentő felületén elküldi a 7. számú melléklet szerinti adatlapot, vagy az alábbi adatokat minimálisan tartalmazó igényt:

a) felhasználó neve és adatai (szervezeti egység, címtárazonosító),
b) korábban igényelt, módosítandó jogosultság megnevezése,
c) a módosított jogosultságigényhez kapcsolódó igényelt erőforrásobjektumok megnevezése, jogosultság, szerepkör meghatározása,
d) igényelt jogosultság kezdeti dátuma, végdátuma.

(4) Központi (kormányhivatalon kívüli jogosultságmenedzsmenttel rendelkező) jogosultságkezelés esetén az érintett szervezeti egység vezetője a központi szerv által biztosított bejelentő felületén elküldi a felhasználó részére korábban kiosztott jogosultság(ok)hoz kapcsolódó módosítási igényeit, ami minimálisan a következő adatokat tartalmazza:

a) felhasználó adott központi rendszerben meglévő azonosító adatai,
b) korábban igényelt, módosítandó jogosultság megnevezése,
c) a módosított jogosultságigényhez kapcsolódó igényelt erőforrásobjektumok megnevezése, jogosultság, szerepkör meghatározása,
d) igényelt jogosultság kezdeti dátuma, végdátuma.

(5) KAÜ azonosítást és hitelesítést használó központi alkalmazások jogosultságkezelése esetén az érintett szervezeti egység vezetője a központi szerv által biztosított bejelentő felületen elküldi a felhasználó részére korábban kiosztott jogosultság(ok)hoz kapcsolódó módosítási igényeit, ami minimálisan a következő adatokat tartalmazza:

a) felhasználó azonosító adatai (4T adatok, illetve adott központi rendszerben kurrens vagy kialakítandó azonosító adatai,
b) a módosított jogosultságigényhez kapcsolódó igényelt erőforrásobjektumok megnevezése, jogosultság, szerepkör meghatározása,
c) igényelt jogosultság kezdeti dátuma, végdátuma.

20. § (1) A kormányhivatali címtárhoz kapcsolódó, IDM-ben kezelt jogosultságok vonatkozásában a jogosultságok nyilvántartása az IDM rendszerben történik. A jogosultság nyilvántartásáért felelős az IFEFV.

(2) A kormányhivatal címtár alapú jogosultságain kívül a jogosultságok nyilvántartása (3)-(5) bekezdésben kerül meghatározásra.

(3) A kormányhivatal kezelésében lévő szakmai rendszereken belüli jogosultságok nyilvántartása a SZEV/AG feladata és felelőssége. A jogosultságok implicit módon az érintett szakmai rendszeren belül elérhetők, azonban nem helyettesítik a szervezeti egységnél vezetett jogosultság nyilvántartást.

(4) A központi (kormányhivatalon kívüli jogosultságmenedzsmenttel rendelkező) jogosultságok nyilvántartásáért felelős – tekintettel arra, hogy a kormányhivatal informatikai feladatokat ellátó szervezeti egység nem része a jogosultságmenedzsment folyamatnak - az igénylő SZEV/AG.

(5) A KAÜ azonosítást és hitelesítést használó központi alkalmazások esetén jogosultság nyilvántartásáért felelős az igénylő SZEV/AG.

21. § (1) Az IDM rendszerben a felhasználó jogosultságainak visszavonását a SZEV/AG kezdeményezi.

(2) ASZEV/AG akadályoztatása vagy egyéb indok miatt, kivételes esetben, az IDM adminisztrátorok a kormányhivatal hibajegy kezelő rendszerébe érkező jelzés alapján végezhetik el ezt a műveletet.

(3) A jogosultságok megszüntetésének igénylése, illetve bejelentése minden esetben az érintett felhasználó szervezeti egységének vezetőjének a feladata és a felelőssége.

(4) A kormányhivatal címtár alapú jogosultságain kívül a jogosultságok megszüntetése (5)-(7) bekezdésben kerül meghatározásra.

(5) Kormányhivatal kezelésében lévő szakmai rendszereken belüli jogosultság megszüntetése: az érintett szervezeti egység vezetője a kormányhivatal bejelentő felületén elküldi a 8. számú mellékletet, vagy a jogosultság megszüntetés igényét, ami minimálisan a következő adatokat kell tartalmaznia:

a) felhasználó neve és adatai (szervezeti egység, címtárazonosító),
b) megszüntetendő jogosultság megnevezése,
c) megszüntetés dátuma.

(6) A központi (kormányhivatalon kívüli jogosultságmenedzsmenttel rendelkező) jogosultság megszüntetése: az érintett szervezeti egység vezetője a központi szerv által biztosított bejelentő felületén elküldi a már meglévő jogosultság megszüntetés igényét, ami minimálisan a következő adatokat kell tartalmaznia:

a) felhasználó adott központi rendszerben meglévő azonosító adatai,
b) megszüntetendő jogosultság megnevezése,
c) megszüntetés dátuma.

(7) A KAÜ azonosítást és hitelesítést használó központi alkalmazások esetén jogosultság megszüntetése: az érintett szervezeti egység vezetője a központi szerv által biztosított bejelentő felületén elküldi a már meglévő jogosultság megszüntetés igényét, ami minimálisan a következő adatokat kell tartalmaznia:

a) felhasználó azonosító adatai (4T adatok, illetve adott központi rendszerben meglévő azonosító adatai,
b) a módosított jogosultságigényhez kapcsolódó igényelt erőforrásobjektumok megnevezése, jogosultság, szerepkör meghatározása,
c) felhasználó adott központi rendszerben meglévő azonosító adatai,
d) megszüntetendő jogosultság megnevezése,
e) megszüntetés dátuma.

V. Fejezet
Tudatosság és képzés

14. A tudatosság és képzés alapelvei

22. § (1) A kormányhivatal a munkahelyi biztonságtudatossági kultúra megteremtése, a „kiberbiztonsági higiénia” fejlesztését szolgáló információk, gondolatok, alkalmazható tudás megszerzése érdekében információbiztonsági képzéseket alakít ki.
(2) Az információbiztonság tudatosság fejlesztését célzó képzési rendszert a következő formában szükséges kialakítani:
(3) Általános információ biztonság tudatosság és adatvédelmi ismereteket fejlesztő képzés: e-learning, alapképzés, valamennyi felhasználó részére: belépéskor egy rövidített változat, illetve évente legalább egy alkalommal teljes változat. Opcionális elemként konzultáció biztosítható.
(4) Információbiztonság megteremtésében, fenntartásában érintett résztvevők részére kiegészítő kurzus: e-learning, kompetenciafejlesztés, közreműködők részére. Junior, mid-senior és senior munkatársak részére eltérő időtartammal, hangsúlyokkal.
(5) Erőforrás, folyamat és adatgazda részére kiegészítő kurzus: e-learning, kompetenciafejlesztés, vezetők részére.
(6) Informatikai üzemeltető, fejlesztő kör részére workshop formában: jelenléti, informatikusok részére, évi 4 alkalommal.
(7) Biztonsági személyzet részére workshop formában: jelenléti, biztonsági személyzet részére, évi 4 alkalommal.
(8) Erőforrás, folyamat és adatgazda részére kiegészítő kurzus: jelenléti, vezetők részére, évi 4 alkalommal.
(9) A képzés rendszerének kialakítását a következő lépések mentén, az alábbi szerkezetben szükséges elvégezni:

a) szervezeti, célcsoportot érintő lehatárolás,
b) az oktatás formájának, módszertanának, gyakoriságának meghatározása, a tartalmi elemek kialakítása,
c) számonkérés, a visszamérés követelményeinek rögzítése,
d) dokumentálás kereteinek kialakítása,
e) visszacsatolás, a képzés fejlesztése.

(10) A további részletszabályokat a Tudatossági és képzési eljárásrend tartalmazza.

15. Általános, valamennyi felhasználót érintő tudatossági képzés

23. § (1) A valamennyi felhasználó részére kialakított információbiztonság tudatosság fejlesztésére szolgáló kötelező alapképzést e-learning képzési formájában kell kialakítani. Így biztosítható az egyenszilárdságú, valamennyi foglalkoztatott részére átadott, a munkavégzés és a szervezeti kultúra adatvédelmi és információbiztonság tudatossági peremfeltételeit szolgáló ismeretanyag.
(4) A képzés kötelező tartalmi elemei:
(5) Bevezető: Az információbiztonság és azon belül is a biztonságtudatosság múltja, jelene, jövője, szerepe, fontosabb szabályzó elemek. Ennek a tömbnek a szerepe a képzésben résztvevő foglalkoztatottak „ráhangolása” a tananyagra.
(6) Alapfogalmak ismertetése: A terminológia ismertetése mellett a fizikai, logikai és adminisztratív biztonság fontosabb elemeinek bemutatása, a biztonság alapvető kérdéseinek ismertetése.
(7) Szabályozási környezet ismertetése: jogszabályok, GDPR, ISO 27001 szabályozó dokumentumok bemutatása, hatályos információbiztonság tartalmát érintő vállalati utasítások. Jogok, kötelezettségek, elvárt magatartás, informatikai üzemeltetést, adatvédelmet, információbiztonságot érintő események esetén általánosan elvárt eljárásrendek ismertetése.

(8) Fenyegetettségek bemutatása: Az információbiztonságot érintő, illetve adatvédelmi vetülettel rendelkező fenyegetettségek fizikai, logikai és adminisztratív területek szerint csoportosított bemutatása a hazai ECDL tananyagokban megismert referenciamodell egyes elemeinek felhasználásával, a következők szerint:

a) a fenyegetés megnevezése,
b) a fenyegetés jellegének és hatásának megjelölése,
c) a fenyegetés bemutatása, hatásmechanizmusának leírása,
d) a veszélyeztetett vagyonelemek leírása,
e) a veszély megelőzésének módja, az elvárt felhasználói magatartás meghatározása,
f) az esemény bekövetkezésének jelei, a felismerésének módja,
g) a veszély elhárítása: a vállalati környezetben elvárt felhasználói magatartás, azonnal végrehajtandó műveletek, dokumentálási és értesítési kötelezettségek leírása,
h) példák, érdekességek a bemutatott fenyegetettség kapcsán, gyakorlati, interaktív elemek alkalmazásával,
i) megtörtént esetek bemutatása.

(9) Social engineering témakör: A pszichológiai manipulációs eszköztár alapvető elemeinek bemutatása:

a) támadás forgatókönyvének ismertetése,
b) humán alapú támadási módszerek ismertetése, például: segítség kérés és nyújtás, kölcsönösség, felépült kapcsolat kihasználása, shoulder surfing és dumpster diving módszerek, tailgating, piggybacking módszerek.

(10) Az alapképzést kiegészítő jelenléti képzés opcionális elemként szükséges beépíteni:

a) a fenyegetettség bemutatása tömbhöz kapcsolódó gyakorlati ismeretek, esettanulmányok, leírások, a hallgatóság bevonásával végrehajtott konzultációk,
b) a social engineering témakörhöz kapcsolódóan a téma támadó oldali szemszögből történő bemutatása, rávilágítva az áldozati szerep elkerülésének gyakorlati módszereire:
   ba) hogyan ismerjük fel, hogy manipulálni próbálnak,
   bb) hogyan ne legyünk áldozatok,
   bc) teendők social engineering támadás esetén.

16. Szerepkör alapú képzés

24. § (1) A kormányhivatalban az információbiztonság szempontjából kialakított szerepkör csoportok részére külön képzési tartalmak kialakítása szükséges, melynek során cél:

a) vezetői elkötelezettség és támogató szerep erősítése, minőségszemélet,
b) az információbiztonság, biztonságszemlélet,
c) a kapcsolódó szabályozók ismerete,
d) az incidens, katasztrófa, ügymenet folytonosságot érintő szerep.

(2) Ebben a pontban kialakított e-learning kurzus tematikáját – figyelemmel a résztvevők stratégiai szemléletét, a szervezet vonatkozásában irányító, erőforrásgazda szerepét – az alábbi tartalommal szükséges kialakítani:

(3) Szabályozási környezet: A szervezet és adatvagyon védelmének szemszögéből bemutatva az egyes szabályozó elemeket (jogszabályok, szabványok, ajánlások, információbiztonsági, adatvédelmi, minősített adatkezelést érintő vállalati utasítások, a biztonsági vezető által kiadott szabályozó dokumentumok). Felhasználói és vezetői szinten meghatározott kötelesség – felelősség rendszerét, követelményeit, a normasértés következményeit.

(4) Social engineering: A támadással összefüggő pszichológiai manipulációs eszköztár kibontása, illetve a védekezési technikák ismertetése során az alábbi témakörök részletes kifejtése:

a) az adathalász technikák pszichológiai hátterének, kommunikációs eszköztárának a bemutatása;
b) nézőpont váltás, mely a támadó oldaláról világít rá a biztonság alapvető kérdéseire;
c) érintett részéről árulkodó jelek elrejtése, a testbeszéd kontrollálása;

d) a támadó testbeszédében a manipulációs szándék felismerése.

(5) A vezetők részére tartott jelenléti konzultációk során az alábbi tartalmi elemek kialakítása szükséges:

a) az információbiztonságot érintő szabályozók szervezeti szintű hatásai kapcsán felvetődött kérdések témájában javasolt a konzultációs forma alkalmazása,
b) a kurzus másik felében, pszichológus, illetve social engineer szakértő bevonása mellett a vezetői e-learning képzésben megjelölt social engineering témákban javasolt a szerepjátékelemekkel gazdagított szituációs gyakorlatok levezetése.

(4) Ütemezés: évi öt alkalom (4+1 tartalék időpont) biztosítása.

25. § (1) A kormányhivatalban az információbiztonság szempontjából kialakított szerepkör csoportok részére külön képzési tartalmak kialakítása szükséges, melynek során cél:

a) elvárt információbiztonsági magatartások erősítése,
b) incidenskezelés operatív végrehajtásával kapcsolatos tevékenységek fejlesztése,
c) kapcsolódó szabályozási környezet ismerete és a benne foglaltak alkalmazása,
d) információbiztonsági kontrolloknak történő megfelelőség

(2) Az operatív szereplők részére az e-learning tananyag tematikáját tekintve az alábbi elemekből épül fel:

(3) Szabályozási környezet: A feladatellátásban részt vevők vonatkozásában megkövetelt elemei: felhasználói jelzések kezelése, kommunikációs formák és csatornák, incidenskezelés eljárásrend protokoll szintű elemei, felhasználók jogai, feladatai, kötelezettségei, üzemeltetők, biztonsági személyzet, incidenskezelők jogai, feladatai, kötelezettségei; Kiemelt hangsúly: junior és mid-senior foglalkoztatottaknak.

(4) Fenyegetettségek kezelése: Az információbiztonságot érintő eljárásrendek ismertetése fizikai biztonság, informatikai üzemeltetés és incidenskezelés területén gyakorlati megközelítésben, példákkal, esettanulmányokkal színesítve.

(5) Kommunikáció, stresszkezelés: Információbiztonságot érintő operatív feladatellátás során elvárt viselkedés, asszertív kommunikáció, stresszel járó szituációk kezelése. Kiemelt hangsúly: senior és mid-senior foglalkoztatottaknak.

(6) Social engineering: A témában az üzemeltetési területen kockázatként megjelenő humán és számítógép alapú technikák gyakorlati példákon, esettanulmányokon keresztüli megközelítése.

(7) Számítógép alapú támadási módszerek bemutatása, például: adathalász technikák (Phishing, Smishing, Vishing, Pharming, Whailing), scam (hamisított weboldalak), baiting, adathordozók szétszórásán alapuló technikák.

(8) Védelem kialakítása: A vállalatnál alkalmazott védelmi kontrollok bemutatása, a szabályozók által kikényszerített megfelelőségek ismertetése, az informatikai rendszer rendszerelemeinek és az üzemeltetés szabályozóinak bemutatása információbiztonsági szempontrendszeren keresztűl. Kiemelt hangsúly: junior és mid-senior foglalkoztatottaknak.

(9) Az érintett szakterület részére külön-külön workshop megtartása szükséges, az adott területen tapasztalt vendégelőadók bevonásával:

(10) Informatikai üzemeltetés, incidenskezelés területén dolgozó foglalkoztatottak részére incidenskezeléssel kapcsolatos (detektálás, első lépések, elhárítás, tapasztalatok levonása, megszerzett tudás integrálása) ismeretek gyakorlatban történő elsajátítása, szimulált környezetben, „játékos” elemek segítségével, vegyes kor és tapasztalati csoportok kialakításával.

(11) Biztonsági személyzet részére a fizikai biztonság környezetével kapcsolatos ismeretek elmélyítésére, a területre jellemző kockázatok, fenyegetettségek kezelésére vonatkozó tartalmi elemekkel, gyakorlati példákon keresztüli megközelítésben, védendő adatvagyon elemei, adatvédelmi kérdések.

(12) Szabályozókkal, szabályozási környezettel kapcsolatos feladatkataszter, RACI felelősségi tábla gyakorlati bemutatása.

(13) Ütemezés: évi öt alkalom (4+1 tartalék időpont) biztosítása.

17. Számonkérés, visszamérés

26. § (1) Az egyes kurzusok kapcsán az alábbi be és kimeneti követelményeket szükséges alkalmazni:
(2) Alapképzés: formája e-learning, valamennyi felhasználót érinti, előzetes szintfelmérést igényel, a kurzus zárásának feltétele a sikeres vizsga.
(3) Alapképzést kiegészítő jelenléti konzultáció: formája jelenléti, valamennyi felhasználót érinti, előzetes szintfelmérést nem igényel, a kurzus zárásának feltétele az aktív részvétel.
(4) Információbiztonság operatív szereplői számára tartott képzés: formája e-learning, az informatikusokat és a biztonsági személyzetet érinti, előzetes szintfelmérést nem igényel, a kurzus zárásának feltétele a sikeres vizsga.
(5) Információbiztonság operatív szereplői számára tartott workshop: formája jelenléti, az informatikusokat és a biztonsági személyzetet érinti, előzetes szintfelmérést nem igényel, a kurzus zárásának feltétele az aktív részvétel.
(6) Erőforrás, folyamat és adatgazda e-learning kurzus: formája e-learning, az erőforrás, folyamat és adatgazdákat érinti, előzetes szintfelmérést nem igényel, a kurzus zárásának feltétele a sikeres vizsga.
(7) Erőforrás, folyamat és adatgazda konzultáció: formája jelenléti, az erőforrás, folyamat és adatgazdákat érinti, előzetes szintfelmérést nem igényel, a kurzus zárásának feltétele az aktív részvétel.

18. Képzési rendszer kialakítása

27. § (1) A fent meghatározott képzési rendszert az IBF alakítja ki az IFEFV, FVFV, HFV, illetve az általuk kijelölt foglalkoztatottak, vezetők bevonásával. Az e-learning képzést a kormányhivatal számára elérhető e-learning rendszeren szükséges kialakítani.
(2) A képzési rendszert kiegészítendő, az IBF opcionálisan az alábbi információbiztonság tudatosítást fejlesztő további eszközöket alkalmazhatja.
(3) Rendszeres hírlevél: legalább 2 havi rendszerességgel, általános információbiztonsági, adatvédelmi témákról.
(4) Soron kívüli tájékoztató levél: adathalász kampányok, rendkívüli események, incidensek kapcsán.
(5) Normatív utasítások, tájékoztatók kiadása: rendszeresen karbantartott, kiadott, megismertetett szabályzatok.
(6) Információ- biztonsági tematikájú aloldal: vállalati intranet oldal kiegészítése.
(7) Kampányok, versenyek, vetélkedők: vállalati eseményekhez kapcsolva és önállóan évi 2 alkalommal.
(8) Információ- biztonsági szakmai nap: évi egy alkalom, meghívott neves szakértőkkel.
(9) Tréningek feladatellátók részére: külső képzés támogatása (CISA, JNCAA, CCNA, ITIL).
(10) Rendszeres értekezlet / workshop: reszponzív, aktualitások, valós problémák szakmai feldolgozása (adathalász szimuláció, ticketing visszamérés, incidenskezelési gyakorlatok, log elemzési tapasztalatok – visszacsatolások, adatszivárgás monitoring, fejlesztés).
(11) Szervezeti rendezvényekre „beinjektálás”: Vezetői, szakági értekezleten információbiztonsági blokk.
(12) Véleményvezérek megnyerése: bevonás, érdekeltté tétel: információbiztonsági és adatvédelmi szempontok vállalati szintű informális erősítéséhez.

VI. Fejezet
Naplózás és elszámoltathatóság

19. A naplózás és elszámoltathatóság alapelvei

28. § (1) Az EIR adatainak nyomon követéséhez az eseményeket naplózni kell. Az IFEFV felelős a naplózási környezet kialakításáért.
(2) A további részletszabályokat a Naplózási és elszámoltathatósági eljárásrend tartalmazza.

20. Naplózással szemben támasztott általános követelmények

29. § (1) A kormányhivatalnál kialakított naplózásnak legalább a következőket kell teljesítenie az EIR-ben:
(2) Olyan elektronikus naplózási rendszert kell kialakítani, hogy utólag minden esetben meg lehessen határozni, hogy ki, mikor, honnan, milyen bizalmas adathoz, milyen célból (olvasás/létrehozás/módosítás/törlés) fért hozzá.
(3) A különböző EIR naplóállományainak egységes értelmezhetősége érdekében olyan naplózási architektúrát kell kialakítani, ami biztosítja, hogy:

a) ahol csak technikailag lehetséges, a naplózás szerveroldalon történjen,
b) automatikus mechanizmus gondoskodjon az egyes rendszerek, eszközök rendszerórájának szinkronizálásáról.

(4) A naplóbejegyzéseket védeni kell az illetéktelen hozzáféréstől. Elektronikus naplóknál ezt megfelelő jogosultsági beállításokkal kell biztosítani, azokhoz csak a naplózási feladatokkal, illetve a napló adatok ellenőrzésével, vizsgálatával megbízott, arra jogosult személyek férhetnek hozzá.

21. Naplózható események meghatározása

30. § A naplózó rendszernek az alábbi típusú események rögzítésére kell kiterjedniük:

a) rendszerindításokat és leállításokat,
b) rendszerriasztásokat, meghibásodási jelentéseket,
c) a rendszerben fellépő hibákat,
d) felhasználók felvételét, törlését, felfüggesztését, jogosultságának módosítását,
e) a felhasználó bejelentkezést vagy sikertelen bejelentkezési kísérleteket,
f) naplózási funkciók indítását és leállítását,
g) naplóállomány létrehozását, törlését (külön jegyzőkönyvben rögzítve),
h) a rendszerdátum, -idő megváltoztatását,
i) szoftverkonfiguráció megváltozását,
j) nyilvános hálózaton keresztüli kapcsolatnál létrehozást és bontást; ellenoldali fél adatait; forgalom jellege; továbbított vagy fogadott állomány neveit, elérési útvonalát,
k) kijelentkezéseket,
l) tűzfal / IPS / terheléselosztó rendszereken átmenő forgalmat,
m) az azonosítási és a hitelesítési mechanizmus használatát,
n) személyi műveleteket, amelyek a rendszer biztonságát érintik.

22. Naplóbejegyzések tartalma

31. § A naplóállományoknak az alábbi információkat kell minimálisan tartalmazni:

a) felhasználó azonosítója,
b) számítógép azonosítója vagy pontos helye,

c) a használt hálózati cím,
d) az esemény dátuma és ideje (jegyezze fel, hogy UTC vagy helyi idő alapján),
e) a bekövetkezett esemény részletei,
f) a használt szoftvert.

23. Naplóbejegyzések tárolása, megőrzése

32. § (1) Az eseménynaplók és az azok kezeléséhez kapcsolódó biztonsági naplók tárolását a következő szempontok figyelembevételével kell megoldani:
a) a napló adatokat időpecséttel kell ellátni,
b) a naplóadatoknak sértetlenül rendelkezésre kell állniuk az esetleges elévülési időn belül,
c) biztosítani kell, hogy az adatokban keletkezésük után változtatást már ne lehessen végrehajtani,
d) az adatok bizalmasságára tekintettel, az adatok nem juthatnak illetéktelenek kezébe.
(2) Mind a rendszergazdai tevékenységet, mind a biztonsági eseményeket nyomon kell követni az egyes EIR-ben. A kiemelt jogosultságokkal bíró felhasználók ne tudjanak nyomtalanul módosítani a naplózási beállításokon.
(3) Gondoskodni kell a naplóállományok rendszeres mentéséről vagy redundáns háttértárolón, több példányban való tárolásáról és rendszeres felülvizsgálatáról.
(4) A naplóbejegyzések tárolásáért és megőrzéséért az IFEFV felelős.

24. Naplózási hiba kezelése

33. § (1) A Naplózásért felelős rendszeradminisztrátor rendszeresen meggyőződik arról, hogy az alkalmazások megfelelően generálják a naplóadatokat, és nem maradnak ki fontos események.
(2) A Naplózásért felelős rendszeradminisztrátor rendszeresen ellenőrzi, hogy a naplók nem foglalnak túl sok helyet és a rendszer megfelelően kezeli a tárolási kapacitást.
(3) Ha egy naplófájl megsérül vagy hiányos, a Naplózásért felelős rendszeradminisztrátor elvégzi a visszaállítást a naplóállományokról készített biztonsági mentésből.
(4) A Naplózásért felelős rendszeradminisztrátor rendszeresen ellenőrzi a naplózási beállításokat, hogy biztosítsa a megfelelő formátumot és adatgyűjtési eljárást.
(5) A Naplózásért felelős rendszeradminisztrátor rendszeresen meggyőződik arról, hogy a naplók nem tartalmaznak érzékeny adatokat, és megfelelő jogosultságkezelés van beállítva.

VII. Fejezet
Értékelés, engedélyezés és monitorozás

25. Az értékelés, engedélyezés és monitorozás alapelvei

34. § (1) A kormányhivatalnak biztosítania kell a megbízhatóságot, átláthatóságot, és a megfelelést a vonatkozó jogszabályi, szabályozási és szabványi követelményeknek. Jelen fejezet a kockázatok folyamatos nyomon követését, a változások engedélyezési eljárásait és az IT-rendszerek felügyeletét szabályozza. Cél a megbízhatóság, átláthatóság, és az informatikai rendszerek és erőforrások biztonsági szintjének folyamatos biztosítása a kockázatok időszakos értékelésével, változtatások engedélyezésével, valamint a rendszerek és események monitorozásával A szabályozás alkalmazandó:
a) új informatikai rendszerek bevezetésekor,
b) meglévő rendszerek módosításakor,
c) rendszeres vagy eseti biztonsági ellenőrzések során,

d) a szervezet által meghatározott biztonsági események után.

(2) A további részletszabályokat a Biztonságértékelési eljárásrend tartalmazza.

26. Kiberbiztonsági audit

35. § (1) A kiberbiztonsági audit célja, hogy objektíven és rendszeresen értékelje az intézmény informatikai rendszereinek és biztonsági intézkedéseinek megfelelőségét, hatékonyságát és szabályosságát, valamint feltárja az esetleges hiányosságokat és kockázatokat.

(2) Az audit kiterjed az informatikai rendszerek biztonsági szintjének auditálására, a folyamatbiztonsági ellenőrzések végrehajtására, az auditálás során feltárt hiányosságok dokumentálására és kezelésére.

(3) Évente legalább egy alkalommal kötelező a kiberbiztonsági audit lefolytatása.

(4) Rendkívüli auditot kell tartani súlyos események, biztonsági incidensek (pl. adatvesztés, jogosulatlan hozzáférés, rendszerleállás) bekövetkeztekor.

(5) Célzott audit végezhető új rendszer bevezetése, jelentős rendszerfejlesztés vagy -módosítás, kiszervezett tevékenység esetén, vagy ha a jogszabályi változás érinti a biztonsági követelményeket

(6) A kiberbiztonsági audit során vizsgálandó területek:

a) informatikai rendszerek biztonsága, hozzáférések, naplózás, sérülékenységek, frissítések vizsgálata;
b) hálózatbiztonság, tűzfalak, szegmentálás, behatolás-észlelés vizsgálata;
c) fizikai biztonság, géptermek, eszközvédelem, belépési kontroll vizsgálata;
d) felhasználói jogosultságkezelés, jogosultsági szintek, szerepkörök megfelelése vizsgálata;
e) adatkezelés és adatvédelem, titkosítás, mentések, törlés, adatvesztés elleni védelem vizsgálata;
f) incidenskezelés, események naplózása, bejelentési és válaszintézkedések vizsgálata;
g) oktatás, tudatosság, felhasználók biztonságtudatossága, oktatások megtartása vizsgálata;
h) szabályozási megfelelés, jogszabályoknak, belső szabályzatoknak való megfelelés vizsgálata;
i) kiszervezett szolgáltatások, szerződések, biztonsági kötelezettségek ellenőrzése vizsgálata.

36. § (1) Az audit előkészítését az IBF, illetve a Főispán által kijelölt szervezeti egység (Pl: Belső Ellenőrzési Osztály) végzi, éves audittervet készítve. Melyet a Főispán hagy jóvá. Az előkészítés során meghatározásra kerül az audit célja, hatóköre, módszertana (interjú, dokumentumelemzés, tesztelés), a vizsgált rendszerek és a felelős személyek köre.

(2) Az auditot az IBF és az informatikai szervezeti egységektől független, illetve a FŐISPÁN által kijelölt szervezeti egység vagy független külső fél végzi. Az audit során dokumentumokat, naplókat, konfigurációkat vizsgálnak, interjúkat folytatnak az érintettekkel, teszteket és helyszíni bejárást végezhetnek.

(3) Az audit során írásos jegyzőkönyv készül, amely tartalmazza a feltárt hiányosságokat, kockázatokat, és a szükséges intézkedéseket. Megadja a hiányosságok pótláshoz szükséges határidőket és a felelősöket. Az elkészült jelentést a főispán hagyja jóvá. Az audit dokumentumait legalább 5 évig meg kell őrizni.

37. § (1) Az IBF felel az audit megszervezéséért, lebonyolításáért, valamint a javasolt intézkedések nyomon követéséért.

(2) Az IÜFV az audit során együttműködik az auditot végzőkkel és biztosítja a szükséges adatokat, információkat.

(3) Az érintett szervezeti egységek vezetői kötelesek az audit során együttműködni, az auditált rendszerekhez, folyamatokhoz hozzáférést biztosítani.

(4) Az audit során a FŐISPÁN által kijelölt szervezeti egység vezetője felelős a függetlenség biztosításáért és a jelentések átadásáért a vezetés számára.

38. § (1) Az auditjelentés alapján intézkedési terv készül. Az intézkedések végrehajtását és státuszát az IBF havonta követi nyomon és dokumentálja. A végrehajtás dokumentálása kötelező.
(2) A következő audit során vizsgálni kell, hogy a korábbi megállapításokat orvosolták-e. A hiányosságok megismétlődése esetén vezetői vizsgálatot kell elrendelni. Az audit során feltárt hiányosságok kezelésére az IBF-nek az érintett szervezeti egységek bevonásával intézkedési tervet kell készíteni.
(3) A végrehajtás eredményét az éves vezetői felülvizsgálat során ismertetni kell.

27. Információcsere

39. § (1) Cél az információcserével kapcsolatos biztonsági követelmények meghatározása a kormányhivatal működése során, annak érdekében, hogy az adatok védelme, a jogosulatlan hozzáférés megelőzése, valamint a szabályozott adatáramlás biztosítva legyen. Különös figyelmet kell fordítani az információcsere értékelésére, engedélyezésére és folyamatos monitorozására.
(2) A szabályozás minden szervezeti egységre és dolgozóra vonatkozik, akik hivatalos feladatkörükben információt adnak át vagy fogadnak más személytől, szervezettől vagy informatikai rendszertől – akár manuálisan, akár automatizált módon, elektronikus csatornákon keresztül.
(3) Az információcsere során a következő szabályozó és szabvány előírásokat kell alkalmazni:
a) GDPR (EU 2016/679) – adattovábbításra és átláthatóságra vonatkozó követelmények
b) ISO/IEC 27002 – információbiztonsági kontrollok
c) NIST SP 800-47 – Interagency Security Information Sharing
(4) Az információcsere típusai lehetnek:
a) belső információcsere: a kormányhivatalon belül történő adat- és információátadás, pl. szervezeti egységek között;
b) külső információcsere: központi államigazgatási szervekkel, más kormányhivatalokkal, önkormányzatokkal, közműszolgáltatókkal, vagy állampolgárokkal történő adatküldés/fogadás;
c) elektronikus információcsere: e-mail, e-ügyintézési rendszerek, gépi interfészek, felhőszolgáltatások, API-k, fájlmegosztók, adathordozók használatával;
d) papír alapú információcsere: fizikai dokumentumok mozgatása és átadása személyesen vagy postai úton;
e) nem szándékos (incidens alapú) információáramlás: véletlenszerű, nem engedélyezett információkiszivárgás, pl. rossz e-mailcímre küldött adat.
40. § (1) Minden külső információcserét megelőzően kötelező:
a) adatminősítés: minősített vagy különleges adat esetén külön eljárás alkalmazása szükséges;
b) kockázatelemzés: értékelni kell az adatvédelmi és információbiztonsági kockázatokat;
c) jogszabályi megfelelés: ellenőrizni kell, hogy van-e jogalapja az adattovábbításnak.
(2) Minden új vagy módosuló információcsere-folyamat esetén kötelező:
a) információbiztonsági értékelést lefolytatni az adat típusának, érzékenységének, céljának és jogalapjának megfelelően;
b) meghatározni az adatminősítési szintet (pl. nyilvános, belső használatra, bizalmas);
c) kockázatértékelést készíteni az információcsere módjáról, csatornájáról, gyakoriságáról, fogadó fél megbízhatóságáról.
(3) Az értékelést az IBF vagy az általa megbízott személy végzi, a Biztonságértékelési Eljárásrend alapján.
(4) Az értékelés után az információcsere csak akkor engedélyezhető, ha:
a) a jogalap (pl. jogszabályi felhatalmazás vagy érintetti hozzájárulás) egyértelműen azonosítható,
b) a megfelelő titkosítási, hitelesítési és hozzáférés-kezelési intézkedések biztosítottak,
c) a külső féllel való együttműködéshez van hatályos adatkezelési megállapodás vagy jogszabályi háttér.
(5) Az engedélyezést az adott szervezeti egység vezetője adja ki, információbiztonsági szempontból az IBF véleményezésével.
a) belső információcsere esetén: SZEV/AG jóváhagyásával,

b) külső adatküldés (jogszabály alapján): ügyintéző, osztályvezető jóváhagyásával,
c) külső adatküldés (eseti): IBF és adatvédelmi tisztviselő együttes jóváhagyásával,
d) minősített adat kezelése: biztonsági vezető jóváhagyása és engedélye alapján.

41. § (1) A jóváhagyott információcsere-folyamatokat a következő módon kell felügyelni:
(2) Minden automatizált vagy érzékeny adatot érintő információcsere-eseményt naplózni kell. A naplóknak tartalmazniuk kell: időpont, küldő, fogadó, adat típusa, adatátvitel módja.
(3) A naplózott eseményeket az IBF legalább negyedévente átvizsgálja. Gyanús vagy rendellenes adatforgalom esetén incidenskezelési eljárás indítandó.
(4) Az információcsere-folyamatokat évente egyszer teljes körűen felül kell vizsgálni:
a) Megfelelnek-e a szabályozásoknak?
b) Történt-e jogosulatlan hozzáférés?
c) Változott-e az adat jellege vagy a csere partnerei?

42. § (1) Az értékelések, naplóellenőrzések és felülvizsgálatok koordinálása feladatok ellátásáért felelős az IBF.
(2) Az adatküldések és -fogadások jóváhagyása, szabályok betartatása feladatok ellátásáért felelős a SZEV/AG.
(3) A Titkosítás, naplózás és biztonsági beállítások megvalósítása feladatok ellátásáért felelős az IFEFV.
(4) Minden foglalkoztatott felelős az információcsere szabályainak betartásáért saját munkavégzése során.

28. Engedélyezés

43. § (1) Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, az érintett szervezet hatókörébe tartozó emberi, fizikai és logikai erőforrásra, eljárási és védelmi követelményszintre és folyamatra.
(2) A felhasználók csak a számukra kijelölt feladatok végrehajtásához szükséges és elégséges jogosultságokat kaphatják meg az információkhoz és a rendszer erőforrásaihoz való logikai hozzáférés során.
(3) A nem indokolt, felesleges jogosultságok megszüntetésének érdekében a hozzáférési jogosultságokat rendszeresen felül kell vizsgálni, és az indokolatlan – a legkisebb jogosultság elvével nem megegyező – hozzáféréseket vissza kell vonni. Ennek végrehajtása a Szervezeti egység vezetők felelőssége.

29. Felügyelet

44. § (1) Tíz sikertelen bejelentkezési kísérletet követően az elektronikus információs rendszernek automatikusan zárolnia kell a fiókot – legyen az felhasználói vagy privilegizált, hagyományos vagy technikai – legalább egy óra időtartamra. A zárolást az informatikai feladatok ellátásáért, üzemeltetésért felelős szervezeti egység foglalkoztatottjai oldhatják fel.
(2) Valós fenyegetés vagy egymás utáni többszöri zárolás esetén haladéktalanul értesíteni kell az IBF-t.
(3) Azokat a fiókokat, melyekbe az alábbiakban meghatározott ideje nem jelentkeztek be sikeresen, felül kell vizsgálni és szükség szerint gondoskodni kell azok letiltásáról és deaktiválásáról:
a) nem technikai fiókok esetében: 30 nap,
b) technikai fiókok esetében: 180 nap.
(4) A szabály alól kivételt képeznek a munkaállomások operációs rendszerének lokális technikai – például adminisztrátori – fiókjai, vagy hivatali e-mail postafiókokhoz tartozó fiókok, melyek jellegüknél fogva inaktív – használaton kívüli – állapotban vannak.

30. Belső rendszerkapcsolatok

45. § Engedélyezi a szervezet által meghatározott rendszerelemeknek vagy rendszerelem kategóriáknak a rendszerhez történő belső kapcsolódását. Minden belső kapcsolat esetében dokumentálja az interfész jellemzőit, a biztonsági követelményeket, továbbá a kommunikációban részt vevő információ jellegét. Meghatározott feltételek teljesülése esetén megszünteti a belső rendszerkapcsolatokat. Meghatározott gyakorisággal felülvizsgálja minden belső kapcsolat további szükségességét.

VIII. Fejezet
Konfigurációkezelés

31. A konfigurációkezelés alapelvei

46. § (1) A kormányhivatal biztosítja, hogy kontroll nélküli konfiguráció ne működhessen a szervezetben, a változáskezelés kontrollált folyamat legyen, csak a megfelelő eljárások lefolytatásával kerülhessen be új konfiguráció az éles rendszerekbe, a jogosulatlanul betöltött konfigurációk időben észlelhetőek legyenek.
(2) A konfigurációkezelés feltételrendszerének kialakításáért az IFEFV a felelős.
(3) A további részletes követelményeket és szabályokat a Konfigurációkezelési eljárásrend tartalmazza.

32. Alapkonfiguráció meghatározása

47. § (1) Az elektronikus információs rendszerekhez egy-egy alapkonfigurációt kell kifejleszteni és karbantartani, valamint változatlan állapotban megőrizni az alapkonfiguráció korábbi verzióit, hogy szükség esetén lehetővé váljon az arra való visszatérés.
(2) Az éles alapkonfiguráció felülvizsgálatát és frissítését rendszeresen, de legalább az elektronikus információs rendszer vagy rendszerelemek telepítésekor, frissítésekor el kell végezni.
(3) Az egyes elektronikus információs rendszerek alapkonfigurációit a rendszerbiztonsági tervekben kell dokumentálni (melyek korábbi verzióit szintúgy meg kell őrizni változatlan formában).

33. Biztonsági hatásvizsgálatok

48. § Az elektronikus információs rendszerekben tervezett változások bevezetése előtt a kormányhivatal felülvizsgálja a tervezett változásokat és elemzi azok kockázatait és információbiztonsági hatásait. A hatásvizsgálat eredménye alapján meg kell határozni, hogy a tervezett változások miatt szükséges-e további védelmi intézkedések bevezetése.

34. Rendszerelem leltár

49. § A rendszerelemekkel történő hatékony elszámolás érdekében az elektronikus információs rendszerek elemeiről leltárt kell vezetni, melynek tartalmát folyamatosan naprakészen kell tartani. Biztosítani kell, hogy a leltár pontosan tükrözze az elektronikus információs rendszert és minden komponenst egyedileg azonosítva tartalmazza az elektronikus információs rendszer összes elemét.

35. Szoftverhasználat

50. § (1) Kizárólag olyan szoftverek és olyan kapcsolódó dokumentációk használhatók a kormányhivatal informatikai rendszereiben, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak, valamint a szerzői jogi vagy más jogszabályi előírásoknak.
(2) A másolatok és az állománymegosztások folyamatos ellenőrzésével biztosítani kell a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk jogszerű használatát, a szerzői joggal védett művek és szoftverek jogosulatlan megosztásának, megjelenítésének, végrehajtásának vagy reprodukálásának megelőzése érdekében.
(3) A kormányhivatal infokommunikációs eszközein csak és kizárólag az informatikai feladatok ellátásért, üzemeltetésért felelős szervezeti egység, valamint az erre jogosult külső felek foglalkoztatottjai telepíthetnek, módosíthatnak, vagy távolíthatnak el szoftvert.
(4) A fenti szabályok szúrópróbaszerű ellenőrzése az IBF feladata és felelőssége, mely feladat elvégzésében az elektronikus információbiztonsági feladatok ellátásában közreműködő személyek segítik.

IX. Fejezet
Készenléti tervezés

36. A készenléti tervezés alapelvei

51. § (1) A rendelet védelmi intézkedés követelménykatalógusa alapján az üzletmenet-folytonosság és a katasztrófa utáni helyreállítás tervezése, a kieső infokommunikációs erőforrás kezelése, rendszer helyreállítása és újraindítása, illetve a mentési rend a végpont és határvédelem kialakítása tartalmazza a kormányhivatal készenléti tervezési folyamatát.
(2) A további részletszabályokat az Üzletmenet-folytonosságra vonatkozó eljárásrend tartalmazza.

37. Üzletmenet-folytonosság tervezése

52. § (1) A kormányhivatalnak meg kell terveznie a működési folyamatait azon esetekre, mikor azokat kiszolgáló elektronikus információs rendszerek valamilyen okból nem állnak rendelkezésre. Ezen eljárásrend kidolgozása, felülvizsgálata az IBF, illetve a szervezet vezetője által kijelölt személyek feladat feladata, a jóváhagyás az IFEFV felelőssége.
(2) Az eljárásrendben kell kidolgozni:
a) az üzletmenet-folytonosságot sértő katasztrófahelyzetek esetén felmerülő feladatokat, melyekhez felelősöket kell rendelni,
b) megfelelő kommunikációs folyamatokat az elektronikus információs rendszer kiesésére, hogy pontosan és kellő gyorsasággal legyen kommunikálva a szervezeteken belül és a szervezetek által kiszolgált ügyfelek felé az ügymenet megszakadása, megkerülő megoldás aktiválása.
(3) A kormányhivatal az Üzletmenet-folytonosságra vonatkozó eljárásrendben részletesen szabályozza a folyamatos működésre felkészítő képzések lebonyolítását. A kormányhivatal folyamatos működésre felkészítő képzést biztosít az EIR felhasználói számára, amely képzés a felhasználók szerepkörének vagy felelősségi körének megfelelő. A képzést a szerepkörbe vagy felelősségbe kerülésüket követő meghatározott időn belül kell elvégezni. Amikor az EIR változásai ezt szükségessé teszik, a képzést frissíteni kell.

38. Kieső infokommunikációs erőforrás kezelése

53. § A kormányhivatal kieső infokommunikációs erőforrás kezelés célja, hogy tartalék infokommunikációs eszközökkel rendelkezzen. Az elsődleges eszközöket érintő fenyegetések, - ezek közé tartozó természeti katasztrófák, szerkezeti hibák, kiber vagy fizikai támadások, valamint a mulasztások vagy szándékos (szervezeten belüli) károkozásból eredő meghibásodás - miatti szolgáltatás kiesés csökkentésének kezelése céljából. A kormányhivatal nyilvántartást vezet típusokként a tartalék infokommunikációs eszközökről.

39. Katasztrófa utáni helyreállítás tervezése

54. § (1) Az elektronikus információs rendszerek működésében bármikor bekövetkezhet olyan nem kívánt esemény (természeti katasztrófa, hardware meghibásodás stb.), melynek eredményeképpen a rendszer működésképtelen lesz.
(2) A kormányhivatal által üzemeltetett elektronikus információs rendszerek folyamatos működése érdekében az ügymenet folytonosságát veszélyeztető meghibásodások kezelésének zökkenőmentes és rövidebb idő alatt történő végrehajtása érdekében a visszaállítás és helyreállítás lépéseit előre meg kell határozni, és azokat katasztrófa utáni helyreállítási tervek (Disaster Recovery Plan, DRP) formájában dokumentálni kell.
(3) A katasztrófa utáni helyreállítási terv célja megfogalmazni azon tevékenységek sorozatát, amellyel helyreállítható a kiesett informatikai erőforrás, ezzel minimalizálva az ügymenetre gyakorolt kedvezőtlen hatást.
(4) A tervben ki kell dolgozni:
a) a helyreállítás folyamatának lépéseit, szerepköreit, felelőseit,
b) a meghatározott követelmények és feladatok dokumentációs rendszerét.
(5) Katasztrófa utáni helyreállítás tervek (DRP) létrehozása informatikai erőforrás kiesése által okozott katasztrófahelyzet bekövetkeztére abban az esetben számíthat a kormányhivatal, ha a leállás megközelíti a kiesett erőforrás által támogatott alapfeladatok, folyamatok maximálisan megengedhető kiesési idejét (MTD). Ebben az esetben nagy a valószínűsége annak, hogy a normál működés szerinti incidenskezelési folyamat keretein belül nem hárítható el a probléma.
(6) A katasztrófa utáni helyreállítási tervben részletezett tevékenységek végrehajtását a katasztrófa utáni helyreállítási terv mellékletben foglalt útmutató alapján kell létrehozni, a helyreállítási terv sablon kitöltésével.

40. Rendszer helyreállítása és újraindítása

55. § (1) A helyreállítás a vészhelyzeti terv tevékenységeinek végrehajtását jelenti, amelyek célja az érintett szervezet alapfeladatainak és alapfunkcióinak helyreállítása. Az újraindítás a helyreállítást követően történik, és magában foglalja az EIR-ek teljes, üzembiztos állapotba való visszaállításának tevékenységeit. A helyreállítási és újra indítási műveletek tükrözik a szervezeti alapfeladatokat és az üzleti (ügymeneti) célkitűzéseket; a helyreállítási pontokat, a helyreállítási időt és az újra indítási célkitűzéseket; valamint az érintett szervezet mérőszámait, amelyek összhangban vannak a vészhelyzeti terv követelményeivel. Az újraindítás magában foglalja azoknak az ideiglenes EIR képességeknek a kikapcsolását, amelyekre a helyreállítási műveletek során szükség lehetett. Az újraindítás továbbá magában foglalja a teljesen helyreállított EIR képességek értékelését, a folyamatos monitorozási tevékenységek újra indítását, az EIR újra engedélyezését, és a tevékenységeket, amelyek az EIR-t és az érintett szervezetet felkészítik a jövőbeli összeomlásokra, szabályok megsértésére, kompromitálódásokra vagy hibákra. A helyreállítási és újra indítási képességek magukban foglalhatják az automatizált mechanizmusokat és a manuális eljárásokat. Az érintett szervezetek a vészhelyzeti tervezés részeként határozzák meg a helyreállítási időt és a helyreállítási pont célkitűzéseket.

(2) A katasztrófa utáni helyreállítási tervek elkészítéséhez a kormányhivatalnak célszerű meghatározni azokat a vészhelyzeti forgatókönyveket, amelyek bekövetkezésére fel szeretne készülni.
(3) A katasztrófa utáni helyreállítási tervek létrehozásakor alapul kell venni a kockázatelemzés eredményeit, amelyből megállapítható, hogy mely fenyegetettségek bírnak olyan mértékű bekövetkezési valószínűséggel és kárhatással, amelyek kritikusan növelik a kockázat szintjét. A vészhelyzeti forgatókönyvek készítésekor szükséges végig gondolni, hogy mely potenciális kockázatok hatása csökkenthető katasztrófahelyzet utáni helyreállítási tervek készítésével és szükség szerinti alkalmazásával. A DR terveket ezen vészhelyzeti forgatókönyvek mentén célszerű kialakítani.
(4) A következő forgatókönyvek létrehozása minimum ajánlott:

a) szerverterem kiesése,
b) gerinchálózat kiesése,
c) egy kritikus szolgáltatás kiesése,
d) több kritikus szolgáltatás kiesése.

(5) A forgatókönyvek kialakítása során a kormányhivatalnak figyelemmel kell lennie arra, hogy az elektronikus információs rendszer utolsó ismert állapotba történő helyreállítása és újraindítása megtörténjen.
(6) A forgatókönyvek kialakításánál meg kell határozni az alapfunkciók újra indításának időpontját és sorrendjét az üzletmenet – folytonossági tervek aktiválást követően. A prioritást az egyes alapfunkciókhoz tartozó helyreállítási időcélokhoz kell igazítani.
(7) A tranzakció alapú elektronikus információs rendszerek esetén tranzakció helyreállítását is tervezni kell.

41. Mentési rend kialakítása

56. § (1) A rendszer legfontosabb elemeinek egyértelmű és visszakereshető azonosítása, illetve az egyes informatikai rendszereket érintő rendkívüli helyzetek megszüntetésének megvalósítása érdekében mentéseket, archiválásokat kell végezni olyan módon, hogy azokból szükség esetén az elektronikus információs rendszer, illetve az abban lévő adatok visszaállíthatók legyenek.
(2) A kormányhivatal meghatározott gyakorisággal mentést készít az EIR-ben tárolt felhasználói, rendszer szintű információkról, illetve az EIR dokumentációjáról, beleértve a biztonságra vonatkozó információkat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.
(3) A mentés, archiválás és visszatöltés tervezésének és üzemeltetésének kialakításáért az IFEFV a felelős.
57. § (1) Biztonsági mentéseknek kell készülniük:

a) az online elérhető (éles, tartalék, fejlesztői) adatbázisokról és fájlrendszer könyvtárakról,
b) az offline elérhető (archivált) adatbázisokról és fájlrendszer könyvtárakról,
c) szoftverek telepítőkészletéről.

(2) A mentés, archiválás, visszatöltés megfelelőségéhez biztosítani kell:

a) a felelős meghatározását,
b) a jogszabályoknak megfelelő módszert (gyakoriság, megőrzési idő, példányszám),
c) megfelelő médiát (méret, írás-olvasási technológia),
d) mentési eszközt (hardver-szoftver),
e) média tárolását, hozzáférés-védelmét (titkosítás, vagy jelszó alkalmazása),
f) a folyamat ellenőrizhetőségét.

58. § (1) A mentések paramétereinek meghatározásához alkalmazandó irányelvek:

a) A mentések tervezése, a visszaállási pontok kialakítása során figyelembe kell venni a rendelkezésre állási elvárások által rögzített, maximálisan megengedett kiesési időket.
b) A mentés rendjét az Üzletmenet-folytonosságra vonatkozó eljárásrend tartalmazza.
c) A mentést követően biztosítani kell egy példány offline - rendszertől függetlenített - elhelyezését, a sikeres mentést követő 1 napon belül.

(2) Az archiválások paramétereinek meghatározásához alkalmazandó irányelvek:

a) Az archiválás céljából készített hosszútávú mentéseknek az adatbázis mellett az azt kezelni képes szoftververziót is tartalmazni kell.
b) Az archiválások gyakoriságát a Szervezeti egység vezetőnek / Adatgazdának az adott adatkörökre vonatkozó jogszabályok figyelembevételével kell meghatároznia.

(3) Gondoskodni kell a mentett és archív állományok adatainak (archivált rendszerek) visszaolvasásához, visszatöltéséhez szükséges berendezés mindenkori rendelkezésre állásáról.
(4) A mentések, archiválások elvégzése során végrehajtandó feladatok:
(5) Változásmenedzsment (elektronikus információs rendszer szinten, tartalomváltozás, médiaváltozás, eszközváltozás, infrastruktúra átszervezés, bővítés):
(6) Az alkalmazásokban tárolt adatok folyamatos elérésére, az üzletmenet-folytonosság biztosítására a kormányhivatalnak törvényi kötelezettsége van, melyet az egyes alkalmazások fejlesztése során is fenn kell tartani.
(7) Abban az esetben, ha a programverzió változtatása adatkonvertálással is jár, akkor a telepítés előtt soron kívül el kell végezni az adatok mentését.
(8) Az automatikus mentésekről értesítést kell küldeni, hiba esetén a Mentésért felelős rendszeradminisztrátornak felül kell vizsgálnia a mentési job-ot és szükség esetén el kell végeznie manuálisan a mentést.
(9) A kormányhivatal mentendő és archiválandó rendszereit kategóriákba szükséges sorolni attól függően, hogy az adott adatok mennyire védendőek. Az egyes kategóriák esetén a mentés gyakorisága és típusa eltérő lehet, illetve a megőrzési idők változhatnak.
59. § (1) A kormányhivatal az alábbi mentési kategóriákat határozza meg:
(2) Magas mentési kategória: naponta legalább 1 teljes mentés, adatbázisok esetén minimum 1 tranzakciós log mentése.
(3) Közepes mentési kategória: hetente legalább 1 teljes mentés, adatbázisok esetén minimum 1 tranzakciós log mentés.
(4) Alacsony mentési kategória: havonta legalább 1 teljes mentés és naponta növekményes mentés.
(5) A fenti kritériumok alapján az alábbiak szerint kerülnek mentésre az egyes rendszerek:

a) alkalmazás kiszolgáló: alacsony,
b) adatbázis kiszolgáló: magas,
c) BackOffice kiszolgáló: közepes,
d) fájlszerver: közepes,
e) virtuális kiszolgálók: közepes,
f) eszköz: alacsony,
g) naplóállomány: közepes.

60. § A napi mentést heti ciklusba kell szervezni (hétfő – kedd – szerda – csütörtök), azaz a hét munkanapjain külön-külön mentést kell készíteni. A napi mentés a következő hét ugyanazon napi mentésével (egy héttel később) írható felül. A heti mentést havi ciklusokba kell szervezni. A heti mentést pénteken kell elvégezni (péntek-1, péntek-2, péntek-3, péntek-4). A havonta képződő pénteki mentések a következő hónap ugyanazon hetéig nem írhatók felül. A hó végi utolsó pénteki mentés képezi a havi mentést (péntek-4), amelyet 1 évig meg kell őrizni (csak azután lehet felülírni). Szükség szerint plusz napokon is kell mentést készíteni (pl. péntek-5, szombat, vasárnap, ünnepnap stb.). Adatbázis mentések esetén a külön egységre archivált adatokat nem lehet felülírni és selejtezni. Minden év utolsó munkanapjával bezáróan archiváló mentést kell végezni minden rendszerről.

42. Végpont és határvédelem

61. § (1) Az elektronikus információs rendszerek üzembiztos működése érdekében folyamatosan felügyelni és védeni kell a támogató rendszereket és rendszerelemeket. A felügyeleti eszközök által biztosított információkat közel valós időben kell feldolgozni és értesíteni kell a meghatározott szerepkörű személyeket.

(2) A kormányhivatali rendszerek rendelkezésre állásának és az adatforgalom bizalmasságának és sértetlenségének biztosítása érdekében külső és belső határvédelmi eszközöket és megoldásokat kell alkalmazni.
(3) A határvédelem és rendszerfelügyelet kialakításáért és működtetéséért az IFEFV a felelős.
(4) A kormányhivatal egészére kiterjedő, folyamatos vírusvédelem és rendszeres vírusellenőrzés biztosítása érdekében automatikus frissítéssel rendelkező, központilag menedzselhető vírusvédelmi rendszert kell kiépíteni. Minden lehetséges lépést meg kell tenni a veszélyes programok által okozott incidensek kiküszöbölésére. Ennek érdekében vírusellenőrző alkalmazásokat kell telepíteni mind a munkaállomásokra, mind pedig a szerverekre és informatikai határvédelmi eszközökre.
(5) A vírusvédelmi rendszer kialakításáért az IFEFV a felelős.
(6) A határvédelemre, rendszerfelügyeletre, vírusvédelemre vonatkozó további részletes követelményeket és szabályokat a Rendszer- és információsértetlenségi eljárásrend tartalmazza.

X. Fejezet
Azonosítás és hitelesítés

43. Az azonosítás és hitelesítés alapelvei (8.1)

62. § (1) Az azonosítás és hitelesítés szabályozásának célja, hogy a kormányhivatal az elektronikus információs rendszerekhez történő hozzáférést csak a felhasználó egyedi azonosítását követően biztosítsa annak érdekében, hogy

a) minden tevékenység összerendelhető legyen egy természetes személlyel, és az
b) összerendelés egyértelmű, megváltoztathatatlan és a
c) későbbiekben visszakereshető legyen.

(2) A további részletszabályokat az Azonosítási és hitelesítési eljárásrend tartalmazza.

44. Azonosítás és hitelesítés (8.2)

63. § (1) A kormányhivatal felhasználói közé tartoznak a személyi hatályban meghatározott személyek. A felhasználók egyedi azonosítása és hitelesítése minden felhasználóra vonatkozik, és a felhasználókat felhasználói névvel azonosítjuk.
(2) A már korábban kiadott felhasználói neveket nem lehet újra kiadni, vagy bármilyen más módon használatba venni. Egyedi elbírálás alapján, jellemzően névváltoztatás esetén, van lehetőség a felhasználói név módosítására, amelyet csak az IBF végezhet el.
(3) A felhasználói név képzése a kormányhivatalban egységes, és ugyanaz a felhasználói név két eltérő operatív címtárbeli konténeren belül sem használható.
(4) Az egyedi azonosítás érdekében a felhasználói névhez tartozó e-mail címet sem lehet ismételten kiadni.
(5) Az elektronikus információs rendszerhez hozzáférést biztosító felhasználói fiókok típusai:

a) a foglalkoztató személye, a felhasználó státusza, a szerződéses kapcsolat szerint lehet:
   aa) belső,
   ab) külső,
b) a létrehozás ideje alapján lehet:
   ba) beépített,
   bb) nem beépített,
c) az elérés típusa alapján lehet:
   ca) helyi,
   cb) távoli,
d) a megszemélyesítés típusa alapján lehet:
   da) megszemélyesített,

db) nem megszemélyesített,

e) jogosultsági szint (privilégiumok) szerint lehet:
   ea) felhasználói,
   eb) technikai,
   ec) rendszergazdai,
   ed) privilegizált.

(6) A felhasználók által végzett tevékenységeket a kormányhivatal az egyedi azonosítás útján egyedileg naplózza. A külsős felhasználók esetén fokozottan kell figyelni az azonosításra és hitelesítésre.

64. § (1) A kormányhivatalban a felhasználói azonosítók az alábbi módon jöhetnek létre:

a) a Humánpolitikai feladatok ellátásáért felelős szervezeti egység rögzíti a humánpolitikai elektronikus információs rendszerben az új belépő dolgozót,
b) a jogosultságkezelő adminisztrátor az Identity Management rendszerben létrehozza a felhasználót.

(2) A belső felhasználók a kormányhivatal felhasználói névképzésének szabályai szerint kapnak felhasználói nevet és a jelszó házirend szerint kapják meg a kezdő jelszót, illetve kezelik a továbbiakban a jelszavaikat.

(3) A külső felhasználók esetén a névképzési szabályokat úgy kell meghatározni, hogy a felhasználói névből egyértelműen kiderüljön, hogy külsős felhasználóról van szó.

65. § (1) A kormányhivatal a beépített fiókok esetén (pl.: guest, admin, root, administrator, stb.) megköveteli, hogy a beépített fiókot

a) nevesíteni kell átnevezéssel, vagy
b) le kell tiltani.

(2) A kormányhivatal a megszemélyesített és nem megszemélyesített fiókok között még további fióktípusokat különböztet meg:

a) természetes személy (1. típusú, általános felhasználói fiók),
b) technikai felhasználó (2. típusú, technikai fiók),
c) hivatali postafiók (3. típusú, technikai hivatali fiók),

(3) A megszemélyesített fiók (1. típusú, általános felhasználói fiók), egyértelműen összekapcsolható egy természetes személlyel. Egy fiók azonosító pontosan egy természetes személyt azonosít.

(4) A nem megszemélyesített fiókok közé tartoznak a technikai felhasználók (2. típusú) és a hivatali postafiókok (3. típusú) fiókok. A nem megszemélyesített fiókok lehetnek a hivatali levelezést biztosító technikai fiókok, illetve egyéb technikai fiókok, amelyek jellemzően rendszer folyamatok futtatását biztosító hozzáférést tesznek lehetővé. A fiókért és annak használatával végzett módosításokért a fiókhoz rendelt szervezeti egység vezetője (SZEV/AG) felelős.

66. § (1) A kormányhivatal a felhasználói fiókok hitelesítésére jelszavakat, fizikai hitelesítőket vagy biometriai adatokat, többtényezős hitelesítés esetén ezek kombinációját használja.

(2) A kormányhivatal által használt elektronikus információs rendszerek vagy központi szolgáltatások esetében az azonosítást legalább egy, de szükség esetén további még legalább egy (2. faktor), hitelesítési mechanizmussal ki kell egészíteni.

(3) A hitelesítési mechanizmus általános módszere a felhasználói azonosítóhoz tartozó jelszó alkalmazása.

(4) A második hitelesítési mód lehet:

a) hitelesítő alkalmazás
b) levelezési fiókba érkező kód,
c) egyszeri bejelentkezési token,
d) biometrikus azonosítás (pl.: ujjlenyomat olvasó).

(5) A sikertelen bejelentkezési kísérleteket az elektronikus információs rendszer naplózza és meghatározott számú sikertelen bejelentkezést követően a felhasználói fiókot átmeneti időre zárolja. A zárolást az Infrastruktúra üzemeltetési rendszergazdák indokolt esetben feloldhatják a zárolási időtartam letelte előtt.

45. Privilegizált fiókok kezelése (8.3)

67. § (1) A privilegizált fiókok olyan alapvető hozzáférési eszközök, amelyek a kormányhivatali rendszerek kezelését a legmagasabb szintű jogosultságokkal teszik lehetővé.
(2) Meg kell különböztetni a privilegizált fiókokat mind az általános felhasználói, mind a rendszergazdai fiókoktól. Jellemzően nem személyazonosságot, nem emberi felhasználót képviselnek, inkább egy kiemelt hozzáférési módot, pl. egyes speciális jogosultságokat igénylő szolgáltatások futtatását biztosító fiókok.
(3) A privilegizált fiókokat nevesíteni kell, megkülönböztetve azonban a felhasználói fiókoktól. Olyan általános névkonvenciót kell létrehozni és alkalmazni, amely egyértelműen megkülönbözteti az érintett privilegizált fiókot a felhasználói fiókoktól, és utal a privilegizált fiók létrehozásának okára, azaz az általa elvégezhető feladatra, vagy az általa elvégezhető szolgáltatás természetére, funkciójára.
(4) A privilegizált fiókkal általános, azaz nem rendszergazdai tevékenységet végezni tilos.
(5) A privilegizált fiók jelszavának tárolásáról és őrzéséről az IÜFV gondoskodik és felel érte.
(6) Az IBF-t tájékoztatni kell minden privilegizált fiók létrehozásáról, mely folyamatban felülbírálati jogkörrel rendelkezik.
(7) A kormányhivatal az alábbi fiókokat tekinti privilegizált fiókoknak:
a) rendszerbe beépített, emelt szintű jogosultságokkal rendelkező fiókok,
b) tenant rendszerek emelt szintű jogosultságait biztosító fiókok,
c) folyamatok futását, futtatását biztosító emelt szintű fiókok.
(8) A kormányhivatal a privilegizált fiókok helyi (helyi hálózati) hozzáférése esetén egyfaktoros hitelesítést követel meg.
(9) VPN kapcsolaton keresztül történő csatlakozás esetén kétfaktoros hitelesítés szükséges a privilegizált fiók hozzáféréshez.
(10) Nyílt internet irányából, VPN használata nélkül a privilegizált fiókba bejelentkezni tilos és a kormányhivatal technikai eszközökkel is lehetetlenné teszi.

46. Szervezeten kívüli felhasználók (8.38)

68. § (1) A kormányhivatal kapcsolódó szabályzatban vagy eljárásrendben meghatározott módon és felhasználói körnek biztosít hozzáférést bizonyos elektronikus információs rendszerekhez, külsős felhasználók számára.
(2) A szervezeten kívüli (külsős) felhasználók felhasználói azonosítóinak képzése során egyértelműen jelezni kell a felhasználó szervezeten kívüli jellemzőjét az „ext_” előtag használatával.
(3) A külsős felhasználók részére a kormányhivatal tájékoztatást nyújt a rájuk vonatkozó információbiztonsági szabályokról és megköveteli azok betartását.

47. Fiókhozzáférés védelme

69. § (1) A kormányhivatal megköveteli a fiókok védelme érdekében a megfelelő erősségű jelszavak használatát.
(2) Egyes hozzáférések esetén egyedi elbírálás alapján kötelezhető a felhasználó a legalább 2 faktor használatával történő belépésre. Ez a feltétel az egyes elektronikus információs rendszerek esetén eltérhet, amelyet az adott elektronikus információs rendszer rendszerbiztonsági tervében kell szerepeltetni.
70. § (1) A jogosultságok nyilvántartása három különböző formában történik:
(2) A kormányhivatal által használt jogosultságmenedzsment rendszerben (IDM), minden olyan esetben, ahol címtár objektumhoz kapcsolva történik meg az azonosítás és hitelesítés.
(3) Implicit módon azon szakrendszerekben, ahol önálló jogosultság menedzsment funkció került a rendszerbe implementálva: a jogosultság kiosztás, kezelés, nyilvántartás, visszavonás a szakrendszeren belül történik.

(4) A Központi Azonosítási Ügynökön (KAÜ) keresztül elérhető információs rendszerek tekintetében a 4T adatok segítségével az érintett szakrendszeren belül történik a jogosultság kiosztás, kezelés, nyilvántartás, visszavonás.
(5) Az a) pontban jelzett esetben a jogosultság nyilvántartási feladatokat az IFEFV biztosítja az IDM rendszer segítségével. A jogosultság nyilvántartás vezetéséért az IFEFV felel.
(6) A b) és c) pontban jelzett esetben a jogosultság nyilvántartás vezetéséért a SZEV/AG felel. A jogosultságok nyilvántartásáért, illetve a jogosultság változás bejelentésével összefüggő feladatok teljesítésért az érintett SZEV/AG a felelős. Kiemelt gondossággal szükséges kezelni a KAÜ rendszerében nyilvántartott jogosultságok visszavonását.
71. § (1) A kezdő jelszót a címtár kapcsolt rendszerek vonatkozásában a kormányhivatali jogosultságmenedzsment rendszer generálja, a saját jogosultságmenedzsment rendszerrel rendelkező információs rendszerek esetén az érintett EIR-ben a rögzített üzleti logika szerint kell kezelni.
(2) Amennyiben a felhasználó a jelszavát elfelejtette, a közvetlen vezetője (vagy bármely felettese) igényelhet a számára új jelszót, amelyet a következő sikeres bejelentkezést követően azonnal meg kell változtatnia. Az IDM adminisztrátorai csak a felhasználó felettes vezetőinek akadályoztatása és kivételes esetben végezhetik el az új jelszó kiadását, egyedi mérlegelés alapján.
(3) A jelszavakat semmilyen körülmények között nem szabad nyilvánosságra hozni, és nem osztható meg senkivel. A felhasználó maga felel a jelszó bizalmasságának megőrzéséért.
(4) Amennyiben a felhasználóban felmerül a jelszava bizalmasságának elvesztése, azt köteles azonnal megváltoztatni és a gyanújáról az IBF-et értesíti. A jelszót a megkövetelt gyakorisággal meg kell változtatni.
72. § A kormányhivatal visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz az elektronikus információs rendszerekhez történő hozzáférés esetén. A visszajátszásos támadásoknak ellenálló hitelesítési eszközöket kell alkalmazni, amelyet az elektronikus információs rendszer rendszerbiztonsági tervében kell meghatározni.
73. § A kormányhivatal lehetővé teszi az elektronikus információs rendszerei használatát megfelelő VPN védelemmel ellátott csatornán keresztül. A megfelelő védelem érdekében ennek használatához kötelező a kétfaktoros bejelentkezési mód. A második faktor módszerét az adott Elektronikus információs rendszer rendszerbiztonsági terve határozza meg.
74. § Az elektronikus információs rendszerhez való hozzáférés esetén használt felhasználói jelszavak esetén kötelező a kriptográfiai védelem. A jelszavakat megfelelő titkosítással kell ellátni a visszafejtés elleni védelem érdekében. Az elektronikus információs rendszernek titkosított módon kell tárolnia a jelszavakat, azok visszaolvasható formában nem kerülhetnek letárolásra.

48. Jelszó politika

75. § (1) A jelszóval kapcsolatos minimális elvárások és követelmények:
a) a jelszóban különbözőnek számítanak a kis- és nagybetűk,
b) a jelszó nem tartalmazhat ékezetes betűt,
c) a jelszó hossza minimum 14 karakter,
d) legalább 1 számjegyet tartalmaz (0..9),
e) legalább 1 kisbetűt tartalmaz (a..z),
f) legalább 1 nagybetűt tartalmaz (A..Z),
g) nem tartalmazhatja a következő értékeket: „1234567890”, „jelszo”, „password”,
h) nem tartalmazhatja a felhasználó nevét, illetve bejelentkezési nevét,
i) a jelszavakat legalább 90 naponként meg kell változtatni,
j) az új jelszónak legalább egy karakterében különböznie kell a legutóbb használt 10 jelszó bármelyikétől.

(2) A kezdeti jelszó, illetve az elfelejtett jelszó esetén kiadott átmeneti jelszó érvényessége 24 óra. A 24 óráig érvényes jelszót első bejelentkezéskor meg kell változtatni.
(3) A jelszó bizalmasságát minden felhasználó köteles megőrizni, azt más személy tudomására hozni szigorúan tilos! Soha, semmilyen körülmények között a jelszót más személlyel megosztani nem szabad.

(4) A jelszó kompromittálódása, vagy annak gyanúja esetén a jelszót azonnal meg kell változtatni, vagy a kapcsolódó fiókot le kell tiltani.
(5) A jelszó egy emlékeztető dokumentum formájában rögzíthető, azonban gondoskodni kell annak megfelelő tárolásáról annak érdekében, hogy más személy kezébe ne kerülhessen.
76. § (1) A rendszergazdai jogosultságú, (privilegizált, megszemélyesített) fiók jelszó követelményei a felhasználói fiókra vonatkozó követelményeket veszi alapul, de azokat szigorodó módon kiegészíti.
(2) A rendszergazdai jogosultságú fiók jelszavának az általános jogú felhasználói jelszavaknál meghatározottakon túl az alábbi feltételeknek kell megfelelnie:

a) a jelszó hossza legalább 16 karakter,
b) legalább 1 speciális karaktert tartalmaz.

77. § A privilegizált, azaz kiemelt jogosultságokkal rendelkező, de nem megszemélyesített fiók jelszó követelményei megegyeznek a rendszergazdai jogosultságokkal rendelkező felhasználói jelszavaknál meghatározottaknál, viszont az ott felsoroltakon túlmenően, de azokkal együtt értelmezve, az alábbi feltételnek kell megfelelnie:

a) a jelszó hossza legalább 20 karakter,
b) legalább 2 speciális karaktert tartalmaz,
c) a jelszót legalább évente 1 alkalommal meg kell változtatni.

78. § (1) A technikai (nem megszemélyesített, nem nevesített) fiók jelszavát a felhasználók nem ismerhetik meg, azt az IÜFV őrzi, az azokhoz kapcsolódó fiókba belépni a napi üzemeltetés során nem szabad és nem is szükséges.
(2) A technikai fiók jelszó követelményei megegyeznek a rendszergazdai fiók jelszó követelményeinél felsoroltakkal kivéve, hogy

a) a jelszót évente 1 alkalommal kötelező megváltoztatni,
b) minden megismerést követően ismét kötelező megváltoztatni.

79. § Azon elektronikus információs rendszerek vagy egyéb rendszerek esetén, amelyeknél a fenti szabályozást nem lehet érvényesíteni (pl. nem alkalmazható speciális karakter), az adott alkalmazás maximális biztonsági lehetőségeit kihasználva kell a jelszavak erősségét beállítani és törekedni kell az alkalmazás megfelelő módosítására vagy cseréjére.

XI. Fejezet
Biztonsági események kezelése

49. A biztonsági események kezelésének alapelvei

80. § (1) A kormányhivatal a rendszereibe bekerülő, illetve ott keletkező adatok, információk informatikai rendszerekben történő adatfeldolgozásával, működésével, üzemeltetésével és tárolásával kapcsolatban felmerülő biztonsági és elektronikus információbiztonsági események kezelésére eseménykezelési szabályozást hoz létre.
(2) A bekezdésben megfogalmazott célok elérése érdekében létrehozza a Biztonsági eseménykezelési eljárásrendet, amely dokumentálja a biztonsági esemény és biztonsági incidens kezelésével kapcsolatos eljárások folyamatát, a feladatok végrehajtásának lépéseit, a végrehajtás során használt eszközöket és nyilvántartásokat, a dokumentáció formáit és az elvárt eredményeket.
(3) A biztonsági eseménykezelés informatikai feltételrendszerének kialakításáért az IFEFV a felelős.

50. Biztonsági események nyomon követése

81. § (1) A biztonsági események kezelésében eltérő szinten vesznek részt a személyek, ennek megfelelően a Biztonsági eseménykezelési eljárásrendben meg kell határozni az egyes szerepköröket.
(2) Minimálisan megkülönböztetendő szerepkörök:

a) alap jogosultságú felhasználó,
b) vezető beosztású, alap jogosultságú felhasználó,
c) általános feladatokat ellátó informatikus, rendszergazda,
d) speciális feladatokat ellátó informatikus, rendszergazda,
e) IBF.

(3) A kormányhivatal gondoskodik a biztonsági események kezelésére vonatkozó, különböző szintű és tartalmú képzésekről a felhasználók számára, szerepkörük szerint.
(4) Az új felhasználóknak a szerepkörüknek megfelelő képzést a munkába állásukat követő 30 napon belül el kell végezniük. A felhasználóknak évente kötelező a képzés megismétlése.
(5) A képzések tervezését és tartalmának kidolgozását, valamint a rendszeres felülvizsgálatot az IBF koordinálja és felügyeli, a feladat végrehajtásában közreműködik az IÜFV és az általa kijelölt Infrastruktúra üzemeltetési rendszergazdák, a képzések létrehozásáért és a felhasználók szerepkörük szerinti elvégzéséért felelős az IFEFV.
(6) A kormányhivatal a Biztonsági eseménykezelési eljárásrendben határozza meg azokat a követelményeket, dokumentációt, jegyzőkönyvek karbantartását, amelyek biztosítják a biztonsági események megfelelő nyomon követését.
(7) Általános elvárás, hogy a végpontvédelmi rendszer automatikus jelzéseit minden esetben nyomon kell követni, a többi esemény típust a Biztonsági eseménykezelési eljárásrend határozza meg.

51. Biztonsági események jelentése

82. § (1) A kormányhivatal a felhasználói számára biztosítja a biztonsági események bekövetkezésének gyanúja vagy tényleges bekövetkezése esetén a bejelentés lehetőségét.
(2) A felhasználók számára kötelező már a biztonsági esemény gyanújának esetében is megtenni a bejelentést. A felhasználók a számukra biztosított biztonsági események kezelésére vonatkozó képzésekből meg kell kapják azokat az információkat, amely alapján felismerhetik a biztonsági esemény bekövetkeztét vagy gyanússá válhatnak számukra bizonyos események, folyamatok.
(3) A kormányhivatal a Biztonsági eseménykezelési eljárásrendben meghatározott dokumentációval biztosítja a bejelentések gyors és hatékony megtörténtét és biztosítja a jelentések megfelelő dokumentálását, nyomon követhetőségét és a tanulságok levonását, azok beépítését a biztonsági eseménykezelési eljárásokba.
(4) Az IBF a biztonsági incidenseket a bekövetkezésüket és felismerésüket követően haladéktalanul jelenti a jogszabályban meghatározott hatóság felé, a hatóság által meghatározott módon.
(5) A kormányhivatal a Biztonsági eseménykezelési eljárásrendben meghatározott módon dokumentálja a biztonsági eseményeket, amelyet felhasznál a kockázatkezelésben, a biztonsági előírások hatékonyságának értékelésében, a biztonsági követelmények meghatározásában a beszerzések esetén, illetve a technológiai termékek kiválasztási kritériumainak meghatározásában.
(6) A kormányhivatal bejelentő felületet működtet a biztonsági események felhasználók általi bejelentésének támogatása érdekében.
(7) A bejelentő felületen tett bejelentést követően egy, a biztonsági eseménnyel kapcsolatos kérelem jön létre, amelynek életútja biztosítja az esemény nyomon követhetőségét.

52. Biztonsági eseménykezelés

83. § (1) A kormányhivatal olyan biztonsági eseménykezelési képességet alakít ki, amely támogatja a biztonsági eseményekre való

a) felkészülést,
b) észlelést és elemzést,
c) elszigetelést,
d) felszámolást és a
e) helyreállítást.

(2) A biztonsági eseménykezelési tevékenységeket össze kell hangolni az üzletmenet-folytonossági szabályozással és tevékenységekkel.

(3) A kormányhivatal a hatályos jogszabályokkal és az egyéb szabályozó dokumentumokkal összhangban biztonsági eseménykezelési tervet dolgoz ki, amelyet a Biztonsági eseménykezelési eljárásrendben rögzít.

(4) A biztonsági eseménykezelési terv:

a) iránymutatást ad a szervezet számára a biztonsági események kezelési módjaira vonatkozóan,
b) ismerteti a biztonsági eseménykezelés struktúráját és szervezetét,
c) átfogó képet nyújt arról, hogy a biztonsági eseménykezelés hogyan illeszkedik az általános szervezeti struktúrába,
d) megfelelő részletességgel tárgyalja a biztonsági események kezelését, megfelelve a kormányhivatal feladataival, méretével, szervezeti felépítésével és funkcióival kapcsolatos egyedi irányvonalakat,
e) meghatározza a bejelentésköteles biztonsági eseményeket,
f) meghatározza a metrikákat a biztonsági eseménykezelési folyamatok működésének mérésére,
g) meghatározza azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési folyamatok bővítésére, hatékonyabbá tételére és fenntartására,
h) meghatározza a biztonsági eseményekkel kapcsolatos információmegosztás módját.

(5) A biztonsági eseménykezelési tervet legalább évente, vagy amennyiben olyan technológiai változás, biztonsági esemény trend figyelhető meg, vagy olyan jellegű biztonsági esemény következik be, amely ezt indokolja, akkor soron kívül felül kell vizsgálni. A felülvizsgálatot kezdeményezheti a Biztonsági eseménykezelési csoport bármely tagja.

(6) A biztonsági eseménykezelési tervet az egyes szakterületeknek jóvá kell hagyniuk, szerepkörüknek megfelelően.

53. Biztonsági események utólagos vizsgálata, visszacsatolás

84. § A biztonsági esemény bekövetkezését követően, az elhárítási feladatok ellátása után az alábbi teendőket kell elvégezni:

a) Teljes és részletes dokumentáció elkészítése.
b) A védelmi intézkedések fejlesztése, szükség esetén fejlettebb eszközök alkalmazása.
c) Szabályozó dokumentumok aktualizálása.
d) Biztonsági eseménykezelési tervek továbbfejlesztése.
e) Bizonyítékok mentése.
f) Ha szükséges, fegyelmi eljárás indítása.

54. Felelősség megállapítása

85. § Amennyiben a biztonsági esemény elhárítása, illetve a visszacsatolás során felmerül valamely személy(ek)re vonatkozóan felelősség, az IBF kötelessége a személyes felelősségre vonási eljárás elindítása. Ennek során az IBF a biztonsági esemény dokumentumaival, bizonyítékaival együtt a kormányhivatal integritás kezelési eljárása szerint elindítja a felelősségre vonási folyamatot.

XII. Fejezet
Karbantartás, informatikai üzemeltetés

55. A karbantartás, informatikai üzemeltetés alapelvei

86. § (1) A kormányhivatal a kiberbiztonsági tv.-ben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, a biztonsági osztályba sorolás követelményeiről, valamint a rendeletben megfogalmazott elvárások teljesítése érdekében az alábbiak szerint dokumentálja a karbantartási és javítási eljárások folyamatát, a feladatok végrehajtásának lépéseit, a végrehajtás során használt eszközöket és nyilvántartásokat, elvárt eredményeket.
(2) A kormányhivatal célja az üzemeltető foglalkoztatottak és külső felek számára rögzíteni azokat a követelményeket, melyeket az EIR üzemeltetése során be kell tartaniuk.
(3) A kormányhivatal a Karbantartási eljárásrendben rögzíti a részletszabályokat és feladatokat, valamint a kötelezően elkészítendő dokumentumok listáját.

56. Karbantartás célja, hozzárendelt erőforrások

87. § Az IFEFV irányításával az üzemeltetési és informatikai referensek által működtetett informatikai és biztonsági eszközökön, berendezéseken, ideértve pl. a tűzoltó- vagy klíma berendezéseket is, (továbbiakban: karbantartást igénylő elem) a szállító vagy gyártó által előírt időszakonként karbantartást végeznek, vagy végeztetnek el.
88. § (1) A kormányhivatal által használt minden olyan elektronikus információs rendszerre, informatikai eszközre, ezek részegységeire, valamint ezek információbiztonságát megvalósító eszközre, berendezésre, üzemeltetésére és működtetésére szolgáló, illetve azt támogató eszközökre. Ide tartoznak még a diagnosztikai és tesztprogramok, valamint a rendszeres karbantartásra és /vagy javításra vonatkozó szolgáltatások is. Az elektronikus információs rendszer körébe tartoznak a hálózatok és biztonsági eszközök, valamint a nyomatkészítő, beolvasó (scanner) és egyéb, az elektronikus információs rendszerrel közvetlen vagy közvetett kapcsolatban álló, az üzemeltetéshez és biztonság megteremtéséhez szükséges eszközök (pl. tűzoltó berendezés vagy rendszer, klíma, szünetmentes tápegység stb.)
(2) A nem a kormányhivatali, vagy közös tulajdonban, illetve kezelésben álló eszközök, rendszerek használata során figyelembe kell venni a tulajdonos, illetve vagyonkezelő vonatkozó előírásait, valamint az eszközre vonatkozóan megkötött, hatályos megállapodásokat. (pl. kormányablak, a szakmai feladatokat ellátó szervezeti egységek, központi irányító szerveinek eszközei, bérelt eszközök stb.)
89. § (1) Az Infrastruktúra üzemeltetési informatikai referensek felmérik, hogy a megfelelő karbantartásokhoz, javításokhoz milyen alkatrészeket, eszközöket, mérőeszközöket, anyagokat stb. kell biztosítani ahhoz, hogy a karbantartás és/vagy javítás elvégezhető legyen.
(2) Az IFEFV felelős azért, hogy a karbantartáshoz és / vagy javításhoz szükséges eszközök rendelkezésre álljanak, valamint az üzembiztonsági szint fenntartásához szükséges tartalék eszközök beszerzése, raktározása, nyilvántartása, azok felhasználása a megfelelő belső szabályzatoknak megfelelően történjenek.
(3) Az elektronikus információs rendszerek karbantartásához kizárólag erre a célra jóváhagyott karbantartási eszközöket lehet használni. A jóváhagyást az IFEFV adja meg, az érintett eszköz ellenőrzését követően.
(4) A jóváhagyott karbantartási eszközökről nyilvántartást kell vezetni. A nyilvántartás vezetése IFEFV felelőssége, az általa kijelölt kijelölt informatikai referensek feladata.

90. § (1) Az informatikai infrastruktúra elemekhez kapcsolódóan a kormányhivatal a következő humánerőforrásokat veszi igénybe:
(2) A kormányhivatal informatikai feladatellátásért felelős szervezet vezetői és foglalkoztatottjai: Feladatellátás minden saját rendelkezésre álló EIR valamennyi infokommunikációs komponense, illetve valamennyi központi szolgáltatásként használt EIR kormányhivatali rendelkezésében álló infokommunikációs komponense tekintetében.
(3) A kormányhivatal ingatlan és ingóság üzemeltetésért felelős szervezeti egység vezetői és foglalkoztatottjai: Valamennyi kormányhivatali kezelésben lévő infokommunikációs eszköz telephelyéhez és üzemeltetési – nem infokommunikációs – elemei tekintetében karbantartási és üzemeltetési feladatok ellátása.
(4) A kormányhivatal humánpolitikai feladatellátásért felelős szervezeti egység vezetői és foglalkoztatottjai: Valamennyi kormányhivatali foglalkoztatott vonatkozásában felhasználói életciklus kezeléséhez kapcsolódó (belépés, változáskezelés, kilépés) humánpolitikai feladatok ellátása.
(5) Külső szolgáltató foglalkoztatottjai: Meghatározott informatikai rendszerelemek vonatkozásában harmadik fél szolgáltatóval kötött megállapodásban foglalt és szabályozott szolgáltatások teljesítéséhez, karbantartásához, üzemeltetéséhez kapcsolódó munkavégzésben részt vevő személyek.

57. Szabályozott karbantartás

91. § Az erre a feladatra kijelölt informatikai referensek összegyűjtik és meghatározzák a rendelkezésére álló dokumentációi alapján, (üzemeltetési vagy karbantartási kézikönyv, utasítás stb.) hogy mely eszközök, berendezések (informatikai, hálózati, üzemeltetési, biztonsági) azok, amelyeken rendszeres karbantartási tevékenységet kell végezni. A rendszeres karbantartások ütemezése az IFEFV feladata és felelőssége, aki ennek céljából évente karbantartási tervet készített az általa kijelölt informatika referens segítségével.
92. § (1) A karbantartási tervnek legalább az alábbiakat kell tartalmaznia:
a) eszköz megnevezése és azonosítója,
b) karbantartásért felelős személy(ek),
c) karbantartás szükségességének ciklusa,
d) karbantartás módja (gyártó általi elvárások).
(2) A végrehajtott karbantartásokat dokumentálni kell és a karbantartásokról nyilvántartást kell vezetni.
(3) Az egyes karbantartást igénylő elemek karbantartásának megtörténtéért és ennek dokumentálásáért az erre a feladatre kijelölt informatikai referensek felelősek. A létrejött dokumentációkat a karbantartási nyilvántartáshoz csatolniuk kell.
(4) Amennyiben a tervezett karbantartás valamely elektronikus információs rendszer leállásával járhat, azt az előre kijelölt karbantartási időben kell elvégezni és a karbantartás időpontjáról az érintett rendszerelem felhasználóit előzetesen, legalább egy héttel előre értesíteni kell. A felhasználók időben történő értesítése az IFEFV felelőssége, aki szükség esetén az érintett alkalmazás üzemeltetőjével konzultációs célból egyeztet.
93. § (1) A karbantartásokat előre meg kell tervezni, amely az informatikai eszközök tekintetében az IFEFV feladata, aki ennek céljából évente karbantartási tervet készített az általa kijelölt informatika referens segítségével, a karbantartási ablakok előzetes meghatározásával együtt.
(2) A karbantartási ablakok idejét az adott SZEV/AG-val egyeztetni kell és ez alapján előzetesen tájékoztatni kell a felhasználókat.
(3) Előre nem tervezett karbantartás esetén minimum 1 héttel előre kell karbantartási ablakot kérni.
(4) A karbantartási tervet az IFEFV hagyja jóvá. A fizikai védelmet biztosító eszközök, berendezések esetében a FVFV felelőssége az eszközök és berendezések karbantartási tervének elkészítése.
(5) Amennyiben a tervezett karbantartás valamely EIR leállásával járhat, azt az előre kijelölt karbantartási időben kell elvégezni és a karbantartás időpontjáról az érintett rendszerelem felhasználóit előzetesen értesíteni kell. A felhasználók időben történő értesítése az IFEFV, illetve az erre kijelölt informatikai referens feladata.

(6) A karbantartásokat és javításokat a szállító vagy a gyártó által előírt módon, ütemezetten kell végrehajtani és dokumentálni kell, valamint felül kell vizsgálni a karbantartásokról és javításokról készült feljegyzéseket. Az egyes karbantartást igénylő elemek karbantartásának megtörténtéért és ennek dokumentálásáért az IFEFV, illetve az erre a feladatra általa kijelölt informatikai referensek felelősek. A dokumentálás megtörténtét az IBF szúrópróbaszerűen ellenőrzi.
(7) Amennyiben egy EIR vagy annak egy vagy több elemének karbantartása vagy javítása azt igényli, hogy kiszállítsák a szervezetből, akkor azt az IFEFV-nek jóvá kell hagynia, e nélkül bármilyen eszköz és berendezés karbantartás vagy javítás céljából történő kiszállítása a kormányhivatal területéről tilos. A jóváhagyás előtt ellenőrizni kell, hogy az eszköz tartalmaz-e adathordozót.
(8) Karbantartásra, javításra vagy cserére eszközt kivinni a kormányhivatal területéről – még garanciális esetben is – kizárólag az eszköz által tartalmazott adathordozó(k) kivételével (amennyiben ez lehetséges) vagy mentést követően, az adathordozón lévő adatok –visszaállíthatatlan törlése után lehetséges. Amennyiben ilyen esetben az adathordozó kivétele vagy visszaállíthatatlan törlése sem végrehajtható, úgy az eszköz kiszállítását kizárólag – az IFEFV jóváhagyásán felül – az IBF és a SZEV/AG jóváhagyásával lehet végrehajtani.
(9) A kiszállítást megelőző vizsgálatok és tevékenységek végrehajtásáért és azok dokumentálásáért az IFEFV, illetve az erre a feladatra általa kijelölt informatikai referens a felelős.
(10) A karbantartások, javítások elvégzését követően meg kell győződni az eszköz megfelelő működéséről és a Karbantartási eljárásrend szerinti biztonsági ellenőrzésnek kell alávetni.

58. Szolgáltatásmenedzsment

94. § (1) A kormányhivatal az informatikai feladatellátása biztonságos és hatékony támogatásához munkaszervezési és szolgáltatásmenedzsment rendszereket, eljárásokat alkalmaz. Az informatikai és üzemeltetési feladatok ellátásánál a támogató rendszerek tekintetében legalább a következő követelményeknek kell megfelelni:
(2) Valamennyi igény bejelentést, hibabejelentést és kérelem (összefoglalva: kérelem) egyedi azonosítóval, a szükséges és elégséges adattartalommal kell létrehozni.
(3) A bejelentés tartalmazzon minden olyan adatot, ami alapján a kérelmet osztályozni, rangsorolni és delegálni lehessen.
(4) A kérelemben rögzített adatok alapján automatikusan, előre rögzített folyamatok mentén, illetve manuálisan, delegálás útján osztályozásra kerül az adott kérelem.
(5) A delegálás során a szükséges erőforrásokkal rendelkező (idő, kompetencia, szükséges eszközök) foglalkoztatott kerül a feladatellátásra kijelölésre.
(6) A munkásszervezési, szolgáltatásmenedzsment rendszerben előre rögzített OLA / SLA alapján szabott időkeret alatt kell az adott kérelemben meghatározott feladatot elvégezni.
(7) A szolgáltatásmenedzsment rendszer a kérelmekről, adatairól naprakész dashboard szolgáltatást, illetve konfigurálható riportokat biztosít.
(8) A kérelmeket érintő munkafolyamat, a megoldás során történt kommunikáció, valamennyi kérelem kezelését érintő aktus naplózott, figyelemmel kísérhető.
95. § A szolgáltatás katalógus kezdeti kialakítását követően a szolgáltatás menedzsment rendszerben rögzített adatok, felhasználói és alkalmazói visszajelzések, illetve a kormányhivatal belső és külső környezetét érintő változások miatt a szolgáltatásmenedzsment rendszerben rögzített kérelmeket és ajánlatokat folyamatosan felül kell vizsgálni. A felülvizsgálatot legalább évente az IFEFV vezetésével az FVFV, IBF és az érintett SZEV/AG bevonásával kell végrehajtani.
96. § (1) A kormányhivatal által üzemeltetett bejelentő, szolgáltatás menedzsment felületen az arra jogosult foglalkoztatott a megfelelő adattartalommal rögzíti a kérelmet.
(2) A kérelem ezt követően kerül kiosztásra / delegálásra a kérelmet érintő erőforrások alapján az IFEFV, illetve az általa delegálásra kijelölt informatikai vezető vagy referens, illetve az FVFV, illetve az általa delegálásra kijelölt üzemeltetési vezető vagy referens által, a szolgáltatásmenedzsment felületen rögzítve.

97. § (1) A kérelmek feldolgozásának, előrehaladás rögzítése adminisztratív részét a delegált foglalkoztatott a szolgáltatásmenedzsment rendszerben rögzíti.
(2) A kérelemben foglaltak elkészültét a kérelmet benyújtó felhasználó részére a kérelmet feldolgozó foglalkoztatott a szolgáltatásmenedzsment rendszerben jelzi. A szolgáltatásmenedzsment rendszerben rögzített adatok alapján az IFEFV, FVF, IBF a meghatározott szolgáltatásokhoz kapcsolódó eljárásrendeket, folyamatokat, erőforrásokat, szabályzatrészeket legalább évente egy alkalommal felülvizsgálja.

XIII. Fejezet
Adathordozók védelme

59. Az adathordozók védelmének alapelvei

98. § (1) A kormányhivatal rendelkezésére álló adathordozók tekintetében (lemezek, merevlemezek, szilárdtest alapú tárolók, mobiltelefonok) az eszközök teljes életciklusában biztosítani kell a tárolt adatok vonatkozásában a bizalmasság, sértetlenség és rendelkezésre állás elveinek betartását, betartatását. Ennek érdekében a tárgyban érintett eszközmozgatásokat dokumentálni kell, a felelősi rendszert ki kell alakítani.
(2) A fentiek biztosítása érdekében szükséges kialakítani:
a) az adathordozók igénylésének, kiadásának és visszavételének, valamint nyilvántartásának szabályozott működtetésének szabályait, kereteit,
b) az adathordozók életciklusának teljes vertikumát, kiemelten az életciklus végén az adathordozó tárolására, törlésére és selejtezésére vonatkozó szabályokat.
(3) A további részletszabályokat az Adathordozók védelmére vonatkozó eljárásrend tartalmazza.

60. Adathordozó életciklus kezelés

99. § A vonatkozó eszközök igénylésénél az érintett foglalkoztatott vezetője SZEV/AG a kormányhivatalnál kialakított igénybejelentő felületen kezdeményezi a következő adattartammal:
a) igénylő szervezeti egység neve,
b) igénylő foglalkoztatott neve,
c) igényelt eszköz adatai,
d) igénylés szakmai indoka.
100. § Amennyiben az eszközigényt az informatikai terület vezetője IFEFV, vagy az általa megbízott foglalkoztatott engedélyezi, ezt a tényt a kormányhivatal által használt felületen rögzíti, illetve a kiadást (átadás-átvételt) az alábbi adattartartalommal a kormányhivatal által használt igény bejelentő felületen rögzíti:
a) átvevő nyilatkozata az IBSZ és a kapcsolódó szabályzókban rögzítettek betartására vonatkozólag,
b) kiadott eszköz típusa, azonosító adatai,
c) kiadott eszköz adattartamára vonatkozó releváns információk,
d) átadás-átvétel tényének és tényadatainak rögzítése (Hely, idő, átadó és átvevő adatai).
101. § A kiadott adathordozóhoz történő hozzáférés kizárólag az igénylő felhasználó részére engedélyezett. Az adathordozó használata során a felhasználó felelőssége az adathordozón tárolt adatok bizalmasságának, sértetlenségének és rendelkezésének állásának biztosítása. A kiadott adathordozó felhasználása kizárólag kormányhivatali feladatellátással összefüggő érdekeket szolgálhat.
102. § (1) A kormányhivatalban csak hivatalos adathordozók használhatók, saját eszközök csatlakoztatása tilos. Az adathordozókat folyamatosan ellenőrizni kell a hivatal által biztosított vírusvédelmi eszközzel.

(2) Cserélhető adathordozók használata esetén az adathordozót birtokló személy felelősséggel tartozik az azon lévő információk kompromittálódása, illetve illetéktelen kézbe kerülése által okozott károkért.
(3) Az adathordozók kizárólag munkavégzés céljából használhatóak a kormányhivatal tevékenységének végzéséhez. A felhasználók munkájához nem kapcsolódó adatok tárolása, illetve az adathordozók magáncélú felhasználása nem engedélyezett.
(4) Az informatikai feladatok ellátásáért felelős szervezeti egység kizárólag az erre a célra biztosított hálózati meghajtókon tárolt adatok bizalmasságáért, sértetlenségéért és rendelkezésre állásáért vállal felelősséget, az ezekről készülő rendszeres biztonsági mentések segítségével. A munkaállomás helyi meghajtóin tárolt adatok bizalmasságáért, sértetlenségéért és rendelkezésre állásáért a felhasználó tartozik felelősséggel.
(5) Amennyiben eszközhasználatra kerül sor a kormányhivatalon kívül, az adathordozókon tárolt adatokat és dokumentumokat a lehető leghamarabb fel kell tölteni a kormányhivatal által biztosított fileszerverre, majd ezt követően az adathordozóról az adatokat törölni szükséges.
(6) Az adathordozók kormányhivatal telephelyein kívülre vitele esetére a következő szabályok betartása kötelező:

a) adathordozó csak engedéllyel vihető ki a kormányhivatal telephelyein kívülre, melyet az IFEFV engedélyez;
b) a telephelyen kívülre történő szállítás esetén az adathordozó biztonságáért a szállítást végző felel;
c) az adathordozón tárolt adatok biztonsági osztályához tartozó előírásokat minden esetben be kell tartani;
d) a telephelyen kívülre történő szállítás során betartandó előírásokról részletesen az Adathordozók védelmére vonatkozó eljárásrend rendelkezik.

(7) Az ismeretlen (nem egyértelműen beazonosítható) tulajdonosú adathordozók használata nem megengedett. Ilyen esetben a talált adathordozót nem szabad a számítógépekhez csatlakoztatni vagy mások számára továbbadni. Az IBF/IFEFV felé azonnal jelenteni kell a megtalálás tényét és át kell adni számára a talált adathordozót.
(8) Az IBF/IÜFV a talált adathordozót és a kormányhivatalba kerülésének módját egyedileg megvizsgálja, vagy megvizsgáltatja elszeparált környezetben (szükség esetén külső szakértők bevonásával), majd a vizsgálat lezárását követően az incidensről jelentést készít.
(9) A nem beépített adathordozókat a napi munkavégzés befejezését követően le kell választani a számítógépekről és elzárva kell tartani (páncélszekrényben, széfben, zárt szekrényben vagy fiókban stb.), erről az adathordozó használójának kell gondoskodnia. Ügyelni kell arra, hogy ilyen adathordozó semmi esetre se maradjon szem előtt (például asztalon hagyva).
(10) A tárolás során a gyártói előírásokat be kell tartani és a gyártó által előírt megfelelő környezeti paramétereket biztosítani kell.
(11) Ha az adathordozó jelölése olvashatatlan vagy megváltoztatandó, a felhasználónak jeleznie kell ezt az Informatikai feladatokat ellátó szervezeti egységnek, amely gondoskodik a szükséges intézkedésekről.
103. § Az adathordozó visszavétele esetén az informatikai terület vezetője IFEFV, vagy az általa megbízott foglalkoztatott a visszavételt (átadás-átvételt) az alábbi adattartartalommal a kormányhivatal által használt igény bejelentő felületen rögzíti:

a) átvevő nyilatkozata a visszavett adathordozó állapotára vonatkozóan,
b) visszavett eszköz típusa, azonosító adatai,
c) visszavett eszköz adattartamára vonatkozó releváns információk,
d) átadás-átvétel tényének és tényadatainak rögzítése (Hely, idő, átadó és átvevő adatai).

104. § (1) Az adathordozók újrafelhasználása (más informatikai környezetben, más felhasználó használatában) csak az adathordozón lévő adatok lehetőség szerinti teljes körű és visszaállíthatatlan módon történő törlést követően engedélyezett.
(2) A selejtezésre előkészített adathordozókat elkülönítve, zárt, ellenőrzött és privilegizált hozzáféréssel rendelkező raktárhelységben, zárt szekrényben kell tárolni. A selejtezendő eszközökből a selejtezést megelőzően az adattároló komponenseket el kell távolítani, és az előző mondatban leírtak szerint kell tárolni.

(3) Az adathordozók megsemmisítését dokumentáltan, saját hatáskörben, vagy szerződött szolgáltatón keresztül kell elvégezni, elvégeztetni. Az adathordozók megsemmisítése roncsolással, megfelelően kicsi (1 cm3) darabokra zúzással, illetve magas hőmérsékleten történő elégetéssel, hamvasztással kell, hogy megtörténjen, melyről jegyzőkönyvet kell készíteni a megsemmisítést végzőknek. A jegyzőkönyvben rögzíteni kell, hogy a megsemmisítést követően az érintett adathordozókról adatok visszaállítása nem lehetséges.

61. Nyilvántartás

105. § Az adathordozókról naprakész nyilvántartást kell vezetnie az Informatikai feladatellátásért felelős szervezeti egységnek, az alábbi adattatalommal:

a) adathordozó megnevezése, azonosító adatai,
b) adathordozót használó felhasználó neve, adatai,
c) adathordozó kiadásának ideje,
d) adathordozó visszavételének ideje,
e) adathordozó állapotára vonatkozó információk,
f) tárolt adatokra vonatkozó információk,
g) megjegyzés.

62. Kivételkezelés

106. § (1) Az adathordozó elvesztésének tényét az érintett felhasználó haladéktalanul köteles bejelenteni a kormányhivatal bejelentő felületén az alábbi adattartammal:

a) érintett adathordozó megnevezése, adatai,
b) érintett felhasználó, adatai,
c) tárolt adatokra vonatkozó információ,
d) nyilatkozat személyes adatok kompromittálódásának lehetőségéről,
e) incidenst érintő releváns adatok.

(2) A bejelentést követően az IBF az IFEFV és az AVF bevonásával kivizsgálja az eszköz elvesztéséből fakadó incidenst és megteszi:

a) FŐISPÁN/FŐIG/IG felé a megfelelő tájékoztatást,
b) adatvédelmi incidens esetén a Nemzeti Adatvédelmi Információszabadság Hatóság felé a bejelentést,
c) információbiztonságot érintő incidens esetén a Nemzeti Kibervédelmi Intézet felé a bejelentést.

107. § (1) Az adathordozó sérülésének tényét az érintett felhasználó haladéktalanul köteles bejelenteni a kormányhivatal bejelentő felületén kialakított felületen az alábbi adattartammal:

a) érintett adathordozó megnevezése, adatai,
b) érintett felhasználó, adatai,
c) tárolt / sérült adatokra vonatkozó információ,
d) a tárolt adatok másodlagos fellelhetőségét érintő releváns adatok.

(2) A bejelentést követően a sérült eszköz visszavételre kerül, amennyiben indokolt, úgy indítható egy újabb adathordozó iránti kiadási igény.

XIV. Fejezet
Fizikai és környezeti védelem

63. A fizikai és környezeti védelem alapelvei

108. § (1) A kormányhivatal az elektronikus információs rendszerei biztonsági osztályba sorolásának megfelelő, kockázatarányos fizikai védelmi intézkedéseket alakít ki és alkalmaz.
(2) A kormányhivatal az elektronikus információs rendszernek helyt adó helyiség alatt azt a helyiséget (termet, szerverszobát, adatközpontot) értelmezi, amelyben az EIR működtetését biztosító hardver eszközök megtalálhatók.
(3) A kormányhivatal helyiségei információbiztonsági szempontból az alábbi biztonsági kategóriákba sorolhatók:
(4) Kiemelten védett kategória: Kiemelten védett helyiségnek kell tekinteni azokat a helyiségeket, ahol bizalmas adatok feldolgozására, tárolására alkalmazott központi informatikai erőforrások, azaz az elektronikus információs rendszer üzemeltetésének eszközei találhatók meg, pl.: szerver, hálózati aggregációs és NTG végpont.
(5) Fokozottan védett kategória: Fokozottan védett helyiségnek kell tekinteni azokat a helyiségeket, ahol az elektronikus információs rendszer üzemeltetését támogató, kiegészítő informatikai erőforrások találhatók (pl.: RACK szekrények), illetve az elektronikus információs rendszer üzemeltetését végző személyek, informatikusok a napi munkájukat végzik.
(6) Védett kategória: A védett kategóriába tartozó helyiségekben végzik a felhasználók az általános napi feladataikat, amelyekbe azonban az ügyfelek nem rendelkeznek szabad bejárással, ott csak felügyelet mellett tartózkodhatnak.
(7) Nyilvános kategória: Nyilvános kategóriába tartoznak a kormányhivatal azon helyiségei, amelyek nem tartoznak egyik fentebb felsorolt kategóriába sem, jellemzően az ügyfelek által szabadon elérhető ügyféltér.
(8) A besorolás folyamatát és a részletes fizikai védelmi intézkedéseket a Fizikai és környezeti védelemre vonatkozó eljárásrend rögzíti.
(9) A fizikai védelmi intézkedéseket az IBF évente legalább egy alkalommal szúrópróba szerűen ellenőrzi.
(10) A kormányhivatal valamennyi helyiségét biztonsági kategóriába kell sorolni, amelyet az IFEFV végez el és az IBF hagy jóvá.

64. Fizikai belépési engedélyek

109. § (1) A kormányhivatal összeállítja, jóváhagyja és kezeli az elektronikus információs rendszernek helyt adó helyiségekbe belépésre jogosultak listáját. A listát IFEFV és a FVFV állítja össze az IBF egyetértésével, amelyet az IFEFV hagy jóvá.
(2) A belépés jogosultságának igazolására az informatikai feladatellátásért felelős szervezeti egység belépést engedélyező dokumentumot (pl.: kitűző) állít ki vagy hitelesítő eszközt (pl.: belépőkártyát) biztosít.
(3) A belépési jogosultsággal rendelkező személyekről az informatikai feladatellátásért felelős szervezeti egység nyilvántartást vezet, amelyet rendszeres időközönként, de legalább 3 havonta ellenőriz.

65. Fizikai belépés ellenőrzése

110. § (1) A kormányhivatal gondoskodik az illetéktelen behatolást vagy hozzáférést, valamint a szándékos károkozást vagy véletlen katasztrófát megakadályozó, szükséges mértékű és kockázatokkal arányos védelmi intézkedések alkalmazásáról. Ennek érdekében a kormányhivatal:

a) Kizárólag a meghatározott be- és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést.
b) Ellenőrzi az egyéni jogosultságokat a létesítménybe való belépés előtt.
c) Fizikai beléptető rendszerek, eszközök, vagy biztonsági személyzet segítségével ellenőrzi a létesítménybe való be- és kilépést.
d) Kiemelten védett és fokozottan védett kategóriába sorolt területeken naplózza a fizikai be- illetve kilépéseket.
e) Ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket.
f) Kíséri a létesítménybe ad-hoc belépésre jogosultakat (vendégeket), és figyelemmel kíséri a tevékenységüket.
g) Megóvja a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző eszközöket;
h) Nyilvántartást vezet a fizikai belépést ellenőrző eszközökről, és meghatározott gyakorisággal frissíti azt.
i) Meghatározott rendszerességgel megváltoztatja a hozzáférési kódokat és kulcsokat, illetve ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az azokkal rendelkező személy elveszíti a belépési jogosultságát.

66. Látogatói naplózás

111. § (1) Az elektronikus információs rendszernek helyt adó helyiségben a kormányhivatal naplózással felügyeli a fizikai hozzáféréseket, folyamatosan figyelemmel kíséri és észleli a fizikai biztonsági eseményeket és szükség esetén azokra reagál. A kormányhivatal rendszeresen átvizsgálja a keletkezett napló eseményeket és elemzi azokat. Amennyiben a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak, a kormányhivatal soron kívül elemzi a naplóeseményeket.
(2) Az elektronikus információs rendszernek helyt adó helyiségen kívüli területek felügyeletét a kormányhivatal biztonsági szolgálat vagy biztonsági kamerák használatával biztosítja.
(3) A kormányhivatal az elektronikus információs rendszernek helyt adó helyiségbe történő belépésekről szóló napló információkat 1 évig őrzi meg.
(4) Az IBF szúrópróbaszerűen megvizsgálja a nyilvántartást és rendellenesség észlelése esetén azonnal jelzi azt az IFEFV.

67. Hozzáférés felügyelet

112. § (1) Az elektronikus információs rendszernek helyt adó helyiségben a kormányhivatal naplózással felügyeli a fizikai hozzáféréseket, folyamatosan figyelemmel kíséri és észleli a fizikai biztonsági eseményeket és szükség esetén azokra reagál. A kormányhivatal rendszeresen átvizsgálja a keletkezett napló eseményeket és elemzi azokat. Amennyiben a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak, a kormányhivatal soron kívül elemzi a naplóeseményeket.
(2) Az elektronikus információs rendszernek helyt adó helyiségen kívüli területek felügyeletét a kormányhivatal biztonsági szolgálat vagy biztonsági kamerák használatával biztosítja.

68. Rendszerelemek ki és beszállítása

113. § (1) A kormányhivatal a Fizikai és környezeti védelemre vonatkozó eljárásrendben meghatározott engedélyezési eljárás útján teszi lehetővé vagy tiltja meg a rendszerelemek létesítménybe való be-, illetve onnan történő kiszállítását. A rendszerelemek mozgatása fokozott figyelmet igényel az elektronikus információs rendszer erőforrásait koncentráltan tartalmazó helyiségek esetében.

(2) Az IFEFV által erre a feladatra kijelölt informatikai vezető vagy referens foglalkoztatottak részletes rendszerelem nyilvántartást vezetnek, amely nyomon követi az egyes rendszer elemek mozgatásának időpontját, forrás- és célállomását, a felelős személyt és a mozgás okát. A nyilvántartás vezetéséért az IFEFV vagy az által erre a feladatra kijelölt informatikai vezető felel.
(3) A nyilvántartás vezetését az IBF szúrópróba szerűen, de legalább évente egyszer ellenőrzi az IFEFV által erre a feladatra kijelölt informatikai vezető vagy referens bevonásával. EIR kiszolgáló infrastruktúrával kapcsolatos követelmények
(4) A kormányhivatal megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információs rendszerek szempontjából érintett létesítményekre vagy helyiségekre érvényes Fizikai és környezeti védelemre vonatkozó eljárásrendet, amely az érintett szervezet elektronikus információbiztonsági, vagy egyéb szabályzatának részét képező fizikai védelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.
(5) Fizikai belépési engedélyek és azok ellenőrzése tekintetében:

a) összeállítja, jóváhagyja és kezeli az elektronikus információs rendszereknek helyt adó létesítményekbe / helyiségekbe belépésre jogosultak listáját;
b) belépési jogosultságot igazoló dokumentumokat (pl. kitűzők, azonosító kártyák, intelligens kártyák) bocsát ki a belépéshez a belépni szándékozó részére, valamint intézkedik ezen jogosultságok visszavonása, érvénytelenítése, törlése, megsemmisítése iránt;
c) rendszeresen felülvizsgálja a belépésre jogosult személyek listáját;
d) eltávolítja a belépésre jogosult személyek listájáról azokat, akiknek a belépése nem indokolt;
e) kizárólag az érintett szervezet által meghatározott be-, és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést;
f) naplózza a fizikai belépéseket;
g) ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket;
h) kíséri a létesítménybe ad-hoc belépésre jogosultakat és figyelemmel követi a tevékenységüket;
i) megóvja a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző eszközt;
j) nyilvántartást vezet a fizikai belépést ellenőrző eszközről;
k) meghatározott rendszerességgel változtatja meg a hozzáférési kódokat és kulcsokat, vagy azonnal, ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az adott személy elveszti a belépési jogosultságát;
l) az egyéni belépési engedélyeket a belépési pontokon ellenőrzi;
m) a kijelölt pontokon való átjutást felügyeli a szervezet által meghatározott fizikai belépést ellenőrző rendszerrel vagy eszközzel;
n) felhívja a szervezet tagjainak figyelmét a rendellenességek jelentésére.

(6) Fizikai hozzáférések felügyelete tekintetében:

a) ellenőrzi az elektronikus információs rendszereknek helyt adó létesítményekbe történt fizikai hozzáféréseket annak érdekében, hogy észlelje a fizikai biztonsági eseményt és reagáljon arra;
b) rendszeresen átvizsgálja a fizikai hozzáférésekről készült naplókat;
c) azonnal átvizsgálja a fizikai hozzáférésekről készült naplókat, ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak;
d) összehangolja a biztonsági események kezelését, valamint a napló átvizsgálások eredményét.

(7) Látogatók ellenőrzése tekintetében:

a) meghatározott ideig megőrzi az elektronikus információs rendszereknek helyt adó létesítményekbe történt látogatói belépésekről szóló információkat;
b) azonnal átvizsgálja a látogatói belépésekről készített információkat és felvételeket, ha a rendelkezésre álló információk jogosulatlan belépésre utalnak.

(8) Vészvilágítás tekintetében: egy automatikus vészvilágítási rendszert alkalmaz és tart karban, amely áramszünet esetén aktiválódik, és amely biztosítja a vészkijáratokat és a menekülési útvonalakat.
(9) Tűzvédelem tekintetében: az elektronikus információs rendszerek számára független áramellátással támogatott észlelő, az informatikai eszközökhöz megfelelő tűzelfojtó berendezéseket alkalmaz, és tart karban.

(10) Hőmérséklet és páratartalom ellenőrzése tekintetében:
a) az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. adatközpont, szerver szoba, központi gépterem) az erőforrások biztonságos működéséhez szükséges szinten tartja a hőmérsékletet és páratartalmat;
b) az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. adatközpont, szerver szoba, központi gépterem) figyeli a hőmérséklet és páratartalom szintjét;
c) biztosítja a víz-, és más, csővezetéken szállított anyag okozta kár elleni védelmet;
d) védi az elektronikus információs rendszert a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzárószelepek hozzáférhetőek, és megfelelően működnek, valamint a kulcsszemélyek számára ismertek;
e) az informatikai erőforrásokat koncentráltan tartalmazó helyiségek tervezése (pl. adatközpont, szerver szoba, központi gépterem) során biztosítja, hogy az a víz-, és más hasonló kártól védett legyen, akár csővezetékek kiváltásával, áthelyezésével is.

(11) Be- és kiszállítás tekintetében: engedélyezi, vagy tiltja, továbbá figyeli és ellenőrzi a létesítménybe bevitt, onnan kivitt információs rendszerelemeket, és nyilvántartást vezet ezekről.
(12) Karbantartók tekintetében:
a) kialakít egy folyamatot a karbantartók munkavégzési engedélyének kezelésére, és nyilvántartást vezet a karbantartó szervezetekről vagy személyekről;
b) megköveteli a hozzáférési jogosultság igazolását az elektronikus információs rendszeren karbantartást végzőktől;
c) 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.

(13) Hozzáférés az adatátviteli eszközökhöz és csatornákhoz tekintetében: az általa meghatározott biztonsági védelemmel ellenőrzi az elektronikus információs rendszer adatátviteli eszközeinek és kapcsolódási pontjainak helyt adó helyiségekbe történő fizikai belépést.
(14) A kimeneti eszközök hozzáférés ellenőrzése tekintetében: kimeneti eszközeihez való fizikai hozzáférést annak érdekében, hogy jogosulatlan személyek ne férjenek azokhoz hozzá.
(15) Behatolás riasztás, felügyeleti berendezések tekintetében: felügyeli a fizikai behatolás riasztásokat és a felügyeleti berendezéseket.
(16) Áramellátó berendezések és kábelezés tekintetében: védi az elektronikus információs rendszert árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben.
(17) Tartalék áramellátás tekintetében: az elsődleges áramforrás kiesése esetére, a tevékenységhez méretezett, rövid ideig működőképes szünetmentes áramellátást biztosít az elektronikus információs rendszer szabályos leállításához vagy a hosszútávú tartalék áramellátásra történő átkapcsoláshoz.
(18) Vészkikapcsolás tekintetében:
a) lehetőséget biztosít az elektronikus információs rendszer vagy egyedi rendszerelemek áramellátásának kikapcsolására vészhelyzetben;
b) gondoskodik a vészkikapcsoló berendezések biztonságos és könnyű megközelíthetőségéről;
c) megakadályozza a jogosulatlan vészkikapcsolást.

(19) Automatikus tűzelfojtás tekintetében: a személyzet által folyamatosan nem felügyelt elektronikus információs rendszerek számára a lehetőségek függvényében automatikus tűzelfojtási képességet biztosít.
(20) Az elektronikus információs rendszer elemeinek elhelyezése tekintetében: úgy helyezi el az elektronikus információs rendszer elemeit, hogy a legkisebb mértékre csökkentse a szervezet által meghatározott fizikai és környezeti veszélyekből adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét.
(21) Ellenőrzés tekintetében: ellenőrzi a karbantartó személyzet által a létesítménybe hozott karbantartási eszközöket, a nem megfelelő vagy jogosulatlan módosítások megakadályozása érdekében.
(22) Időben történő javítás tekintetében: karbantartási támogatást szerez be a meghatározott elektronikus információs rendszerelemekhez.
114. § A kormányhivatal valamennyi telephelye vonatkozásában vagyonvédelmi rendszereket telepít, illetve külső szolgáltatóval kialakít és üzemeltet.

115. § A kormányhivatal független energiaforrással rendelkező tűzérzékelő rendszert tart fenn valamennyi helyisége, de kiemelten az elektronikus információs rendszernek helyt adó helyiségek vonatkozásában. Valamennyi, az elektronikus információs rendszer erőforrásait tartalmazó, illetve elérhetőségét biztosító helyiség esetén a kormányhivatal biztosítja a megfelelő tűzoltó eszközt. A kormányhivatal Tűzvédelmi szabályzata tartalmazza az egyes helyiségek besorolásának megfelelően a szükséges tűzoltó eszköz meghatározását.
116. § (1) A kormányhivatal a kiemelten védett, azaz az elektronikus információs rendszerek erőforrásait koncentráltan tartalmazó helyiségeket védi a csővezeték rongálódásból származó károkkal szemben. Ennek érdekében biztosítani kell, hogy a főelzáró szelepek hozzáférhetők és működőképesek, valamint a felelős szerepköröket betöltő személyek számára ezek ismertek legyenek.
(2) Az elektronikus információs rendszerek erőforrásait koncentráltan tartalmazó helyiségek kialakítása során törekedni kell a vízkár kockázatának csökkentésére, lehetőség szerint elkerülve a csővezeték helyiségen belüli vagy annak közvetlen falazatában való vezetését. Ennek hiányában törekedni kell a főelzáró szelepek mellett vagy helyett, csak az érintett helyiségre vonatkozó elzáró szelep alkalmazására.
(3) A vízbetörés elleni védekezés részeként dokumentálni szükséges a kockázatos területen haladó vízvezetékek karbantartását és rendszeres ellenőrzését, amelyet a Fizikai és környezeti védelemre vonatkozó eljárásrend határoz meg.
117. § A kormányhivatal az informatikai erőforrásokat koncentráltan tartalmazó helyiségeire vonatkozóan környezeti feltételekhez kapcsolódó követelményeket határoz meg a Fizikai és környezeti védelemre vonatkozó eljárásrendben. A környezeti feltételek meghatározása minimálisan tartalmazza a hőmérsékletre és páratartalomra vonatkozó követelményeket.
118. § (1) Az elektronikus információs rendszerek erőforrásait koncentráltan tartalmazó helyiségekben a kormányhivatal jelzőrendszert működtet, amely a Fizikai és környezeti védelemre vonatkozó eljárásrendben meghatározott eseményekről értesítést küld az érintetteknek.
(2) Legalább az alábbi jelzéseket kell megvalósítani:

a) tűzjelzés,
b) behatolásjelzés,
c) hőmérséklet emelkedés jelzés,
d) páratartalom emelkedés jelzés.

XV. Fejezet
Tervezés

69. A tervezés alapelvei

119. § (1) Biztonság tervezés vonatkozásában a fő cél, hogy a kormányhivatal rendelkezésében álló infokommunikációs infrastruktúra elemek (EIR-ek, hardver, szoftver és humán rendszerelemek) vonatkozásában biztosított legyen:

a) tervezés szinten az információbiztonság és kibervédelmi szempontok alkalmazása,
b) felhasználás szinten egy a szervezet biztonsági osztályának megfelelő egyenerősségű, biztonságtudatos normakövetés,
c) üzemeltetés és folyamatfejlesztés szinten az információbiztonság és kibervédelmi szempontok érvényesítése.

(2) A további részletszabályokat a Biztonságtervezési eljárásrend tartalmazza.

70. Biztonsági követelmények kiválasztása

120. § (1) A kormányhivatal rendelkezésében lévő EIR-ek biztonsági követelményeinek meghatározásához az alábbi szabályzókkal és dokumentációkkal kell rendelkezni:

a) a kormányhivatal Szervezeti és Működési Szabályzata,
b) az Információbiztonsági Irányítási Rendszer dokumentumai,
c) az elektronikus információs rendszerek rendszerbiztonsági tervei,
d) az elektronikus információs rendszerek egyéb tervei, üzemeltetési leírásai,
e) a kormányhivatal infrastruktúrájára vonatkozó architektúra leírások.

(2) A dokumentumcsoportba tartozó szabályzókat és dokumentációkat az adott szabályzatban vagy dokumentumban előírt gyakoriság szerint kell felülvizsgálni, frissíteni, illetve minden olyan esetben, amikor szervezeti, műszaki, vagy egyéb változások indokolttá teszik.

71. Biztonsági követelmények testre szabása

121. § (1) Az egyes EIR-ek biztonsági követelményeit az adott EIR-hez tartozó rendszerbiztonsági tervben kell rögzíteni.
(2) Az adott EIR-hez kapcsolódó biztonsági követelmények meghatározása az IBF feladata.

72. Rendszerbiztonsági terv

122. § (1) A kormányhivatal kezelésében lévő EIR-ekhez a rendszerbiztonsági terv elkészítése az IÜFV feladata és az IFEFV felelőssége.
(2) A rendszerbiztonsági terv sablont a 9. számú melléklet tartalmazza.
(3) A rendszerbiztonsági terv részben vagy egészében helyettesíthető az adott EIR rendszerdokumentációjának biztonsági részével is, amennyiben az tartalmi szempontok tekintetében megfelel az elvárásoknak.
(4) A Rendszerbiztonsági tervek készítésébe az érintett SZEV/AG-t is be kell vonni. Az elkészített Rendszerbiztonsági terveket csak az arra jogosultak ismerhetik meg.
(5) Az elektronikus információs rendszerek rendszerbiztonsági terveit a változáskezelési folyamat részeként folyamatosan naprakészen kell tartani, mely az IÜFV feladata és az IFEFV felelőssége.

73. Viselkedési szabályok, infokommunikációs rendszerek használatát érintő korlátozások

123. § (1) A kormányhivatal infokommunikációs rendszerével, a rendszer üzemeltetésével vagy a rendszer elhelyezésére szolgáló objektummal kapcsolatban álló felhasználóknak kötelessége jelenteni olyan nem várt egyedi, vagy sorozatos információbiztonsági eseményeket, amelyek nagy valószínűséggel veszélyeztetik a kormányhivatali tevékenységet és fenyegetik az információbiztonságot. A bejelentést a kormányhivatal által működtetett bejelentő felületen keresztül köteles a felhasználó elvégezni. Ennek akadályoztatása esetén, telefonon vagy e-mailen keresztül kell megtenni a bejelentést az IFEFV, illetve az általa erre a feladatra kijelölt informatikai vezető vagy referens, vagy az IBF részére.
(2) A biztonsági események, biztonsági incidensek megelőzése érdekében az informatikai eszközök kezelésével kapcsolatos felhasználói és biztonsági ismereteket el kell sajátítani.
(3) Tartózkodni kell minden olyan tevékenységtől, amely az informatikai rendszerben a bizalmasság, sértetlenség vagy rendelkezésre állás sérülését okozhatja:
(4) A hivatali adatok nem hivatali céllal történő kijuttatása, magán célú felhasználása, vagy harmadik személy rendelkezésére bocsátása tilos.

(5) A felhasználónak az alapértelmezett jelszavakat az első belépés után kötelessége azonnal megváltoztatni, továbbá a későbbiekben köteles a jelszavát az előírt gyakorisággal és módon megváltoztatni.
(6) A felhasználó a számítógépre csak saját nevében és jelszavával léphet be, és az alkalmazásokat csak saját nevében használhatja, más felhasználó azonosítóját átmeneti jelleggel sem szabad használni.
(7) A felhasználó azonosítójával és jelszavával az informatikai rendszerben végrehajtott műveletekért személyesen felel.
(8) A jelszavak nem hozhatók nyilvánosságra és nem oszthatók meg senkivel, azok bizalmasságának megőrzéséért a felhasználó személyesen felel.
(9) Ha a felhasználónak a legkisebb gyanúja is felmerül, a jelszó biztonságának integritása felől, azt köteles azonnal megváltoztatni és gyanújáról az IBF-et értesíteni.
(10) Az informatikai rendszerek használata csak hivatalos célokra engedélyezett, kizárólag azokat a feladatokat szabad elvégezni, amelyek a felhasználó vagy üzemeltető munkájának ellátásához szükségesek, függetlenül attól, hogy a rendszer esetleg ennél szélesebb körű tevékenységet enged meg.
(11) A kormányhivatal eszközein csak a kormányhivatal által engedélyezett programokat szabad használni, a számítógépekre szoftver telepítése - függetlenül a szoftver származási helyétől - szigorúan tilos.
(12) A hivatali adattároló eszközökön tilos magánjellegű, vagy a hivatali munkához nem kapcsolódó dokumentumokat, fényképeket, videókat tárolni.
(13) A saját használatra átvett számítógép rendszerszintű beállításainak módosítása (ebbe nem értendők bele az irodai programok felhasználói beállításai), felhasználó számára nem engedélyezett, a kormányhivatal által rendszeresített biztonsági funkciókat (például automatikus képernyővédő-aktiválás) kikapcsolni, megkerülni tilos.
(14) A számítógéptől való hosszabb (több mint 5 perc) távollét esetén a felhasználó köteles a munkaállomást, vagy mobil számítástechnikai eszközt zárolni, vagy kilépni a rendszerből.
(15) A munkaállomást illetéktelen személy (pl. ügyfél) jelenléte mellett a felhasználó nem hagyhatja felügyelet nélkül.
(16) A felhasználó felelős a személyes használatra kiadott eszközök rendeltetésszerű használatáért és őrzéséért, a rábízott informatikai berendezések állapotának, állagának megőrzéséért.
(17) A nem mobil informatikai eszközök mozgatása és/vagy leltárkörzet szerinti másik helyiségbe való áthelyezése a felhasználó által nem végezhető.
(18) Az informatikai hálózat fizikai megbontása, a számítástechnikai eszközök lecsatlakoztatása (kivételt képeznek a hordozható eszközök), illetve bármilyen, különösen a kormányhivatal által előírt védelmi megoldásokkal nem rendelkező számítástechnikai eszköz hálózatra történő fizikai csatlakoztatása és/vagy beszerelése tilos.
(19) Az informatikai eszközöket a munka befejeztével, illetve a munkaidő végeztével áramtalanítani kell, amennyiben azok folyamatos üzemben tartása nem indokolt.
124. § (1) A kormányhivatal az alábbiak szerint szabályozza a közösségi médiahasználatot a munkahelyi környezetben:
(2) A kormányhivatal által biztosított infokommunikációs eszközökön a közösségi média oldalak magáncélú használata nem engedélyezett.
(3) A munkaidőn kívül privát eszközökön megvalósított magáncélú használat esetén elvárt az adatvédelem és titoktartás követelményeinek betartása, tilos a kormányhivatal által kezelt adatok bizalmasságának megsértése.
(4) A kormányhivatal közösségi média oldalakon hivatali célból regisztrált fiókjait kizárólag az arra felhatalmazott személyek kezelhetik, a kormányhivatal hatáskörébe és illetékességébe tartozó közérdekű információk közzététele érdekében.
(5) A hivatali közösségi fiók kezelésére vonatkozó felhatalmazásnak tartalmaznia kell a kijelölt személyek ide vonatkozó pontos feladatleírását, hogy nem megfelelő magatartás esetén egyértelmű legyen, kit terhel a felelősség.

(6) A közzétételi feladatok ellátása során kiemelt figyelmet kell fordítani arra, hogy a kormányhivatal által megosztott tartalmak minden esetben megfeleljenek a közösségi média oldalak használati feltételeinek.
125. § A kormányhivatal által a felhasználó részére munkavégzés céljából biztosított informatikai eszközök, valamint az állam intézményei számára a közfeladatok ellátásához szükséges hálózati infrastruktúrát megvalósító Nemzeti Távközlési Gerinchálózat (NTG) magáncélú – így különösen a hálózati adatforgalom jelentős emelkedését okozó streaming és médiamegosztó szolgáltatások használata szigorúan tilos.
126. § (1) A felhasználókat tájékoztatni kell arról, hogy az interneten és a kormányhivatal belső hálózatán végzett tevékenységük megfigyelés alatt állhat.
(2) A kormányhivatal rendelkezésében lévő EIR-ekhez, az igénybe vett központi rendszerekhez, valamint a központi szolgáltató által biztosított szolgáltatásokhoz tartozó hivatali célú felhasználónév és jelszó használata külső weboldalakon vagy alkalmazásokban való fiók létrehozásakor tilos.
(3) Tilos a kormányhivatalban az alapkonfigurációba nem tartozó – különösen az ismeretlen, nem hitelesített forrásból származó – nem jogtiszta szoftverelemek letöltése, tárolása, telepítése, beleértve a böngészőket is. Tilos továbbá böngészőbővítmények letöltése és telepítése, a böngészők biztonsági beállításának megváltoztatása, a mobilkommunikációs eszközök tekintetében is.
127. § Tilos bármilyen fájlmegosztó alkalmazást letölteni vagy használni a munkavégzéshez kiadott eszközökön. A P2P (például BitTorrent, eMule, DC++) alkalmazások alapvető működési elve, hogy a felhasználók közvetlenül egymással osztanak meg fájlokat, nem pedig egy központi szerveren keresztül.
128. § (1) A kormányhivatal szervezeti egységeinek a középirányító által felügyelt külső szervezetek üzemeltetésében lévő GroupWise levelező rendszert kell használni mind belső, mind külső levelezés tekintetében. Ettől eltérő egyedi levelezőrendszerek használata nem megengedett.
(2) A postafiók használata kizárólag kormányhivatali tulajdonú, vagy annak védelmével egyenértékű biztonsági megoldásokkal védett saját tulajdonú számítógépen engedélyezett, tekintettel arra, hogy az elektronikus postafiók megnyitását követően a hivatali levél tartalma és annak csatolt dokumentuma(i), eltárolódhatnak a számítógép adattárolóján.
(3) A GroupWise levelező rendszer hivatali mobiltelefonon keresztül történő elérése indokolt esetben, a SZEV/AG igénylését követően az IFEFV engedélye alapján történhet.
(4) Tilos a postafiókot használatba venni publikus helyen elhelyezett számítógépeken és publikus hálózathoz kapcsolódó mobil eszközökön (pl. kávézóban, hotelben), vagy más idegen eszközökön (pl. ismerős számítógépe, tabletje).
(5) A hivatali levelezőrendszer a munkavégzéssel kapcsolatos ügyintézést szolgálja. A levelező rendszer tárterülete korlátozott, ennek tudatában, ahol lehet, csatolmányok helyett hivatkozásokat kell használni.
(6) Az elektronikus levelek tartalma teljes bizonyossággal csak abban az esetben tekinthető hitelesnek, ha azt a feladó a hitelesítés módjával kapcsolatos jogszabályokban meghatározottak szerinti elektronikus aláírással hitelesítette.
(7) A kormányhivatali e-mail címekhez tartozó postafiókokat magáncélra – online regisztrációhoz, hírlevél feliratkozáshoz, fórum feliratkozáshoz – használni szigorúan tilos.
(8) A hivatali postafiókba érkező elektronikus levelek kormányhivatalon kívüli e-mail címre történő automatikus átirányításának beállítása tilos.
(9) Hivatali kommunikációra tilos magánjellegű postafiókot (pl. Gmail, Freemail) használni.
(10) A használat során figyelemmel kell lenni arra, hogy a személyes e-mail cím tulajdonosának távolléte esetén az elektronikus postafiók figyelése nem biztosított.
(11) A személyes hivatali e-mail postafiók felhasználója a levelező programban - távolléte esetén - automatikus továbbítást vagy automatikus válaszadási üzenetet állíthat be. Az üzenetben tájékoztatható az e-mail feladója, hogy a címzett mettől-meddig van távol és távollétében ki helyettesíti, valamint a helyettesítő milyen elérhetőségekkel rendelkezik, illetve, hogy a feladó levele továbbításra került-e.
(12) A levelezés során nevesített postafiókokat a hozzárendelt felhasználó használhatja. Másik felhasználó postafiókjának használata (helyettesítés) kizárólag a SZEV/AG felhatalmazásával, jogosultság igénylését követően történhet.

(13) Az elektronikus üzenetet aláírással kell ellátni, a kormányhivatal arculatra vonatkozó szabályozásának megfelelően.
129. § (1) Nem megengedettek a levelezésben az alábbiakban bemutatásra kerülő viselkedési formák és tevékenységek. Levelezési etikett:
(2) E-mail-eket nem szabad tömeges mennyiségben (levelező lista) küldeni vagy továbbítani, kivéve, ha hivatali célból szükség van arra és pontosan ismert a címzettek köre.
(3) Zavaró, indokolatlanul nagy méretű, félreinformáló és lánc levelek küldése és továbbítása tilos.
(4) Az e-mail nyelvezetének mindig tiszteletteljesnek kell lennie, közízlést, személyiségi jogokat nem sérthet.
(5) Másokra nézve sértő, másokat vallási, etnikai, politikai vagy egyéb alapon zaklató tevékenység nem folytatható, profitszerzést célzó direkt üzleti célú tevékenység, reklámok terjesztése tilos.
(6) E-mail üzenetben a „Címzett”-et meg kell szólítani, továbbá a levél befejezéseként aláírással kell ellátni.
(7) Az elektronikus levélnek kötelező tárgyat adni, mert ellenkező esetben a levelező rendszerek kártékonynak vélhetik és törölhetik azt. Tárgy nélkül elküldött elektronikus levelet – annak észlelése esetén – újra kell küldeni a tárgy megadásával.
130. § (1) Fokozott elővigyázatossággal kell kezelni az ismeretlen feladótól érkező idegen nyelvű, esetleg magyartalan, illetve helyesírási hibákat tartalmazó, témaidegen e-maileket. A levél alapos értelmezése, lefordítása nélkül ezek mellékleteit megnyitni, illetve a levél szövegében található hivatkozásokra rákattintani TILOS! Indokolt esetben, amikor nem dönthető el egyértelműen a levél hitelessége, akkor segítséget kell kérni az Informatikai feladatok ellátásáért és üzemeltetésért felelős szervezeti egység foglalkoztatottjától. A gyanúsnak, kártékonynak ítélt elektronikus levelet további vizsgálat és indokolt esetben központi letiltás céljából mellékletként továbbítani kell a központi üzemeltetés NOÉ SPAM fiókjába.
(2) Az informatikai rendszerek biztonsága érdekében az elektronikus levelezés használata naplózásra, az elektronikus levelek gépi tartalomszűrésre, szükség esetén korlátozásra, biztonsági kockázat vagy a vonatkozó szabályok megsértésének gyanúja esetén a felhasználó előzetes értesítése vagy hozzájárulása nélkül ellenőrzésre kerülhetnek. Az ellenőrzést az IBF kezdeményezése vagy a felhasználó SZEV/AG, mint adatkezelőnek indoklással alátámasztott kérése alapján az IFEFV, a FŐISPÁN, FŐIG/IG rendelheti el. Az ellenőrzést az IBF és az informatikai feladatok ellátásáért és üzemeltetésért felelős szervezeti egység kijelölt foglalkoztatottjai közösen végzik. A vizsgálat végrehajtásáról és annak megállapításairól jegyzőkönyv készül.
131. § (1) Személyes postafiókok jellemzői:
(2) A személyes, hivatali célú postafiókhoz tartozó felhasználói nevet és kezdeti jelszót az informatikai feladatok ellátásáért felelős szervezeti egység hozza létre, amelyet a postafiók használatba vételét követően azonnal meg kell változtatni. A jelszó módosítását követően az új jelszót csak a postafiók tulajdonosa ismerheti.
(3) A kormányhivatali személyes e-mail címeket a családnév. utónév@[MEGYE].gov.hu konvenció szerint kell képezni. Ettől eltérni csak kivételes esetben (pl. azonos nevek megkülönböztetése céljából) lehet.
132. § (1) Hivatali postafiókok adminisztrálása és használata:
(2) Csoportos és technikai e-mail címeket az illetékes szakterülettel történő egyeztetés után az informatikai feladatok ellátásáért felelős szervezeti egység hoz létre. A szervezeti e-mail postafiókokhoz (pl. informatika@[MEGYE].gov.hu) a hozzáférés a személyes hivatali e-mail postafiókon keresztül, helyettesítés funkció használatával lehetséges. A jogosultság igénylés alapján az informatikai feladatok ellátásáért felelős szervezeti egység beállítja a hivatali postafiókban a felhasználó részére a meghatalmazotti jogosultságot. A jogosultság beállítását követően az újonnan jogosultsággal rendelkező személy személyes postafiókjában fel kell csatolni a helyettesített fiókot.
(3) A hivatali szervezeti e-mail címekhez tartozó elektronikus postafiókot a SZEV/AG által kijelölt személy köteles rendszeresen figyelni. A szervezeti e-mail fiókok hitelesítési adatait az informatikai feladatok ellátásáért felelős szervezeti egység kezeli, azt a felhasználók részére nem adja ki. A felhasználói hozzáférés a személyes hivatali célú postafiókon keresztül helyettesítés funkció használatával lehetséges.

(4) Ha az e-mail postafiókba érkezett levél más szervezeti egység hatáskörébe tartozik, úgy azt haladéktalanul továbbítani kell az illetékes szervezeti egység hivatali e-mail címére, illetve - tisztázatlan hatáskör esetén - a hivatali központi e-mail címre. A folyamatos működés érdekében az illetékes vezetőnek a helyettesítésről is gondoskodnia kell.
(5) A hivatalos ügyirathoz kapcsolódó anyagokat a személyes hivatali e-mail cím helyett a hivatali központi, illetve a szervezeti egységek hivatali e-mail címére kell kérni. A kimenő elektronikus leveleket – lehetőség szerint – személyes hivatali e-mail címek helyett a címzett szervezet hivatali e-mail címére kell elküldeni. Iktatott hivatali, fontos, sürgős elektronikus levelek küldése esetén olvasási visszaigazolást kell kérni.
133. § A kormányhivatal központi és a szervezeti egységek hivatali e-mail címeihez tartozó postafiókjaiból bármilyen mappa vagy levél törlése tilos

XVI. Fejezet
Személyi biztonság

74. A személyi biztonság alapelvei

134. § (1) A személyi biztonság alapelveinek meghatározásánál elsődleges cél, hogy a felhasználók szervezeten belül eltöltött életciklusa vonatkozásában az egyes események (belépés, változáskezelés, kilépés) szabályozottak legyenek, illetve megfeleljenek a szervezet és a használt EIR-ek biztonsági követelményeinek.
(2) A további részletszabályokat a Személyi biztonságra vonatkozó eljárásrend tartalmazza.

75. Ellátandó feladatkörök biztonsági szempontú besorolása

135. § (1) Minden feladatkört elektronikus információbiztonsági kategóriába kell sorolni. Az egyes feladatkörök kockázati szintjét az alábbi szempontok szerint kell meghatározni:
(2) Fokozott biztonsági kategóriába tartozik minden olyan feladatkör, melynek betöltésével járó feladatok és felelősségek:

a) nemzetbiztonsági ellenőrzést igényelnek, vagy
b) bármely elektronikus információs rendszerben kizárólag privilegizált jogosultsággal végezhetők, vagy
c) egyéb szempontok alapján kiemelt kockázatot hordoz magában.

(3) Alap biztonsági kategóriába tartozik minden olyan feladatkör, mely az előbbi (fokozott) kategóriába nem került besorolásra.
(4) Az álláshelyeken ellátandó feladatkörök kockázati besorolásának elvégzése és arról naprakész nyilvántartás vezetése a Humánpolitikai feladatok ellátásáért felelős szervezeti egység feladata és felelőssége, mely feladat ellátásában segítséget nyújt az IBF és az elektronikus információbiztonsági feladatok ellátásában közreműködő személyek.
(5) A Humánpolitikai feladatok ellátásáért felelős szervezeti egység feladata és felelőssége továbbá a vonatkozó jogszabályok alapján a nemzetbiztonsági ellenőrzés alá tartozó feladatkörök felmérése, és azokról naprakész nyilvántartás vezetése.

76. Személyek háttérellenőrzése

136. § Hozzáférési jogosultság csak olyan egyén részére engedélyezhető, aki az általa betöltött álláshelyen ellátandó feladatkör biztonsági kategóriája szerinti követelményeknek megfelel. Az érintett személy ellenőrzését a Humánpolitikai feladatok ellátásáért felelős szervezeti egység végzi meghatározott személyzeti ellenőrzési kritériumok alapján, mielőtt a hozzáférés engedélyezésre kerül. Ismételt ellenőrzésre kerül sor, ha változás történik a felhasználó jogosultsági szintjében vagy feladatkörében. Ha az érintett feladatköre miatt nemzetbiztonsági ellenőrzésre van szükség, akkor a kormányhivatal kezdeményezi azt.

77. Személyek felelősségvállalása jogviszony kezdetekor

137. § (1) A kormányhivatallal jogviszonyt létesítő foglalkoztatottak a Felhasználói Felelősségvállalási Nyilatkozat (10. számú melléklet) aláírásával elismerik, hogy a jelen szabályzatban meghatározott biztonsági elvárásoknak, előírásoknak eleget tesznek. A nyilatkozat megtételével dokumentált módon elfogadják a rájuk vonatkozó hozzáférési szabályokat.
(2) A kormányhivatallal jogviszonyt létesítő foglalkoztatottak a Titoktartási Nyilatkozat (11. számú melléklet) aláírásával elismerik, hogy a jelen szabályzatban meghatározott titoktartási, adatvédelmi elvárásoknak, előírásoknak eleget tesznek. A nyilatkozat megtételével dokumentált módon elfogadják a rájuk vonatkozó titoktartási szabályokat.
(3)[2] A nyilatkozatok mindenkor aktuális verziójának a felhasználóval történő aláíratása és adminisztrálása a foglalkoztatott HSZE feladata és felelőssége.

78. Személyek jogviszonyának változása

138. § (1) A korábban engedélyezett hozzáférési jogosultságokat felül kell vizsgálni minden olyan esetben, amikor a felhasználó a kormányhivatalon belül más munkakörbe, áthelyezésre vagy átirányításra kerül.
(2) A felülvizsgálatot a foglalkoztatott szervezeti egység vezetője végzi, valamint szükség szerint kezdeményezi a hozzáférési jogosultságok módosítását.

77. Személyek jogviszonyának megszűnése

139. § (1) Valamennyi természetes személynek az elektronikus információs rendszerhez és információ feldolgozó eszközökhöz való hozzáférését le kell tiltani, valamint a személyhez kapcsolódó összes hitelesítő eszközt és jogosultságot vissza kell vonni, amikor jogviszonya megszűnik.
(2) Ha az érintett részéről fennállhat az ügymenetet vagy elektronikus információbiztonságot sértő magatartás veszélye, a jogosultságokat még az érintett tájékoztatását megelőzően vissza kell vonni!
(3) A jogosultságok visszavonását - az IDM által automatikusan kezelt jogosultságok kivételével - az érintett felhasználó Szervezeti egységének vezetője kezdeményezi, a végrehajtása az adott rendszer informatikai üzemeltetésért felelős szervezeti egység foglalkoztatottjainak feladata.
140. § (1) A jogviszony megszűnésekor a kormányhivatal visszaveszi a felhasználótól a számára használatra átadott valamennyi infokommunikációs eszközt, adathordozót, egyéb releváns, a szervezet elektronikus információs rendszeréhez kapcsolódó biztonsági eszközöket.
(2) Amennyiben nem kerül hiánytalanul visszaszolgáltatásra minden kiadott eszköz, abban az esetben ezt a Szervezeti egysége vezetőjének jeleznie kell az adott eszközök üzemeltetéséért felelős vezető felé, aki a szükséges intézkedést kezdeményezi.

[2] Módosította az 1/2026. (I. 19.) főispáni utasítás 2. §-a. Hatályos 2026. 01. 20-tól

141. § A humánpolitikai feladatok ellátásáért felelős szervezeti egység feladata tájékoztatni a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló információbiztonsági követelményekről, titoktartási kötelezettségekről, valamint arról, hogy a szervezet fenntartja magának a hozzáférés jogát a kilépő személy által korábban használt és kezelt elektronikus információs rendszerekhez és szervezeti információkhoz.

78. Külső személyekhez kapcsolódó biztonsági követelmények

142. § (1) Az elektronikus információs rendszerekkel, illetve a szervezet által kezelt adatokkal kapcsolatba kerülő, vagy az elektronikus információbiztonságra közvetlen módon hatást gyakorló külső szolgáltatókkal olyan írásbeli megállapodást kell kötni, amely tartalmaz minden olyan elektronikus információbiztonsági és személyi biztonsági követelményt, amely jelen szabályzatban vagy egyéb dokumentumban szabályozásra került.
(2) Az együttműködés során rendelkezésre bocsátott üzleti titkok és bizalmas információk megőrzésének szabályait és módját a Titoktartási nyilatkozat (12. számú melléklet) rögzíti.
(3) A külső szolgáltatók számára a kormányhivatalon belüli kapcsolattartó igényli meg, valamint felügyeli a szükséges jogosultságokat, szükség esetén a visszavonásukat kezdeményezi. A külső szolgáltatók hozzáférését a hozzáférés indokának megszűntekor, illetve a szerződés lejártakor azonnal meg kell szüntetni.
(4) Az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködők esetében gondoskodni kell arról, hogy a Kibertv.-ben foglaltak szerződéses kötelemként teljesüljenek.
(5) Külső szervezettel kötött megállapodásokban az alábbiakat kell megkövetelni:

a) a szerződést érintő, elektronikus információbiztonsági szerep- és felelősségi körök – beleértve a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is – mindkét fél általi meghatározását és dokumentálását;
b) a szerződő fél -szerződés teljesítésében közreműködő- foglalkoztatottjai feleljenek meg a kormányhivatal által meghatározott személybiztonsági követelményeknek (szükség esetén a Nemzetbiztonsági ellenőrzést is beleértve);
c) ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik a kormányhivatal elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor a szerződő fél soron kívül küldjön értesítést az érintett szervezeti egység vezetőjének.

(6) Az IBF véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szerződéseit.
(7) A kormányhivatal rendszeresen ellenőrzi a szerződő fél személybiztonsági követelményeknek való megfelelését.

79. Fegyelmi intézkedések

143. § A munkáltatói jogkör gyakorlója fegyelmi eljárást kezdeményez azokkal a kormánytisztviselőkkel szemben, akik nem tartják be az információbiztonsági szabályokat és eljárásokat. A fegyelmi felelősség részletszabályait a kormányhivatal Közszolgálati Szabályzata tartalmazza.

80. Álláshelyen ellátandó feladatokról szóló tájékoztató

144. § A biztonsági szerepköröket és felelősségeket bele kell foglalni a kormányhivatal álláshelyein ellátandó feladatokról szóló tájékoztatókba. Az álláshelyen ellátandó feladatokról szóló tájékoztatásokat felül kell vizsgálni és frissíteni kell a biztonsági szerep- és felelősségi körök változása esetén, továbbá amikor jelentős változások történnek az elektronikus információs rendszerben vagy a biztonsági környezetben. Az álláshelyen ellátandó feladatmeghatározások kialakításának részletszabályait a kormányhivatal Közszolgálati Szabályzata tartalmazza.

XVII. Fejezet
Kockázatkezelés

81. A kockázatkezelés alapelvei

145. § (1) A kockázatkezelés egy gyűjtőfogalom, azoknak az eszközöknek és módszereknek az összessége, amelyek elősegítik a kockázatok azonosítását, számszerűsítését és mérséklését. Fontos, hogy a kockázatkezelés folyamata nem szünteti meg a kockázati tényezőket, csak abban segít, hogy a hatásuk számszerűsíthető és alakítható legyen. A kockázatkezelés nem egyszeri tevékenységet jelent, hanem egy ciklikusan ismétlődő programfolyamat.
(2) A kormányhivatalnak a környezetükből, a szabályozásból, a működésükből, a személyi állományukból származó számos kockázattal kell szembenézniük. A jelentkező kockázatokra reagálni kell, szükséges azok kezelése, menedzselése.
(3) A további részletszabályokat a Kockázatelemzési és kockázatkezelési eljárásrend tartalmazza.

82. Szervezet rendelkezésében lévő elektronikus információs rendszerek nyilvántartása

146. § (1) Az elektronikus információs rendszerek nyilvántartása az információbiztonsági kockázatelemzés hatókörébe tartozó vagyonnyilvántartás (továbbiakban vagyonleltár) egyik területe. Vagyonelemként legalább a következő adatok kerülnek meghatározásra:

a) vagyonelem típus (adat, szoftver, hardver, szolgáltatás, humán, helyiség stb.),
b) vagyonelem megnevezés,
c) SZEV/AG megnevezése.

(2) Az elektronikus információs rendszerek és rendszerelemek vagyonelemekből épülnek fel, ezért meg kell határozni azon vagyonelemeket, amelyeket egy-egy elektronikus információs rendszer használ, hogy a továbbiakban meghatározható legyen az elektronikus információ rendszer bizalmassága, sértetlensége és rendelkezésre állása a vagyonelemekből származtatva.
(3) A vagyonleltár elkészítését követően számba kell venni az elektronikus információs rendszereket és fel kell sorolni az őket alkotó vagyonelemeket.

83. Adatvagyon nyilvántartása

147. § (1) Az információbiztonsági kockázatelemzés hatókörébe tartozó vagyonleltár az IBF állítja össze és aktualizálja a Szervezeti egység vezető / Adatgazdák, IFEFV, (vagy az általuk kijelölt foglalkoztatottak) bevonásával, valamint az adott területért felelős vezetők támogatása mellett.
(2) A kormányhivatal adatvagyonának nyilvántartására elsődlegesen az informatikai szakterületen kezelt adatvagyon nyilvántartás, illetve a pénzügyi területen kezelt eszköznyilvántartás szolgál.
148. § (1) A vagyonleltárnak a következő területek mindegyikére ki kell terjednie:
(2) Infrastruktúra, az elektronikus információs rendszereket magukba foglaló épületek, helyiségek:

a) szerverterem,
b) Back Office helyiség,
c) Front Office helyiség.

(3) Hardverek, az informatikai rendszert alkotó fizikai elemek:
a) asztali munkaállomások,
b) hordozható számítógépek,
c) kiszolgálók (szerverek),
d) hálózati eszközök,
e) nyomatelőállító eszközök,
f) adattárolók (storage).

(4) Adatbázisok:
a) MS SQL
b) Oracle
c) Maria DB

(5) Alkalmazások:
a) operációs rendszer,
b) irodai szoftverek,
c) üzleti alkalmazás,
d) biztonsági alkalmazás (vírusirtó, tűzfal).

(6) Szolgáltatások:
a) levelezés,
b) intranet,
c) file szolgáltatás,
d) nyomtatási szolgáltatás,
e) címtárszolgáltatás.

(7) Emberi erőforrások:
a) vezetők,
b) felhasználók,
c) az elektronikus információs rendszereket üzemeltető, fejlesztő, karbantartó dolgozók.

(8) Adatok, dokumentumok, feljegyzések:
a) az elektronikus információs rendszerek üzemeltetéséhez, karbantartásához, fejlesztéséhez szükséges dokumentumok, valamint
b) a rendszer által létrehozott dokumentumok, feljegyzések.

(9) Rendszerben kezelt adatkörök

(10) Nyilvántartások

(11) Tervek

(12) Dokumentációk

(13) Kézikönyvek

(14) Kiszervezett szolgáltatások, amelyeket a kormányhivatal nem a saját erőforrásaival valósít meg, hanem szerződés alapján kiadta a feladatokat harmadik félnek.

84. Biztonsági osztályba sorolás

149. § (1) A biztonsági osztályok leírják a szervezeti működésre, a szervezeti eszközökre és az egyénekre gyakorolt lehetséges káros hatásokat vagy negatív következményeket, ha a szervezeti információ és rendszerek a bizalmasság, a sértetlenség vagy a rendelkezésre állás elvesztése miatt veszélybe kerülnek. A kormányhivatalok biztonsági osztályozásba sorolási folyamatot az egész szervezetre kiterjedően végzik, közvetlenül bevonva az informatikai felelősöket, az információbiztonsági felelősöket, a rendszerek tulajdonosait, az üzleti- és ügymeneti folyamatok felelőseit, valamint az adatgazdákat.

A szervezetek figyelembe veszik a lehetséges hatásokat más szervezetekre nézve, valamint ha releváns, akkor a nemzetbiztonsági hatásokkal is számolni kell a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal összhangban. A biztonsági osztályba sorolás elősegíti a EIR(-ek) rendszerelem leltárának fejlesztését, azzal, hogy rendszerelemeket rendel az információk feldolgozásához, tárolásához és továbbításához, valamint megjeleníti az ezekhez kapcsolódó biztonsági követelményt rendszerelem leltárra vonatkozó követelménnyel együtt.

(2) 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.

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

a) a biztonsági osztályokhoz tartozó védelmi követelményeket jogszabály rögzíti, illetve a biztonsági osztályba sorolás és a védelmi intézkedések bevezetésének támogatására kockázatmenedzsment keretrendszert működtet,
b) a nemzeti adatvagyont kezelő rendszerek esetében a jogszabályi előírásoknak megfelelően,
c) a biztonsági osztályokat a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából, hogy milyen nagyságú káresemény következhet be csekély, közepes vagy nagy, „alap”, „jelentős” és „magas” fokozatú skála szerint kell megállapítani.

(4) A szervezetnek az EIR fejlesztési életciklusa során rendszeresen felül kell vizsgálnia a biztonsági osztályba sorolást, hogy biztosítsa a biztonsági osztályok pontosságát és relevanciáját., de legalább 2 évente felül kell vizsgálni.

(5) A kormányhivatal vezetőjének vagy meghatalmazott képviselőjének jóvá kell hagynia a biztonsági osztályba sorolási döntést. A biztonsági osztályba sorolást szervezeti szinten kell végrehajtani, az IBF, az adatvédelmi tisztviselő(k), az EIR tulajdonosok, az alapfeladatok és üzleti folyamatok tulajdonosai, valamint az adatgazdák közvetlen bevonásával.

150. § (1) Az EIR előzetes biztonsági osztályba sorolása során az EIR által kezelt adatköröket kell a bizalmasság, sértetlenség és rendelkezésre állás alapján osztályba sorolni.

(2) A kapott értékeket a maximum elv alapján összesíteni kell, úgy, hogy az alkalmazások bizalmasság, sértetlenség és rendelkezésre állás szerinti kárértékeit nem átlagoljuk, hanem azok maximumát vesszük. Az alkalmazás biztonsági osztályát összevonva úgy fejezzük ki, hogy a bizalmasság, sértetlenség, rendelkezésre állás hármasból a legnagyobb értéket vesszük.

(3) Amellett, hogy az érintett szervezetre érvényes minden kötelezettséget figyelembe kell venni, az EIR kialakítása során implementálni kell és fent kell tartani a fenti folyamat eredményeként kapott biztonsági osztályhoz tartozó, a rendelet 2. melléklete szerinti védelmi intézkedés katalógusban meghatározott minimális követelményeket.

151. § (1) Az EIR előzetes osztályba sorolás eredményét a Főispán hagyja jóvá. A szervezet vezetője felel azért, hogy az EIR biztonsági osztályának meghatározása megfelel a jogszabályoknak és kockázatoknak, valamint a besorolásban felhasznált adatok teljeskörűek.

(2) A projekteken belül minden egyes újonnan implementálandó EIR esetében el kell végezni az előzetes biztonsági osztályba sorolást, illetve a projekt hatókörének, illetve a kezelt adatok körének minden változása esetén azt dokumentált módon felül kell vizsgálni.

(3) Új EIR-ek implementálásának esetén az előzetes biztonsági osztályba sorolást a szervezeteknek célszerű a beszerzéssel, illetve a projekt menedzsmenttel kapcsolatos szabályozási környezetük részévé tenni, hogy ezzel is támogassák az információbiztonság növelésére tett törekvések hatékony irányításához és felügyeletéhez szükséges intézkedések hatékony megvalósítását.

(4) A rendszerbiztonsági tervben szerepeltetni kell az elvégzett kockázatelemzés releváns adatait és következtetéseit, valamint az előzetes biztonsági osztályba sorolás eredményét.

85. Kockázat azonosítás

152. § (1) A kockázatok azonosítása, értékelése és a kezelésük módszereinek megtervezése. A tervezéskor be kell azonosítani a kulcsfontosságú kockázati tényezőket. Szükséges elemezni azok hatásmechanizmusát és a hozzájuk kapcsolódó bekövetkezési és kihatási valószínűségeket. Hatékony védekezés abban az esetben valósítható meg, ha a kormányhivatal felső vezetése ismeri a fennálló veszélyeket és olyan információk birtokában van, amelyek ismeretében el tudja dönteni, hogy melyekkel és miképpen tud és akar foglalkozni.
(2) Az IBF feladata karbantartani a fenyegetettségek listáját, amelyek a kormányhivatalra relevánsak, valamint meg kell határoznia, hogy adott vagyonelem csoportokra vonatkozóan mekkora az alapértelmezett bekövetkezési valószínűsége egy-egy adott fenyegetettségnek.
(3) A következő lépésként fel kell tárni az adott vagyonelem esetében értelmezhető fenyegetettségeket.
(4) A vagyonelemre irányuló fenyegetettségek akkor veszélyesek, ha a megtámadott vagyonelemnek van a fenyegetettségek által kihasználható sérülékenysége, gyenge pontja. A sérülékenység rendszerint a vagyonelemnek vagy környezetének valamilyen tulajdonsága, jellemzője, biztonsági hiányossága. A sérülékenység jellege lehet technikai, fizikai, eljárásbeli, szabályozatlanság vagy képesség hiány.

86. Kockázat elemzés

153. § (1) A kockázatelemzés, ahhoz nyújt segítséget, hogy a leghatékonyabb kockázatkezelési megoldást válasszuk. Az általános szabály az, hogy a kockázatelemzési folyamat végrehajtása nagymértékben függ a kockázat várható következményeitől.
(2) Kockázatelemzés során az egyes kockázatok következményeit és a bekövetkezés valószínűségét és ezek együttes hatását kell értékelni.
(3) Ha egy fenyegetettség bekövetkezik, akkor kárt okozhat a vagyonelemben. Az informatikai kockázatok értékeléséhez meg kell határozni a kár nagyságát az ügyviteli hatások felmérése alapján, és a fenyegetettség bekövetkezésének valószínűségét, amelyek együttesen alkotják a kockázatot. Minél gyakrabban következik be egy fenyegetettség és minél nagyobb az általa okozott kár, annál nagyobb a kockázat.

87. Sérülékenység menedzsment

154. § (1) A sérülékenység menedzsment egy állandóan változó folyamat, amely nemcsak a sérülékenységek eseti megállapítására korlátozódik, hanem a rendszereink osztályozását, a sérülékenység elhárítás folyamatát, a kockázati szintek elemzését, illetve az informatikai rendszerek változásait is képes kezelni.
(2) Az EIR-ek biztonsági osztálya meghatározza a sérülékenységi vizsgálatok gyakoriságát és mélységét. A szervezet meghatározza az összes EIR-e, illetve azok rendszerelemeinek szükséges biztonsági vizsgálatát, biztosítva, hogy a potenciális biztonsági réseket tartalmazó eszközök, például a hálózatra kötött nyomtatók, szkennerek és másolók se maradjanak figyelmen kívül. Az egyedileg fejlesztett szoftverek biztonsági vizsgálatai eltérő megközelítéseket igényelhetnek, például statikus elemzést, dinamikus elemzést, bináris elemzést vagy a három megközelítés valamilyen egyvelegét. A szervezetek ezeket az elemzési megközelítéseket különböző eszközökben (pl. webalkalmazás szkennerek, statikus elemző eszközök, bináris elemzők) és forráskód-vizsgálatok során is használhatják. A biztonsági vizsgálat például tartalmazhatja patch-ek vizsgálatát, olyan funkciók, portok, protokollok és szolgáltatások vizsgálatát, amelyeknek nem szabadna elérhetőnek lenniük felhasználói eszközök által, helytelenül konfigurált vagy helytelenül működtetett konfigurációk vizsgálatát.
(3) A sérülékenységek szkennelési folyamatának automatizálása, amennyiben technológiai szempontból lehetséges, igénybe vehető az NBSZ NKI Automatizált Sebezhetőségdetektáló Rendszere (ASR), illetve az Automatizált Károskód Elemző Rendszer is.

88. Kockázat értékelés, kezelés

155. § (1) A kockázatértékelés célja a kockázatok rangsorolása, mégpedig a bekövetkezésük valószínűségének, kihatásuk és kezelhetőségük függvényében. Annak megállapítása, hogy melyek a legkockázatosabb területek, ahol intézkedéseket kell foganatosítani.
(2) A kockázatok kiértékelésekor a fenyegetettség észlelhető/várható valószínűségét és a bekövetkezése esetén okozott hatást, kárt kell figyelembe vennünk. A kockázati érték e két mutatónak a szorzata. Az észlelhető/várható valószínűségének meghatározása során az alkalmazott védelmi intézkedéseket figyelembe kell vennünk.
(3) A kockázati tényezők származtatásakor nem a lehetséges legnagyobb kárértéket, hanem a releváns, bekövetkezési valószínűséggel korrigált fenyegetettségek által okozható kárt, káros hatást kell figyelembe venni. Ezt a kockázati szorzótáblával tudjuk elérni. A szorzótábla sorát a fenyegetettség előfordulási valószínűsége, oszlopát a bizalmasság, sértetlenség és rendelkezésre állás szempontokhoz tartozó kárérték közül a legmagasabb kategória határozza meg.
(4) A kockázati szorzótáblát a 13. számú melléklet tartalmazza.
156. § Az EIR vagy az általa kezelt adatok bizalmasságának elvesztése esetén a kár mértékének táblázatát a 14. számú melléklet tartalmazza.
157. § (1) Az sértetlenség az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanság) is, illetve az EIR elemeinek azon tulajdonsága, amely arra vonatkozik, hogy az EIR eleme rendeltetésének megfelelően használható. A sértetlenség olyan EIR-eknél lehet vezető szempont, ahol fontos, hogy a kezelt adatokat illetéktelenül senki ne változtathassa meg, pl. nemzeti adatvagyont kezelő EIR-ek, közhiteles nyilvántartások, mérő-, érzékelő rendszerek.
(2) Az EIR vagy az általa kezelt adatok sértetlenségének elvesztése esetén a kár mértékét a 15. számú melléklet tartalmazza.
158. § (1) A rendelkezésre állás az adat, illetve az EIR elemeinek olyan állapota, amelyben az arra jogosultak által a szükséges időben és időtartamra használható. Azoknál a EIR-eknél, ahol alapvető igény a működés fenntartása, ott a rendelkezésre állás kiemelt fontosságú.
(2) Az EIR vagy az abban tárolt adatok rendelkezésre állásának elvesztése esetén (nem elérhető a rendszer vagy az adat) a kár mértékét a 16. számú melléklet tartalmazza.
(3) A következő lépésként - az előbbiekben felállított kárérték táblázatok felhasználásával - meg kell ítélnie az adatgazdának, hogy mekkora kár éri a szervezetet, hogy ha az EIR sértetlensége, rendelkezésre állása vagy az EIR-ben kezelt adat bizalmassága, sértetlensége vagy rendelkezésre állása sérül.
(4) A táblázatunkat kiegészítettük három oszloppal (B- bizalmasság, S-sértetlenség, R- rendelkezésre állás), melyek a bizalmasság, sértetlenség és a rendelkezésre állás becsült kárérték szintjeit tartalmazzák. A minta táblázatot a 17. számú melléklet tartalmazza.

89. Nyilvántartások, kockázatkezelés időszakos felülvizsgálata

159. § (1) A kockázatfelmérést a kormányhivatal – az IBF kezdeményezésére – legalább háromévente felülvizsgálja, aktualizálja. A felmérés felülvizsgálatát időközben el kell végezni, ha sérülékenységi audit eredményei indokolják, továbbá abban az esetben, ha változik:

a) elektronikus információs rendszer biztonsági állapotát befolyásoló körülménye,
b) elektronikus információs rendszer működési környezete,
c) a kockázatok változása (új fenyegetettségek és sebezhetőségek megjelenése).

(2) A SZEV/AG és a kockázatgazdák felelőssége, hogy a változásokról a szükséges információkat időben eljuttassák az IBF részére. Az aktualizálást az IBF koordinálja.

XVIII. Fejezet
Rendszer- és szolgáltatás beszerzés

90. Rendszer- és szolgáltatás beszerzés alapelvei

160. § (1) A beszerzési szabályzat és eljárások a Beszerzések követelménycsoportba tartozó védelmi intézkedésekkel foglalkoznak, amelyek az EIR-ekben, illetve a szervezetben bevezetésre kerülnek.
(2) A beszerzések során a biztonsági elvárások ellenőrzésének felelőse az IBF, konzulensként az IÜFV vesz részt. A beszerzések feltételrendszerének kialakításáért az IFEFV a felelős.
(3) A kormányhivatal az informatikai beszerzések során az információbiztonsági követelményeket már az életciklus tervezési, fejlesztési, beszerzési szakaszában figyelembe veszi és folyamatosan nyomon követi.
(4) A kormányhivatal olyan eljárást alakít ki, mely biztosítja, hogy az IBF a beszerzési követelményeket már a beszerzés kezdetén érvényesíteni tudja.
(5) A kormányhivatal az általa kialakítandó beszerzési eljárásban a biztonsági osztályoknak megfelelően a szállítók számára is meghatározza a törvény által előírt követelményeket.
(6) A rendszer és szolgáltatás beszerzésekre, valamint a fejlesztésekre vonatkozó részletes információbiztonsági követelményeket és szabályokat az Informatikai beszerzési eljárásrend tartalmazza.
(7) A rendszer- és szolgáltatásbeszerzés során az alábbi alapelveket kell figyelembe venni: biztonság már a tervezés során (Security by design), a lehetőleg folyamatos rendelkezésre állás biztosítása, minimális jogosultság elve, törekedni kell az életciklus alapú kezelésre, a biztonsági követelményeknek kockázatarányosnak kell lenni, a meglévő környezettel való kompatibilitásra törekedni kell, valamint nem utolsó sorban a jogszabályi megfelelés és auditálhatóságkritériumait is szem előtt kell tartani.

91. Rendszer erőforrások rendelkezésre állása, biztosítása

161. § (1) Az információbiztonság érdekében történő erőforrás tervezés magában foglalja a rendszerrel és rendszerszolgáltatásokkal kapcsolatos beszerzést, fenntartást és az ellátási lánccal kapcsolatos kockázatokat a rendszer fejlesztési életciklusban. A kormányhivatal az üzletmenet és üzleti folyamatok tervezése során meghatározza az EIR vagy rendszerszolgáltatás magas szintű információbiztonsági követelményeit. Ez magában foglalja a kockázatkezelési stratégiák, a biztonsági szabályok és eljárások, valamint a biztonsági technológiák meghatározását.
(2) Biztosítja az EIR és annak szolgáltatásai védelméhez szükséges erőforrásokat, a beruházás tervezés részeként. Ez magában foglalja a szükséges pénzügyi forrásokat, a személyzetet és a technológiai eszközöket.
(3) Elkülönített tételként kezeli az EIR-ek biztonságát a beruházás tervezési dokumentumaiban. Ez azt jelenti, hogy a biztonsági költségeket külön kell kezelni a többi költségtől, és külön költségvetési tételként kell szerepeltetni.

92. Rendszer fejlesztési életciklusa

162. § (1) A jól definiált rendszerfejlesztési életciklusok alapját képezik a szervezeti információs rendszerek sikeres fejlesztésének, megvalósításának és üzemeltetésének. A szükséges biztonsági követelmények alkalmazása a rendszerfejlesztési életciklus során az információbiztonság, a fenyegetések, sérülékenységek, kedvezőtlen hatások és kritikus üzleti célok/üzleti funkciók kockázatainak alapvető megértését igényli. A követelmény alapján kialakítandó biztonsági tervezés alapelvei akkor alkalmazhatók megfelelően, ha a szakértők, akik az EIR-eket és a rendszerelemeket tervezik, fejlesztik és tesztelik, megértik a biztonsági elvárásokat.

A biztonsági követelmények a szervezeti architektúrába történő hatékony implementálása segít annak biztosításában is, hogy a fontos biztonsági szempontok a rendszer teljes életciklusa során érvényesüljenek, és hogy ezek a megfontolások közvetlenül kapcsolódjanak a szervezeti működési célokhoz és az üzleti folyamatokhoz.
(2) Ez a folyamat megkönnyíti továbbá az információbiztonsági architektúrák integrálását a szervezeti architektúrába, összhangban a szervezet kockázatkezelési stratégiájával. Mivel egy rendszerfejlesztési életciklusban több szervezet is részt vesz (pl. külső beszállítók, fejlesztők, integrátorok, szolgáltatók), a beszerzési és ellátási lánc kockázatkezelési funkciói és intézkedései jelentős szerepet játszanak az EIR hatékony felügyeletében, annak teljes életciklusa alatt.
(3) Az EIR-ek teljes életútján, minden életciklusukban figyelemmel kell kísérni azok információbiztonsági helyzetét. A fejlesztési életciklus egészére meg kell határozni és dokumentálni az információbiztonsági szerepköröket és felelősségeket. Azonosítani az információbiztonsági szerepkörökkel és felelősségi körökkel rendelkező személyeket.

93. Beszerzésekre vonatkozó információbiztonsági követelmények

163. § (1) Az informatikai rendszerek beszerzésére, fejlesztésére vonatkozó biztonsági követelményeket az érintett elektronikus információs rendszer biztonsági osztályával összhangban kell meghatározni a beszerzés tervezési szakaszában, melynek teljesülését az IBF-nek kell ellenőrizni.
(2) Külső elektronikus információs rendszer igénybevétele esetén a szolgáltatási szerződésekben ki kell kötni, hogy a szolgáltatási szerződés alapján igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek a kormányhivatal információbiztonsági követelményeinek.
(3) Figyelemmel kell kísérni az elektronikus információs rendszerek biztonsági elemeinek megbízhatóságát és teljesítményét.
(4) A szervezet a beszerzési folyamat során – beleértve a fejlesztést, az adaptálást, a rendszerkövetést és a karbantartást is – a szerződéseiben egységes nyelvezetet alkalmaz, továbbá követelményként rögzíti az alábbiakat:

a) a funkcionális biztonsági követelményeket,
b) a mechanizmusok erősségére vonatkozó követelményeket,
c) a biztonság garanciális követelményeit,
d) az érintett EIR biztonsági osztályát és az ahhoz tartozó, illetve a szervezet által meghatározott további biztonsági követelmények teljesítéséhez szükséges védelmi intézkedéseket,
e) a biztonsággal kapcsolatos dokumentációs követelményeket,
f) a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket,
g) az EIR fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat,
h) a felelősség megosztását vagy az információbiztonságért és az ellátási lánc kockázatkezeléséért felelős felek azonosítását,
i) a teljesítési kritériumokat.

94. Elektronikus információs rendszerre vonatkozó dokumentáció

164. § (1) Az elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a rendszerkövetést, vagy karbantartást is) szerződésekben követelményként meg kell határozni a következőket:

a) elvárt biztonsági osztályt, funkcionális biztonsági követelményeket,
b) a garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint),
c) a biztonsággal kapcsolatos dokumentációs követelményeket,
d) az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.

(2) A kormányhivatal kidolgozza vagy beszerzi az EIR, rendszerelem vagy rendszerszolgáltatás adminisztrátori és üzemeltetői dokumentációját, amely tartalmazza:

a) az EIR, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurációját, telepítését és üzemeltetését,
b) a biztonsági funkciók hatékony használatát és karbantartását, valamint
c) az ismert sérülékenységeket a konfigurációval és a rendszergazdai vagy privilegizált funkciók használatával kapcsolatban.

(3) A kormányhivatal kidolgozza vagy beszerzi a rendszer, rendszerelem vagy rendszerszolgáltatás felhasználói dokumentációját, amely tartalmazza:

a) a felhasználók számára elérhető biztonsági funkciókat és mechanizmusokat és ezek hatékony használatának módját,
b) a felhasználói interakció biztonságos módját,
c) a felhasználók felelősségét az EIR, rendszerelem, rendszerszolgáltatás biztonságának fenntartásában.

(4) Amennyiben nem áll rendelkezésre vagy nem létezik adminisztrátori, üzemeltetői és felhasználói dokumentáció, úgy a szervezet dokumentálja az EIR, rendszerelem vagy rendszerszolgáltatás dokumentációjának beszerzésére tett kísérleteket, valamint végrehajtja a szervezet által meghatározott intézkedéseket; és a dokumentációkat eljuttatja a szervezet által meghatározott személyeknek vagy szerepköröknek.

95. Biztonságtervezési elvek

165. § (1) A szervezet az általa meghatározott biztonságtervezési elveket alkalmazza és megköveteli a specifikáció, a tervezés, a fejlesztés, a megvalósítás és az EIR, valamint a rendszerelemek módosítása során. A biztonságtervezési elvek szorosan kapcsolódnak a rendszer fejlesztési életciklushoz és annak minden fázisában alkalmazandóak. A szervezetek a biztonságtervezési elveket alkalmazhatják új rendszerek fejlesztésekor vagy fejlesztés alatt álló rendszereken. Meglévő rendszerek esetén a szervezetek a biztonságtervezési elveket alkalmazzák a rendszer fejlesztései és módosításai során - amennyire ez lehetséges - figyelembe véve a rendszereken belüli hardver-, szoftver- és firmware-elemek jelenlegi állapotát.

(2) A biztonságtervezési elvek alkalmazása segíti az érintett szervezetet megbízható, biztonságos és ellenálló rendszerek fejlesztésében, csökkenti a zavarokkal, veszélyekkel, fenyegetésekkel szembeni érzékenységet.

96. Külső elektronikus információs rendszerek szolgáltatása

166. § (1) A külső EIR szolgáltatásokat külső szolgáltató nyújtja, az érintett szervezetnek nincs közvetlen kontrollja a szükséges intézkedések végrehajtásában, vagy az intézkedések hatékonyságának értékelésében. A szervezetek különféle módokon alakítanak ki kapcsolatokat külső szolgáltatókkal, többek között üzleti partnerségek, szerződések, szervezetek közötti megállapodások, üzletági megállapodások, licenszmegállapodások stb. révén. A külső rendszer szolgáltatások használatából eredő kockázatok kezelésének felelőssége továbbra is az azt jóváhagyó szerepkörnél marad.

(2) A szervezeteken kívüli szolgáltatások esetében a bizalmi lánc megköveteli, hogy a fogyasztó-szolgáltató vonatkozásában minden szolgáltató megfelelő védelmet alakítson ki és biztosítson a szolgáltatásnyújtás során. Ebben a bizalmi láncban a bizalom mértéke és jellege a szervezetek és a külső szolgáltatók közötti kapcsolatok függvényében változik. Az érintett szervezetek dokumentálják a külsős kapcsolataikat, melyek monitorozhatóak. A külső rendszerszolgáltatások dokumentációja tartalmazza a kormányzati, szolgáltatói, felhasználói biztonsági feladatokat és felelősségeket, valamint a szolgáltatási szintre vonatkozó megállapodásokat. A szolgáltatási szintre vonatkozó megállapodások meghatározzák az alkalmazott rendelkezésekkel kapcsolatos elvárásokat, leírják a mérhető eredményeket, és meghatározzák az eljárást valamelyik fél követelményeknek való nem megfelelésére.

97. Nem támogatott rendszerelemek kezelése

167. § (1) A rendszerelemek támogatása magában foglalja a szoftverjavításokat, a firmware-frissítéseket, a cserealkatrészeket és a karbantartási szerződéseket.
(2) A nem támogatott rendszerelemek cseréje alóli kivételek közé tartoznak a kritikus ügymeneti vagy üzleti képességeket biztosító rendszerek, ahol nem állnak rendelkezésre újabb technológiák, vagy ahol az EIR-ek annyira elszigeteltek, hogy a csereelemek telepítése nem lehetséges.
(3) Az alternatív támogatási források arra az igényre vonatkoznak, hogy folyamatos támogatást nyújtsanak az eredeti gyártók, fejlesztők vagy szállítók által már nem támogatott rendszerelemekhez, amennyiben ezek az elemek továbbra is alapvető fontosságúak a szervezeti ügymeneti és az üzleti funkciók szempontjából.
(4) Szükség esetén a szervezetek a kritikus szoftverelemekhez testreszabott javítások kifejlesztésével házon belüli támogatást hozhatnak létre, vagy alternatívaként külső szolgáltatók szolgáltatásait vehetik igénybe, akik szerződéses kapcsolatok révén folyamatos támogatást nyújtanak a kijelölt, nem támogatott elemekhez. Az ilyen szerződéses kapcsolatok közé tartozhatnak a nyílt forráskódú szoftverek értéknövelő szállítói.
(5) A nem támogatott rendszerelemek használatának megnövekedett kockázata csökkenthető például az ilyen elemek nyilvános vagy nem ellenőrzött hálózatokhoz való csatlakoztatásának megtiltásával, vagy az elszigetelés más formáinak megvalósításával.

98. Külső felekkel kötött megállapodások információbiztonsági követelményei

168. § Külső felekkel kötött szerződésekbe egyértelműen be kell építeni az információbiztonsági követelményeket. Egyértelműen szabályozni kell a hozzáféréseket. Rögzíteni kell a felelősségi köröket és az elszámoltathatóság kritériumait, valamint az auditáláshoz való jogot. A kormányhivatalnak 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 a Biztonságelemzési eljárásrend alapján.

XIX. Fejezet
Rendszer és kommunikációvédelem

99. A rendszer és kommunikációvédelem alapelvei

169. § A kormányhivatal megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belüli szabályozásában meghatározott személyek vagy szerepkörök számára kihirdeti a Rendszer- és kommunikációvédelmi eljárásrendet, mely a rendszer- és kommunikációvédelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő, valamint meghatározott gyakorisággal felülvizsgálja, és frissíti a Rendszer- és kommunikációvédelmi eljárásrendet.

100. Szoláltatásmegtagadással járó támadások elleni vedelem

170. § (1) A kormányhivatalok határvédelmét a Nemzeti Infokommunikációs Szolgáltató Zrt. látja el. A szolgáltatásmegtagadással járó események számos belső és külső ok miatt következhetnek be, például egy támadás vagy a szervezeti igények támogatására irányuló tervezés hiánya miatt a nem megfelelő szintű kapacitás és a sávszélesség miatt.

(2) A szolgáltatásmegtagadással járó események keletkezésének és hatásainak korlátozására vagy kiküszöbölésére a kormányhivatal a NISZ szolgáltatásait veszi igénybe. A NISZ feladata a megfelelő határvédelmi eszközök üzemeltetése, amelyek képesek arra, hogy megvédjék a belső hálózatok rendszerelemeit attól, hogy a szolgáltatásmegtagadással járó támadások közvetlenül érintsék őket.
(3) A kormányhivatal továbbá lehetőség szerint biztosítja a megnövelt hálózati kapacitás és sávszélesség alkalmazását, szolgáltatás redundanciával kombinálva, ami csökkentheti a szolgáltatásmegtagadással járó eseményekre való fogékonyságot.
171. § (1) A kormányhivatal biztosítja, hogy az EIR kialakítása és működtetése úgy valósuljon meg, hogy - az védjen a túlterheléses, úgynevezett szolgáltatás megtagadás (denial-of-service attack -DoS), vagy az elosztott túlterheléses támadás (distributed denial-of-service attack, DDoS) jellegű támadásokkal szemben, vagy korlátozza azok kihatásait a megtagadás jellegű támadások listája alapján, meghatározott biztonsági intézkedések bevezetésével.
(2) A DoS/DDoS elleni védelem akkor releváns, amennyiben az elektronikus információs rendszer rendelkezik internet felőli eléréssel pl. http, HTTPS, VPN. RDP
(3) Ezek kialakításáért az IFEFV felel, a végrehajtást a feladatra kijelölt hálózati rendszeradminisztrátor végzi. Ennek érdekében az alábbiakról kell gondoskodni:

a) biztosítani kell az érintett rendszert alkotó szoftverek naprakészségét;
b) az érintett rendszer kártékony kód elleni védelmét meg kell valósítani;
c) az érintett rendszert a legszűkebb funkcionalitás elvének megfelelően úgy kell konfigurálni, hogy csak a működéshez elengedhetetlenül szükséges portok, protokollok és szolgáltatások legyenek engedélyezve;
d) a védelemnek elemeznie kell az eseményeket, minden befelé irányuló gyanús tevékenységeket, mielőtt azok kárt okozhatnának tudni kell blokkolnia;
e) a védelemnek képesnek kell lenni olyan szabályok kezelésére, amelyek részletesen leírják a korlátozásokat alhálózati hosztokra és eszközökre: a szabályok alapján korlátozni kell a ki- és bemenő forgalmat, hacsak nem engedélyezett és ismert szolgáltatásról van szó e kell tudni állítani mind a bejövő, mind a kimenő forgalom ellenőrzését;
f) a védelemnek valós idejű protokoll-analízist, forgalom-monitorozást és analízist is végre kell hajtania, ezáltal képesnek kell lennie a támadások felismerésére.;
g) a védelemnek a DDoS támadás azonosítása esetén azonnal értesíteni kell az IFEFV-et és az IBF-et.

(4) Az érintett szervezet által meghatározott időközönként sérülékenység vizsgálatot kell végezni vagy végeztetni, és a feltárt sebezhetőségek szervezeti kockázati kitettségét értékelni kell, és a megfelelő intézkedéseket meg kell tenni.
(5) Az IÜFV által kijelölt referensnek naprakész nyilvántartást kell vezetnie:

a) az engedélyezett protokollokról, és
b) a hálózati határvédelem információbiztonsági architektúra elemeinek beállításairól.

(6) A kormányhivatal biztosítja, hogy az EIR-ek kizárólag felügyelt interfészeken keresztül érhetők el külső rendszerek számára. A felügyelt interfészekhez a felhasznált eszközök szerepét és védelmi képességeit kihasználó forgalomáramlás ellenőrzési szabályokat kell kialakítani. Az alkalmazott protokolloknak és védelmi eszközöknek

a) védeni kell az összes átvitelre kerülő információk bizalmasságát és sértetlenségét;
b) dokumentálni kell minden kivételt a forgalomáramlási szabályok alól, a kivételt alátámasztó alapfeladattal és az igényelt kivétel időtartamával együttesen dokumentálva;
c) az IÜFV által kijelölt referensnek meghatározott gyakorisággal felül kell vizsgálni a forgalomáramlási szabályok alóli kivételeket, és el kell távolítania azokat a kivételeket, amelyeket közvetlen alapfeladat már nem indokol.

101. Határvédelem

172. § (1) Amennyiben a határvédelmi feladatok ellátása a kormányhivatal felelősségi körébe tartozik, a feladatok végrehajtását IÜFV által kijelölt határvédelmi adminisztrátor végzi, közreműködve az IBF-fel.
(2) Amennyiben a kormányhivatal ezen feladatok ellátására külső szolgáltatót vesz igénybe, a szolgáltatási szerződésben rögzített feladatokat és a kapcsolódó Rendszer és kommunikációvédelmi eljárásrendben megfogalmazott követelmények teljesülését az IFEFV köteles nyilvántartani és ellenőrizni.

102. Végpontvédelem

173. § (1) A kormányhivatal számítógépes hálózatára tilos olyan munkaállomást csatlakoztatni, amely:
a) nem bizalmas hálózati kapcsolattal is rendelkezik,
b) nem tagja a kormányhivatal kontrollált munkakörnyezetének (címtár, tartomány).
(2) A kormányhivatal számára bizalmas hálózati kapcsolatnak számít a belső számítógépes hálózat, minden egyéb hálózat nem bizalmas hálózatnak számít, amelyről azt kell feltételezni, hogy veszélyt jelent a kormányhivatal információbiztonsága számára.
(3) A távoli hozzáféréssel rendelkező felhasználók jogosultságait a SZEV/AG legalább évente egyszer dokumentált módon felülvizsgálja.
(4) A kormányhivatal számítógép-hálózata és külső hálózatok közötti kapcsolat során csak a Konfigurációkezelési eljárásrendben engedélyezett protokollok továbbíthatók, minden egyéb protokoll továbbítása tilos.
(5) A kormányhivatal elektronikus információs rendszere biztonsága érdekében a hálózatot – szegmentálással – egymástól jól elkülöníthető logikai tartományokba kell osztani. Az egyes tartományok közti adatforgalmat lehetőség szerint tűzfal alkalmazásával szűrni kell.
(6) A kormányhivatalnak a kontrollok hatékonyabb működtetése érdekében a külső kapcsolatai számát a szükséges minimumra kell korlátozni a nem használt funkciók, protokollok, portok tiltásával.
174. § (1) A határvédelmi rendszernek alkalmasnak kell lennie legalább az alább felsorolt típusú, különböző támadási formák ellen:
a) erőmegoldások (brute force),
b) alkalmazás réteg támadások (Exploit),
c) szolgáltatás megtagadás (DoS, DDoS),
d) DNS, IP mérgezés (Spoofing),
e) portfigyelés (Portscan),
f) TCP-deszinkronizáció,
g) ICMP protokollon alapuló támadások,
h) SMB relay,
i) hálózat lehallgatása (Sniffing),
j) Man-in-the-middle,
k) webes támadások,
l) Rogue AP,
m) dictionary attack,
n) fragmentation attack,
o) csomagtámadások.
(2) A határvédelmi rendszernek legalább az alábbi technikai megoldásokat kell megvalósítania:
a) TLS szűrés,
b) bejövő kapcsolatok vírusszűrése,
c) kimenő kapcsolatok web szűrése,
d) kimenő kapcsolatok Application Control szűrése,
e) belső (LAN szegmensek között) kapcsolatok vírus alapú szűrése,
f) belső (LAN szegmensek között) kapcsolatok Application Control szűrése,

g) IPSec VPN kapcsolat,
h) TLS VPN kapcsolat,
i) behatolás- detektálás és jelzés,
j) behatolás elhárítás,
k) virtuális szegmentáció,
l) naplófájlok küldése a központi napló szerverhez,
m) napi biztonsági frissítés álljon rendelkezésre.

(3) A határvédelmi eszközök menedzselését csak titkosított csatornán lehet végezni, ezért az eszközökön csak az SSH, HTTPS vagy SNMP menedzsment protokollt lehet engedni az arra jogosult felhasználók részére.

(4) A menedzselhető és biztonságos hálózati architektúra kialakításánál elsődleges szempont az irodai, valamint az irányító rendszerek hálózatának szeparálása.

(5) A hálózati szegmensek felosztása alapvetően az alábbi szempontok figyelembevételével kell, hogy történjen:

a) lokáció szerinti csoportok,
b) jogosult felhasználói kör,
c) rendszerek biztonsági besorolása,
d) egységes szabályrendszer,
e) működés kritikussága,
f) hálózatból ki- és belépő forgalom mértéke.

(6) A hálózat szegmentációja és szegregációja számos különböző módszerrel valósítható meg:

a) hálózatok fizikai szeparációja,
b) hálózatok logikai szeparációja,
c) hálózati forgalom szűrése a hálózati forgalom egyes rétegeiben.

(7) A hálózati szeparáció és szegmentáció kialakításakor az alábbi alapelvek követésével kialakítható a mélységi védelem (defense-in-depth koncepciója):

(8) A szegmentáció és szegregáció ne kizárólag a hálózati réteg szintjén valósuljon meg, hanem az adatkapcsolati rétegtől egészen az alkalmazás rétegig, amennyiben a szegmentáció nem a fizikai rétegben valósul meg.

(9) A rendszereknek a működésükhöz, a felhasználóknak a munkájuk elvégzéséhez éppen szükséges jogosultságok legyenek biztosítva.

(10) Az adatok és a rendszerek az alapján kerüljenek különválasztásra, hogy milyen biztonsági védelmet követelnek meg. Ez magában foglalja az eltérő hardver elemek, platformok használatát, valamint a virtualizációs megoldásokat is.

(11) „Whitelist” alapú szűrés alkalmazása, vagyis alapértelmezetten minden hálózati forgalom legyen tiltott, és csak a működéshez szükségesek kerüljenek engedélyezésre.

103. Kriptográfiai védelem

175. § (1) A kriptográfia számos biztonsági megoldás támogatására alkalmazható, beleértve a minősített és az ellenőrzött, nem minősített információk védelmét, a digitális aláírások biztosítását és végrehajtását, valamint az információk elkülönítésének érvényesítését, amikor a jogosult személyek rendelkeznek a szükséges engedélyekkel, de nincsenek meg a szükséges formális hozzáférési jóváhagyások.

(2) Az IBF megvizsgálja és dönt arról, hogy az adatátvitel során az információk jogosulatlan felfedése ellen szükséges-e kriptográfiai mechanizmusokat alkalmazni, vagy erre nincs szükség, mert az átvitel meghatározott alternatív fizikai ellenintézkedéssel védett. Az elektronikus információs rendszereket minden esetben úgy kell kialakítani és működtetni, hogy az megvédje a továbbított információk sértetlenségét.

(3) A kormányhivatal elektronikus információs rendszereiben csak szabványos, egyéb jogszabályokban biztonságosnak minősített kriptográfiai műveletek valósíthatók meg. Az általánosan alkalmazandó kriptográfiai szabványok közé tartozik az NKI által jóváhagyott kriptográfia.

(4) A kriptográfiai kulcsokat házon belül a kulcsok előállítására és kezelésére vonatkozó előírások alapján, vagy a (Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő) megbízható partnerrel kell generáltatni.
(5) Az adatátvitel során az adatok titkosítása védi meg az információt a jogosulatlan közzétételtől és a módosítástól. Ezért a kormányhivatalnak ki kell választania a megfelelő kriptográfiai mechanizmusokat, amelyeket az EIR alkalmazni fog az adatátvitel során. Ez magában foglalhatja a TLS és az IPSec (Internet Protocol Security) protokollokat, amelyek biztosítják az adatok bizalmas és integritását az átvitel során.
(6) A titkosítási algoritmusokat csak validált, a FIPS 140-2 szabvány szerinti, vagy azzal egyenértékű alkalmazások használhatják.
(7) A különböző kriptográfiai mechanizmusok együttes használata kell ahhoz, hogy a bizalmasság és a sértetlenség teljeskörűen megvalósuljon. A szimmetrikus kriptográfiai algoritmusok (pl. AES) a bizalmasságot biztosítják, a hash algoritmus és a HMAC alkalmazása pedig az adatok sértetlenségét biztosítják a kommunikáció során. A kriptográfiai mechanizmus használatát kapcsolatosan naplózni kell az adatátviteli eseményeket, a hitelesítési eseményeket és az esetleges biztonsági eseményeket is.
(8) Minden kriptográfiai kulcsot védeni kell módosítás, elvesztés és rongálás ellen, a titkos és magánkulcsokat védeni kell a jogosulatlan felfedés ellen. A kulcsok létrehozására, tárolására és archiválására használt rendszert fizikailag is védeni kell és a kormányhivatal többi központi elemét tartalmazó gépteremben kell elhelyezni. Ezen előírások betartásáért az IFEFV a felelős.
176. § (1) Kulcsok kezelése:
(2) Szoftveres kulcs létrehozása: A kulcsok létrehozása az IFEFV által erre a feladatra kijelölt infrastruktúra üzemeltetési rendszergazda feladata, szoros együttműködésben az IBF-fel. A kulcsok előállítása minden esetben csak naprakész és megfelelően konfigurált rendszerelemeken (szoftver és hardver egyaránt) kerülhet sor. Az átadás után gondoskodni kell a biztonságos megsemmisítésről is.
(3) Hardveres kulcs létrehozása: A gyártó ajánlásai kell létrehozni a kulcsot. Ha kulcs aktiválásához jelszó vagy PIN kód szükséges, akkor a kormányhivatali jelszókezelési eljárásoknak meg kell felelnie (kiemelt figyelemmel a kezdeti jelszó / PIN létrehozásánál). A kulcstárolásnál gondoskodni kell arról, hogy a kulcsokat ne lehessen exportálni az tároló eszközről.
(4) Mind a létrehozás, mind az átadás folyamatában gondoskodni kell arról, hogy a kriptográfiai eszközök tartalmát harmadik fél elől rejtve maradjanak, másolat ne készüljön. Az átadott eszközökről nyilvántartást kell vezetni, melynek az elkészítését és karbantartását az IBF, illetve IBM végzi.
(5) A kriptográfiai kulcsok cseréje a létrehozás, átadás és megsemmisítés leírt folyamatok szerint kerül végrehajtásra.
(6) Aszimmetrikus kulcspár részét képező kulcs megsemmisítése:

a) ha a kriptográfiai kulcsot azonosításra használták, akkor a kulccsal való hozzáférést logikailag is meg kell szüntetni;
b) ha a kriptográfiai kulcsot hitelesítésre használták, akkor a kulcs és a regisztráció visszavonásáról is gondoskodni kell.

(7) A kriptográfiai kulcs megsemmisítésekor kiemelt figyelmet kell fordítani az alábbiakra:

a) hardveres kulcs esetén az adathordozók helyreállíthatatlanságot biztosító törlésére vonatkozó előírásokat;
b) szoftveres kulcs esetén a biztonságos adatmegsemmisítésről gondoskodni kell (biztonsági másolatokat is!).

(8) A kulcsok megsemmisítéséről az IÜFV által erre a feladatra kijelölt infrastruktúra üzemeltetési rendszergazda gondoskodik, melynek végrehajtásáról jegyzőkönyvet készít, melyet az IBF-nek ad át.

104. Hálózati eszköz védelem

177. § (1) A kormányhivatal rendelkezésében álló hálózati eszközök tekintetében felügyeleti rendszert kell üzemeltetni, melynek segítségével a hálózati eszközök egységes monitoring eszközkészlettel és felülettel vizsgálhatók.

(2) Az EIR-nek meg kell szakítania a hálózati kapcsolatot egy munkaszakaszra épülő kétirányú adatcsere befejezésekor, ha a hálózati inaktivitás a megállapított időtartamot elérte. A konkrét idő meghatározása az alkalmazás és technológia függvényében kell, hogy meghatározásra kerüljön. Az időtartam meghatározásának felelőse alkalmazásfejlesztés során az Alkalmazás fejlesztésért felelős vezető, infrastrukturális szolgáltatás esetén az IFEFV, végrehajtója a Hálózati rendszeradminisztrátor. Fentiek miatt tilos olyan információs rendszerkapcsolatok kialakítása, amelyek mesterségesen fenntartanak kapcsolatot, akkor is, ha tényleges munkavégzés és/vagy adatcsere nem történik (pl. autopolling)

178. § Az IT infrastruktúra fejlesztésért felelős vezető az IBF közreműködésével meghatározza:

a) az elfogadható és a nem elfogadható mobilkódokat és mobilkód technológiákat (kerülendő az ActiveX, VBscript, PDF-be ágyazott szkriptek, Office makrók és nem aláírt VBA kódok használata);
b) biztosítja, hogy a beszerzések, fejlesztések során a mobil kódokra és mobilkód technológiákra való korlátozások minden esetben kerüljenek figyelembe vételre;
c) az elektronikus információs rendszernek tiltania kell a letöltés és végrehajtás funkció automatikus végrehajtását;
d) dönt arról, hogy engedélyezi vagy tiltja mobil adathordozók (CD, DVD, USB eszköz) esetében az úgynevezett. automatikus végrehajtás funkciót.

179. § (1) A nem engedélyezett mobilkódokat tiltani kell távoli számítógépről, vagy hálózaton keresztül történő letöltés, illetve elektronikus levelezés esetén egyaránt. A vírusvédelmi rendszernek képesnek kell lennie a mobil kódok ellenőrzésére, futtatásuk tiltására.

(2) Az elektronikus levelezés biztonsága érdekében előírás, hogy az elektronikus levelezést biztosító hálózati szegmensben is szükséges a vírusvédelmi eszköz biztosítása. A szűrésnek ki kell terjednie a levélbe illesztett scriptek, active-x komponensek ellenőrzésére. Mellékletek esetében a tömörített állományokban, az egymásba ágyazott tömörítésekben is szükséges az ellenőrzés elvégzése.

(3) A hálózati eszközök (pl. routerek, switchek, tűzfalak, access pointok) védelme a rendszer- és kommunikációvédelem egyik kulcseleme, mivel ezek az eszközök irányítják és felügyelik az adatforgalmat, és ha sérülékenyek, az egész informatikai rendszer veszélybe kerülhet.

180. § (1) Gondoskodni kell ezen eszközök védelméről:

(2) Megfelelően kialakított, zárt, hozzáférésvédett helyiség (pl. szerver- vagy patch szoba), amelyhez kizárólag jogosult személyek férhetnek hozzá (beléptetőkártya, naplózás).

(3) Külön VLAN-okba helyezni a különböző funkciókat (pl. felhasználók, szerverek, vendéghálózat).

(4) Gyári jelszavak, admin felhasználók, nyitott portok azonnali módosítása, valamint csak szükséges szolgáltatások legyenek engedélyezve (pl. SNMP csak v3 verzióban) és az adminisztrációhoz csak biztonságos protokollokat használjunk (pl. SSH, HTTPS). Többfaktoros hitelesítés (MFA) alkalmazása ajánlott.

(5) A hozzáférés IP-cím szerint korlátozható, illetve tűzfal konfigurálható a jogosulatlan forgalom tiltására, ACL-ek használata port és IP-szűrésre.

(6) Gondoskodni kell a támogatott eszközök gyártói biztonsági frissítéseinek rendszeres telepítéséről, és a hibajavítások figyeléséről CVE-adatbázis vagy gyártói értesítések alapján.

(7) Az adminisztrációs események naplózása (pl. belépés, konfigurációmódosítás) szükséges, a naplókat központi loggyűjtőbe tárolása fontos.

(8) Hálózati forgalom rendszeres monitorozása (IDS/IPS, NetFlow, SNMP).

(9) Konfigurációs fájlokat biztonságosan, titkosított tárolón menteni ajánlott

181. § (1) Vezeték nélküli hálózati hozzáférés kialakítására az eKH VPN-en csak a NISZ Zrt. engedélyével, az általuk kialakított VLAN-on keresztül van lehetőség.

(2) A vezeték nélküli hozzáférés kialakítása során

a) WPA3 (vagy minimum WPA2) titkosítás használata szükséges,
b) az SSID elrejtése kötelező, és
c) MAC-cím szűréssel kell biztosítani az engedélyezett eszközök kapcsolódását.

(3) Az IÜFV feladata, hogy a hálózati eszköz felügyeleti rendszer jelzései alapján:

a) szükséges karbantartási folyamatokat megindítsanak,
b) incidens esetén az IBF-felé eszkalálják a feladatot,

c) ügymenet, illetve üzletmenet folytonosságot érintően az érintett SZEV/AG bevonásával gondoskodjon az eszköz pótlásáról.

105. Biztonságos cím és névfeloldási szolgáltatás alkalmazása

182. § (1) A kormányhivatal informatikai rendszerében a névfeloldási szolgáltatását úgy kell konfigurálni, hogy a hiteles forrást biztosító DNS kiszolgáló (autoritatív DNS) kriptográfiai megoldást (digitális aláírás) is alkalmazzon. A DNS kiszolgálónak olyan biztonságos tranzakciókat kell megvalósítania a név/cím feloldási kérésekre, amely az adott hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozóan is hiteles forrást biztosít.
(2) DNSSEC esetén a rekurzív névszerverekbe konfigurálni kell egy-vagy több nyilvános kulcsot, melyek a bizalmi lánc kiindulópontjai lesznek. A konfigurációt úgy kell elvégezni, hogy a magasabb szinten aláírt, delegált zónában használt publikus kulcs alapján bizalmi lánc alakulhasson ki, mely során digitális aláírások láncolatán keresztül bizonyítható a DNS információ hitelessége.
(3) Az IFEFV által erre a feladatra kijelölt infrastruktúra üzemeltetési rendszergazdák kötelessége gondoskodni arról, hogy az informatikai rendszerek komponensei kivétel nélkül hiteles forrást biztosító DNS szolgáltatást használjon.
(4) Abban az esetben, ha az érintett szervezet elektronikus információs rendszere név/cím feloldási szolgáltatást biztosít a saját, vagy másik szervezet számára, akkor ezt olyan módon kell megvalósítani, hogy

a) a név/cím feloldási szolgáltatást megvalósító elektronikus információs rendszerek, rendszer elemek hibatűrő (fürt (cluster), HAC stb.) vagy más redundáns felépítéssel, magas rendelkezésre állással kell megvalósítani;
b) a külső és a belső szerepköröket szeparáltságáról gondoskodni kell, tehát külön DNS kiszolgálót kell használni a belső hálózat kiszolgálására és külön kiszolgálónak kell biztosítania az internetes DNS kiszolgálókkal történő kapcsolattartást.

106. Folyamatok elkülönítése

183. § Amennyiben szükséges, alkalmazni kell folyamat izolációs technológiákat, mint például a sandboxingot vagy a virtualizációt, hogy logikailag elválassza a szoftvereket és firmware-eket a többi szoftvertől, firmware-től és adattól.

XX. Fejezet
Rendszer és információ sértetlenség

107. A rendszer és információ sértetlenség alapelvei

184. § (1) A rendszer- és információsértetlenség fenntartását biztosító rendelkezéseket a kormányhivatal által üzemeltetett EIR-ek és egyéb támogató rendszerek tekintetében kell alkalmazni. Szolgáltató által üzemeltetett EIR vagy támogató rendszer esetén az üzemeltetési szolgáltatási szerződésben kötelemként kell érvényesíteni a rendelkezéseket, és azokat a szolgáltatónak kell biztosítania.
(2) A rendszer- és információsértetlenség feltételrendszerének kialakítása az IFEFV felelőssége. A részletes követelményeket és szabályokat a Rendszer- és információsértetlenségi eljárásrend tartalmazza.

108. Hibajavítás

185. § A kormányhivatal által üzemeltetett EIR-ek és egyéb támogató rendszerek vonatkozásában a hibajavítási eljárásokat úgy kell kialakítani, hogy az informatikai feladatokat ellátó szervezeti egység foglalkoztatottjai a lehető leghamarabb informálódjanak a legújabb sérülékenységekről, és képesek legyenek azokat a lehető legrövidebb időn belül kezelni.

186. § (1) A sérülékenységek kezelése történhet (összhangban a Konfiguráció kezelési eljárásrenddel):

a) az eszköz vagy szoftver gyártója által kiadott, biztonsági szempontból releváns szoftver- vagy firmware-frissítések, javítások (patch-ek) telepítésével,
b) a konfigurációs beállítások módosításával vagy javításával,
c) kerülő megoldás (workaround) alkalmazásával pl. egyes funkciók letiltásával.

(2) A gyártók által kiadott, biztonsági szempontból releváns szoftver- vagy firmware-frissítések, javítások (patch-ek) telepítését rendszeresen el kell végezni minden informatikai eszközön és szoftveren, a kiadást követő alábbi határidők szerint:

a) biztonsági, kritikus besorolással:
   aa) kiszolgálók és infrastruktúra eszközök esetén 2 hét,
   ab) kliens gépek esetén 3 hét,
   ac) egyéb eszközök esetén 4 hét,
b) biztonsági, de nem kritikus besorolással:
   ba) kiszolgálók és infrastruktúra eszközök esetén 1 hónap,
   bb) kliens gépek esetén 2 hónap,
   bc) egyéb eszközök esetén 2 hónap.

(3) Kiszolgálóknak és infrastruktúra eszközöknek minősülnek az alábbiak:

a) szerver hardverek és operációs rendszereik, hypervisor-ok,
b) szerver oldali alkalmazások (pl. adatbázisok, webkiszolgálók),
c) routerek, switchek, storage-ok, kamerák, stb.

109. Kártékony kódok elleni védelem

187. § (1) A kormányhivatal egészére kiterjedő, folyamatosan működő, kártékony kódok elleni védelem és ellenőrzés biztosítása érdekében automatikus frissítésű, központilag menedzselhető kiszolgáló- és végpontvédelmi rendszert kell kiépíteni. Minden lehetséges lépést meg kell tenni a veszélyes programok által okozott incidensek kiküszöbölésére. Ennek érdekében vírusellenőrző alkalmazásokat kell telepíteni a munkaállomásokra, a szerverekre és az informatikai határvédelmi eszközökre.

(2) A kártékony kódok elleni védelmi feladatok elvégzéséhez olyan vírusellenőrző programokkal kell rendelkezni a kormányhivatalnak, amely(ek) segítségével az előforduló összes platform ellenőrizhető, és ezeknek a programoknak a vírusdefiníciós állományait rendszeresen frissíteni kell.

(3) A szervereken és munkaállomásokon központi felügyeleti rendszert kell alkalmazni.

(4) A szervereken és munkaállomásokon a valós idejű védelem folyamatos működését garantálni kell, amely biztosítja a felhasználó által végzett munkafolyamatok során igénybe vett állományok (adatok, programok) használat előtti vírusellenőrzését. A külső forrásból származó cserélhető adathordozókat használatba vétel előtt automatikus kártékony kód ellenőrzés alá kell vetni.

(5) A valós idejű védelem mellett hetente legalább egyszer teljes körű vírusellenőrzést kell végezni előre ütemezett módon, automatikusan.

(6) Kártékony kód elleni védelem nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép és mobil eszköz nem üzemeltethető.

(7) A jogosultságok kialakításánál figyelembe kell venni, hogy a felhasználók nem állíthatják le a gépükön futó vírusellenőrző szoftvert, és nem változtathatják meg annak beállításait.

(8) A vírusellenőrző alkalmazásnak minden esetben rezidensként (minden írást és olvasást ellenőrizve) kell futnia a memóriában.

110. Elektronikus információs rendszerek monitorozása

188. § (1) Az EIR-ek teljes életciklusában meg kell valósítani és biztosítani az EIR-ben kezelt adatok és információk bizalmasságát, sértetlenségét és rendelkezésre állását, valamint az EIR és elemeinek sértetlenségét és rendelkezésre állását. Ennek érdekében az EIR-ek kritikus rendszerelemeit, illetve biztonsági eszközeit folyamatosan monitorozni kell. A monitorozásnak minimálisan az alábbi témákra kell kiterjednie:

a) határvédelmi incidensek, és hálózati illegális tevékenység,
b) vírusvédelmi incidensek,
c) jogosultság kezelési incidensek,
d) mentési feladatok sikeres/sikertelen végrehajtása,
e) külső beszállítók és szolgáltatók felhasználóinak tevékenységei, távoli elérések naplózása,
f) rendszergazdák tevékenységei,
g) biztonsági riasztórendszerek naplózása.

(2) Azonosított rendellenes esemény, illetve incidens gyanú esetén az IÜFV által kijelölt IÜR a Biztonsági eseménykezelési eljárásrend szerinti prioritásnak megfelelően riasztja a felelősöket.

111. Biztonsági riasztások és tájékoztatások

189. § (1) Az IBF-nek folyamatosan figyelemmel kell kísérnie a jogszabályban kijelölt szervezetek által kiadott biztonsági riasztásokat, figyelmeztetéseket és iránymutatásokat. A tudomására jutott naprakész biztonsági – fenyegetésekre és sebezhetőségekre vonatkozó – információkat, eljárásokat és technikákat megosztja az IFEFV-vel és IÜFV-vel, valamint az érintett szervezeti egységekkel.

(2) Az IBF továbbá a biztonsági iránymutatások alkalmazása érdekében felülvizsgálja az érintett eljárásrendeket és az EIR-ekre vonatkozó biztonsági intézkedéseket.

112. Információ kezelés és megőrzése

190. § (1) Az EIR-ek kimeneti információinak kezelése a fővárosi és vármegyei kormányhivatalok Egységes Iratkezelési Szabályzatáról szóló 1/2023. (I. 12.) MvM utasítás és a kormányhivatal Egyedi Iratkezelési Szabályzata (a továbbiakban együtt: Iratkezelési Szabályzat) előírásainak figyelembe vételével történhet meg.

(2) Az EIR-ek kimeneti információinak (nyomtatásban, nyomatképzésben megjelenő információk) biztonsága érdekében az Iratkezelési Szabályzattal összhangban a következő – az előállított nyomatok teljes életciklusában érvényes – előírások betartása kötelező:

a) gondoskodni kell a kimeneti információ tartalmi ellenőrzéséről;
b) gondoskodni kell arról, hogy a kimeneti információhoz történő fizikai és logikai hozzáférés kizárólag az arra jogosított személyekre korlátozódjon;
c) gondoskodni kell arról, hogy a jogosult személyek időben megkapják az elkészült kimeneti információkat;
d) biztosítani kell a kimeneti információk biztonságos tárolását;
e) biztosítani kell, hogy a megsemmisítési eljárások során a kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.

XX. Fejezet
Ellátási lánc kockázatkezelése

113. Az ellátási lánc kockázatkezelése alapelvei

191. § (1) Az ellátási lánc kockázatkezelés célja, hogy a kormányhivatal az itt megfogalmazott szabályokat alkalmazza minden olyan esetben, amelyben informatikai szolgáltatást vagy eszközöket szerez be, vagy ha rendszerfejlesztési tevékenységet végez vagy végeztet.
(2) A további részletszabályokat az Ellátási láncra vonatkozó kockázatelemzési és kockázatkezelési eljárásrend tartalmazza.

114. Ellátási láncra vonatkozó követelmények és folyamatok (19.4)

192. § (1) A beszerzés folyamatában olyan biztonsági dokumentációs előírásokat kell készíteni, amelyek az informatikai rendszerek teljes életciklusára vonatkoznak. A szabályozás vonatkozik a beszerzési és közbeszerzés esetekre is, a kormányhivatal beszerzésre vonatkozó szabályzataival és eljárásrendjeivel összhangban.
(2) Az Informatikai beszerzés teljes életciklusára ki kell terjednie a biztonsági megfelelősségnek, azaz a beszerzési tervek, és az igények engedélyeztetési folyamatába is be kell építeni azokat a követelményeket, amelyek majd a megfelelő biztonságot jelentik. A beszerzési folyamat lépéseibe: ajánlati kiírás, ajánlatok elbírása, szállító kiválasztása, szerződéskötés, a szerződés tárgyának átvételi procedúrája és a beüzemelés lépései sem zárják le teljesen a beszerzés biztonsági folyamatának követését, ugyanis a beszerzés folyamata során gondolni kell a majdani üzemeltetés során jelentkező olyan folyamatos beszerzésekre, ami az informatikai rendszer használatát biztosítják. (pl. alkatrész utánpótlás vagy szoftver rendszerek követése). Jelen szabályozás az adminisztratív védelem feltételeit teremti meg a biztonság érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések felsorolásával.
(3) Az IBF-nek véleményezési joga van minden olyan beszerzés esetében, amelynek közvetlen vagy közvetett hatása lehet az információbiztonságra.

115. Ellátási láncra vonatkozó kockázatmenedzsment

193. § (1) A kormányhivatal függősége a külső szolgáltatóktól származó termékektől, rendszerektől és szolgáltatásoktól, valamint a szolgáltatókkal való kapcsolatok jellege, növekvő kockázatot jelent. A tevékenységek, amelyek növelhetik a biztonsági vagy adatvédelmi kockázatokat, magukban foglalják a jogosulatlan gyártást, a hamisítványokra való cserét, vagy azok használatát, a módosításokat, a lopást, a rosszindulatú szoftverek és hardverek beillesztését, valamint a nem megfelelő gyártási és fejlesztési gyakorlatot az ellátási láncban.
(2) Az ellátási lánc kockázatkezelése összetett, többoldalú feladat, amely koordinált erőfeszítést igényel a szervezeten belül a bizalmi kapcsolatok kiépítéséhez és a belső és külső érdekeltekkel való kommunikációhoz. Az ellátási lánc kockázatkezelési tevékenységek (SCRM) magukban foglalják a kockázatok azonosítását és értékelését, a megfelelő kockázat válaszintézkedések meghatározását, a kockázatkezelési tervek kidolgozását a válaszintézkedések dokumentálására, és a teljesítmény ellenőrzését a tervekkel szemben.
(3) Az ellátási lánc kockázatkezelési (SCRM) terv (a rendszer szintjén) implementáció specifikus, biztosítja a szabályzatok végrehajtását, követelményeket, korlátozásokat és következményeket. Ez lehet önálló vagy beépíthető a rendszer biztonsági és adatvédelmi terveibe.
(4) Az ellátási lánc kockázatkezelési terv kezeli a kockázatkezelési követelmények végrehajtását és nyomon követését, valamint a rendszerek fejlesztését/fenntartását a rendszerfejlesztési életcikluson (SDLC) keresztül az ügymeneti és üzleti funkciók támogatása érdekében. A kockázatkezelési tervek

tartalmazzák a szervezet ellátási lánc kockázattűrésének értékeit, az elfogadható ellátási lánc kockázatcsökkentő stratégiákat vagy követelményeket, egy folyamatot az elfogadható kockázat kiértékelésére és nyomon követésére, a tervek alkalmazásáról, illetve az arról való tájékoztatás folyamatát, valamint egy összefoglalót a megtett intézkedések szükségességéről és az érintett személyekről és szerepkörökről.
(5) Ezek mellett az ellátási lánc kockázatkezelési tervei a megbízható, biztonságos, személyes adatokat védő és rugalmas rendszerelemek és -rendszerek fejlesztésére vonatkozó követelményekkel is foglalkoznak, beleértve az életciklus-alapú rendszerek biztonságtechnikai folyamatainak részeként megvalósított biztonsági tervezési elvek alkalmazását.

116. Beszerzési stratégiák, eszközök és módszerek (19.13)

194. § A kormányhivatal az elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben szerződéses követelményként az alábbiakat követeli meg.
195. § (1) Az informatikai rendszerek beszerzése alapos tervezést igényel. Meg kell határozni a biztonsági rendszerfunkciókat úgy, hogy a felhasználói igényeket is figyelembe vesszük a beszerzési kiírásban, majd a szerződésben.
(2) A biztonságos üzemeltetés érdekében ki kell alakítani a rendszerfrissítések és az új változatok átvételi követelményeit is. Ezek közé kell, hogy tartozzon:

a) a dokumentált tesztelés, melynek nem csupán az újonnan bevezetett funkciókra, hanem
b) lehetőleg a teljes rendszerre és általános biztonsági szempontokra is ki kell terjednie;
c) az üzemelésre való átvételt pedig minden esetben vezetői jóváhagyásnak és oktatásnak kell megelőznie, és ezeket a követelményeket a szerződésnek is tartalmaznia kell.
d) elegendő védelmet kell beépíteni a rendszerbe a nem szándékos (felhasználói vagy szoftver) hibák ellen,
e) a rendszernek a megkívánt szinten ellent kell állnia a szándékos behatolási kísérleteknek illetve a biztonsági funkciókat kikerülni akaró támadásoknak.

(3) A funkcionális biztonsági követelmények meghatározása az IBF és az IÜFV feladata.
196. § (1) A kormányhivatal csak olyan informatikai rendszert használ, amely megfelelő rendelkezésre állással bír, azaz meghatározott szolgáltatási szintet tud biztosítani. A fentiekben említett biztonsági követelményeket már a rendszerfejlesztési életciklus korai szakaszában be kell építeni a rendszerekbe.
(2) A garanciális biztonsági követelmények meghatározása az IFEFV, illetve az erre a feladatra kijelölt informatikai vezető vagy referens feladata, konzultálva a szervezeti egység vezetőkkel.
197. § (1) A beszerzési dokumentációkban meg kell határozni a beszerzendő informatikai rendszer átvételéhez szükséges dokumentációk formai és tartalmi követelményeit, aminek meglétét az átvételkor ellenőrizni kell. Az elvárt dokumentációkkal kapcsolatos előírásokat az Alkalmazásfejlesztési szabályzat tartalmazza.
(2) A biztonsággal kapcsolatos dokumentációs követelmények meghatározása az IFEFV, illetve az erre a feladatra kijelölt informatikai vezető vagy referens feladata.
198. § (1) Minden beszerzett vagy egyedileg fejlesztett szoftver (amennyiben rendelkezésre áll a dokumentációjával együtt) egy-egy példányát az Informatikai feladatok ellátásáért felelős szervezeti egység által kezelt szoftver archívumban kell elhelyezni. Itt kell tárolni a szoftverek és hardverek dokumentációjának és kézikönyvének egy-egy példányát (akár elektronikus formában, akár papíron).
(2) A beszerzés dokumentációkban ki kell térni arra, hogy az informatikai rendszerek átvételi eljárásának részét képezik ezeknek a dokumentumoknak az átvétele. Kizárólag olyan szoftvereket és kapcsolódó dokumentációt szabad átvenni, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak, a szerzői jogi, és más jogszabályoknak. (pl. adójogszabályok)

(3) A jelen helyzetben előfordulhat, hogy az információs rendszer/komponens életkora miatt vagy a fejlesztők és szállítók támogatásának hiánya miatt képtelenség a szükséges dokumentációk megszerzése. Ezekben az esetekben, az Informatikai szervezeteknek kell újra előállítani a dokumentációkat, ha az ilyen dokumentáció elengedhetetlen a biztonsági szabályozások hatékony végrehajtásához, illetve működéséhez.

117. Beszállítókkal történő kommunikáció

199. § A kormányhivatal megállapodásokat köt és eljárásokat hoz létre a rendszer, rendszerelem vagy rendszerszolgáltatás beszállítói láncában részt vevő szervezetekkel. Az egyezmények és eljárások létrehozása elősegíti a beszállítói láncban részt vevő szervezetek közötti kommunikációt. A felmérések vagy naplók eredményei tartalmazhatnak nyílt forrású információkat, amelyek hozzájárultak egy döntéshez vagy eredményhez, és segíthetnek a beszállítói láncban részt vevő szervezetnek megoldani egy problémát vagy javítani a folyamatait.

118. Rendszerek vagy rendszerelemek vizsgálata

200. § (1) Az ellátási lánc kockázatkezelésének egyik kritikus területe a rendszerek és rendszerelemek vizsgálata, amely biztosítja, hogy a hivatal által használt informatikai rendszerek, eszközök és komponensek megbízható, biztonságos forrásból származzanak, megfeleljenek a vonatkozó előírásoknak, és ne rejtsenek rejtett biztonsági kockázatokat.
(2) Alapelvek:
(3) Bizalom elve: csak olyan rendszerelemek (szoftver, hardver, firmware stb.) használhatók, amelyek eredete, fejlesztője/gyártója és működése megbízhatónak minősül.
(4) Átláthatóság elve: a rendszerelemek származása, fejlesztési folyamata, és karbantartása átlátható kell legyen.
(5) Minimális jogosultság és funkcionalitás: csak a szükséges komponenseket kell beépíteni, minimális jogosultságokkal.
201. § (1) A kormányhivatal köteles az alábbi vizsgálatokat elvégezni minden új rendszer vagy rendszerelem beszerzése, bevezetése előtt, valamint időszakosan a működtetés során is:
(2) Eredetvizsgálat:
a) gyártó/fejlesztő megbízhatóságának ellenőrzése (referenciák, tanúsítványok, székhely ország),
b) beszállítói lánc átláthatósága,
c) nemzetbiztonsági kockázat szempontjából kockázatos országokból származó komponensek kerülése.
(3) Technikai vizsgálat:
a) sebezhetőségi vizsgálat (pl. CVE-ellenőrzés, statikus és dinamikus kódelemzés),
b) káros kód keresése (malware, backdoor),
c) verziókezelés, frissíthetőség és támogatás vizsgálata.
(4) Kompatibilitás és integritás ellenőrzés:
a) a rendszer meglévő környezettel való kompatibilitásának igazolása,
b) digitális aláírás, hash-érték ellenőrzése az integritás biztosítására.
(5) Jogszabályi és szabályozási megfelelés:
a) a vonatkozó jogszabályok (pl. NIS2, Infotv.),
b) kormányrendeletek (pl. 1089/2025. Korm. határozat) és
c) belső szabályzatok figyelembevételével.
(6) Ajánlott gyakorlatok:
a) fekete- és fehérlisták alkalmazása a beszállítókról és gyártókról,
b) sandbox környezet használata az új rendszerelemek kipróbálására,
c) független biztonsági auditok megrendelése kritikus komponensek esetén,
d) automatizált eszközök (pl. vulnerability scanner, supply chain risk tool) alkalmazása.

(7) A rendszerelemek kivonásakor is vizsgálni kell:

a) tartalmaznak-e adathordozókat,
b) van-e szükség adatmentésre, adattörlésre, fizikai megsemmisítésre,
c) biztonságos módon történik-e az átadás vagy leselejtezés.

119. Rendszerelem hitelessége

202. § (1) Hamisított alkatrészek érkezhetnek gyártóktól, fejlesztőktől, szállítóktól és szerződéses partnerektől. A hamisítás elleni szabályok és eljárások támogatják a hamisítás elleni védelmet, valamint további védelmet biztosítanak a kártékony kódok ellen is. Emiatt a ki kell alakítania a hamisítás elleni szabályokat és eljárásokat, jelenteni kell a hamisított rendszerelemeket és azok forrását a kormányhivatal által meghatározott személyeknek vagy szerepköröknek. Dokumentálnia kell, amennyiben hamisított rendszerelemeket vagy alkatrészeket fedez fel és fel kel vennie a kapcsolatot a hamisított alkatrész forrásával, vagy az illetékes hatósággal.
(2) A konfigurációfelügyelet magában foglalja a változások naplózását, amelyeket a rendszerelemen végeznek, beleértve a szervizelést és a javítást is. A naplózás lehetővé teszi a kormányhivatal számára, hogy nyomon követhesse a rendszerelem teljes élettartamát, és biztosítsa, hogy minden változást megfelelően dokumentálnak és ellenőriznek.

120. Rendszerelem selejtezése, megsemmisítése

203. § (1) Az adatok, dokumentációk, eszközök vagy rendszerelemek bármikor selejtezhetők a rendszerfejlesztési életciklus során. A selejtezés során bekövetkezett esetleges kompromittálódás érinti a fizikai és logikai adatokat, beleértve a papíralapú vagy digitális formában meglévő rendszerdokumentációt; a szállítással és kézbesítéssel kapcsolatos dokumentációt; a szoftverkóddal rendelkező memóriakártyákat; illetve routereket vagy szervereket, amelyek állandó adathordozóval rendelkeznek és bizalmas, vagy védett információkat tartalmazhatnak. Emellett az rendszerelemek megfelelő selejtezése segít megakadályozni, hogy az említett elemekkel kétes eredetű árukat forgalmazó piactereken kereskedjenek.
(2) Ennek megfelelően a kormányhivatalnak meg kell határoznia, mely adatokat, dokumentációkat, eszközöket és rendszerelemeket kell selejteznie, valamint ki kell dolgoznia egy módszertant és technikákat a selejtezésre, melyet ezután alkalmaznia kell. Dokumentálnia kell a selejtezést és annak tárgyát képező rendszerelemet, alkatrészt vagy adatot, valamint gondoskodnia kell az érintett elemek kivezetéséről rendszerelem leltárból.

ZÁRÓ RENDELKEZÉSEK

204. § (1) Az IBSZ módosítását a szervezeti egységek vezetői indokolt, írásbeli kérelemmel kezdeményezik a főispánnál.
(2) Jelen utasítást szükség szerint – különösen jogszabály, közjogi szervezetszabályozó eszköz, ügyrend vagy szabályzat vonatkozó módosítása esetén – de legalább évente felül kell vizsgálni, amelynek végrehajtásáért a Pénzügyi, Gazdálkodási és Informatikai Főosztály vezetője a felelős.
(3) A kormányhivatal 2025. október 31-ig az IBSZ-ben jelzett eljárások kidolgozását elvégzi. A kidolgozásért felelős az IFEFV, a kidolgozást végzi az IBF és az IÜFV, illetve az általa kijelölt informatikai referensek.
205. § (1) Jelen utasítás a közzétételét követő napon lép hatályba.
(2) Hatályát veszti az 1/2019. számon kiadott, a Veszprém Megyei Kormányhivatal Információbiztonsági Szabályzata elnevezésű szabályzat.

Veszprém, 2025. július 9.

Takács Szabolcs
főispán

1. számú melléklet
7/2025. (VII. 9.) főispáni utasításhoz

Információbiztonságban érintett szerepkörök listája

KH szerepkör	Kód	Magyarázat	Hozzárendelt feladatkörök	Hozzárendelt személy(ek)
Szervezet vezetője	**FISP**	Szervezet vezetője, legfelsőbb felelős, szabályozó dokumentumok kormányhivatali kiadásáért felelős szerepkör	Főispán	
Főigazgató	**FŐIG**	Szakmai végrehajtásért felelős szerepkör, FISP közvetlen beosztottja, helyettese.	Főigazgató	
Elektronikus információs rendszer biztonságáért felelős személy	**IBF**	A törvényben előírt, elektronikus információs rendszer biztonságáért felelős szerepkör.	Megbízott elektronikus információs rendszer biztonságáért felelős személy	
Szervezeti Egység Vezető/Adatgazda	**SZEV/AG**	Adott szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik. Felelőse továbbá az informatikai fejlesztési igények gyűjtéséért, továbbításáért.	Valamennyi hivatalvezető, főosztályvezető és osztályvezető	
Informatikai biztonsági megbízott	**IBM**	Elektronikus információbiztonsággal kapcsolatos feladatok ellátásában közvetlen az IBF irányítása alatt, közreműködő szerepkörök.	Az IBF és az osztályvezető kivételével az Informatikai Osztály valamennyi foglalkoztatottja, valamint az Agrár- és Vidékfejlesztést Támogató Főosztály informatikusa	
Informatikai feladatok ellátásáért felelős vezető	**IFEFV**	Főosztályvezető/osztályvezető(k), aki(k) az informatikai szolgáltatások üzembiztos működtetéséért (fejlesztéséért és üzemeltetéséért) felelős(ek). (Informatikai	A Pénzügyi, Gazdálkodási és Informatikai Főosztály vezetője	

KH szerepkör	Kód	Magyarázat	Hozzárendelt feladatkörök	Hozzárendelt személy(ek)
		főosztályvezető hiányában, több osztályvezető esetén az ügyrend és a beosztási okiratban meghatározott feladatok alapján oszlik meg a szerepkör.)		
IT infrastruktúra fejlesztésért felelős vezető	**IIFFV**	Informatikai infrastruktúrával kapcsolatos fejlesztésekért felelős szerepkör.	A Pénzügyi, Gazdálkodási és Informatikai Főosztály vezetője	
Alkalmazás fejlesztésért felelős vezető	**AFV**	Elektronikus információs rendszerekkel, alkalmazásokkal kapcsolatos fejlesztésekért felelős szerepkör.	A Pénzügyi, Gazdálkodási és Informatikai Főosztály vezetője	
IT üzemeltetésért felelős vezető	**IÜFV**	Informatikai infrastruktúra üzemszerű működtetéséért felelős szerepkör, az informatikai hibabejelentésekhez használható ügyfélszolgálat/helpdesk felelőse.	Az Informatikai Osztály vezetője	
Alkalmazás üzemeltetéséért felelős vezető	**AÜFV**	Információs rendszerek, alkalmazások üzembiztos működtetéséért felelős szerepkör.	Az Informatikai Osztály vezetője	
Alkalmazás támogatásért felelős vezető	**ATFV**	Információs rendszerekkel, alkalmazásokkal kapcsolatos ügyfélszolgálati/helpdesk feladatok felelőse.	Az Informatikai Osztály vezetője	
Határvédelmi rendszeradminisztrátor	**HVRA**	Határvédelmi megoldások és szolgáltatások üzemeltetésének felelőse, mely területtel kapcsolatosan a rendszergazdáknak feladatokat adhat.	Az Informatikai Osztály feladatkörében kijelölt foglalkoztatottja (informatikai referens)	
Vírusvédelmi rendszeradminisztrátor	**VRA**	Vírusvédelmi megoldások és szolgáltatások üzemeltetésének felelőse, mely területtel kapcsolatosan a rendszergazdáknak feladatokat adhat.	Az Informatikai Osztály feladatkörében kijelölt foglalkoztatottja (informatikai referens)	

KH szerepkör	Kód	Magyarázat	Hozzárendelt feladatkörök	Hozzárendelt személy(ek)
Mentésért felelős rendszeradminisztrátor	**MFRA**	Mentési megoldások és szolgáltatások üzemeltetésének felelőse, mely területtel kapcsolatosan a rendszergazdáknak feladatokat adhat.	Az Informatikai Osztály feladatkörében kijelölt foglalkoztatottja (informatikai referens)	
Tanúsítványokért felelős rendszeradminisztrátor	**TFRA**	Tanúsítványkezelési megoldások és szolgáltatások üzemeltetésének informatikus felelőse, mely területtel kapcsolatosan a rendszergazdáknak feladatokat adhat. A tanúsítványok igénylésével és szétosztásával kapcsolatos humánpolitikai feladatok ellátása.	Az Informatikai Osztály feladatkörében kijelölt foglalkoztatottja (informatikai referens); a Humánpolitikai Osztály feladatkörében kijelölt foglalkoztatottja (humánpolitikai referens)	
Patch menedzsment rendszeradminisztrátor	**PMRA**	Biztonsági frissítési megoldások és szolgáltatások üzemeltetésének felelőse, mely területtel kapcsolatosan a rendszergazdáknak feladatokat adhat.	Az Informatikai Osztály feladatkörében kijelölt foglalkoztatottja (informatikai referens)	
Adatbázis rendszeradminisztrátor	**ARA**	Adatbázis szolgáltatások üzemeltetésének felelőse, mely területtel kapcsolatosan a rendszergazdáknak feladatokat adhat.	Az Informatikai Osztály feladatkörében kijelölt foglalkoztatottja (informatikai referens)	
Hálózati rendszeradminisztrátor	**HRA**	Hálózati megoldások és szolgáltatások üzemeltetésének felelőse, mely területtel kapcsolatosan a rendszergazdáknak feladatokat adhat.	Az Informatikai Osztály feladatkörében kijelölt foglalkoztatottja (informatikai referens)	
Naplózásért felelős rendszeradminisztrátor	**NFRA**	Naplózási megoldások és szolgáltatások üzemeltetésének felelőse, mely területtel kapcsolatosan a rendszergazdáknak feladatokat adhat.	Az Informatikai Osztály feladatkörében kijelölt foglalkoztatottja (informatikai referens)	
Infrastruktúra üzemeltetési rendszergazdák	**IÜR**	Informatikai infrastruktúra üzemszerű működtetésében közreműködő szerepkörök.	Valamennyi informatikai referens	

KH szerepkör	Kód	Magyarázat	Hozzárendelt feladatkörök	Hozzárendelt személy(ek)
Alkalmazás támogató rendszergazdák	**ATRG**	Információs rendszerekkel, alkalmazásokkal kapcsolatos ügyfélszolgálati/helpdesk feladatokban közreműködő szerepkör.	Valamennyi informatikai referens	
Jogosultságkezelő adminisztrátor	**JGA**	Informatikai jogosultságok kezelésére szolgáló megoldások és szolgáltatások üzemeltetésének felelőse, mely területtel kapcsolatosan a rendszergazdáknak feladatokat adhat.	Valamennyi informatikai referens	
Naplóelemző	**NE**	Naplóesemények értékelését és elemzését megvalósító szerepkör.	Az Informatikai Osztály feladatkörében kijelölt foglalkoztatottja (informatikai referens)	
Fizikai védelemért felelős vezető	**FVFV**	Az elektronikus információbiztonság fizikai védelmét biztosító intézkedésekért felelős szerepkör.	A Beszerzési, Beruházási és Üzemeltetési Osztály vezetője	
Belső ellenőrzési szakterület vezető	**BESZV**	Az elektronikus információbiztonság működésének belső ellenőrzési feladatait ellátó felelős szerepkör.	A Belső Ellenőrzési Osztály vezetője	
Belső ellenőr	**BE**	Az elektronikus információbiztonság működésének belső ellenőrzési feladataiban közreműködő szakértő szerepkör.	A Belső Ellenőrzési Osztály valamennyi foglalkoztatottja	
Diszpécser	**DP**	A bejelentéseket a helpdesk alkalmazásban rögzíti.	Valamennyi informatikai referens	
Ügyfélszolgálati foglalkoztatott	**ÜSZM**	A helpdesk alkalmazásban rögzített informatikai igények és hibajegyek első vonalbeli kezelője.	Valamennyi informatikai referens	

KH szerepkör	Kód	Magyarázat	Hozzárendelt feladatkörök	Hozzárendelt személy(ek)
Humánpolitikai feladatok ellátásáért felelős szervezeti egység	**HSZE**	A szervezet információbiztonsággal kapcsolatos humánpolitikai feladatait ellátó szervezeti egység, úgymint nyilatkozatok adminisztrációja, kilépési és belépési folyamatok irányítása.	Jogi, Humánpolitikai és Koordinációs Főosztály Humánpolitikai Osztály	
Humánpolitikai feladatok ellátásáért felelős vezető	**HSZV**	A szervezet információbiztonsággal kapcsolatos humánpolitikai feladatainak ellátásáért felelős szerepkör.	A Humánpolitikai Osztály vezetője	
Alkalmazásfejlesztő	**AF**	Informatikai alkalmazások fejlesztési feladataiért felelős külső vagy belső szerepkör.	-	
Incidens menedzser	**IM**	A bejelentett hibajegyek szolgáltatás szint megállapodásokban (SLA vagy OLA) rögzített követelmények szerinti megoldásáért felelős szerepkör.	Valamennyi informatikai referens	
BC menedzser (Business Continuity - Üzletmenet Folytonosság)	**BCM**	Az üzletmenet folytonossági tervek kialakításáért, karbantartásáért, oktatásáért felelős szerepkör.	A Pénzügyi, Gazdálkodási és Informatikai Főosztály vezetője	
DR menedzser (Disaster Recovery - Katasztrófa utáni helyreállítás)	**DRM**	A katasztrófa utáni helyreállítási tervek kialakításáért, karbantartásáért, oktatásáért felelős szerepkör.	Az Informatikai Osztály vezetője	
Informatikai beszerzési referens	**IBR**	Informatikai tárgyú beszerzések adminisztratív (ajánlatkérés, szerződéskötés, számlázás) lebonyolításáért felelős szerepkör.	A Beszerzési, Beruházási és Üzemeltetési Osztály vezetője	
Projektvezető	**PV**	Projektszerű informatikai fejlesztések esetén kinevezett felelős, aki fejlesztés lebonyolításának egyszemélyes felelőse.	A Pénzügyi, Gazdálkodási és Informatikai Főosztály vezetője	

KH szerepkör	Kód	Magyarázat	Hozzárendelt feladatkörök	Hozzárendelt személy(ek)
Tűzvédelmi felelős	**TVF**	A tűzvédelmi feladatok ellátásában közreműködő és azokat koordináló szerepkör.	A Humánpolitikai Osztály feladatkörében kijelölt foglalkoztatottja (munka- és tűzvédelmi referens)	
Munkavédelmi felelős	**MVF**	A munkavédelmi feladatok ellátásában közreműködő és azokat koordináló szerepkör.	A Humánpolitikai Osztály feladatkörében kijelölt foglalkoztatottja (munka- és tűzvédelmi referens)	

2. számú melléklet
7/2025. (VII. 9.) főispáni utasításhoz

A kormányhivatal eljárásrendjei

Ssz.	Eljárásrend neve
	Hozzáférés-felügyeleti eljárásrend
	Tudatossági és képzési eljárásrend
	Naplózási és elszámoltathatósági eljárásrend
	Biztonságértékelési eljárásrend
	Konfigurációkezelési eljárásrend
	Üzletmenet-folytonosságra vonatkozó eljárásrend
	Üzletmenet-folytonossági tervek (Valamennyi EIR-re vonatkozóan)
	Azonosítási és hitelesítési eljárásrend
	Biztonsági eseménykezelési eljárásrend
	Karbantartási eljárásrend
	Adathordozók védelmére vonatkozó eljárásrend
	Fizikai és környezeti védelemre vonatkozó eljárásrend
	Biztonságtervezési eljárásrend
	Személyi biztonságra vonatkozó eljárásrend
	Kockázatelemzési és kockázatkezelési eljárásrend
	Informatikai beszerzési eljárásrend
	Rendszer- és kommunikációvédelmi eljárásrend
	Rendszer- és információsértetlenségi eljárásrend
	Ellátási láncra vonatkozó kockázatelemzési és kockázatkezelési eljárásrend

3. számú melléklet
7/2025. (VII. 9.) főispáni utasításhoz

A kormányhivatal rendelkezésében lévő elektronikus információs rendszerek

Elektronikus információs rendszer rövid neve (ha van)	**Elektronikus információs rendszer leírása, tartalmazott rendszer neve**	**Elvárt biztonsági osztály**
Fájlmegosztás, intranet	A kormányhivatal napi, funkcionális feladatellátást támogató állományok tárolására alkalmazott szerver tárterületek, intranet felületek.	Alap

4. számú melléklet
7/2025. (VII. 9.) főispáni utasításhoz

A kormányhivatal által használt központi rendszerek

Rendszer neve:	Szakrendszer/ Funkcionális alkalmazás/ Szakmai feladatellátást támogató alkalmazás	Megjegyzés	Pontosítás, Információ (link, szakterület, funkció)

5. számú melléklet
7/2025. (VII. 9.) főispáni utasításhoz

A kormányhivatal által igénybe vett, központi szolgáltató által biztosított szolgáltatások és támogató rendszerek

Szolgáltatás, támogató rendszer neve:	Szolgáltatás, támogató rendszer rövid leírása	Megjegyzés	Pontosítás, Információ (link, szakterület, funkció)

6. számú melléklet
7/2025. (VII. 9.) főispáni utasításhoz

A kormányhivatal rendelkezésében lévő vagy a kormányhivatal által használt egyéb támogató rendszerek

EIR csoport megnevezése	Üzemeltető	Adatgazda	Rövid leírás
Beléptető rendszerek	Informatikai üzemeltetésért felelős szervezeti egység	Kormányhivatal	A kormányhivatal meghatározott telephelyein az elzárt infrastruktúra elemeket tartalmazó helyiségek szabályozott és naplózott beléptetést biztosító rendszere.
Kamerás megfigyelő rendszerek	Informatikai üzemeltetésért felelős szervezeti egység	Kormányhivatal	A kormányhivatal meghatározott telephelyein az elzárt infrastruktúra elemek védelme érdekében képrögzítést biztosító rendszer.

7. számú melléklet[3]
7/2025. (VII. 9.) főispáni utasításhoz

Az IBF személye és elérhetősége

Az IBF neve	Az IBF e-mail elérhetősége	Az IBF telefonos elérhetősége
Boda Melinda	boda.melinda@freemail.hu	+36202143955

[3] Módosította az 1/2026. (I. 19.) főispáni utasítás 3. §-a. Hatályos 2026. 01. 20-tól

8. számú melléklet
7/2025. (VII. 9.) főispáni utasításhoz

	Jogosultság igénylési, módosítási, megszüntetési űrlap			
IGÉNYLŐ ADATAI:				
Neve:		e-mail címe:		
Szervezeti egysége:				
Feladatköre / vezetői szintje:				
Jogosultság adatai(aláhúzandó)**:**	**Változás dátuma: 20……...év …….. hó …….. nap**			
Oka: (aláhúzandó)	jogviszony megszűnése	tartós távollét	álláshely-váltás	feladatkör változása
Jellege: (aláhúzandó)	igénylés	törlés	módosítás	
Tartama: (aláhúzandó)	állandó	ideiglenes, lejárat dátuma: 20 év	hó	nap

KÖZVETLEN VEZETŐ TÖLTI KI
(kormánytisztviselő esetén osztályvezető, osztályvezető esetén főosztályvezető/hivatalvezető)

IGÉNY PONTOS LEÍRÁSA ÉS INDOKLÁSA

Név: …….. ……..……., Dátum: 20 év hó nap vagy időbélyegző szerint	_____ aláírás

ADATGAZDA TÖLTI KI
(hivatalvezető vagy a főispán által közvetlenül vezetett önálló szervezeti egység vezetője, akkor is ki kell tölteni, ha azonos a közvetlen vezetővel.)

Neve: ..... ……..……., Dátum: 20 év hó nap vagy időbélyegző szerint	_____ aláírás

INFORMATIKAI OSZTÁLY TÖLTI KI
(amennyiben szakmai engedélyezés szükséges)

Neve: ..... Szakmai szempontból engedélyezem / nem engedélyezem. ……..……., Dátum: 20 év hó nap vagy időbélyegző szerint	_____ osztályvezető

Kérjük megjelölni, hogy az igénylőlap összesen hány oldalas: ……

	Jogosultság igénylési, módosítási, megszüntetési űrlap	
ELEKTRONIKUS IRATKEZELŐ RENDSZER (POSZEIDON) JOGOSULTSÁG IGÉNY		
Egyetlen szervezeti egységhez köthető szerepkörök (aláhúzandó)		
Közvetlen vezető	*Ügykezelő*	*Kiemelt ügykezelő*
Ügyintéző I.	*Ügyintéző II.*	*Ügyintéző III.*
Nem szervezeti egységhez köthető szerepkörök (aláhúzandó)		
Vezető I.	*Lekérdező I.*	*Lekérdező II.*
WEB-es elérésű felület jogosultságai (vékony kliensű iktatás, workflow)(aláhúzandó)		
Közvetlen vezető	*iktató-ügyintéző (partner rögzítő)*	
Iktatókönyvek és egyéb igények felsorolása:		
HIVATALI KAPU HOZZÁFÉRÉS IGÉNY		
Születési név: …….	Születési hely: …….	
Anyja neve: …….	Idő: ……..….	
EGYÉB JOGOSULTSÁG, SZOFTVER, MAPPA VAGY ESZKÖZ IGÉNYLÉS		
SZ(Szoftver), M(Mappa), E(Eszköz)	Megnevezés / Leírás / Útvonal	hozzáférési szint / egyéb

9. számú melléklet
7/2025. (VII. 9.) főispáni utasításhoz

Veszprém Vármegyei Kormányhivatal
Rendszerbiztonsági terv a
… rendszerhez

Verzió:
Dátum:

A DOKUMENTUM ADATAI

Cím	<Rendszer neve> rendszerbiztonsági terve
Leírás	A rendszer műszaki felépítésének, paramétereinek, szervezeti és technológiai környezetének bemutatása, biztonsági osztályának meghatározása és a rendszerrel kapcsolatos védelmi intézkedések megvalósításának leírása.

VÁLTOZATOK

Kiadás dátuma	Szerző	Verzió	Leírás
2025.XX.XX		1.0	Első változat

[*Jelen dokumentum egy sablon, amely a rendszerbiztonsági tervhez kapcsolódó alapkövetelményeket határozza meg, annak fejezeteit rögzíti, és rövid tartalommal segíti az egyes fejezetekhez kapcsolódó elvárások körvonalazását. A [ ] zárójelek közötti útmutató részek a sablon kitöltésekor törölhetők.*]

1 Bevezetés

1.1 A dokumentum célja

Ez a rendszerbiztonsági terv áttekintést nyújt a <Rendszer neve> biztonsági követelményeiről, és ismerteti a rendszer által továbbítandó, feldolgozandó vagy tárolandó adatoknak megfelelő biztonsági elvárások biztosítása érdekében alkalmazott, vagy tervezett védelmi intézkedéseket és ellenőrzéseket. A rendszerbiztonsági terv meghatározza továbbá a rendszerhez hozzáférő valamennyi személy felelősségét és elvárt viselkedését.

Jelen rendszerbiztonsági terv célja

- megfelelő, költséghatékony biztonsági védelem kialakításának elősegítése a rendszerek fejlesztési szakaszában, illetve a rendszer életciklusának további fázisaiban a biztonsági ellenőrzések értékelésével és a vezetőség által adott felhatalmazás dokumentálásával,
- a biztonsági tevékenységek következetes végrehajtásának és személyi változások esetén történő fenntartásának támogatása,
- a biztonsági követelményeknek való megfelelés támogatása,
- a biztonsági intézkedések minőségbiztosításának támogatása.

1.2 Fogalmak és rövidítések definíciója

A dokumentumban használt rövidítések jelentését az alábbi táblázat tartalmazza.

[A vegye fel a további magyarázatot igénylő, a dokumentumban használt rövidítéseket és fogalmakat!]

Fogalom	Meghatározás

2 A rendszer átfogó ismertetése

2.1 Megnevezés

Rendszer megnevezése	
Rendszer egyedi azonosítója	

2.2 A rendszer célja, hatóköre

[Adjon rövid (egy-három bekezdéses) leírást a rendszer funkciójáról/céljáról.
Ha a rendszer általános támogatási rendszer, sorolja fel az általa támogatott összes alkalmazást. Írja le az egyes alkalmazások funkcióját és a feldolgozott információkat.]

2.3 A rendszer alapfeladatait biztosító modulok

Az <Rendszer neve> az alábbi főbb funkciókat valósítja meg az egyes moduljain keresztül. Az alábbi táblázat az információs rendszer moduljait sorolja fel:

Modul megnevezése	A modul célja, fő funkciói

2.4 A rendszer jelenlegi státusza

[A rendszer működési állapotára vonatkozóan a következők közül egyet vagy többet jelezzen. Ha egynél több állapot van kiválasztva, sorolja fel, hogy az egyes állapotok a rendszer mely részeire vonatkoznak.]
A rendszer jelenleg a következő táblázatban feltüntetett életciklus-fázisban van.

A rendszer jelenlegi státusza		
☒	Üzemel	A rendszer élesüzemi használatban van
☐	Fejlesztés alatt	A rendszer tervezése, fejlesztése vagy bevezetése folyamatban van.
☐	Jelentős változtatás alatt	A rendszer jelentős változás, fejlesztés vagy átalakítás alatt áll.
☐	Egyéb	Kérjük írja le részeletesen a fázist:

2.5 A rendszer típusa

Azok a rendszerek, alkalmazások, amelyek az általuk tartalmazott, feldolgozott, tárolt vagy továbbított információk miatt, vagy az szervezet küldetése szempontjából kiemelt fontosságúak, különleges irányítási felügyeletet igényelnek fő alkalmazásnak tekinthetők. A fő alkalmazások olyan rendszerek, amelyek egyértelműen meghatározott funkciókat látnak el, és amelyeknél a biztonsági megfontolások és igények könnyen azonosíthatók (pl. pénzügyi tranzakciók kezelése). Egy fő alkalmazás számos egyedi programból, valamint hardver-, szoftver- és távközlési komponensből állhat.
Az általános támogató rendszer közös funkciókkal rendelkező azonos közvetlen irányítás alatt álló informatikai erőforrások összekapcsolt halmaza. Ilyenek lehetnek a közösen használt feldolgozó infrastruktúra beleértve annak operációs rendszerét és segédprogramjait is, valamint a kommunikációs hálózat. Egy fő alkalmazást futtathat egy általános támogató rendszer. Az általános támogató rendszer rendszerbiztonsági terve ilyen esetben referenciaként szolgálhat a fő alkalmazási rendszer biztonsági tervében. Egy általános támogató rendszer akkor tekinthető fő alkalmazásnak, ha különleges vezetői figyelmet igényel, magasak a fejlesztési, üzemeltetési vagy karbantartási költségei; és az általa kezelt adatok jelentős szerepet játszanak az szervezeti működésben.
[Jelölje meg, hogy a rendszer egy fő alkalmazás vagy egy általános támogató rendszer. Ha a rendszer kisebb alkalmazásokat is tartalmaz, azokat a 2.1 pontban kell felsorolni.]

☒ Főalkalmazás ☐ Általános támogató rendszer

3 Szervezeti feladatok és felelősségek elhatárolása

[*A Rendszerrel kapcsolatosan nem alkalmazható szerepkörök törölhetők a felsorolásokból, illetve szükség esetén a lista bővíthető*]

3.1 Engedélyezésért felelős vezető

Az engedélyezésért felelős vezető a szervezeti felsővezetés azon tagja, aki jogosult hivatalosan felelősséget vállalni egy információs rendszer a szervezet számára elfogadható kockázati szinten történő működtetéséért a szervezeti működés, a vagyonelemek vagy a személyek tekintetében.
Az engedélyezésért felelő vezetőnek a rendszerbiztonsági tervekkel kapcsolatban a következő feladatai vannak:

- jóváhagyja a rendszerbiztonsági terveket,
- engedélyezi az információs rendszer üzembehelyezését és működtetését, esetleg (felvállalható) kockázatok felvállalása mellett engedélyezi az üzembehelyezést, vagy
- megtagadja az információs rendszer üzemeltetésének engedélyezését (vagy ha a rendszer már működik, leállítja az üzemeltetését), ha elfogadhatatlan biztonsági kockázatok állnak fenn.

Név	
Beosztás	
Szervezeti egység	
Telefonszám	
Email	

3.2 Rendszertulajdonos

A rendszertulajdonos az információs rendszer beszerzéséért, fejlesztéséért, integrálásáért, módosításáért, üzemeltetéséért és karbantartásáért teljeskörűen felelős szervezeti tisztségviselő.
A rendszer tulajdonosa a rendszerbiztonsági tervekkel kapcsolatban a következő felelősséggel rendelkezik:

- kidolgozza a rendszerbiztonsági tervet az adatgazdákkal, az információbiztonsági felelőssel, a rendszergazdával és a kulcsfelhasználókkal együttműködve,
- biztosítja a rendszerbiztonsági terv karbantartását, és hogy a rendszert az elfogadott biztonsági követelményeknek megfelelően telepítik és üzemeltetik,
- biztosítja, hogy a rendszer felhasználói és a támogató személyzet megkapják a szükséges biztonsági képzést (pl. a viselkedési szabályokra vonatkozó oktatás).

a)

Név	
Beosztás	
Szervezeti egység	
Telefonszám	
Email	

3.3 Adatgazda

Az adatgazda a szervezet olyan tisztviselője, aki jogszabályi vagy műszaki szempontú rendelkezési jogkörrel rendelkezik az érintett adatokkal kapcsolatban és felelős az információk létrehozásának, begyűjtésének, feldolgozásának, terjesztésének és megsemmisítésének ellenőrzéséért.
Az adatgazda rendszerbiztonsági tervekhez kapcsolódó feladatai a következőket jelentik:

- meghatározza az adatok megfelelő használatára és védelmére vonatkozó szabályokat,
- biztosítja a biztonsági követelményekre és a védelmi intézkedésekre vonatkozó információkat a rendszertulajdonos számára,
- eldönti, hogy kinek lehet hozzáférése az információs rendszerhez, és milyen típusú jogosultságok vagy hozzáférési jogok kerüljenek meghatározásra,
- támogatja a rendszerrel kapcsolatos védelmi intézkedések azonosítását és értékelését.

[Amennyiben a rendszernek több adatgazdája van, mindegyiket fel kell sorolni az irányítása alá tartozó adatkörökkel együtt. Ilyen esetben adatgazdánkként egy táblázatot kell kitölteni]

Adatkörök	pl. számlázási adatok, vevő/ügyféladatok, termékadatok
Név	
Beosztás	
Szervezeti egység	
Telefonszám	
Email	

3.4 Informatikai vezető

Az informatikai vezető az szervezet szintjén felelős az információ biztonsági program kialakításáért és fenntartásáért, illetve a következő biztonság tervezési felelősségekkel rendelkezik:

- kijelöli a rendszer biztonságtervezési felelősét,
- biztosítja a rendszerbiztonság tervezésének kezelésére vonatkozó szabályzatok, eljárások és ellenőrzési módszerek kialakítását és karbantartását,
- biztosítja az általános, minden rendszerre érvényes védelmi intézkedések azonosítását, megvalósítását, értékelését és folyamatos fejlesztését,
- biztosítja a rendszerbiztonsági tervekkel kapcsolatosan felelősséggel rendelkező személyek képzését,
- támogatja a szervezet vezetőit a rendszer biztonsági terveivel kapcsolatos felelősségük ellátásában.

Név	
Beosztás	
Szervezeti egység	
Telefonszám	
Email	

3.5 Információbiztonsági felelős

Az információbiztonsági felelős az a személy, aki a szervezeten belül felelős a szervezet információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséért és fenntartásáért, és elvégzi vagy irányítja ezen tevékenységek tervezését, szervezését, koordinálását és ellenőrzését.
Az információbiztonsági felelős feladatai a rendszerbiztonsági tervezéssel kapcsolatban:

- átveszi az informatikai vezető felelősségét a rendszerek biztonsági tervezésével kapcsolatban,
- a rendszerbiztonsági tervek kialakításának, felülvizsgálatának és elfogadásának összehangolása az információs rendszer tulajdonosaival és az engedélyező vezetővel,
- az általános biztonsági ellenőrzések azonosításának, végrehajtásának és értékelésének összehangolása,
- a rendszerbiztonsági tervek kialakításához és felülvizsgálathoz szükséges szakmai kompetenciák kialakításának, fejlesztésének támogatása vagy oktatása.

b)

Név	
Beosztás	
Szervezeti egység	
Telefonszám	
Email	

3.6 Üzemeltetésbiztonsági felelős

Az üzemeltetésbiztonsági felelős olyan személy, akit a megfelelő jogkörrel rendelkező vezető (pl. informatikai vezető, rendszertulajdonos, információbiztonsági felelős) jelöl ki annak biztosítása érdekében, hogy a megfelelő üzemeltetésbiztonsági tevékenységeket végrehajtsák és folyamatosan fenntartsák az üzemeltetés biztonságát.
Az üzemeltetésbiztonsági felelős feladatai a biztonságtervezéssel kapcsolatban a következők:

- segítségnyújtás az információbiztonsági felelősnek a közös biztonsági ellenőrzések meghatározásában, végrehajtásában és értékelésében,
- a rendszerbiztonsági terv fejlesztésének és karbantartásának aktív támogatása, a rendszerváltoztatások összehangolása az információs rendszer tulajdonosával és a változtatások biztonsági hatásának felmérése.

Név	
Beosztás	
Szervezeti egység	
Telefonszám	
Email	

3.7 Rendszer üzemeltetési felelősségek

Üzemeltetési feladat	Szervezeti egység/személyek
Alkalmazásüzemeltetés	

Szerver operációs rendszer üzemeltetés	
Hardver infrastruktúra	
Hálózatüzemeltetés	
Adatközponti infrastruktúra elemek üzemeltetése	
Rendszerfelügyelet	

3.8 Végfelhasználók és privilegizált felhasználók száma

[Az alábbi táblázatban adja meg a rendszer felhasználóinak és rendszergazdáinak hozzávetőleges számát. Tartalmazza az összes privilegizált hozzáféréssel rendelkező személyt, például rendszergazdákat, adatbázis-adminisztrátorokat, alkalmazás-adminisztrátorokat stb. Szükség szerint adjon hozzá sorokat a különböző szerepkörök meghatározásához. Itt érdemes feltüntetni a technikai felhasználókat is, különösen, azokat, amelyek privilegizált jogosultságokkal is rendelkeznek, vagy a rendszer működése, üzemeltetése szempontjából nélkülözhetetlenek, alapértelmezettek.]

Az alábbi táblázat <Rendszer neve> felhasználóinak hozzávetőleges számát mutatja.

Szerep	Külső/belső	Privilégiumok és betöltött szerepkörök	Felhasználószám
pl. Rendszergazda	Belső	Adatbázis adminisztrátor	5
pl. Felhasználó	Külső/Belső	Felhasználó	100

4 Biztonsági osztályba sorolás

4.1 A rendszer által kezelt és tárolt adatok osztályozása

[Az alábbiakban megadott adatosztályozási módszertan, amelynek részleteit a 418/2024. (XII. 23.) Korm. rendelet 1. melléklete írja le, a Kiberbiztonsági tv. 9. § (1) és (2) bekezdésben meghatározott szervezetek számára kötelező az ott előírt esetekben, a többi szervezet számára opcionális.]

Az elektronikus információs rendszer által kezelt, vagy feldolgozott adatokat az alábbi táblázat foglalja össze. A táblázatban szerepeltetni kell a rendszer által kezelt összes adatkört. A kezelés alatt értendő az adatok keletkezése, feldolgozása, megjelenítése, átadása és tárolása is. A táblázat egyes mezőit az alábbiak szerint kell kitölteni:

- **Adatcsoport megnevezése**: az adatkör megnevezése.
- **Kezelt adatok fajtája**: az adott adatkört kezelő rendszer modul(ok) neve/azonosítója. Minden olyan modult fel kell sorolni, ahol az adott adatkör adatai keletkeznek, tárolódnak, feldolgozásra kerülnek.
- **Bizalmasság szerinti besorolás**: 418/2024. (XII. 23.) Korm. rendelet 1. melléklet 2. pont szerint
- **Sértetlenség és rendelkezésre állás szerinti besorolás**: 418/2024. (XII. 23.) Korm. rendelet 1. melléklet 3. pont szerint.
- **Adatosztályozás eredménye:** 418/2024. (XII. 23.) Korm. rendelet 1. melléklet 4. pont szerint.
-

Adatcsoport megnevezése	Kezelt adatok fajtája	Bizalmasság szerinti besorolás	Sértetlenség és rendelkezésre állás szerinti besorolás	Adatosztályozás eredménye
		[B1; B2; B3; B4]	*[SR1; SR2]*	*[F1; F2; F3; F4]*

4.2 A rendszer biztonsági osztálya

Szervezet elvégezte a Rendszer által kezelt vagy feldolgozott adatok azonosítását, a releváns fenyegetettségek meghatározását és ehhez kapcsolódóan a lehetséges kárértékek beazonosítását. A biztonsági osztályba sorolás 7/2024. (VI. 24.) MK rendelet szerinti szempontrendszerét az alábbi táblázat mutatja.

[*Kérjük tegyen X-et a táblázat Igen/Nem oszlopaiba, attól függően, hogy az adott sorban igaz (Igen) vagy hamis (Nem) a rendszerre vonatkozó állítás.]*

Pont.	Besorolási kritérium	Igen	Nem
2.2.2.1.	az elektronikus információs rendszerben jogszabály által nem védett adat vagy legfeljebb kis mennyiségű személyes adat sérülhet		
2.2.2.2.	a szervezet üzleti vagy ügymenete szempontjából csekély értékű, vagy csak belső (szervezeti) szabályzóval védett adat vagy rendszer sérülhet		
2.2.2.3.	a lehetséges társadalmi-politikai hatás a szervezeten belül kezelhető		
2.2.2.4.	a közvetlen és közvetett anyagi kár a szervezet éves költségvetésének vagy nettó árbevételének 1%-át nem haladja meg		
2.2.3.1.	nagy mennyiségű személyes adat, illetve különleges személyes adat sérülhet		
2.2.3.2.	személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket)		
2.2.3.3.	a szervezet üzleti vagy ügymenete szempontjából érzékeny folyamatokat kezelő rendszer, információt képező adat vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat sérülhet		
2.2.3.4.	a káresemény lehetséges társadalmi-politikai hatásai a szervezettel szemben bizalomvesztést eredményezhetnek, a jogszabályok betartása vagy végrehajtása elmaradhat, vagy a szervezet vezetésében személyi felelősségre vonást kell alkalmazni		
2.2.3.5.	a közvetlen és közvetett anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 1%-át, de nem haladja meg annak 10%-át		
2.2.4.1.	különleges személyes adat nagy mennyiségben sérülhet		
2.2.4.2.	emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be		
2.2.4.3.	nemzeti adatvagyon helyreállíthatatlanul megsérülhet		

2.2.4.4.	az ország, a társadalom működőképességének fenntartását biztosító kritikus infrastruktúra rendelkezésre állása nem biztosított		
2.2.4.5.	a szervezet üzleti vagy ügymenete szempontjából nagy értékű, üzleti titkot vagy különösen érzékeny folyamatokat kezelő rendszer vagy információt képező adat tömegesen vagy jelentősen sérülhet		
2.2.4.6.	súlyos bizalomvesztés állhat elő a szervezettel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok is sérülhetnek		
2.2.4.7.	a közvetlen és közvetett anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 10%-át		

[Amennyiben a szervezet a fentitől eltérő módszert alkalmaz a biztonsági osztályba sorolásra, akkor kérjük írja le a besorolás módszerét! *Az alábbiakban adja meg az előzetes biztonsági osztályba sorolás eredményét.]*

	<Rendszer neve> biztonsági osztálya
A rendszer biztonsági osztálya	***[Alap; Jelentős; Magas]***

5 A <Rendszer neve> műszaki megoldásainak bemutatása

Ez a fejezet a rendszert olyan mélységben ismerteti, ami a rendszerrel kapcsolatos védelmi szabályozások és folyamatok megértéséhez szükséges. Az alábbi alfejezetek mellett további információk is szerepeltethetők.

5.1 A <Rendszer neve> főbb elemei és adatkapcsolatai

5.1.1 A rendszer főbb moduljai, alrendszerei

A rendszer modul, alrendszer az információs rendszer olyan fő egysége vagy összetevője, amely egy vagy több konkrét funkciót lát el.

Rendszer modul /alrendszer megnevezése	Funkció

5.1.2 Rendszer környezete és határai

5.2 Rendszer logikai felépítésének bemutatása

[Ebben a fejezetben adjon részletes topológiai leírást és ábrát, amely világosan ábrázolja a rendszer határait, a rendszer összeköttetéseit és a kulcsfontosságú eszközöket. (Megjegyzés: ehhez nem kell minden munkaállomást vagy asztali számítógépet ábrázolni, de minden egyes használt operációs rendszerhez, a hordozható komponensekhez (ha van ilyen), az összes virtuális és fizikai szerverhez (pl. fájl, nyomtatás, web, adatbázis, alkalmazás), valamint a hálózatba kapcsolt munkaállomásokhoz tűzfalakhoz, útválasztókhoz, kapcsolókhoz, másolókhoz, nyomtatókhoz, laboreszközökhöz, kézi számítógépekhez tartozik egy példány.) Ha a diagramon más rendszerek olyan komponenseit is fel kell tüntetni, amelyek összekapcsolódnak/interfésznek ezzel a rendszerrel, akkor a rendszerhatárokat a biztonsági tervekre vagy a többi rendszer(ek) nevére és tulajdonosára való hivatkozással kell jelölni a diagramon.]

5.2.1 A rendszer topológiája

[Az alábbiakban illesszen be egy rendszertopológia ábrát! Adjon az ábrával összhangban lévő leírást, amely egyértelműen felsorolja és leírja az egyes rendszerelemeket!]

5.2.2 A rendszer hardver környezetének összefoglaló bemutatása

[Írja le a rendszert kiszolgáló hardver elemeket vagy hivatkozásként adja meg a rendszerelemek nyilvántartásának helyét!]

5.2.3 A rendszer szoftver környezetének összefoglaló bemutatása

[Írja le vagy hivatkozzon az összes szoftver (rendszerszoftver és alkalmazási szoftver) komponens teljes és pontos felsorolására, beleértve a gyártmányt/OEM-et, modellt, verziót, szervizcsomagokat!]

Hoszt	Funkció	Verzió	Patch szint	IP cím	Virtualizált (Igen / Nem)
	Operációs rendszer	Windows Server 2022		255.255.255.255	Igen
	IIS	ASP .Net 4.5		255.255.255.255	Igen
	Alkalmazás			255.255.255.255	Igen
	Database SQL Server	MS SQL 2016		123.45.678	Igen

5.2.4 A rendszer kapcsolatainak összefoglaló bemutatása

[Sorolja fel az összekapcsolt rendszereket és rendszerazonosítókat (adott esetben), adja meg a rendszert, a nevet, a szervezetet, a rendszer típusát (fő alkalmazás vagy általános támogató rendszer)!]

Megnevezés	**Forrás rendszer**	**Cél rendszer**	**Interfész technológia típus**	**Interfész funkcionalitás összefoglaló leírása**

5.3 Portok, protokollok és szolgáltatások

Portok (TCP/UDP)	**Protokollok**	**Szolgáltatások**	**Szolgáltatás kliens**

5.4 A rendszer fizikai környezete

[Ismertesse az egyes rendszerelemek fizikai elhelyezését, a fizikai környezet védelem jellemzőit. Ide tartozik például a szerverek elhelyezése, a géptermek megközelíthetősége, beléptető rendszere, videokamerás megfigyelése stb.]

6 Alapvető biztonsági események meghatározása

[Kérjük sorolja fel a rendszer szempontjából releváns biztonsági eseményeket és azok azonosítási és felügyeleti megoldását! Releváns események lehetnek pl.:

- *Felhasználói bejelentkezések és kijelentkezések*
- *Rendszerkonfiguráció változások*
- *Hozzáférési kísérletek (sikertelen bejelentkezések, jogosulatlan hozzáférési kísérletek, például sikertelen fájlhozzáférések vagy adatbázis-lekérdezések)*
- *Rendszerhibák és figyelmeztetések*
- *Hálózati forgalom anomália (szokatlan vagy gyanús hálózati tevékenységek, például nagy mennyiségű adatforgalom vagy ismeretlen IP-címekről érkező kérések)*
- *Adatmanipuláció (adatok létrehozása, módosítása vagy törlése, különösen érzékeny vagy bizalmas adatok esetén)*
- *Fájlhozzáférések (pl. rendszerfájlok, érzékeny dokumentumok)*
- *Felhasználói jogosultságok módosítása*
- *Rendszerindítások és leállások]*

7 Kapcsolódó dokumentumok

7.1 Kapcsolódó jogszabályok, megfelelés elvárások

[Sorolja fel azokat a jogszabályokat vagy rendeleteket, amelyek a rendszerben lévő adatok bizalmasságára, sértetlenségére vagy rendelkezésre állására vonatkozó különleges követelményeket állapítanak meg!]

Dokumentum címe	Típusa	Kiadás dátuma

7.2 Kapcsolódó szabályzatok és dokumentumok

[Sorolja fel azokat a szervezeti dokumentumokat, amelyek a rendszer tervezési, implementációs vagy üzemeltetési fázisában meghatározza a rendszerrel kapcsolatos viselkedési szabályokat!]

Dokumentum címe	Típusa	Kiadás dátuma

8 Védelmi intézkedések megvalósítása

[A Rendszer kialakítása és üzembehelyezése során implementálni kell a biztonsági osztályhoz tartozó, 7/24 (VI. 24.) MK rendelet védelmi intézkedés katalógusban meghatározott, a rendszer biztonsági osztályához tartozó követelményeket.]

Az elektronikus információs rendszerre vonatkozó biztonsági elvárások meghatározásának célja az elektronikus információs rendszer és az általa kezelt adatok kockázatokkal arányos védelmének kialakítása, a jogosulatlan hozzáférés elkerülése, az elvárt rendelkezésre állási követelmények teljesítése.

Ez a szakasz a rendszer biztonsági osztályához tartozó 7/24 (VI. 24.) MK rendelet 2. melléklet szerinti védelmi intézkedés katalógusban meghatározott minimálisan elvárt védelmi intézkedéseket

tartalmazza. Eltérő rendelkezés hiányában minden egyes védelmi intézkedés esetében az információs rendszer tulajdonosa felelős az védelmi intézkedések megvalósításáért. A jogszabály által meghatározott védelmi intézkedésektől való egyedi eltéréseket indokolni kell.

[Az alábbi védelmi intézkedések kiegészítése szükséges abban az esetben, ha a 7/24 (VI. 24.) MK rendelet 2. melléklet szerinti kiegészítő kontrollok, vagy egyéb intézkedések alkalmazását a szervezet, akár helyettesítő intézkedésként, akár más okból szükségesnek ítéli meg.]

[Az egyes követelményeknél szükséges megadni, hogy általános, rendszer specifikus, hibrid követelményről van-e szó. Általános követelményről döntően akkor beszélünk, ha követelmény szervezeti szintű és a megvalósítása alapvetően szervezeti feladatként jelentkezik. Rendszerspecifikus a követelmény, ha alapvetően az érintett rendszerre vonatkozik és a megvalósítása fejlesztői feladat. A követelmény akkor hibrid, ha a megvalósításban szerepe van vagy lehet a szervezetnek és a fejlesztőnek egyaránt. Nem alkalmazható követelményről akkor beszélhetünk, ha az adott követelményt valamilyen oknál fogva teljességgel kizárjuk az érintett rendszer kapcsán (pl. a biometrikus azonosításra vonatkozó követelményt kizárhatjuk, ha a rendszerben ilyen típusú azonosítási/hitelesítési eljárást nem alkalmazunk)]

8.1 HOZZÁFÉRÉS-FELÜGYELET

8.1.1 Szabályzat és eljárásrendek

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	2.1.

A szervezet:

Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint

- a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó hozzáférés-felügyeleti szabályzatot, amely

- meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá

- összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.

- a hozzáférés-felügyeleti eljárásrendet, amely a hozzáférés-felügyeleti szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

Kijelöl egy, a szervezet által meghatározott személyt, aki a hozzáférés-felügyeleti szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.

Felülvizsgálja és frissíti az aktuális hozzáférés-felügyeleti szabályzatot, a hozzáférés-felügyeleti eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.

A védelmi intézkedés státusza (csak egy választható):
☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.1.2 Fiókkezelés

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	2.2.

A szervezet:

Meghatározza és dokumentálja a rendszerben engedélyezett és kifejezetten tiltott fióktípusokat.

Kijelöli a fiókkezelőket.

Kialakítja a csoport- és szerepkör tagsági feltételeket és kritériumokat.

Meghatározza:

- a rendszerben engedélyezett felhasználókat. - a csoport- és szerepkör tagságokat. - a hozzáférési jogosultságokat és a felhasználói fiókokhoz tartozó szükséges jellemzőket minden egyes felhasználói fiókra. A meghatározott szerepköröket betöltő személyek jóváhagyását kéri a felhasználói fiókok létrehozására vonatkozó kérelmek esetén. Létrehozza, engedélyezi, módosítja, letiltja és törli a fiókokat a meghatározott irányelvek, eljárások, előfeltételek és kritériumok alapján. Nyomon követi a fiókok használatát. Értesíti a fiókkezelőket és a meghatározott személyeket vagy szerepköröket a következő esetekben: - meghatározott időn belül, amikor a fiókok már nem szükségesek. - meghatározott időn belül, amikor a felhasználók jogviszonya megszűnik. - meghatározott időn belül, amikor a rendszerhasználat vagy az egyén számára szükséges ismeretek megváltoznak. Engedélyezi a rendszerhez való hozzáférést a következők alapján: - érvényes hozzáférési engedély; - tervezett rendszerhasználat; - egyéb, a szervezet által meghatározott jellemzők. Ellenőrzi a felhasználói fiókokat a fiókkezelési követelmények betartása szempontjából, a meghatározott gyakorisággal. Létrehoz és végrehajt egy folyamatot a megosztott vagy csoport felhasználói fiókok hitelesítési adatainak megváltoztatására az egyének csoportból történő eltávolításának esetére. Összehangolja a fiókkezelési folyamatokat a felhasználók jogviszonyának megszűntetési folyamataival.
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva
Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.1.3 Hozzáférési szabályok érvényesítése

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	2.15.
Az EIR a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott logikai hozzáférési jogosultságokat az információkhoz és a rendszer erőforrásaihoz.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.1.4 Sikertelen bejelentkezési kísérletek

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	2.71.
A szervezet: Az általa meghatározott esetszám korlátot alkalmazza a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire. EIR-je automatikusan zárolja a felhasználói fiókot vagy csomópontot a meghatározott időtartamra, vagy ameddig a rendszergazda fel nem oldja annak zárolását, vagy késlelteti a következő bejelentkezési lehetőséget a meghatározott algoritmus szerint. Továbbá értesíti a rendszergazdát, ha a sikertelen próbálkozások maximális számát túllépték.		
A védelmi intézkedés státusza (csak egy választható):		

☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva
Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.1.5 A rendszerhasználat jelzése

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	2.75.1.

Az EIR a rendszer használata előtt megjelenít a felhasználóknak egy meghatározott rendszerhasználati értesítést vagy üzenetet, amely biztonsági értesítést tartalmaz a szervezetre vonatkozó, hatályos jogszabályi előírásokban, irányelvekben, szabályozásokban, eljárásrendekben, szabványokban és útmutatókban meghatározottak szerint és tartalmazza, hogy:

- a felhasználók a szervezet EIR-ét használják.

- a rendszer használatát megfigyelhetik, rögzíthetik, naplózhatják.

- a rendszer jogosulatlan használata tilos és büntető- vagy polgári jogi felelősséggel jár.

- a rendszer használata az előbbiekben részletezett feltételek elfogadását jelenti.

Az EIR mindaddig fenntartja a rendszerhasználati értesítést a képernyőn, amíg a felhasználók nem fogadják el a használati feltételeket és nem tesznek egyértelmű lépéseket a rendszerbe való bejelentkezésre vagy a rendszerhez való további hozzáférésre.

Nyilvánosan hozzáférhető rendszerek esetén az értesítés legalább az alábbiakat tartalmazza:

- a felhasználók a szervezet EIR-ét használják.

- a rendszer használatát megfigyelhetik, rögzíthetik, naplózhatják.

- a rendszer jogosulatlan használata tilos és büntető- vagy polgári jogi felelősséggel jár.

A védelmi intézkedés státusza (csak egy választható):
☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.1.6 Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	2.88.

A szervezet:

Azonosítja azon felhasználói tevékenységeket, amelyek - a szervezeti célokkal és üzleti funkciókkal összhangban - az EIR-ben azonosítás vagy hitelesítés nélkül is végrehajthatók.

A rendszerbiztonsági tervben dokumentálja és megindokolja azokat a felhasználói tevékenységeket, amelyek azonosítás vagy hitelesítés nélkül is végrehajthatók.

A védelmi intézkedés státusza (csak egy választható):
☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.1.7 Távoli hozzáférés

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	2.100.

A szervezet:

Kidolgozza és dokumentálja az engedélyezett távoli hozzáférés minden egyes típusára vonatkozóan a használati korlátozásokat, a konfigurációs vagy csatlakozási követelményeket és az alkalmazási útmutatókat.

Engedélyezési eljárást folytat le a rendszerhez való távoli hozzáférés minden egyes típusára, az ilyen kapcsolatok lehetővé tételét megelőzően
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva
Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.1.8 Vezeték nélküli hozzáférés

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	2.108.
A szervezet: A vezeték nélküli hozzáférés minden egyes típusára vonatkozóan konfigurációs követelményeket, kapcsolódási követelményeket és alkalmazási útmutatást alakít ki. Engedélyezési eljárást folytat le a rendszerhez való vezeték nélküli hozzáférés minden egyes típusára, az ilyen kapcsolatok lehetővé tételét megelőzően		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.1.9 Mobil eszközök hozzáférés-ellenőrzése

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	2.113.
A szervezet: Kialakítja a konfigurációs követelményeket, kapcsolódási követelményeket és alkalmazási útmutatót az általa ellenőrzött mobil eszközök számára, beleértve azokat az eseteket is, amikor ezek az eszközök a szervezet által ellenőrzött területen kívül helyezkednek el. Engedélykötelessé teszi a szervezet rendszereihez mobil eszközökkel történő kapcsolódást.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.1.10 Külső elektronikus információs rendszerek használata

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	2.115.
A szervezet: Meghatározza a felhasználási feltételeket, és megállapítja, hogy az elvárt követelmények megvalósultak-e a külső rendszerekben, összhangban a külső rendszereket birtokló, üzemeltető, illetve karbantartó más szervezetekkel létrehozott bizalmi kapcsolatokkal, amelyek lehetővé teszik az arra jogosult személyek számára, hogy: - hozzáférjenek a rendszerhez külső rendszerekből; és - feldolgozzák, tárolják vagy továbbítsák a szervezet által ellenőrzött információkat külső rendszerek használatával; vagy megtiltja a meghatározott típusú külső rendszerek használatát.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.1.11 Nyilvánosan elérhető tartalom

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	2.124.
A szervezet: Kijelöli azokat a személyeket, akik jogosultak arra, hogy információkat tegyenek nyilvánosan hozzáférhetővé. Képzést biztosít a jogosult személyek számára, hogy biztosítsa, hogy a nyilvánosan hozzáférhető információk nem tartalmaznak nem nyilvános információkat. Áttekinti az információ tervezett tartalmát a nyilvánosan hozzáférhető rendszerbe történő közzététel előtt, annak érdekében, hogy biztosítsa, hogy nem tartalmaznak nem nyilvános információkat. Meghatározott gyakorisággal áttekinti a nyilvánosan hozzáférhető rendszer tartalmát a nem nyilvános információk szempontjából, és eltávolítja az ilyen információkat, ha felfedezik őket.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.2 NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG

8.2.1 Szabályzat és eljárásrendek

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	4.1.
A szervezet: Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó naplózásra és elszámoltathatóságra vonatkozó szabályzatot, amely meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. a naplózási és elszámoltathatósági eljárásrendet, amely a naplózásra és elszámoltathatóságra vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. Kijelöl egy, a szervezet által meghatározott személyt, aki a naplózásra és elszámoltathatóságra vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. Felülvizsgálja és frissíti az aktuális naplózásra és elszámoltathatóságra vonatkozó szabályzatot és a naplózási és elszámoltathatósági eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.2.2 Naplózható események

Követelmény:	Biztonsági osztály:	**Alap**

☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	4.2.
A szervezet: Meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az EIR-t. Egyezteti a naplózási elvárásokat a naplózási információt igénylő szervezeti egységekkel, hogy iránymutatással és információkkal segítse a naplózandó események kiválasztását. Meghatározza az EIR-en belül naplózandó eseménytípusokat, és az azokhoz kapcsolódó gyakoriságot vagy az azt szükségessé tevő eseményeket. Indokolja, hogy a kiválasztott eseménytípusok, miért alkalmasak a biztonsági események utólagos kivizsgálásának támogatására; Meghatározott gyakorisággal felülvizsgálja és frissíti a naplózásra kiválasztott eseménytípusokat.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.2.3 Naplóbejegyzések tartalma

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	4.3.
A szervezet biztosítja, hogy a naplóbejegyzésekből az alábbi információk megállapíthatóak legyenek: milyen típusú esemény történt; mikor történt az esemény; hol történt az esemény; miből származott az esemény; és mi volt az eseménynek a kimenetele, valamint az eseményhez kapcsolódó személyek, alanyok, objektumok.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.2.4 Naplózás tárkapacitása

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	4.5.
A szervezet elegendő méretű tárkapacitást biztosít a naplózásra, figyelembe véve a naplózási funkciókat és a meghatározott megőrzési követelményeket.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.2.5 Naplózási hiba kezelése

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	4.7.
A szervezet naplózási hiba esetén:		

Riasztja a meghatározott személyeket vagy szerepköröket a szervezet által meghatározott időn belül. További meghatározott intézkedéseket hajt végre.
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva
Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.2.6 Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	4.13.
A szervezet: Meghatározott gyakorisággal felülvizsgálja és elemzi a rendszer naplóbejegyzéseit a nem megfelelő vagy szokatlan tevékenységre utaló jelek és az ilyen tevékenységek lehetséges hatásai szempontjából. Jelenti ezeket a szervezet által meghatározott személyeknek vagy szerepköröknek. Módosítja a naplóbejegyzések felülvizsgálatának, elemzésének és jelentésének szintjét, amennyiben hiteles információk és információforrások alapján a kockázat változik.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.2.7 Időbélyegek

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	4.24.
A szervezet: Belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához. Időbélyegeket rögzít a naplóbejegyzésekben, amelyek megfelelnek a szervezet által meghatározott pontosságra vonatkozó követelményeknek, a koordinált világidőt használják és magukba foglalják a helyi időeltolódást.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.2.8 Naplóinformációk védelme

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	4.25.
Az EIR: Megvédi a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben. Jogosulatlan hozzáférés, módosítás vagy a naplóinformáció törlésének észlelésekor értesíti a meghatározott személyeket vagy szerepköröket.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.2.9 A naplóbejegyzések megőrzése

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	4.38.
A szervezet a naplóbejegyzéseket a jogszabályi és a szervezeten belüli információmegőrzési követelmények szerint meghatározott időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.2.10 Naplóbejegyzések létrehozása

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	4.40.
Az EIR: Biztosítja a naplóbejegyzés generálási képességet a "Naplózható események" pontban meghatározott naplózható eseményekre. Lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az EIR egyes elemei által. Naplóbejegyzéseket állít elő a "Naplózható események" pont szerinti eseményekre az "Naplóbejegyzések tartalma" pontban meghatározott tartalommal.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.3 ÉRTÉKELÉS, ENGEDÉLYEZÉS ÉS MONITOROZÁS

8.3.1 Szabályzat és eljárásrendek

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	5.1.
A szervezet: Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó biztonságértékelési szabályzatot, amely meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel. szabályozásokkal, szabványokkal és ajánlásokkal. A biztonságértékelési eljárásrendet, amely a biztonságértékelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. Kijelöl egy, a szervezet által meghatározott személyt, aki a biztonságértékelési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. Felülvizsgálja és frissíti az aktuális biztonságértékelési szabályzatot és a biztonságértékelési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.3.2 Biztonsági értékelések

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	5.2.

A szervezet:

Kiválasztja az elvégzendő értékelés típusának megfelelő értékelő személyt vagy csoportot.

Biztonságértékelési tervet készít, amely leírja az értékelés hatókörét, beleértve:

az értékelendő védelmi intézkedéseket, azok kiterjesztését és továbbfejlesztését;

a védelmi intézkedések hatékonyságának megállapításához használt értékelési eljárásokat;

az értékelési környezetet, az értékelő csoportot, az értékelő szerepköröket és feladataikat.

Biztosítja, hogy a biztonságértékelési tervet az engedélyezésre jogosult felelős vagy kijelölt képviselője az értékelés elvégzése előtt felülvizsgálja és jóváhagyja.

Meghatározott gyakorisággal értékeli az EIR és működési környezete védelmi intézkedéseit, kontrollálja a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelő működését.

Elkészíti a biztonságértékelés eredményét összefoglaló jelentést.

Gondoskodik a biztonságértékelés eredményét összefoglaló jelentésnek a szervezet által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismeréséről.

A védelmi intézkedés státusza (csak egy választható):
☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.3.3 Biztonsági értékelések – Kiberbiztonsági audit

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	5.4.

A 1. § (2) bekezdés hatálya alá tartozó szervezet független auditorokat alkalmaz az EIR védelmi intézkedéseinek értékelésére.

A védelmi intézkedés státusza (csak egy választható):
☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.3.4 Információcsere

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	5.7.

A szervezet:

Jóváhagyja és szabályozza az információcserét az EIR és más rendszerek között, összhangban a kapcsolódásokra és az információcserére vonatkozó biztonsági megállapodásokkal, továbbá figyelembe veszi a szolgáltatási szintre, a felhasználókra és a titoktartásra vonatkozó, valamint a szervezet által meghatározott egyéb megállapodásokat.

Minden egyes információcsere-megállapodás keretében dokumentálja az egyes rendszerek interfészeinek jellemzőit, biztonsági követelményeit, védelmi intézkedéseit és felelősségi körét, valamint rögzíti a megosztott információk hatásának szintjét is.

Rendszeres időközönként felülvizsgálja és frissíti a megállapodásokat.

A védelmi intézkedés státusza (csak egy választható):
☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.3.5 Az intézkedési terv és mérföldkövei

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	5.10.

A szervezet:

Intézkedési tervet dolgoz ki, amelyben mérföldköveket határoz meg az EIR-ben tervezett korrekciós intézkedések dokumentálására, hogy a védelmi intézkedések értékelése során feltárt gyengeségeket vagy hiányosságokat kijavítsák, valamint a rendszer ismert sérülékenységeit csökkentsék vagy megszüntessék.

Rendszeresen frissíti az intézkedési tervet és a mérföldköveket, figyelembe véve a védelmi intézkedések értékeléseit, a független auditokat és felülvizsgálatokat, valamint a folyamatos felügyeleti tevékenységek eredményeit.

A védelmi intézkedés státusza (csak egy választható):
☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.3.6 Engedélyezés

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	5.12.

A szervezet:

Kijelöl egy engedélyezésért felelős személyt, aki az EIR-ért felel.

Kijelöl egy felelős személyt, aki a szervezeti EIR-ekre vonatkozó közös, más rendszerekből áthozott (átörökített) biztonsági követelmények elfogadásáért felel.

Biztosítja, hogy az engedélyezésért felelős személy az EIR használatbavételét megelőzően:

elfogadja a közös, más rendszerekből áthozott (átörökített) biztonsági követelmények alkalmazását; és

a szervezet vezetőjével engedélyezteti a rendszer működését.

Biztosítja, hogy a közös biztonsági követelményekért felelős személy engedélyezze a közös, más rendszerekből áthozott (átörökített) biztonsági követelmények használatát.

Rendszeresen felülvizsgálja az engedélyeket.

A védelmi intézkedés státusza (csak egy választható):
☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.3.7 Folyamatos felügyelet

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	5.15.

A szervezet kidolgozza a rendszerszintű folyamatos felügyeleti stratégiát és megvalósítja a folyamatos felügyeletet a szervezeti szintű stratégiával összhangban, amely magában foglalja a következőket:

A rendszerszintű metrikák meghatározását.

Rendszeres felügyelet biztosítását a védelmi intézkedések hatékonyságának értékelésére.

A védelmi intézkedések folyamatos értékelését.

Az EIR és a szervezet által meghatározott mutatók folyamatos nyomon követését.

A védelmi intézkedésekről gyűjtött és feldolgozott információ összegzését és kiértékelését.

A védelmi intézkedések értékelése és elemzése alapján végrehajtott válaszintézkedéseket.

az EIR biztonsági állapotáról rendszeres időközönként történő jelentés a kijelölt személyeknek.

A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva
Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.3.8 Folyamatos felügyelet – Kockázatmonitorozás

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	5.18.
A szervezet biztosítja, hogy a kockázatmonitorozás szerves része legyen a folyamatos felügyeleti stratégiának, amely a következőket tartalmazza: a hatékonyság ellenőrzését; a megfelelés ellenőrzését; és a változások nyomon követését.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.3.9 Belső rendszerkapcsolatok

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	5.25.
A szervezet: Engedélyezi a szervezet által meghatározott rendszerelemeknek vagy rendszerelem kategóriáknak a rendszerhez történő belső kapcsolódását. Minden belső kapcsolat esetében dokumentálja az interfész jellemzőit, a biztonsági követelményeket, továbbá a kommunikációban részt vevő információ jellegét. Meghatározott feltételek teljesülése esetén megszünteti a belső rendszerkapcsolatokat. Meghatározott gyakorisággal felülvizsgálja minden belső kapcsolat további szükségességét.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.4 KONFIGURÁCIÓKEZELÉS

8.4.1 Szabályzat és eljárásrendek

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	6.1.
A szervezet: Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó konfigurációkezelési szabályzatot, amely meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.		

A konfigurációkezelési eljárásrendet, amely a konfigurációkezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. Kijelöl egy, a szervezet által meghatározott személyt, aki a konfigurációkezelési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. Felülvizsgálja és frissíti az aktuális konfigurációkezelési szabályzatot és a konfigurációkezelési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva
Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.4.2 Alapkonfiguráció

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	6.2.
A szervezet: Kifejleszti, dokumentálja és karbantartja az EIR alapkonfigurációját. Elvégzi az EIR alapkonfigurációjának felülvizsgálatát és frissítését: meghatározott időközönként; ha azt a meghatározott körülmények indokolják, vagy az EIR vagy rendszerelemek telepítésekor vagy frissítésekor.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.4.3 Biztonsági hatásvizsgálatok

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	6.15.
A szervezet még a változtatások bevezetése előtt megvizsgálja az EIR-ben tervezett változtatásoknak az információbiztonsági hatásait.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.4.4 A változtatásokra vonatkozó hozzáférés korlátozások

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	6.18.
A szervezet meghatározza, dokumentálja, jóváhagyja és érvényesíti azokat a fizikai és logikai hozzáférési korlátozásokat, amelyek az EIR változtatásaihoz kapcsolódnak.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.4.5 Konfigurációs beállítások

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	6.23.

A szervezet

Kialakítja és dokumentálja a rendszerelemekben alkalmazott egységes biztonsági konfigurációs beállításokat, amelyek az üzemeltetési követelményekkel összhangban lévő legkorlátozottabb üzemmódot képviselik.

Elvégzi a konfigurációs beállításokat az EIR valamennyi elemében.

Azonosítja, dokumentálja és elfogadja a meghatározott rendszerelemek konfigurációs beállításaiban a működési követelmények által meghatározott konfigurációs beállításoktól való eltéréseket.

Figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait a szervezeti szabályzatokkal és eljárásokkal összhangban.

A védelmi intézkedés státusza (csak egy választható):
☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.4.6 Legszűkebb funkcionalitás

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	6.26.

A szervezet:

Az EIR-t úgy konfigurálja, hogy az csak az ügy- és üzletmenet szempontjából szükséges szolgáltatásokat nyújtsa.

Meghatározza a tiltott vagy korlátozott funkciókat, portokat, protokollokat, szoftvereket és szolgáltatásokat.

A védelmi intézkedés státusza (csak egy választható):
☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.4.7 Rendszerelem leltár

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	6.36.

A szervezet:

Leltárt készít az EIR elemeiről.

A leltár pontosan tükrözi az EIR-t.

A leltár tartalmazza a rendszeren belül található összes elemet.

Megakadályozza az elemek kettős elszámolását.

A leltár a nyomon követés és a jelentéstétel szempontjából a szükséges részletességet biztosítja.

A leltárban szereplő információk lehetővé teszik a rendszerelemekkel történő hatékony elszámolást.

Meghatározott gyakorisággal felülvizsgálja és frissíti a rendszerelemek leltárát.

A védelmi intézkedés státusza (csak egy választható):
☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.4.8 A szoftverhasználat korlátozásai

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	6.47.

A szervezet:

Kizárólag olyan szoftvereket és olyan kapcsolódó dokumentációt használ, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak, valamint a szerzői jogi vagy más jogszabályi előírásoknak.

A másolatok és megosztások ellenőrzésére nyomon követi a mennyiségi licenc alá eső szoftverek és a kapcsolódó dokumentációk használatát.

Ellenőrzi és dokumentálja az állománymegosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett művek jogosulatlan terjesztésére, megjelenítésére, előadására vagy sokszorosítására.

A védelmi intézkedés státusza (csak egy választható):
☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.4.9 Felhasználó által telepített szoftver

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	6.49.

A szervezet:

Megfogalmazza az EIR vonatkozásában a szervezetre érvényes követelményeket, amelyek meghatározzák a szoftverek felhasználó általi telepítési lehetőségeit.

Érvényesíti a szoftvertelepítésre vonatkozó szabályokat a szervezet által meghatározott módszerek szerint.

Meghatározott gyakorisággal ellenőrzi a szabályok betartását

A védelmi intézkedés státusza (csak egy választható):
☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.5 KÉSZENLÉTI TERVEZÉS

8.5.1 Szabályzat és eljárásrendek

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	7.1.

A szervezet:

Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint

a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó üzletmenet-folytonosságra vonatkozó szabályzatot, amely

meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá

összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.

az üzletmenet-folytonosságra vonatkozó eljárásrendet, amely az üzletmenet-folytonosságra vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

Kijelöl egy, a szervezet által meghatározott személyt, aki az üzletmenet-folytonosságra vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.

Felülvizsgálja és frissíti az aktuális üzletmenet-folytonosságra vonatkozó szabályzatot és az üzletmenet-folytonosságra vonatkozó eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva
Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.5.2 Üzletmenet-folytonossági terv

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	7.2.

A szervezet:

Kidolgozza az EIR-re vonatkozó üzletmenet-folytonossági tervet, amely:

meghatározza az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;

tartalmazza a helyreállítási célokat, a helyreállítási prioritásokat és metrikákat;

kijelöli a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket és azok elérhetőségeit;

meghatározza az EIR összeomlása, kompromittálódása vagy hibája ellenére is biztosítandó szolgáltatásokat;

tartalmazza az EIR végleges, teljeskörű helyreállításának tervét, mely garantálja, hogy az eredetileg tervezett és megvalósított védelmi intézkedések a helyreállítás után ne sérüljenek;

szabályozza az üzletmenet-folytonossági információk megosztását; és

a szervezet által meghatározott személyek vagy szerepkörök által felülvizsgált és jóváhagyott.

Megfogalmazza, és a szervezetre érvényes követelmények szerint dokumentálja, valamint A szervezeten belül kizárólag a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyek és szervezeti egységek számára kihirdeti az EIR-ekre vonatkozó üzletmenet-folytonossági tervet.

Összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével;

Meghatározott gyakorisággal felülvizsgálja az EIR-hez kapcsolódó üzletmenet-folytonossági tervet.

Az EIR vagy a működési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálja az üzletmenet-folytonossági tervet.

Tájékoztatja az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket.

Az üzletmenet-folytonossági terv tesztelése, gyakorlata vagy tényleges alkalmazása során levont tanulságokat beépíti a tesztelési és gyakorlati folyamatokba.

Gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető és módosítható.

A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva
Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.5.3 A folyamatos működésre felkészítő képzés

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	7.10.

A szervezet:

Az EIR felhasználói számára szerepkörüknek vagy felelősségi körüknek megfelelő folyamatos működésre felkészítő képzést tart:

szerepkörbe vagy felelősségbe kerülésüket követő meghatározott időn belül;

amikor az EIR változásai ezt szükségessé teszik; a szervezet által meghatározott gyakorisággal. Meghatározott gyakorisággal vagy meghatározott eseményeket követően felülvizsgálja és frissíti a folyamatos működésre felkészítő képzés tartalmát.
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva
Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.5.4 Az elektronikus információs rendszer mentései

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	7.35.
A szervezet: Meghatározott gyakorisággal mentést készít az EIR-ben tárolt felhasználói szintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal. Meghatározott gyakorisággal mentést készít az EIR-ben tárolt rendszerszintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal. Meghatározott gyakorisággal mentést készít az EIR dokumentációjáról, beleértve a biztonságra vonatkozó információkat 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 biztonsági tárolási helyszínen.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.5.5 Az elektronikus információs rendszer helyreállítása és újraindítása

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	7.43.
A szervezet a meghatározott helyreállítási idővel és helyreállítási ponttal kapcsolatos célkitűzésekkel összhangban lévő időtartam alatt gondoskodik az EIR utolsó ismert, üzembiztos állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.6 AZONOSÍTÁS ÉS HITELESÍTÉS

8.6.1 Szabályzat és eljárásrendek

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	8.1.
A szervezet: Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó azonosítási és hitelesítési szabályzatot, amely		

meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel. szabályozásokkal, szabványokkal és ajánlásokkal. az azonosítási és hitelesítési eljárásrendet, amely az azonosítási és hitelesítési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. Kijelöl egy, a szervezet által meghatározott személyt, aki az azonosítási és hitelesítési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. Felülvizsgálja és frissíti az aktuális azonosítási és hitelesítési szabályzatot és az azonosítási és hitelesítési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva
Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.6.2 Azonosítás és hitelesítés

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	8.2.
A szervezet egyedileg azonosítja és hitelesíti a felhasználókat, és egyedi azonosítóhoz kapcsolja a felhasználók által végzett tevékenységeket.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.6.3 Azonosítás és hitelesítés (felhasználók) – Privilegizált fiókok többtényezős hitelesítése

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	8.3.
A szervezet többtényezős hitelesítést alkalmaz a privilegizált fiókokhoz való hozzáféréshez.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.6.4 Azonosítás és hitelesítés (felhasználók) – Hozzáférés a fiókokhoz – Visszajátszás elleni védelem

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	8.7.
A szervezet visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a privilegizált és a nem privilegizált fiókokhoz való hozzáféréshez.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.6.5 Azonosító kezelés

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	8.14.

A szervezet:

Az egyéni, csoport, szerepkör vagy eszköz azonosítók kiosztását a szervezet által meghatározott személyek vagy szerepkörök engedélyéhez köti.

Kiválaszt egy azonosítót, amely azonosítja az egyént, csoportot, szerepkört, szolgáltatást vagy eszközt.

Hozzárendeli az azonosítót a kívánt egyénhez, csoporthoz, szerepkörhöz, szolgáltatáshoz vagy eszközhöz.

Meghatározott ideig megakadályozza az azonosítók újbóli felhasználását.

A védelmi intézkedés státusza (csak egy választható):
☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.6.6 A hitelesítésre szolgáló eszközök kezelése

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	8.21.

A szervezet a hitelesítő eszközöket az alábbiak szerint kezeli:

A kezdeti hitelesítő eszköz kiosztásának részeként ellenőrzi a hitelesítő eszközt megkapó egyén, csoport, szerepkör, szolgáltatás vagy eszköz identitását.

Meghatározza a szervezet által kiadott hitelesítő eszköz kezdeti tartalmát.

Biztosítja, hogy a hitelesítő eszközök a tervezett felhasználáshoz megfelelő erősségű mechanizmussal rendelkezzenek.

Adminisztratív eljárásokat alakít ki és hajt végre a kezdeti hitelesítő eszközök kiosztásához, az elveszett, kompromittált vagy sérült hitelesítő eszközökhöz, valamint a hitelesítő eszközök visszavonásához.

Gondoskodik a hitelesítő eszközök kezdeti tartalmának megváltoztatásáról az első használat előtt.

Gondoskodik a hitelesítő eszközök tartalmának megváltoztatásáról vagy frissítéséről meghatározott gyakorisággal, vagy amikor meghatározott események bekövetkeznek.

Megvédi a hitelesítő eszközök tartalmát az illetéktelen nyilvánosságra hozatal és módosítás ellen.

Megköveteli, hogy az egyének és eszközök konkrét védelmi intézkedéseket alkalmazzanak, illetve hajtsanak végre a hitelesítő eszközök védelme érdekében.

Megváltoztatja a csoporthoz vagy szerepkörhöz rendelt fiókok hitelesítő eszközeinek tartalmát, amikor a fiókokhoz tartozó tagok közül valaki eltávolításra kerül.

A védelmi intézkedés státusza (csak egy választható):
☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.6.7 A hitelesítésre szolgáló eszközök kezelése – Jelszó alapú hitelesítés

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	8.22.

A szervezet:

Fenntartja a gyakran használt, könnyen kitalálható vagy kompromittált jelszavak listáját, és ezt a listát a szervezet által meghatározott gyakorisággal frissíti, továbbá minden olyan esetben, amikor a szervezeti jelszavakat közvetlenül vagy közvetett módon veszélyeztetik.

Ellenőrzi, hogy a felhasználók által létrehozott vagy módosított jelszavak szerepelnek-e a gyakran használt, könnyen kitalálható vagy kompromittált jelszavak listáján. A jelszavakat csak kriptográfiailag védett csatornákon keresztül továbbítja. A jelszavakat egy jóváhagyott, sózott kulcsszármaztatási funkcióval, lehetőleg egykulcsos hash-t használva tárolja. Megköveteli a jelszó azonnali megváltoztatását fiókvisszaállítás esetén. Engedélyezi a felhasználóknak hosszú jelszavak és jelmondatok kiválasztását, beleértve a szóközöket és a nyomtatható karaktereket. Automatizált eszközökkel támogatja a felhasználókat az erős jelszavak kiválasztásában. A jelszavakra a szervezet által meghatározott összetételi és komplexitási szabályokat érvényesíti.
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva
Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.6.8 Hitelesítési információk visszajelzésének elrejtése

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	8.36.
Az EIR fedett visszacsatolást biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt a jogosulatlan személyek általi felfedésétől és felhasználásától.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.6.9 Hitelesítés kriptográfiai modul esetén

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	8.37.
Az EIR olyan mechanizmusokat alkalmaz a kriptográfiai modul hitelesítéséhez, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának, a hatályos törvényeknek, a végrehajtási utasításoknak, szabályzatoknak, szabványoknak.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.6.10 Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	8.38.
Az EIR egyedileg azonosítja és hitelesíti a szervezeten kívüli felhasználókat, tevékenységüket, valamint a nevükben futó folyamatokat.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.6.11 Azonosítás és hitelesítés (szervezeten kívüli felhasználók) – Meghatározott azonosítási profilok használata

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	8.39.
A szervezet meghatározott profilokat alkalmaz az azonosítási folyamat során.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.6.12 Újrahitelesítés

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	8.43.
A szervezet meghatározott körülmények vagy helyzetek esetén megköveteli a felhasználótól az újrahitelesítést.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.7 KOCKÁZATKEZELÉS

8.7.1 Sérülékenységek ellenőrzése

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	15.9.
A szervezet: Meghatározott folyamat szerint rendszeresen vagy eseti jelleggel ellenőrzi az EIR sérülékenységeit, illetve minden olyan esetben, amikor új, az EIR-t potenciálisan érintő sérülékenységeket azonosítanak és jelentenek. Kijavítja a valós sérülékenységeket a meghatározott válaszidőn belül, a kockázatkezelési eljárásoknak megfelelően.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.7.2 Sérülékenységmenedzsment – Sérülékenységi információk fogadása

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	15.18.
A szervezet létrehoz egy csatornát, amelyen keresztül fogadhatja a szervezeti EIR-ekben és rendszerelemekben található sérülékenységekről szóló jelentéseket.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.7.3 Kockázatokra adott válasz

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	15.20.
A szervezet a kockázatmenedzsment szabályokkal összhangban reagál a biztonsági értékelések, ellenőrzések és vizsgálatok megállapításaira.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.8 RENDSZER- ÉS SZOLGÁLTATÁSBESZERZÉS

8.8.1 Beszerzések

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	16.7.
A szervezet a beszerzési folyamat során - beleértve a fejlesztést, az adaptálást, a rendszerkövetést és a karbantartást is - a szerződéseiben egységes nyelvezetet alkalmaz, továbbá követelményként rögzíti az alábbiakat: A funkcionális biztonsági követelményeket. A mechanizmusok erősségére vonatkozó követelményeket. A biztonság garanciális követelményeit. Az érintett EIR biztonsági osztályát és az ahhoz tartozó, illetve a szervezet által meghatározott további biztonsági követelmények teljesítéséhez szükséges védelmi intézkedéseket. A biztonsággal kapcsolatos dokumentációs követelményeket. A biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket. Az EIR fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat. A felelősség megosztását vagy az információbiztonságért és az ellátási lánc kockázatkezeléséért felelős felek azonosítását. A teljesítési kritériumokat.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.8.2 Beszerzések – Alkalmazandó védelmi intézkedések funkcionális tulajdonságai

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	16.8.
A szervezet megköveteli a beszerzett EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak leírását.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.8.3 Az elektronikus információs rendszerre vonatkozó dokumentáció

Követelmény:	Biztonsági osztály:	**Alap**

☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	16.15.

A szervezet:

Kidolgozza vagy beszerzi az EIR, rendszerelem vagy rendszerszolgáltatás adminisztrátori és üzemeltetői dokumentációját, amely tartalmazza:

az EIR, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurációját, telepítését és üzemeltetését;

a biztonsági funkciók hatékony használatát és karbantartását; valamint

az ismert sérülékenységeket a konfigurációval és a rendszergazdai vagy privilegizált funkciók használatával kapcsolatban.

Kidolgozza vagy beszerzi a rendszer, rendszerelem vagy rendszerszolgáltatás felhasználói dokumentációját, amely tartalmazza:

a felhasználók számára elérhető biztonsági funkciókat és mechanizmusokat és ezek hatékony használatának módját;

a felhasználói interakció biztonságos módját;

a felhasználók felelősségét az EIR, rendszerelem, rendszerszolgáltatás biztonságának fenntartásában.

Amennyiben nem áll rendelkezésre vagy nem létezik adminisztrátori, üzemeltetői és felhasználói dokumentáció, úgy a szervezet dokumentálja az EIR, rendszerelem vagy rendszerszolgáltatás dokumentációjának beszerzésére tett kísérleteket, valamint végrehajtja a szervezet által meghatározott intézkedéseket; és

a dokumentációkat eljuttatja a szervezet által meghatározott személyeknek vagy szerepköröknek.

A védelmi intézkedés státusza (csak egy választható):
☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.8.4 Támogatással nem rendelkező rendszerelemek

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	16.99.

A szervezet:

lecseréli a rendszerelemeket, amikor azok támogatása már nem elérhető a fejlesztőtől, szállítótól vagy gyártótól; illetve

a támogatással már nem rendelkező rendszerelemekhez alternatív támogatást biztosít, amelyet belső erőforrásokkal vagy a szervezet által meghatározott külső szolgáltatók bevonásával valósít meg.

A védelmi intézkedés státusza (csak egy választható):
☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.9 RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM

8.9.1 Szabályzat és eljárásrendek

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	17.1.

A szervezet:

Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint

a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó rendszer- és kommunikációvédelmi szabályzatot, amely

meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá

összhangban van a szervezetre vonatkozó hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.

a rendszer- és kommunikációvédelmi eljárásrendet, amely a rendszer- és kommunikációvédelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. Kijelöl egy, a szervezet által meghatározott személyt, aki a rendszer- és kommunikációvédelmi szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. Felülvizsgálja és frissíti az aktuális rendszer- és kommunikációvédelmi szabályzatot és a rendszer- és kommunikációvédelmi eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva
Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.9.2 Szolgáltatásmegtagadással járó támadások elleni védelem

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	17.12.
A szervezet: védekezik a meghatározott szolgáltatásmegtagadással járó támadások ellen, vagy korlátozza azok hatásait; és alkalmazza azokat a védelmi intézkedéseket, amelyek segítségével elérheti a szolgáltatásmegtagadással járó támadások elleni védekezés célját.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.9.3 A határok védelme

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	17.17.
A szervezet: Ellenőrzi a kommunikációt a menedzselt külső interfészein, valamint a rendszer kulcsfontosságú menedzselt belső interfészein. A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól. Csak a szervezet biztonsági architektúrájával összhangban lévő határvédelmi eszközökön keresztül, menedzselt interfészek segítségével kapcsolódik külső hálózatokhoz vagy külső EIR-ekhez.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.9.4 Kriptográfiai kulcs előállítása és kezelése

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	17.49.
A szervezet előállítja és kezeli a kriptográfiai kulcsokat a szervezet által meghatározott előállítási, szétosztási, tárolási, hozzáférési és megsemmisítési követelményekkel összhangban.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.9.5 Kriptográfiai védelem

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	17.53.
A szervezet: meghatározza a kriptográfia szervezeten belüli felhasználási területeit; és megvalósítja az egyes kriptográfiai felhasználási területekhez szükséges kriptográfiai megoldásokat.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.9.6 Együttműködésen alapuló informatikai eszközök

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	17.54.
A szervezet: tiltja az együttműködésen alapuló számítástechnikai eszközök (például: kamerák, mikrofonok) és alkalmazások távoli aktiválását, a szervezet által meghatározott kivételekkel; és egyértelmű visszajelzést ad a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.9.7 Biztonságos név/cím feloldási szolgáltatás (hiteles forrás)

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	17.69.
Az EIR: A név- és címfeloldási kérésekre a hiteles névfeloldási adatokon kívül az információ eredetére és a tartalom sértetlenségére vonatkozó kiegészítő adatokat is biztosít. Amennyiben egy elosztott, hierarchikus névtér részeként működik, jelzi a gyermektartományok biztonsági állapotát is, és ha azok támogatják a biztonságos névfeloldási szolgáltatásokat, lehetővé teszi a szülő- és gyermektartományok közötti bizalmi lánc ellenőrzését.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.9.8 Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás)

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	17.71.

Az EIR eredet-hitelesítést és adatsértetlenség-ellenőrzést kér és hajt végre a hiteles forrásból származó név- és címfeloldó válaszokon.
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva
Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.9.9 Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	17.72.
A szervezet számára név- és címfeloldási szolgáltatást együttesen biztosító EIR-ek hibatűrő képességgel rendelkeznek, és alkalmazzák a belső és a külső szerepkörök szétválasztását.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.9.10 A folyamatok elkülönítése

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	17.108.
Az EIR elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.10 RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG

8.10.1 Szabályzat és eljárásrendek

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	18.1.
A szervezet: Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó rendszer- és információsértetlenségi szabályzatot, amely meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. a rendszer- és információsértetlenségi eljárásrendet, amely a rendszer- és információsértetlenségi szabályok és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. Kijelöl egy meghatározott személyt, aki a rendszer- és információsértetlenségi szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. Felülvizsgálja és frissíti az aktuális rendszer- és információsértetlenségi szabályzatot és a rendszer- és információsértetlenségi eljárásokat a meghatározott gyakorisággal és a meghatározott események bekövetkezését követően.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		

Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.10.2 Hibajavítás

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	18.2.
A szervezet: Azonosítja, jelenti és kijavítja az EIR hibáit. A hibajavítással kapcsolatos szoftverfrissítéseket telepítés előtt teszteli a hatékonyság és a potenciális mellékhatások szempontjából. A biztonsági szempontból releváns szoftver- és firmware-frissítéseket a frissítések kiadását követő meghatározott időtartamon belül telepíti. A hibajavítást beépíti a szervezet konfigurációkezelési folyamatába.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.10.3 Kártékony kódok elleni védelem

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	18.8.
A szervezet: Kártékony kódok elleni védelmi mechanizmusokat alkalmaz a rendszer belépési és kilépési pontjain, hogy felderítse és megfelelő módon eltávolítsa a kártékony kódokat. A védelmi mechanizmusokat automatikusan frissíti minden olyan esetben, amikor új verziók jelennek meg összhangban a szervezet konfigurációkezelési szabályaival. A kártékony kódok elleni védelmi mechanizmusokat úgy konfigurálja, hogy: Meghatározott időközönként átvizsgálja a rendszert, és valós időben ellenőrzi a külső forrásokból származó fájlokat a végpontokon, a hálózati belépési vagy kilépési pontokon a biztonsági szabályzatnak megfelelően, amint a fájlokat letöltik, megnyitják vagy futtatják. Kártékony kód észlelésekor blokkolja vagy karanténba helyezi a kártékony kódokat, vagy a szervezet által meghatározott egyéb intézkedéseket hajt végre; továbbá riasztást küld a szervezet által meghatározott személyeknek vagy szerepköröknek. Ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az EIR rendelkezésre állására.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.10.4 Az EIR monitorozása

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	18.13.
A szervezet: Monitorozza a rendszert, hogy észlelje: A támadásokat és a potenciális támadásokra utaló jeleket összhangban a meghatározott felügyeleti célokkal;		

Az engedély nélküli helyi, hálózati és távoli kapcsolatokat. Azonosítja a rendszer jogosulatlan használatát a meghatározott technikák és módszerek alkalmazásával. Aktiválja a belső felügyeleti képességeket vagy telepíti a felügyeleti eszközöket: az egész rendszerre kiterjedően a szervezet által meghatározott információk gyűjtése érdekében; illetve a rendszeren belül ad-hoc módon meghatározott helyeken a szervezet által meghatározott információk gyűjtése érdekében. Elemzi az észlelt eseményeket és rendellenességeket. Módosítja a rendszerfelügyeleti tevékenység szintjét, amikor változik a szervezeti műveletekkel, az eszközökkel, az egyénekkel, a külső szervezetekkel kapcsolatos kockázati szint. Jogi állásfoglalást kér a rendszerfelügyeleti tevékenységekről. Biztosítja a szervezet által meghatározott rendszerfelügyeleti információkat a meghatározott személyeknek vagy szerepköröknek a szervezet által meghatározott gyakorisággal.
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva
Védelmi intézkedés (tervezett) **megvalósításának részletei**

8.10.5 Biztonsági riasztások és tájékoztatások

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	18.37.
A szervezet: Folyamatosan fogadja a meghatározott külső szervezetektől a biztonsági figyelmeztetéseket, tanácsokat és iránymutatásokat. Szükség esetén belső biztonsági riasztásokat, tanácsokat és iránymutatásokat készít. Biztonsági riasztásokat, tanácsokat és iránymutatásokat ad ki a meghatározott személyeknek vagy szerepkörökben dolgozóknak, a kijelölt szervezeti egységeknek és a kijelölt külső szervezeteknek. A biztonsági iránymutatásokat az azokban foglaltak szerint alkalmazza.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

8.10.6 Információ kezelése és megőrzése

Követelmény:	Biztonsági osztály:	**Alap**
☐ Rendszer specifikus ☐ Általános ☐ Hibrid ☐ Nem alkalmazható	Referencia (7/2024 MK):	18.67.
A szervezet az EIR-ben lévő és az onnan kikerülő információk kezelése és megőrzése során a szervezetre vonatkozó, hatályos jogszabályok, irányelvek, szabályozások, szabványok és ajánlások és működési követelmények szerint jár el.		
A védelmi intézkedés státusza (csak egy választható): ☐ Megvalósítva ☐ Részben megvalósítva ☐ Nincs megvalósítva		
Védelmi intézkedés (tervezett) **megvalósításának részletei**		

Jóváhagyta:
Név:
Beosztás:

Kelt: <város>, <dátum>

10. számú melléklet
7/2025. (VII. 9.) főispáni utasításhoz

Felhasználói Felelősségvállalási Nyilatkozat

(új belépő részére)

A nyilatkozat célja a felhasználókban tudatosítani, hogy munkájuk során a lehető legnagyobb gondossággal járjanak el az elektronikus információs rendszerekben tárolt adatok használatakor annak érdekében, hogy az adatok bizalmassága, sértetlensége, és rendelkezésre állása a felhasználó szándékos, vagy gondatlan magatartásából ne sérüljön, illetve a felelősségük számonkérhető legyen.
Az informatikai infrastruktúrában tárolt adatok – melyek az érintettek (kormánytisztviselők, munkavállalók, szerződéses partnerek) személyes adatait tartalmazza - a kormányhivatal tulajdonát képezik.

Alulírott .....
Szervezeti egység .....
Anyja neve: .....
Születési helye és ideje: .....
Szerződéses partner esetén cégnév: .....
mint a kormányhivatal kormánytisztviselője/munkavállalója/szerződéses partnere kijelentem, hogy az Információ biztonsági szabályzatban foglaltakat megismertem, a rám vonatkozó szabályokat megértettem és azokat magamra nézve kötelező érvényűnek elismerem.

Kelt: ……..., ……..

……
nyilatkozattevő

11. számú melléklet
7/2025. (VII. 9.) főispáni utasításhoz

Titoktartási Nyilatkozat

(új belépő részére)

Alulírott

Név: .....
Születési hely, idő:.....
Szervezeti egység: .....
mint a Veszprém Vármegyei Kormányhivatal (a továbbiakban: kormányhivatal) kormányzati szolgálati jogviszonyban vagy munkaviszonyban álló foglalkoztatottja vagy a kormányhivatallal munkavégzésre irányuló egyéb jogviszonyban álló személy (a továbbiakban együtt: felhasználó) jelen Titoktartási Nyilatkozat (a továbbiakban: nyilatkozat) aláírásával kötelezettséget vállalok arra, hogy:

a) a kormányhivatal által rendelkezésemre bocsátott, vagy a munkavégzésem során megismert minősített, személyes és bizalmas adatokat (a továbbiakban: érzékeny adatok) a mindenkor hatályos, az adatok védelmére vonatkozó jogszabályokban, valamint a kormányhivatal tevékenységét szabályozó belső szabályzatokban meghatározott módon kezelem és megőrzöm azok bizalmasságát,

b) az érzékeny adatokat semmilyen formában, semmilyen eszközzel, illetve semmilyen céllal nyilvánosságra nem hozom, azokat harmadik személlyel nem közlöm, illetéktelennek nem adom át, nem terjesztem, nem teszem közzé, nem reprodukálom, nem fejtem vissza, és mindent megteszek annak érdekében, hogy ezen adatok titkosságát megőrizzem, azokat harmadik személy részére nem teszem hozzáférhetővé,

c) a tudomásomra jutott személyes adatokat, egyéb személyes információkat szintén bizalmasan kezelem AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény rendelkezéseinek, valamint jelen nyilatkozatban vállaltak betartásával.

Tudomásul veszem, hogy jelen nyilatkozatban leírtak megszegéséért polgári jogi és büntetőjogi felelősséggel tartozom, a munkavégzésre irányuló jogviszony megszűnését követően is.

Kelt: ……..., …….

……..…….....…
kormánytisztviselő/munkavállaló/megbízott

12. számú melléklet
7/2025. (VII. 9.) főispáni utasításhoz

Titoktartási Nyilatkozat

(nem a Veszprém Vármegyei Kormányhivatal alkalmazásában álló személyek részére)

Alulírott:
Cégnév: .....
Székhely: .....
Cégjegyzék szám: .....
Képviselő személy:
Név: .....
Születési hely, idő:.....
Lakcím vagy személyi igazolvány szám:.....
(a továbbiakban: vállalkozó)

alulírott napon és helyen az alábbi nyilatkozatot (a továbbiakban: nyilatkozat) teszi.

I. Előzmény

A Vállalkozó és a Veszprém Vármegyei Kormányhivatal (székhely: 4024 Debrecen, Piac utca 54., a továbbiakban: kormányhivatal) ……. szerződésszámú/iktatószámú szerződést (a továbbiakban: szerződés) kötöttek.

A kormányhivatal üzleti titkainak és nem nyilvános információinak titokban maradása érdekében a vállalkozó jelen nyilatkozatot teszi.

II. Fogalmak, értelmező rendelkezések

Jelen Nyilatkozat és a Szerződés alkalmazásában az alábbi kifejezések a következők szerint értelmezendők:

Bizalmas információ: üzleti titoknak, valamint személyes adatnak minősülő információk, ideértve az azokból levonható következtetéseket is, amelyet a kormányhivatal a Szerződéssel összefüggésben a Vállalkozó részére átad, vagy amely a Szerződés teljesítése során egyéb módon a Vállalkozó tudomására jut.

Üzleti titok: az üzleti titok védelméről szóló 2018. évi LIV. törvény 1. § (1) bekezdése értelmében a gazdasági tevékenységhez kapcsolódó, titkos – egészben, vagy elemeinek összességeként nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető -, ennélfogva vagyoni értékkel bíró olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek a titokban tartása érdekében a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja.

Védett ismeret (know-how): az üzleti titok védelméről szóló 2018. évi LIV. törvény 1. § (2) bekezdése értelmében az üzleti titoknak minősülő, azonosításra alkalmas módon rögzített, műszaki, gazdasági vagy szervezeti ismeret, megoldás, tapasztalat vagy ezek összeállítása.

A fentiekre tekintettel üzleti titoknak minősülnek különösen - de nem kizárólagosan - a kormányhivatal belső szabályzatai, a know-how, az informatikai és fizikai hozzáférés ellenőrzését biztosító adatok (felhasználónevek és jelszavak), üzleti vagy üzemi folyamatok és módszerek, tervek és specifikációk, pénzügyi adatok, szoftverek és adatbázisok, valamint más szellemi alkotások.

Üzleti titoknak minősül továbbá a kormányhivatal minden stratégiai elképzelése, üzleti, ügyviteli folyamatai, valamint a Szerződés eredményeképpen megvalósuló együttműködés során a kormányhivatallal kapcsolatban a Vállalkozó tudomására jutott minden adat, információ, tény, megoldás, továbbá a Vállalkozó részére a kormányhivatal által átadott adatok, információk, tények, megoldások stb.

A Vállalkozó és/vagy munkavállalója, alkalmazottja és/vagy közreműködője tudomására jutott valamennyi tény, információ, adat szintén üzleti titkot képez.

Személyes adat: az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 3. § 2. pontjában foglaltaknak megfelelően az érintettre vonatkozó bármely információ.

Nem minősülnek bizalmas információnak, így a Vállalkozó átadhat, nyilvánosságra hozhat, terjeszthet és használhat olyan információkat:

a) amelyek titoktartási kötelezettség nélkül már a birtokában vannak, kivéve, ha azok bármely okból kormányhivatal üzleti titkainak, vagy kormányhivatal ügyfeleire vonatkozó titkoknak minősülnek,
b) amelyeket egyedileg dolgozott ki és független a kormányhivatal üzleti titkaitól,
c) amelyeket titoktartási kötelezettség nélkül, nem a kormányhivataltól, hanem más forrásból szerzett, kivéve, ha azok bármely okból kormányhivatal üzleti titkainak, vagy kormányhivatal ügyfeleire vonatkozó titkoknak minősülnek,
d) amelyek az információ közlésekor nyilvánosan hozzáférhetők, vagy hozzáférhetővé váltak, és ez nem a Vállalkozó hibájából történt.

III. A Nyilatkozat tárgya

A Vállalkozó a Szerződés teljesítése eredményeképpen megvalósuló együttműködés során a kormányhivatallal kapcsolatban, avagy arra vonatkozó, valamint vele kapcsolatba hozható, bármely formában és módon tudomására jutott bizalmas információk kezelése és megőrzése érdekében az alábbiak szerint nyilatkozik:

1. A Vállalkozó kötelezettséget vállal arra, hogy a kormányhivatal bizalmas információit időbeli korlátozás nélkül megőrzi. A Vállalkozó az együttműködés tényét részleteit, valamint az annak alapján, illetve során szerzett, tudomására jutott, avagy rendelkezésére bocsátott bizalmas információkat titokként kezeli, azokat csak a kormányhivatal, - illetve szükség esetén a titok jogosultjának együttes - előzetes írásbeli hozzájárulásával, a kormányhivatal által meghatározott célokra használja fel, vagy jogszabály által előírt esetekben szolgáltatja ki harmadik személynek, hozza nyilvánosságra, másolja, avagy reprodukálja. A titoktartási kötelezettség kiterjed a Szerződésre és jelen Nyilatkozatra egyaránt. Vállalkozó felelős minden olyan vagyoni és nem vagyoni kárért, ami bizonyítottan ezen kötelezettségek megsértéséből ered, kártérítési felelőssége kiterjed a gazdagodása megtérítésére is. Ha a Vállalkozó vagy olyan munkavállalója, alvállalkozója, teljesítési segédje, akinek magatartásáért felelősséggel tartozik, megsérti jelen Nyilatkozatban foglalt titoktartási kötelezettségét, azért a Vállalkozó teljes kártérítési felelősséggel tartozik.
2. A titoktartási kötelezettség a Vállalkozót, annak munkavállalóit, alkalmazottait, vagy munkavégzésre irányuló egyéb jogviszonyban álló, általa foglalkoztatottak, valamint az általuk az együttműködés során igénybe vett közreműködőket kölcsönösen, időbeli korlátozás nélkül terheli minden olyan bizalmas információnak minősülő tény, adat, információ, megoldás stb. vonatkozásában, mely a tárgyalások, illetve az együttműködés során, bármilyen formában és módon a kormányhivatalról, vagy vele kapcsolatban, valamint arra vonatkozóan tudomására jut.
3. A jelen Nyilatkozat körébe tartozó információ átadása a következőképpen történhet:
a) adathordozó átadással (pl. papír, USB kulcs, CD stb.),
b) az információkhoz való hozzáférés engedélyezésével (pl. számítógépes hozzáférési jogosultság),
c) szóban és/vagy vizuális bemutatással.
4. A Vállalkozó kötelezettséget vállal arra, hogy a kormányhivatal hivatali tevékenységére vonatkozó információk rögzítésére semmiféle technikai eszközt vagy más eszközt nem alkalmazhat.
5. A Vállalkozó kötelezettséget vállal arra, hogy az együttműködés során a tudomására jutott bizalmas információnak minősülő anyagokat, adatokat, dokumentumokat, információkat a hatályos jogszabályok szerinti módon és ideig megőrzi. Ezeket harmadik személyeknek nem adhatja át, nyilvánosságra nem hozhatja, a Vállalkozó és a kormányhivatal közötti szerződés teljesítésének elősegítésén túl, az ott szabályozott céltól eltérően nem használhatja fel, és a kormányhivatal érdekeit sértő vagy veszélyeztető módon nem kezelheti, nem módosíthatja, valamint nem semmisítheti meg.
5. A Vállalkozó kifejezetten tudomásul veszi, hogy a kormányhivatalról, illetve annak ügyfeleiről tudomására jutott bizalmas információ illetéktelen harmadik személlyel történő szóbeli közlése is nyilvánosságra hozatalnak minősül.
6. A Vállalkozó köteles az iratkezelése során arról gondoskodni, hogy a bizalmas információt tartalmazó iratokhoz illetéktelen személyek ne férjenek hozzá. A dokumentumokat elzárt helyen köteles őrizni. Vállalkozó gondoskodik továbbá a titoktartási kötelezettsége megtartásához szükséges összes feltétel megvalósításáról, megtesz minden olyan biztonsági követelményt, amely ehhez szükséges, és amely az illetéktelen személyek bizalmas információhoz történő hozzáférését megakadályozza.

7. A Vállalkozó szavatol azért, hogy rendelkezik azokkal a feltételekkel, melyek alkalmasak arra, hogy tevékenysége és működése során az átvett és a Szerződés során tudomására jutott személyes adatokat az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény rendelkezéseinek betartásával és annak megfelelően kezelje.
8. A Vállalkozó vállalja, hogy munkavállalóival, alkalmazottaival, vagy munkavégzésre irányuló egyéb jogviszonyban álló, általa foglalkoztatott személyekkel, valamint az általa az együttműködés során igénybe vett közreműködőkkel szemben teljeskörűen érvényre juttatja jelen Nyilatkozat titoktartásra vonatkozó rendelkezéseit.
9. A Vállalkozó vállalja, hogy a tudomására jutott titoktartási kötelezettség megsértésről a kormányhivatalt haladéktalanul értesíti, valamint a kormányhivatallal együttműködik a jogsértés körülményeinek feltárásában.
10. A Vállalkozó a Szerződést és annak eredményét üzleti referenciaként csak a kormányhivatal előzetes írásbeli hozzájárulásával jogosult említeni, vagy arra hivatkozni.
11. A Vállalkozó tudomásul veszi, hogy a titoktartási kötelezettséggel való visszaélés súlyos szerződésszegésnek minősül - ideértve a Vállalkozó munkavállalói vagy alvállalkozói általi visszaéléseket is - és a kormányhivatal jogosult a Szerződésben a súlyos szerződésszegés esetére vonatkozó jogkövetkezmények alkalmazására.

A Vállalkozó a Nyilatkozatot elolvasás és értelmezés után, mint akaratával mindenben megegyezőt, jóváhagyólag írta alá.

Kelt: ……..., ……..

……
Vállalkozó

13. számú melléklet
7/2025. (VII. 9.) főispáni utasításhoz

Kockázati szorzótábla

Kárérték szint	Előfordulási valószínűsége				
	1. nem értelmezhető	2. csekély	3. közepes	4. nagy	5. nagyon nagy
1. nem értelmezhető	Alacsony	Alacsony	Alacsony	Közepes	Közepes
2. csekély kár	Alacsony	Alacsony	Közepes	Közepes	Közepes
3. közepes kár	Alacsony	Közepes	Közepes	Közepes	Magas
4. nagy kár	Közepes	Közepes	Közepes	Magas	Magas
5. nagyon nagy kár	Közepes	Közepes	Magas	Magas	Magas

14. számú melléklet
7/2025. (VII. 9.) főispáni utasításhoz

A kár mértéke az EIR vagy az általa kezelt adatok bizalmasságának elvesztése esetén

Kárérték szint/Kárfajta	Közvetlen anyagi kár	Társadalmi-politikai hatás	Bizalmasság sérülése
1. nem értelmezhető	Az érintett szervezet költségvetéséhez képest jelentéktelen	Nincs bizalomvesztés, a probléma a szervezeten belül marad és meg is oldható	Elhanyagolható
2. csekély kár	Eléri a szervezet költségvetésének 1%-át	Az érintett szervezeten belül kezelhető	Belső szabályozóval védett adat vagy néhány személyes adat bizalmassága sérülhet. Az üzlet vagy ügymenet szempontjából csekély értékű, és/vagy csak belső szabályzóval védett adat vagy EIR bizalmassága sérül.
3. közepes kár	Eléri a szervezet költségvetésének 5%-át	Bizalomvesztés a szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettség sérülhet	Nagy mértékű személyes adat bizalmassága vagy különleges adat bizalmassága sérülhet
4. nagy kár	Eléri a szervezet költségvetésének 10%-át	Jogszabályok betartása vagy végrehajtása elmaradhat, bizalomvesztés a szervezeten belül, a felső vezetésben vagy vezetésben személyi felelősségre vonást kell alkalmazni.	Tömeges különleges személyes adat bizalmassága sérülhet
5. nagyon nagy kár	Eléri a szervezet költségvetésének 15%-át	Súlyos bizalomvesztés a szervezettel szemben, alapvető emberi vagy társadalom működése szempontjából kiemelt jogok sérülhetnek.	Kiemelten tömeges különleges adat bizalmassága sérülhet

15. számú melléklet
7/2025. (VII. 9.) főispáni utasításhoz

A kár mértéke az EIR vagy az általa kezelt adatok sértetlenségének elvesztése esetén

Kárérték szint/Kárfajta	Közvetlen anyagi kár	Adat, információs rendszer sérülés	Társadalmi-politikai hatás
1. jelentéktelen kár	Az érintett szervezet költésvetéséhez képest jelentéktelen	Az érintett szervezet költésvetéséhez képest jelentéktelen	A probléma a szervezeten belül marad és meg is oldható
2. csekély kár	Eléri a szervezet költségvetésének 1%-át	Az üzlet vagy ügymenet szempontjából csekély értékű, és/vagy csak belső szabályzóval védett adat, vagy EIR sérül.	A társadalmi hatás az érintett szervezeten belül kezelhető
3. közepes kár	Eléri a szervezet költségvetésének 5%-át	Az üzlet- vagy ügymenet szempontjából érzékeny folyamatokat kezelő EIR, információt képező adat vagy egyéb jogszabállyal védett adat sérül.	Bizalomvesztés a szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettség sérülhet
4. nagy kár	Eléri a szervezet költségvetésének 10%-át	Az üzlet- vagy ügymenet szempontjából nagy értékű, üzleti titkot, vagy különösen érzékeny folyamatokat kezelő EIR vagy információt képező adattömegesen, vagy jelentősen sérül	Jogszabályok betartása vagy végrehajtása elmaradhat, bizalomvesztés a szervezeten belül, a felső vezetésben vagy vezetésben személyi felelősségre vonást kell alkalmazni.
5. nagyon nagy kár	Eléri a szervezet költségvetésének 15%-át	A nemzeti adatvagyon helyreállíthatatlanul megsérül	Súlyos bizalomvesztés a szervezettel szemben, alapvető emberi vagy társadalom működése szempontjából kiemelt jogok sérülhetnek.

16. számú melléklet
7/2025. (VII. 9.) főispáni utasításhoz

A kár mértéke az EIR vagy az abban tárolt adatok rendelkezésre állásának elvesztése esetén

Kárérték szint/Kárfajta	Közvetlen anyagi kár	Társadalmi-politikai hatás	Rendelkezésre állás
1. jelentéktelen kár	Az érintett szervezet költésvetéséhez képest jelentéktelen	A probléma a szervezeten belül marad és meg is oldható	Az érintett szervezet működése szempontjából jelentéktelen adat vagy EIR rendelkezésre állása nem biztosított.
2. csekély kár	Eléri a szervezet költségvetésének 1%-át	A társadalmi hatás az érintett szervezeten belül kezelhető	Az üzlet vagy ügymenet szempontjából csekély értékű, és/vagy csak belső szabályzóval védett adat vagy EIR rendelkezésre állása nem biztosított.
3. közepes kár	Eléri a szervezet költségvetésének 5%-át	Bizalomvesztés a szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettség sérülhet	Az üzlet- vagy ügymenet szempontjából érzékeny folyamatokat kezelő EIR, információt képező adat vagy egyéb jogszabállyal védett adat rendelkezésre állása nem biztosított.
4. nagy kár	Eléri a szervezet költségvetésének 10%-át	Jogszabályok betartása vagy végrehajtása elmaradhat, bizalomvesztés a szervezeten belül, a felső vezetésben vagy vezetésben személyi felelősségre vonást kell alkalmazni.	Az üzlet- vagy ügymenet szempontjából nagy értékű üzleti adat vagy EIR rendelkezésre állása nem biztosított.
5. nagyon nagy kár	Eléri a szervezet költségvetésének 15%-át	Súlyos bizalomvesztés a szervezettel szemben, alapvető emberi vagy társadalom működése szempontjából kiemelt jogok sérülhetnek. Az ország, a társadalom működőképességének fenntartását biztosító EIR rendelkezésre állása nem biztosított.	Az ország, a társadalom működőképességének fenntartását biztosító létfontosságú EIR rendelkezésre állása nem biztosított;

17. számú melléklet
7/2025. (VII. 9.) főispáni utasításhoz

A bizalmasság, sértetlenség és a rendelkezésre állás becsült kárérték szintjei

Rendszer funkció	Támogatott folyamat	A rendszerben kezelt adatok	B	S	R	Besorolás indoklása
Funkció	Folyamat	Adatkör1				