Veszprém Megyei Kormányhivatal

Informatikai Biztonsági Szabályzat

Tartalomjegyzék

A *jogalkotásról szóló 2010. évi CXXX. törvény 23. § (4) bekezdés i) pontja* alapján, figyelemmel *az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 11. § (1) bekezdés f) pontjára*, az elektronikus információs rendszerek védelmére vonatkozóan a Veszprém Megyei Kormányhivatalban az alábbi vezetői utasítást adom ki.

I. A szabályzat célja

Az Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) célja, hogy a Kormányhivatal működése és szolgáltatásai során biztosítsa a Kormányhivatal által kezelt, feldolgozott, továbbított, valamint tárolt adatok kockázattal arányos védelmét (bizalmasság, sértetlenség és rendelkezésre állás) a felmerülő veszélyforrások ellen. A védelmet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) és az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet szerinti (a továbbiakban együttesen: jogszabály), valamint az alkalmazott szabványi előírások alapján valósítja meg.

Az IBSZ célja továbbá az Informatikai Biztonsági Politikában (a továbbiakban: IBP) megfogalmazott általános elektronikus információbiztonsági irányelvek érvényre juttatásának biztosítása, az ehhez szükséges egyes elektronikus információbiztonsági szerepkörök, feladatok, folyamatok szabályainak, eljárásainak, követelményeinek a meghatározása az elektronikus információbiztonsággal összefüggésben.

II. A szabályzat hatálya

A szabályzat célja fejezetben meghatározott célok elérése érdekében a szabályzat hatálya az alábbi területekre terjed ki.

II.1 Tárgyi hatály

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

II.2 Területi hatály

A szabályzat területi hatálya kiterjed a Kormányhivatal székhelyére, minden telephelyére, továbbá mindazon objektumokra és helyiségekre, ahol a Kormányhivatal elektronikus információs rendszereket működtet, üzemeltet vagy fejleszt.

II.3 Személyi hatály

A szabályzat személyi hatálya kiterjed a Kormányhivatalnál bármely munkavégzésre irányuló jogviszonyban (munkaviszonyban) álló természetes személyre, azzal a megjegyzéssel, hogy a Kormányhivatal által használt elektronikus információs rendszerek külső üzemeltetőire, fejlesztőire, szerződéses úton történő egyéb alkalmazóira e szabályzat rendelkezéseinek megtartását szerződésben, vagy egyéb megállapodásban rögzíteni kell.

A munkaviszonyon érteni kell az összes alább felsorolt jogviszonyt is.

Jelen Szabályzat rendelkezései alkalmazandók az agrár- és vidékfejlesztést támogató szakterülete vonatkozásában is, amennyiben a főosztály feladatellátásában részt vevő felettes szerv eljárásrendje eltérő szabályokat nem állapít meg.

Az agrár- és vidékfejlesztést támogató szakterület feladatellátásához szükséges informatikai rendszerekhez való hozzáférés és jogosultságkezelés eljárásrendje tekintetében a rendszereket központi szolgáltatóként biztosító szervezet eljárásrendjét kell alkalmazni.

A Kormányhivatal az agrár- és vidékfejlesztést támogató szakterület által helyben használt hardver és szoftver elemek vonatkozásában biztosítja a megfelelő üzembiztonsági és rendelkezésre állási körülményeket a folyamatos munkavégzés biztosítása érdekében.

III. A szabályzattal kapcsolatos feladatok

A szabályzattal kapcsolatos feladatokat és felelősségeket az alábbi táblázat szemlélteti:

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
Szabályzat elkészítése, felülvizsgálata és módosítása	IBF	IBF	Informatikai Biztonsági Tanács az elektronikus információs rendszer üzemeltetéséért, fejlesztéséért felelős szervezeti egységek vezetői, IBM	KMB
Szabályzat elfogadása és kihirdetése	KMB	KMB	-	-
Szabályzat betartásának ellenőrzése	IBF	IBF	az elektronikus információs rendszer üzemeltetéséért, fejlesztéséért felelős szervezeti egységek vezetői, IBM	-

III.1 A szabályzat elkészítése, felülvizsgálata és módosítása

A szabályzat elkészítése, felülvizsgálata és szükség szerinti módosítása az **Informatikai biztonsági felelős** feladata és felelőssége, együttműködve az Informatikai Biztonsági Tanács munkacsoporttal. A szabályzat elkészítésében, felülvizsgálatában és módosításában közreműködnek az elektronikus információbiztonsági feladatok ellátásában közreműködő személyek, szervezeti egységek, munkacsoportok, valamint az elektronikus információs rendszer üzemeltetéséért, fejlesztéséért felelős szervezeti egységek vezetői. A szabályzatot felül kell vizsgálni minden olyan esetben – de legalább évente egyszer –, amikor azt az elektronikus információbiztonságot érintő szervezeti, műszaki, jogszabályi vagy egyéb változások indokolttá teszik.

A felülvizsgálat eredményéről az **Informatikai biztonsági felelős** tájékoztatja a **Kormánymegbízottat**.

III.2 A szabályzat elfogadása és kihirdetése

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

III.3 A szabályzat betartásának ellenőrzése

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

III.4 Kivételkezeléssel kapcsolatos feladatok

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

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

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

A kivételkezelés irányelvei:

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

IV. Az informatikai biztonság szervezete

IV.1 Informatikai biztonsági szerepek és felelősségek

IV.1.1 Kormánymegbízott (KMB)

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

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

Feladatai: Mint a Kormányhivatal első számú vezetője, köteles gondoskodni a jogszabályi megfelelésnek a következők szerint:

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

IV.1.2 Főigazgató / Igazgató (FŐIG/IG)

Hatásköre: A Kormányhivatal működését és személyi állományát érintő döntések meghozatala és a rá delegált munkáltatói jogok gyakorlása.

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

Feladatai: Mint a Kormányhivatal második számú vezetője, köteles a Kormánymegbízott által részére delegált informatikai biztonsági feladatokat ellátni.

IV.1.3 Informatikai Biztonsági Felelős (IBF)

Az Ibtv. értelmében a Kormányhivatalnak az elektronikus információs rendszer biztonságáért felelős személyt (Informatikai biztonsági felelős, a továbbiakban: IBF) kell megbíznia. A megbízólevélnek kifejezetten ki kell kitérnie az Ibtv. 13 § (1) – (7) bekezdése szerinti feladatok ellátását érintő személyes felelősségre és jogkörökre.

Amennyiben a szervezet elektronikus információs rendszereinek mérete vagy biztonsági igényei indokolják, a szervezeten belül elektronikus információbiztonsági szervezeti egység hozható létre, amelyet az elektronikus információs rendszer biztonságáért felelős személy vezet.

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

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

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

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

Továbbá biztosítja az Ibtv.-ben meghatározott követelmények teljesülését:

- a Kormányhivatal valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők tevékenysége során,

- ha a Kormányhivatal az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők az Ibtv. hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

IV.1.4 Informatikai Biztonsági Megbízott (IBM)

Hatásköre: Az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy, közreműködik az elektronikus információbiztonsággal kapcsolatos vezetői döntések előkészítésében, kivizsgálja az informatikai rendkívüli eseményeket, elvégzi a rendszeres biztonsági ellenőrzéseket, és javaslatokat tesz a hibák kijavítására. Ezen tevékenysége során szorosan együttműködik a biztonság megvalósításában résztvevő informatikai és egyéb szakemberekkel.

Felelőssége: Gondoskodik az elektronikus információbiztonsági ellenőrzések módszereinek és rendszerének kialakításáról és működtetéséről, valamint részt vesz a katasztrófa-elhárítási terv összeállításában és a működésfolytonosság biztosításában.

Feladatai: Mint az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy, az alábbiakban segíti és támogatja az Informatikai biztonsági felelős munkáját:

- felügyeli a beruházásokat, a fejlesztéseket és az ügyvitelt elektronikus információbiztonsági szempontból,
- munkája során felügyeli és ellenőrzi az elektronikus információbiztonsági követelmények megvalósulását, a szabályzatokban és eljárásrendekben foglaltak szabályszerű végrehajtását,
- a Szervezeti és Működési Szabályzat (a továbbiakban: SZMSZ), az ügyrend és a beosztási okirat alapján az informatikai rendszer szereplőinek jogosultságai ellenőrzésében közreműködik,
- az informatikai rendkívüli eseményeket, az esetleges rossz szándékú hozzáférési kísérletet, illetéktelen adatfelhasználást, visszaélést kivizsgálja, javaslatot tesz az Informatikai biztonsági felelősnek a további intézkedésekre, a felelősségre vonásra,
- összehangolja a biztonságot meghatározó, befolyásoló területek tevékenységét az informatikai biztonság érdekében,
- végrehajtja és/vagy támogatja a külső és belső auditok eredményes elvégzését.

IV.1.5 Szervezeti egység vezetők / Adatgazdák (SZEV / AG)

Hatáskörük: A szervezeti egységükhöz tartozó rendszerekhez és adatokhoz a hozzáférési – igénylés, módosítás, visszavonás – jogosultságok elbírálása, továbbá a szervezeti egységek dolgozói felé utasítási jogkörrel rendelkeznek.

Felelősségük: A közvetlen munkatársaik körében, illetve hatáskörébe tartozó elektronikus információs rendszerekben kezelt adatok informatikai biztonsági követelményeinek betartatása és az elektronikus információbiztonsági kontrollok működtetése, a Felhasználói Felelősségvállalási Nyilatkozatok adminisztrálása. Felelősségük továbbá a területükhöz tartozó személyes adatoknak a személyes adatok kezelésére vonatkozó jogszabályok szerinti, illetve a hivatali adatoknak a vonatkozó

jogszabályoknak és elvárásoknak megfelelő kezelése, valamint az ezekhez kapcsolódó hozzáférési jogosultságok szabályozása valamint felülvizsgálata.

Feladataik: Az IBIR szabályozó dokumentumokban rögzítettek szerint.

IV.1.6 Humánpolitikai feladatok ellátásáért felelős vezető (HSZV)

Hatásköre: A Kormányhivatal teljes területén általános humánpolitikai vonatkozásában ellenőrzési, véleményezési, javaslattételi, kezdeményezési, betekintési és hozzáférési jog illeti meg.

Felelőssége: A vonatkozó törvények és szabályok alapján a feladatkörök elektronikus információbiztonsági besorolása, a nemzetbiztonsági ellenőrzés alá eső feladatkörök felmérése és ellenőrzése, részvétel az informatikai biztonsági oktatások lebonyolításának szervezésében, fegyelmi eljárások nyilvántartása, a kilépők tájékoztatása a jogokról és kötelezettségekről.

Feladatai: Az IBIR szabályozó dokumentumokban rögzítettek szerint.

IV.1.7 Informatikai feladatok ellátásáért felelős vezető (IFEFV)

Hatásköre: Utasítási joggal rendelkezik az informatikai feladatokat ellátó szervezeti egységek munkatársai felé, valamint véleményezési, tájékoztatási joga van az informatikai üzemeltetést és fejlesztést érintő stratégiai és koncepcionális kérdésekben. Jogosult továbbá az elektronikus információbiztonság megszervezésére és ellenőrzésére.

Felelőssége: Irányítási jogkörének megfelelően az informatikai feladatokat ellátó szervezeti egységek és az elektronikus információs rendszerek szabályzatoknak és előírásoknak megfelelő működtetése.

Feladatai: Az IBIR szabályozó dokumentumokban rögzítettek szerint.

IV.1.8 IT üzemeltetésért felelős vezető (IÜFV)

Az IT üzemeltetésért felelős vezető feladatait az *Informatikai üzemeltetési eljárásrend* tartalmazza.

IV.1.9 Alkalmazás fejlesztésért felelős vezető (AFFV)

Az Alkalmazás fejlesztésért felelős vezető feladatait az *Alkalmazásfejlesztési szabályzat* tartalmazza.

IV.1.10 Alkalmazás támogatásért felelős vezető (ATFV)

Hatásköre: Utasítási joggal rendelkezik az alkalmazás támogató feladatokat ellátó szervezeti egység(ek) munkatársai felé, valamint véleményezési, tájékoztatási joga van az alkalmazás támogatást érintő stratégiai és koncepcionális kérdésekben.

Felelőssége: Irányítási jogkörének megfelelően az alkalmazás támogató feladatokat ellátó szervezeti egység(ek) szabályzatoknak és előírásoknak megfelelő működtetése.

Feladatai: Az IBIR szabályozó dokumentumokban rögzítettek szerint.

IV.1.11 Alkalmazás üzemeltetésért felelős vezető (AÜFV)

Az Alkalmazás üzemeltetésért felelős vezető feladatai az IBIR szabályozó dokumentumokban rögzítettek szerint *végzi.* .

IV.1.12 IT infrastruktúra fejlesztésért felelős vezető (IIFFV)

Hatásköre: Utasítási joggal rendelkezik az IT infrastruktúra fejlesztési feladatokat ellátó szervezeti egység(ek) munkatársai felé, valamint véleményezési, tájékoztatási joga van az IT infrastruktúra fejlesztést érintő stratégiai és koncepcionális kérdésekben.

Felelőssége: Irányítási jogkörének megfelelően az IT infrastruktúra fejlesztési feladatokat ellátó szervezeti egység(ek) szabályzatoknak és előírásoknak megfelelő működtetése.

Feladatai: Az IBIR szabályozó dokumentumokban rögzítettek szerint.

IV.1.13 Fizikai védelemért felelős vezető (FVFV)

Hatásköre: A Kormányhivatal teljes területén általános fizikai biztonsági és vagyonvédelmi vonatkozásában ellenőrzési, véleményezési, javaslattételi, kezdeményezési, betekintési és hozzáférési jog illeti meg.

Felelőssége: A vonatkozó törvények és szabályok alapján a fizikai védelmi szabályzatok, dokumentumok kialakítása, frissítése. A fizikai biztonsággal és vagyonvédelemmel kapcsolatos tervek, utasítások, szabályzatok elkészítése.

Feladatai: Az IBIR szabályozó dokumentumokban rögzítettek szerint.

IV.1.14 Tűzvédelmi felelős (TVF)

A Kormányhivatal tűzvédelemre vonatkozó szabályzása alapján előírt feladatok végrehajtásában működik közre.

IV.1.15 Munkavédelmi felelős (MVF)

A Kormányhivatal munkavédelemre vonatkozó szabályzása alapján előírt feladatok végrehajtásában működik közre.

IV.1.16 Rendszerüzemeltetést végző munkatársak

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

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

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

IV.1.17 Szervezeten belüli vagy kívüli felhasználók

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

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

Feladataik: Minden rendellenességet a szabályzatokban meghatározottak szerint haladéktalanul jelenteniük kell.

IV.2 Kapcsolattartás a hatóságokkal

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
Kapcsolattartás a hatóságokkal	IBF	IBF	-	KMB

A jogszabályokban meghatározott hatóságokat az **Informatikai biztonsági felelős** tájékoztatja az elektronikus információs rendszerek biztonsági eseményeiről és incidenseiről, valamint teljesíti a Kormányhivatal jogszabályi előírásként megfogalmazott elektronikus információbiztonsággal összefüggő adatszolgáltatási kötelezettségeit is, továbbá kapcsolatot tart fenn a jogszabály által kijelölt hatósággal.

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

A jogszabály által kijelölt hatóság részére az **Informatikai biztonsági felelős** az Ibtv. alapján előírt adatait be kell jelentenie.

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

V. Biztonsági szintbe és osztályba sorolás, informatikai biztonsági kockázatelemzés

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
Biztonsági szintbe és osztályba sorolás	IBM, SZEV/AG	IBF	-	KMB
Informatikai biztonsági kockázatelemzés	IBM, SZEV/AG, IFEFV, IIFFV, AFV, IÜFV, AÜFV, ATFV	IBF	-	KMB
Cselekvési terv készítése	IBF, IBM, IFEFV, IIFFV, AFV, IÜFV, AÜFV, ATFV	SZEV/AG,		KMB

A biztonsági szintbe és osztályba sorolást, valamint az informatikai biztonsági kockázatelemzést az **Informatikai biztonsági felelős** koordinálja az:

- **Szervezeti egység vezetők / Adatgazdák,**
- **Informatikai biztonsági megbízott,**
- **Informatikai feladatok ellátásáért felelős vezető,**
- **IT infrastruktúra fejlesztésért felelős vezető,**
- **Alkalmazás fejlesztésért felelős vezető,**
- **IT üzemeltetésért felelős vezető,**
- **Alkalmazás üzemeltetéséért felelős vezető,**
- **Alkalmazás támogatásért felelős vezető)**

(illetve az általuk kijelölt munkatársak) bevonásával.

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

V.1.1 Biztonsági szintbe és osztályba sorolás

A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében az elektronikus információs rendszereket – ideértve a rendszer által kezelt adatokat – biztonsági osztályba kell sorolni, a bizalmasságuk, a sértetlenségük, valamint a rendelkezésre állásuk szempontjából.
Az elektronikus információs rendszerek biztonsági osztályba sorolását az alábbi alapkövetelmények figyelembe vételével kell végrehajtani:

- a biztonsági osztályokhoz tartozó védelmi követelményeket jogszabály rögzíti,

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

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

A biztonsági szintbe és osztályba sorolást a szervezet vagy az elektronikus információs rendszer – illetve az abban kezelt adatok – jelentős megváltozása esetén, de legalább 3 évente felül kell vizsgálni.
A szervezet, szervezeti egységek elvárt biztonsági szintbe, valamint az elektronikus információs rendszerek elvárt biztonsági osztályba sorolását *az 1. számú függelék* tartalmazza.

V.1.1.1 Cselekvési terv készítése

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

A cselekvési terv elkészítése és folyamatos nyomon követése az **Informatikai biztonsági felelős** feladata, együttműködve az elektronikus információbiztonsági feladatok ellátásában közreműködő személyekkel, szervezeti egységekkel és munkacsoportokkal. A cselekvési terv elfogadása a **Kormánymegbízott** feladata.

V.1.2 Informatikai biztonsági kockázatelemzés

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

A felmerült kockázatok kezelésére intézkedési terveket kell készítenie az Informatikai biztonsági felelős közreműködésével az érintett erőforrás és adatgazdák által melyek a feltárt kockázatok függvényében az alábbiakat kell, hogy tartalmazzák:

- a kockázatok csökkentésére tett javaslatokat a technikai eszközök megváltoztatására, vagy fejlesztésére (pl.: új védelmi eszközök alkalmazása, vagy a jelenlegi átkonfigurálása),
- a kockázatok csökkentésére tett javaslatokat az érvényben lévő szabályozás megváltoztatására,

- a kockázatok csökkentésére tett javaslatokat a személyi állományra vonatkozóan (pl.: motiváció, a fegyelmi eljárások szigorítása, oktatás, stb.),
- a kockázatok tudatos felvállalására irányuló javaslatot, ha a védelmi intézkedés anyagi vonzata nagyobb, vagy közel azonos, mint a fenyegetettség által elszenvedhető anyagi kár.

VI. Üzletmenet- (ügymenet-) folytonosság tervezése

Az elektronikus információs rendszerek vonatkozásában kialakítandó Üzletmenet folytonosságra vonatkozó eljárásoknak az alábbi biztonsági osztályok szerint növekvő és egymásra épülő elvárásoknak kell megfelelni:

- 2-es biztonsági osztály: Üzletmenet-folytonosság tervezési (Business continuity planning, a továbbiakban: BCP) és Katasztrófa utáni helyreállítási tervezési (Disaster recovery planning, a továbbiakban: DRP) szabályzás és tervek kidolgozása és oktatása, kritikus rendszerelemek meghatározása
- 4-es biztonsági osztály: 2-es biztonsági osztály + BCP és DRP tesztelések, Tartalék feldolgozási helyszín kialakítása, szolgáltatás alapú hatáselemzés

Mindkét fenti követelményeket teljesíteni kell a kritikus informatikai szolgáltatások és infrastruktúra elemek esetében is.

VI.1 Üzletmenet-folytonossági eljárásrend

A Kormányhivatalnak *Üzletmenet-folytonosságra vonatkozó eljárásrendben* meg kell terveznie a működési folyamatait azon esetekre, mikor az azokat kiszolgáló elektronikus információs rendszerek valamilyen okból nem állnak rendelkezésre. Ezen eljárásrend kidolgozása, felülvizsgálata a **BC menedzser** és a **DR menedzser** feladata, a jóváhagyás az **Informatikai feladatok ellátásáért felelős vezető** felelőssége.

Az eljárásrendben kell kidolgozni:

- az üzletmenet-folytonosságot sértő katasztrófahelyzetek esetén felmerülő feladatokat, melyekhez felelősöket kell rendelni,
- a megfelelő kommunikációs folyamatokat az elektronikus információs rendszer kiesésére, hogy megfelelően és kellő gyorsasággal legyen kommunikálva a szervezeteken belül és a szervezetek által kiszolgált ügyfelek felé is az ügymenet megszakadása és a megkerülő megoldás aktiválása, és
- a meghatározott követelmények és feladatok dokumentációs rendszerét.

A Kormányhivatalnak *Katasztrófa utáni helyreállítási tervében (DRP)* ki kell dolgoznia azon eljárásait, amelynek keretében az informatikai erőforrások kiesése esetén a helyreállítást megvalósítja. Ezen eljárásrend kidolgozása, felülvizsgálata a **BC menedzser** és a **DR menedzser** feladata, a jóváhagyás az **Informatikai feladatok ellátásáért felelős vezető** felelőssége.

A tervben kell kidolgozni:

- a helyreállítás folyamatának lépéseit, szerepköreit, felelőseit, és
- a meghatározott követelmények és feladatok dokumentációs rendszerét.

VII. A biztonsági események és incidensek kezelése

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
A biztonsági esemény és incidenskezelés informatikai feltételrendszerének kialakítása	IFEFV, IÜFV, IIFFV	IFEFV	IBF, IM, IBM	FŐIG/IG

A Kormányhivatal rendszereibe bekerülő, illetve ott keletkező adatok, információk informatikai rendszerekben történő adatfeldolgozásával, működésével, üzemeltetésével és tárolásával kapcsolatban felmerülő biztonsági és elektronikus információbiztonsági események kezelése végett esemény és incidenskezelési szabályozást kell létrehozni.

A biztonsági esemény és incidenskezelés informatikai feltételrendszerének kialakításáért az **Informatikai feladatok ellátásáért felelős vezető** a felelős.

A biztonsági esemény és incidenskezelésre vonatkozó további részletes követelményeket és eljárásokat, továbbá szabályokat a *Biztonsági esemény és incidenskezelési eljárásrend* tartalmazza.

VII.1.1 Biztonsági osztály szerinti követelmények

Az elektronikus információs rendszerek vonatkozásában kialakítandó biztonsági esemény és incidenskezelési eljárásoknak az alábbi biztonsági osztályok szerint növekvő és egymásra épülő elvárásoknak kell megfelelni:

- 3-as biztonsági osztály: Biztonsági eseménykezelés szabályozása, figyelése, kezelése, valamint ezen tevékenység tervezése
  - Biztonsági eseménykezelési terv kidolgozása és kihirdetése
  - Események figyelése, kezelése
- 4-es biztonsági osztály: 3-as osztály + Biztonsági események figyelésének, támogatásának automatizálása, tervszerű működés tesztelése
  - Központi értékelő és riasztási rendszer (Security information and event management, a továbbiakban: SIEM rendszer)
  - A biztonsági események kezelésének tesztelése
  - A biztonsági eseménykezelés tesztelésének egyeztetése a kapcsolódó tervekért (pl. BCP, DRP) felelős szervezeti egységekkel.

VII.1.1.1 Általános követelmények

A Kormányhivatalnál kialakított biztonsági esemény és incidenskezelés során legalább a következőket kell teljesíteni:

- Az incidens bejelentését követően be kell azonosítani és kategorizálni a biztonsági eseményt és kategóriától függően a megfelelő személyt értesíteni kell.
- A biztonsági és elektronikus információbiztonsági események tárolására, kezelésére, követésére belső Helpdesk rendszert kell kialakítani, amelybe:
    - automatikusan, vagy
    - diszpécser vagy felelős informatikai feladatokat ellátó munkatárs (a továbbiakban: Diszpécser) útján manuálisan kerülnek be a biztonsági események.
- Megfelelő kompetenciával rendelkező incidenskezelő csoport létrehozása, mely szükség esetén bevonható az incidens elhárításába, kezelésébe.
- Biztonsági eseménykezelési terv kidolgozása, amely:
    - szabályozza a biztonsági eseménykezelési folyamatokat és eljárásokat,
    - ismerteti a biztonsági eseménykezelés szervezeti felépítését és annak illeszkedését a biztonsági irányítási, eseménykezelési, értesítési és kommunikációs szervezetbe és folyamatokba,
    - meghatározza az egyes incidens szinteken értesítendő/bevonandó vezetők (személyek, szerepkörök) értesítését és bevonását a döntési folyamatokba.

VIII. Az emberi erőforrások biztonsága

VIII.1 A munkaviszony kezdetét megelőzően

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
Feladatkör elektronikus információbiztonsági besorolása	HSZE	HSZV	IBF, IBM	-
Nemzetbiztonsági ellenőrzés alá eső munkakörök	HSZE	HSZV	-	-

VIII.1.1 Munkakörök elektronikus információbiztonsági besorolása

Minden munkakört elektronikus információbiztonsági kategóriákba kell sorolni, az alábbi szempontok szerint:

- **Fokozott** biztonsági kategóriába tartozik minden olyan munkakör, melynek betöltése, ellátása:
    - nemzetbiztonsági ellenőrzést igényel (lásd: *„Nemzetbiztonsági ellenőrzés alá eső munkakörök"* c. fejezetben), vagy
    - bármely elektronikus információs rendszerben privilegizált jogosultsággal rendelkezik, vagy
    - egyéb szempontok alapján kiemelt kockázatot hordoz magában.

- **Alap** biztonsági kategóriába tartozik minden olyan munkakör, mely az előbbi (fokozott) kategóriába nem került besorolásra.

A besorolás elvégzése és arról naprakész nyilvántartás vezetése, továbbá a felhasználók követelmények szempontjából történő megfelelésének folyamatos ellenőrzése a Humánpolitikai feladatok ellátásáért felelős szervezeti egység feladata és felelőssége, mely feladat ellátásában segítséget nyújt az **Informatikai biztonsági felelős** és az elektronikus információbiztonsági feladatok ellátásában közreműködő személyek.

VIII.1.2 Nemzetbiztonsági ellenőrzés alá eső munkakörök

A humánpolitikai feladatokat ellátó szervezeti egység feladata és felelőssége a vonatkozó jogszabályok alapján felmérni a nemzetbiztonsági ellenőrzés alá tartozó feladatköröket, amelyekről naprakész nyilvántartást kell vezetnie. E feladattal kapcsolatban a felhasználók jogszabályi követelményeknek történő megfelelését folyamatosan ellenőrizni kell.

VIII.2 A munkaviszony kezdetekor fellépő kötelezettségek

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
Felhasználói Felelősségvállalási Nyilatkozat	SZEV/AG	SZEV/AG	-	-
Kezdeti jogosultságok és eszközök	a vonatkozó szabályzat szerint	a vonatkozó szabályzat szerint	-	-
Informatikai biztonsági oktatások	HSZE, IBF	IBF	-	-

VIII.2.1 Felhasználói Felelősségvállalási Nyilatkozat

A jog-, munka-, szerződéses viszonyban álló munkatársak a Felhasználói Felelősségvállalási Nyilatkozat (*2. számú függelék*) aláírásával elismerik, hogy a jelen Szabályzatban meghatározott biztonsági elvárásoknak, előírásoknak eleget tesznek.

A nyilatkozat mindenkor aktuális verziójának a felhasználóval történő aláíratása és adminisztrálása a munkatárs **szervezeti egység vezetőjének** a feladata és felelőssége.

VIII.2.2 Kezdeti jogosultságok és eszközök igénylése

A belépő munkatárs munkavégzéséhez szükséges infokommunikációs eszközöket és jogosultságokat a munkatárs szervezeti egységének vezetője igényli meg az *Informatikai üzemeltetési eljárásrendben* foglaltak szerint.

Kezdeti jogosultságok között kell érteni a szükséges informatikai biztonsági oktatás megvalósításához használt e-Learning rendszert, ahol ilyen rendelkezésre áll.

VIII.2.3 Informatikai biztonsági oktatások

Az új belépők számára az IBSZ-ben foglalt előírások tudatosítása az **Informatikai biztonsági felelős** felelőssége. A képzés tartalmának és felépítésének összhangban kell lennie az új belépő által betöltendő feladatkörrel.

Az oktatásokon a felhasználókat fel kell készíteni a számukra kijelölt szerepkörökkel és felelősségekkel összhangban a lehetséges fenyegetések felismerésére, az elektronikus információs rendszerek informatikai biztonsági szabályoknak megfelelő használatára, az informatikai biztonsági események és incidensek szabályszerű kezelésére.

A naprakész informatikai biztonsági oktatási anyagok elkészítése az **Informatikai biztonsági felelős** felelőssége.

VIII.2.4 Informatikai biztonsági oktatások speciális munkakörök esetén

Az **Informatikai biztonsági felelős** és az elektronikus információs rendszerek biztonságával összefüggő feladatok ellátásában részt vevő személyek számára biztosítani kell a megfelelő szakmai éves továbbképzést a 26/2013. (X. 21.) KIM rendelettel összhangban. Továbbá igény szerint egyéb képzéseken való részvételt is biztosítani kell indokolt esetben.

VIII.3 A munkaviszony fennállása során

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
Az elektronikus információbiztonság tudatosítása	IBF, SZEV/AG	IBF	-	-
Viselkedési szabályok betartatása	SZEV/AG	SZEV/AG	IBF, informatikai feladatok ellátásért felelős szervezeti egység	-
Szoftverhasználati szabályok	SZEV/AG	SZEV/AG	IBF, informatikai feladatok ellátásért felelős szervezeti egység	-
Fegyelmi eljárások	HSZE, IBF, SZEV/AG	Munkáltatói jogkör gyakorlója	-	KMB

VIII.3.1 Az elektronikus információbiztonság tudatosítása

Az **Informatikai biztonsági felelős** indokolt esetben, de legalább évente egyszer ismételt képzésről gondoskodik a biztonságtudatosság növelése érdekében, mely során a legfontosabb változásokról

részletes tájékoztatást ad az érintetteknek. A képzés tartalmának és felépítésének összhangban kell lennie az érintettek által betöltött munkakörrel és annak elektronikus információbiztonsági besorolásával.
Az oktatáson való részvétel minden felhasználó számára kötelező, aki a munkavégzése során informatikai rendszert használ. A részvételért a felhasználó szervezeti egységének vezetője a felelős, annak dokumentálása, illetve a megfelelő dokumentálási keretek biztosítása pedig az **Informatikai biztonsági felelős** feladata.

A felhasználók a szabályzatokat érintő változásokról, valamint a legfontosabb informatikai biztonsági eseményekről és trendekről az oktatások mellett alkalmi jelleggel kiegészítő tájékoztatást kaphatnak, mely az **Informatikai biztonsági felelős** feladata és felelőssége.

VIII.3.2 Viselkedési szabályok, felhasználó felelőssége

A kormányhivatali információs rendszerrel, a rendszer üzemeltetésével vagy a rendszer elhelyezésére szolgáló objektummal kapcsolatban álló felhasználóknak kötelessége jelenteni olyan nem kívánt vagy nem várt egyedi vagy sorozatos informatikai biztonsági eseményeket, amelyek nagy valószínűséggel veszélyeztetik a Kormányhivatali tevékenységet és fenyegetik az informatikai biztonságot. A bejelentést a Helpdesk bejelentő felületen keresztül köteles a felhasználó elvégezni. Ennek akadályoztatása esetén, telefonon vagy e-mailen keresztül kell elvégezni a bejelentést.

Informatikai biztonsággal kapcsolatos bejelentések elérhetőségeit a szabályzat *3. számú függeléke* „Biztonsági események bejelentési elérhetőségei" tartalmazza.

Az elektronikus levelezésre és az Internetes böngészésre vonatkozó szabályok:

- A hivatali levelezőrendszer a munkavégzéssel kapcsolatos ügyintézést szolgálja. A levelező rendszer tárterülete korlátozott, ennek tudatában ahol lehet, csatolmányok helyett hivatkozásokat kell használni (pl. fájl szerveren az elérési út).
- A hivatali levelező kliens beállításait nem szabad módosítani vagy privát e-mail fiókokat (pl. Gmail, Freemail) hozzáadni.
- Ismeretlen helyről származó, gyanús e-mail megnyitásakor a felhasználó köteles mérlegelni, hogy a levél vagy csatolmánya vírust tartalmazhat, az észlelt kockázatot jelezze az informatikai és információbiztonsági szervezet irányába.
- Hivatali e-mail címet magáncélra – online regisztrációhoz, hírlevél feliratkozáshoz, fórum feliratkozáshoz – nem szabad használni.
- A levelezés során nevesített postafiókokat kizárólag a hozzárendelt felhasználó használhatja, más postafiókjának használata tilos.

Nem megengedettek továbbá az alábbiakban bemutatásra kerülő viselkedési formák és tevékenységek:

- hivatali kommunikációra magánjellegű postafiókot (pl. Gmail, Freemail) használni;

- zavaró, indokolatlanul nagy méretű, félreinformáló és lánc levelek küldése;
- másokra nézve sértő, mások vallási, etnikai, politikai vagy másokat egyéb módon sértő, zaklató tevékenység folytatása;
- profitszerzést célzó direkt üzleti célú tevékenység, reklámok terjesztése;
- a hivatali adattároló eszközökön tilos magánjellegű, vagy a hivatali munkához nem kapcsolódó dokumentumokat, fényképeket, videókat tárolni;
- idegen, a Kormányhivatal által előírt védelmi megoldásokkal nem rendelkező infokommunikációs eszközöket a Kormányhivatal hálózataihoz csatlakoztatni.

A Kormányhivatal elektronikus levelezési rendszerének használata:

- A Kormányhivatalok szervezeti egységeinek a GroupWise levelező rendszert kell használni mind belső mind külső levelezés tekintetében. Ettől eltérő egyedi levelezőrendszerek használata nem megengedett. A levelező rendszer szerver oldali üzemeltetését a Miniszterelnökség felügyelete mellett külső szervezetek látják el.
- A kliens program tekintetében a GroupWise klienst kell használni.
- GroupWise használata számítógépen keresztül:
    - A számítógépre telepített kliens program segítségével vagy a https://webmail.kh.gov.hu webcímen elérhető WebAccess alkalmazás útján. Az interneten történő bejelentkezési lehetőség a kormányhivatali és az otthoni környezetben is elérhető. Mindkét felhasználási mód esetében használható a helyettesítés funkció.
    - A fiók használata azonban kizárólag kormányhivatali vagy saját – kizárólag abban az esetben, ha a saját eszköz a kormányhivatali eszközök védelmével egyenértékű biztonsági megoldásokkal védett – tulajdonú számítógépen engedélyezett, tekintettel arra, hogy az elektronikus postafiók megnyitását követően a hivatali levél tartalma és/ vagy annak csatolt dokumentuma(i), eltárolódhatnak a számítógép adattárolóján.
    - Tilos a postafiókot használatba venni publikus helyen elhelyezett számítógépeken és egyéb mobil eszközökön (pl. kávézóban, hotelben, stb.), vagy más idegen eszközökön (pl. ismerős számítógépe, tabletje, stb.).
- GroupWise használata mobiltelefonon keresztül:
    - A GroupWise levelező rendszer hivatali mobiltelefonon keresztül történő elérése indokolt esetben, igénylés után lehetséges, a felettes vezető igénylése és az **Informatikai feladatok ellátásáért felelős vezető** engedélye alapján.
- Külső kapcsolatokban az elektronikus levelezést minden esetben hivatalos szervezeti fejlécű levélpapírra írott levélhez, nyilvánosság szempontjából pedig (a titkosított levelek kivételével) a nyílt levelezőlaphoz hasonlóan kell kezelni.

- 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.
- Mások elektronikus levelezésének figyelése, levélcímének (elektronikus személyazonosságának) használata, leveleinek elolvasása tilos!
- Lánclevelek indítása és továbbítása nem engedélyezett!
- 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 **Informatikai biztonsági felelős** kezdeményezése vagy a felhasználó **szervezeti egység vezetőjének**, mint adatkezelőnek indoklással alátámasztott kérése alapján az **Informatikai feladatok ellátásáért felelős vezető**, a **Kormánymegbízott** vagy a **Főigazgató/Igazgató** rendelheti el. Az ellenőrzést az **Informatikai biztonsági felelős** és az **Informatikai feladatok ellátásáért felelős szervezeti egység** kijelölt munkatársai közösen végzik. A vizsgálat végrehajtásáról és annak megállapításairól jegyzőkönyv készül.
- A hivatali szervezeti e-mail címekhez tartozó elektronikus postafiókot a szervezeti egység vezetője által kijelölt személy köteles rendszeresen figyelni. A szervezeti e-mail fiókokhoz a hozzáférés a személyes hivatali célú postafiókon keresztül helyettesítés funkció használatával lehetséges. A felhasználói nevet és jelszót az **Informatikai feladatok ellátásáért felelős szervezeti egység** kezeli, azt a felhasználók részére nem adja ki.
- A használat során figyelemmel kell lenni arra, hogy a személyes e-mail cím tulajdonosának távolléte esetén az elektronikus postafiók figyelése nem biztosított.
- A kormányhivatal központi és a szervezeti egységek hivatali e-mail címeihez tartozó postafiókot legalább óránként egyszer, míg a személyes e-mail címekhez tartozó postafiókot naponta legalább háromszor kell ellenőrizni.
- 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.
- 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, mivel azok folyamatos figyelése biztosított. 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.
- Az elektronikus üzenetet aláírással kell ellátni, a Kormányhivatal arculatra vonatkozó szabályozásának megfelelően.
- A személyes hivatali e-mail postafiók felhasználója a levelező programban - távolléte esetén - köteles automatikus válaszadási üzenetet beállítani. Az üzenetben tájékoztatást kell adni az e-

mail feladójának, hogy a címzett mettől-meddig van távol és távollétében ki helyettesíti, valamint a helyettesítő milyen elérhetőségekkel rendelkezik.

- A hivatali e-mail címek igénylése a szervezeti egységek vezetőinek feladata.
- A kormányhivatali e-mail címekhez tartozó postafiókok magáncélú használata tilos.
- A hivatali postafiókokba ismeretlen vagy ismert feladótól vagy e-mail címről érkező, de értelmetlen szöveget tartalmazó elektronikus levelet (amely általában értelmetlennek tűnő gyanús csatolmányt is tartalmaz), kéretlen reklámüzenetet (spam) – a fennálló vírusveszély miatt – megnyitni TILOS! Ezeket az e-maileket haladéktalanul és véglegesen törölni kell (a törölt elemek mappából is).

  Fokozott elővigyázatossággal kell kezelni az ismeretlen feladótól érkező idegen nyelvű, esetleg magyartalan, illetve helyesírási hibákat tartalmazó e-maileket is. 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 törlés szükségessége, akkor segítséget kell kérni az **Informatikai feladatok ellátásáért felelős szervezeti egység** munkatársától. A vírusgyanús elektronikus levelet tilos továbbítani, szükség esetén az informatikai szakterület munkatársa a felhasználó munkaállomásán vizsgálja meg az e-mailt.
- Az elektronikus levélnek kötelező tárgyat adni, mert ellenkező esetben a levelező rendszerek vírusnak vélhetik és törölhetik azt. Tárgy nélkül elküldött elektronikus levelet – annak észlelése esetén – újra kell küldeni a tárgy megadásával.
- A kormányhivatal központi és a szervezeti egységek hivatali e-mail címeihez tartozó postafiókjaiból bármilyen mappa vagy levél törlése tilos.
- Az elektronikus levelek kormányhivatalon kívüli e-mail címre történő automatikus átirányításának beállítása tilos.
- Az elektronikus levelezés etikettje:
  - E-mail-eket nem szabad tömeges méretben (levelező lista) küldeni vagy továbbítani, kivéve, ha hivatali célból szükség van arra és pontosan ismert a címzettek köre.
  - Az e-mail nyelvezetének mindig tiszteletteljesnek kell lennie, közízlést, személyiségi jogokat nem sérthet.
  - E-mail üzenetben a „Címzett"-et meg kell szólítani, illetve a levél befejezéseként aláírással kell ellátni.

Személyes postafiókok jellemzői:

- 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.

- A postafiókból alapértelmezett beállítás szerint maximum 100 címzettnek lehet egyidejűleg levelet küldeni. Egy levél maximális mérete pedig maximum 60 MB lehet az alapértelmezett beállítás alapján;
- A kormányhivatali személyes e-mail címeket a vezetéknév.keresztnév@[MEGYE].gov.hu konvenció szerint kell képezni. Ettől eltérni csak kivételes esetben (pl. azonos nevek megkülönböztetése céljából) és csak az **Informatikai feladatok ellátásáért felelős vezető** engedélyével lehet.

Hivatali postafiókok adminisztrálása:

- 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.
- A **Szervezeti egység vezetőnek** nyilván kell tartania a szervezeti egység hivatali postafiókjainak használatához korábban megkért jogosultságokat. Amennyiben a hivatali postafiók kezelési joggal rendelkező munkatársának a munkaviszonya megszűnik, vagy másik szakterületre kerül, vagy a postafiók kezelői jogosultságát a **Szervezeti egység vezetője** a továbbiakban nem kívánja a felhasználó részére biztosítani, a **Szervezeti egység vezetőjének** kezdeményeznie kell a felhasználó hivatali postafiók kezelői jogosultságainak visszavonását.
- A hivatali fiókokra beállított felhasználói jogosultságok nyilvántartása a jogosultságok megfelelőségének kontrollálása a **Szervezeti egység vezetőjének** a felelőssége.

A hivatali postafiókok archiválása: A hivatali levelező rendszerből levelet törölni nem szabad. Ennek biztosítása érdekében automatikus archiválási rendszert kell kiépíteni és üzemeltetni, amely már a levél postafiókba történő érkezése pillanatában az archiválási tartós tárhelyen is elhelyezi a levél másolatát.

A jelszókezelés általános szabályai:

- A felhasználó a számítógépre csak saját nevében és jelszavával léphet be, és az alkalmazásokat csak saját nevében használhatja.
- A jelszavak nem hozhatók nyilvánosságra és nem oszthatók meg senkivel.
- A jelszavak bizalmasságának megőrzéséért a felhasználó személyesen felel.

- Ha a felhasználónak a legkisebb gyanúja is felmerül, a jelszó biztonságának integritása felől, azt köteles azonnal megváltoztatni és gyanújáról az **Informatikai biztonsági felelőst** értesíteni és a jelszót azonnal meg kell változtatnia.
- Más felhasználó azonosítóját átmeneti jelleggel sem szabad használni.
- A felhasználó köteles a jelszavát az előírt gyakorisággal és módon megváltoztatni.
- A felhasználónak az alapértelmezett jelszavakat az első belépés után kötelessége azonnal megváltoztatni.

A Felhasználó jogai és kötelességei:

- A felhasználó azonosítójával és jelszavával az informatikai rendszerben végrehajtott műveletekért személyesen felel.
- A számára kiosztott jogosultságokkal a rendszer erőforrásait és szolgáltatásait (hálózati tárhelyek, hálózati nyomtatás, stb.) használhatja.
- A nem mobil informatikai eszközök áthelyezése és/vagy leltárkörzet szerinti másik helyiségbe való áthelyezése a felhasználó által nem végezhető.
- Az informatikai eszközöket és szoftvereket rendeltetésszerűen kell használni.
- A felhasználó felelős a személyes használatra kiadott eszközök rendeltetésszerű használatáért és őrzéséért.
- Felelős a rábízott informatikai berendezések állapotának, állagának megőrzéséért.
- Az informatikai eszközöket a munka befejeztével, illetve a munkaidő végeztével áramtalanítani kell, amennyiben azok folyamatos üzemben tartása nem indokolt.
- Az informatikával kapcsolatos igényeit (kivéve a fogyóeszközök) a **Szervezeti egység vezetője** felé jelezheti.
- A számítógéptől való hosszabb (több mint 5 perc) távollét esetén a Felhasználó köteles a munkaállomást, vagy mobil számítástechnikai eszközt zárolni, vagy kilépni a rendszerből.
- A számítógépekre szoftver telepítése - függetlenül a szoftver származási helyétől - szigorúan tilos.
- A saját használatra átvett számítógép rendszerszintű beállításainak módosítása (ebbe nem értendők bele az irodai programok felhasználói beállításai), felhasználó számára nem engedélyezett.
- Az informatikai hálózat fizikai megbontása, a számítástechnikai eszközök lecsatlakoztatása (kivételt képeznek a hordozható eszközök), illetve bármilyen számítástechnikai eszköz hálózatra történő fizikai csatlakoztatása és/vagy beszerelése tilos.
- A hivatali adatok nem hivatali céllal történő kijuttatása, magán célú felhasználása, vagy harmadik személy rendelkezésére bocsátása tilos.
- A munkaállomást illetéktelen személy (pl. ügyfél) jelenléte mellett a felhasználó nem hagyhatja felügyelet nélkül.
- Az informatikai rendszerek használata csak hivatalos célokra engedélyezett;

- A használt informatikai eszközök kezelésével kapcsolatos felhasználói és biztonsági ismereteket el kell sajátítani.
- Az informatikai rendszerekben csak 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.
- A Kormányhivatal által rendszeresített biztonsági funkciókat (például automatikus képernyővédő-aktiválás) kikapcsolni, megkerülni tilos.
- A Kormányhivatal eszközein csak a Kormányhivatal által engedélyezett eszközöket és programokat szabad használni.
- Tartózkodni kell minden olyan tevékenységtől, amely az informatikai rendszerben a bizalmasság, sértetlenség vagy rendelkezésre állás sérülését okozhatja.

Felhasználók szerepe a vírusvédelemben:

- A felhasználókat meg kell ismertetni a kártékony kód felmerülésének esetében követendő előírásokkal, mivel aktív szerepet tölt be a tudatosság az előírt kártékony kódok elleni védelem alkalmazásában. Ha a felhasználók kellő odafigyelést tanúsítanak a vírusvédelemmel kapcsolatban, akkor a műszaki megoldásokkal együtt nagymértékben csökkenthető a kártevő programok okozta kockázat.
- A felhasználót tájékoztatni kell, hogy amennyiben a munkaállomás indítását követően az tapasztalható, hogy a vírusvédelmi program nem indult el (pl. ikonja nem látható), vagy ki van kapcsolva, akkor a munkavégzés megkezdése nem engedélyezett, az esetleges vírusfertőzésért a felhasználó felel. Ilyen esetben a munkaállomást le kell állítani, és értesíteni kell a **Diszpécsert**.
- Amennyiben a felhasználó a vírusvédelmi rendszer által generált riasztás kap, azt haladéktalanul jelentenie kell a **Diszpécser** felé.
- A Kormányhivatali belső hálózathoz nem (vagy régen) csatlakoztatott számítógépen (pl. notebook) a vírusvédelmi rendszer frissítése a felhasználó feladata és felelőssége. A belső hálózathoz vagy Internethez nem csatlakoztatott munkaállomások esetén a vírusdefiníciós állományok frissítését a belső hálózathoz, vagy Internethez kapcsolódáskor el kell végezni a rendszernek automatikusan. A manuális frissítés elvégzésében a **Diszpécser** tud segítséget nyújtani.

A **Szervezeti egység vezető / Adatgazda** (külső személyek esetén a Kormányhivatal kijelölt kapcsolattartója) a felelős azért, hogy a fenti szabályokat az érintettekkel ismertesse.

VIII.3.3 Szoftverhasználati szabályok

Kizárólag olyan szoftvereket és dokumentációkat szabad használni, amelyek megfelelnek a vonatkozó szerződésbeli, szerzői jogi vagy más jogszabályi elvárásoknak.
A számítógépek és a fájlmegosztások folyamatos ellenőrzésével biztosítani kell a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk jogszerű használatát, vagyis: hogy ezt a

lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.

A számítógépeken csak és kizárólag az informatikai feladatok ellátásért, üzemeltetésért felelős szervezeti egység, valamint az erre jogosult külső felek munkatársai telepíthetnek, módosíthatnak, vagy távolíthatnak el bármilyen fajta szoftvert.

A fenti szabályok szúrópróbaszerű ellenőrzése az **Informatikai biztonsági felelősnek** a feladata és felelőssége, mely feladat elvégzésében az informatikai feladatok ellátásért felelős szervezeti egység munkatársai is segítik.

VIII.4 Jogosultság változás egyes esetei

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
Munkavégzés tartós szünetelése	a vonatkozó szabályzat szerint	SZEV/AG	HSZE	-
Jogviszony fennállása esetén a feladat változások kezelése (Felülvizsgálat)	a vonatkozó szabályzat szerint	SZEV/AG	HSZE	-
Hozzáférési jogosultságok visszavonása	informatikai feladatellátásáért felelős szervezeti egység	SZEV/AG	HSZE	-
Infokommunikációs eszközök visszaszolgáltatása	informatikai feladatellátásáért felelős szervezeti egység	SZEV/AG	HSZE	-
Tájékoztatás a jogokról és kötelezettségekről	HSZE	HSZV	-	-

VIII.4.1 Munkavégzés tartós szünetelése

A munkavégzés várhatóan 1 hónapnál hosszabb szünetelése – GYES, GYED, hosszantartó betegség – esetén a felhasználó jogosultságait a távollét időszakára le kell tiltani – de törölni nem szabad –, mely a munkatárs **szervezeti egységének vezetőjének** a felelőssége, *az Informatikai üzemeltetési eljárásrendben* foglaltakkal összhangban.

VIII.4.2 Felülvizsgálat

A korábbi jogosultságokat legalább három havonta felül kell vizsgálni, szükség esetén gondoskodni kell azok módosításáról vagy visszavonásáról, mely a munkatárs **szervezeti egységének vezetőjének** a felelőssége, az *Informatikai üzemeltetési eljárásrendben* foglaltakkal összhangban.

A kilépő dolgozó **Szervezeti egységének vezetője** gondoskodik a jogosultság visszavonásáról, másik feladatkörbe történő áthelyezés esetén pedig az új **Szervezeti egység vezetője** igényli az új jogosultságok megadását.

VIII.4.3 Hozzáférési jogosultságok visszavonása

Valamennyi munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban álló természetes személynek az információkhoz és információ feldolgozó eszközökhöz való hozzáférési jogosultságát fel kell függeszteni, amikor alkalmazásuk megszűnik, szerződésük, illetve megállapodásuk lejár. Ha az érintett részéről fennállhat az ügymenetet vagy elektronikus információbiztonságot sértő magatartás veszélye, a jogosultságokat még az érintett tájékoztatását megelőzően vissza kell vonni!

A jogosultságok visszavonását az érintett felhasználó **Szervezeti egységének vezetője** kezdeményezi, a végrehajtása az adott rendszer üzemeltetésért felelős szervezeti egység munkatársainak feladata.

VIII.4.4 Infokommunikációs eszközök visszaszolgáltatása

Valamennyi felhasználónak vissza kell szolgáltatnia a Kormányhivatal számára valamennyi használatra átvett infokommunikációs eszközt, amikor alkalmazásuk, szerződésük, illetve megállapodásuk lejár, illetve megszűnik.

Amennyiben nem kerül visszaszolgáltatásra az eszköz, abban az esetben ezt a **Szervezeti egységének vezetőjének** jeleznie kell az adott eszköz üzemeltetéséért felelős vezető felé, aki a szükséges intézkedést kezdeményezi.

VIII.4.5 Tájékoztatás a jogokról és kötelezettségekről

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 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.

VIII.5 Külső felekkel kötött megállapodások

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
Általános szabályok érvényesítése	Kormányhivatalon belüli kapcsolattartó	KMB	-	IBF
Különleges követelmények érvényesítése	HSZE	KMB	-	IBF

VIII.5.1 Általános szabályok

Az informatikai rendszerekkel, illetve a szervezet által kezelt adatokkal kapcsolatba kerülő, vagy az elektronikus információbiztonságra közvetlen módon hatást gyakorló külső felekkel olyan írásbeli megállapodást kell kötni, amely tartalmaz vagy utal minden olyan elektronikus információbiztonsági követelményre, mely az IBSZ-ben vagy egyéb dokumentumban szabályozásra került. Az

együttműködés során rendelkezésre bocsátott üzleti titkok és bizalmas információk megőrzésének szabályait és módját *Titoktartási nyilatkozatban* (*4. számú függelék*) kell rögzíteni.
A külső beszállítók és szolgáltatók számára a Kormányhivatalon belüli kapcsolattartó igényli meg, valamint felügyeli a szükséges jogosultságokat, szükség esetén a visszavonásukat kezdeményezi.
A külső beszállítók és szolgáltatók hozzáférését a hozzáférés indokának megszűnte után, illetve a szerződés lejártakor azonnal meg kell szüntetni.
Az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködők esetében gondoskodni kell arról, hogy az Ibtv.-ben foglaltak szerződéses kötelemként teljesüljenek.

VIII.5.2 Különleges követelmények

Külső szervezettel kötött megállapodásokban az alábbiakat kell megkövetelni:

- a szerződést érintő, elektronikus információbiztonsági szerep- és felelősségi körök – beleértve a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is – mindkét fél általi meghatározását és dokumentálását;
- a szerződő fél -szerződés teljesítésében közreműködő- munkatársai feleljenek meg a kormányhivatal által meghatározott személybiztonsági követelményeknek (szükség esetén a Nemzetbiztonsági ellenőrzést is beleértve);
- 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 soron kívül küldjön értesítést az érintett szervezeti egység vezetőjének.

A Kormányhivatalnak rendszeresen ellenőriznie kell a szerződő fél személybiztonsági követelményeknek való megfelelését.

IX. Fizikai védelem

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
Fizikai biztonsági környezet kialakítása	**IFEFV,** FVFV által kijelölt személy(ek)	**IFEFV,** FVFV	IBF, IBM	-

Az információs rendszerek biztonsági osztályának és a Kormányhivatal biztonsági szintbe sorolásának megfelelő, kockázatarányos fizikai védelmi intézkedéseket kell kialakítani és alkalmazni. A fizikai védelmi intézkedéseket az **Informatikai biztonsági felelős** legalább évente egyszer szúrópróbaszerűen ellenőrzi.

A Kormányhivatal informatikai helyiségek megfelelő kategóriába (zónába) besorolása az **Informatikai feladatok ellátásáért felelős vezető** feladata együttműködve a Fizikai védelemért felelős vezető ,

figyelembe véve az ott elhelyezésre kerülő informatikai eszközök által tárolt adatokra, folyamatokra vonatkozó **Szervezeti egység vezetői/Adatgazdai** besorolást.

A kategóriák besorolásának folyamatát és a részletes fizikai védelmi intézkedéseket a *Fizikai védelmi eljárásrendben* kell rögzíteni.

IX.1 Biztonsági osztály szerinti követelmények

Az elektronikus információs rendszerek vonatkozásában kialakítandó fizikai védelmi megoldásoknak az alábbi biztonsági osztályok szerint növekvő és egymásra épülő elvárásoknak kell megfelelni a kiemelten védett kategóriájú helyiségek esetében:

- 2-es biztonsági osztály: fizikai védelmi eljárásrend, fizikai belépési engedélyek és azok ellenőrzése
- 3-as biztonsági osztály: 2-es osztály + Fizikai hozzáférések felügyelete, látogatók ellenőrzése, Vészvilágítás, Tűzvédelem, hőmérséklet és páratartalom ellenőrzés, csővezeték rongálódásából származó károk elleni védelem, Be- és kiszállítás felügyelete, Karbantartók ellenőrzése
- 4-es biztonsági osztály: 3-as osztály + hozzáférés ellenőrzés az adatátviteli eszközökhöz és csatornákhoz, kimeneti eszközök hozzáférés ellenőrzése, behatolás riasztás, felügyeleti berendezések, áramellátó berendezések és kábelezés, tartalék áramellátás, vészkikapcsolás, Automatikus tűzelfojtás, az elektronikus információs rendszer elemeinek elhelyezése, karbantartási eszközök ellenőrzése, karbantartási támogatás.

IX.1.1 Általános követelmények

A Kormányhivatalnak gondoskodnia kell az illetéktelen behatolást vagy hozzáférést, valamint a szándékos károkozást vagy véletlen katasztrófát megakadályozó, szükséges mértékű – kockázatokkal arányos – védelmi intézkedések alkalmazásáról. Ennek érdekében a Kormányhivatal:

- ellenőrzés alatt tartja a be- és kilépési pontokat, naplózza a fizikai belépéseket;
- ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket;
- kíséri a létesítménybe ad-hoc belépésre jogosultakat (vendégeket), és figyelemmel kíséri a tevékenységüket;
- megóvja a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző eszközöket;
- felügyeli a fizikai behatolás riasztásokat és a felügyeleti berendezéseket;
- védi az elektronikus információs rendszert árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben;
- az elsődleges áramforrás kiesése esetére szünetmentes áramellátást biztosít az elektronikus információs rendszer szabályos leállításához vagy a hosszútávú tartalék áramellátásra történő átkapcsoláshoz;
- automatikus vészvilágítási rendszert alkalmaz és tart karban, amely áramszünet esetén aktiválódik, és amely biztosítja a vészkijáratokat és a menekülési útvonalakat;

- az elektronikus információs rendszerek számára független áramellátással támogatott észlelő, az informatikai eszközökhöz megfelelő tűzelfojtó berendezéseket alkalmaz, és tart karban;
- az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben az erőforrások biztonságos működéséhez szükséges szinten tartja a hőmérsékletet és páratartalmat;
- az informatikai erőforrásokat koncentráltan tartalmazó helyiségek tervezése során biztosítja, hogy az a víz-, és más hasonló kártól védett legyen, akár csővezetékek kiváltásával, áthelyezésével is;
- szabályozza, továbbá figyeli és ellenőrzi a létesítménybe bevitt, onnan kivitt információs rendszerelemeket, és nyilvántartást vezet ezekről;
- kialakít egy folyamatot a karbantartók munkavégzési engedélyének kezelésére, és nyilvántartást vezet a karbantartó szervezetekről vagy személyekről.

Az adott biztonsági osztályú elektronikus információs rendszert tartalmazó szerverszobára vonatkozóan a jogszabály által meghatározott követelményeket az *5. számú függelék* tartalmazza.

A Kormányhivatal helyiségei informatikai biztonsági szempontból négy kategóriába sorolhatók:

- Kiemelten védett kategória: Kiemelten védett helyiségnek kell tekinteni azokat a helyiségeket, ahol bizalmas adatok feldolgozására, tárolására alkalmazott központi informatikai erőforrások találhatók. A kiemelten védett helyiségek egyben zárt területnek is minősülnek, ezért az ott meghatározott szabályokat is be kell tartani velük kapcsolatban.
- Fokozottan védett kategória: Fokozottan védett helyiségnek kell tekinteni azokat a helyiségeket, ahol bizalmas adatok feldolgozására, tárolására alkalmazott kiegészítő informatikai erőforrások találhatók.
- Védett (Alap) kategória: A Kormányhivatal azon területei, melyek az általános munkavégzésre szolgálnak (pl. irodahelyiségek, folyosók, közlekedők).
- Nyilvános kategória: A Kormányhivatal azon területei, melyek nem tartoznak a védett kategóriákba (pl. ügyféltér).

X. Biztonságtervezés

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
Információbiztonsági architektúra készítése, felülvizsgálata	a vonatkozó szabályzatok szerint	a vonatkozó szabályzatok szerint	IBF	-
Rendszerbiztonsági terv készítése, felülvizsgálata	informatikai feladatok ellátásért felelős szervezeti egység	IFEFV	IBF, IBM	-
Felhasználókkal szembeni elvárások	informatikai feladatok ellátásáért felelős	IFEFV	HSZE, jogi feladatokat ellátó szervezeti	-

	szervezeti egység, IBF, IBM, SZEV/AG		egység	

X.1 Információbiztonsági architektúra

A Kormányhivatal infrastruktúrájának információbiztonsági architektúra leírásaként az alábbiakkal kell rendelkezni:

- a Kormányhivatalok Szervezeti és Működési Szabályzatai
- az Informatikai Biztonsági Irányítási Rendszer dokumentumai
- az elektronikus információs rendszerek Rendszerbiztonsági tervei
- az elektronikus információs rendszerek egyéb tervei, üzemeltetési leírásai
- a Kormányhivatalok infrastruktúrájára vonatkozó tűzfal és hálózati architektúrák

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.

A fentieken túlmenően a szervezet folyamatosan figyelemmel kíséri az elektronikus információs rendszerek biztonsági állapotát, valamint sérülékenység vizsgálatok segítségével feltárja az esetleges biztonsági hiányosságokat. (A sérülékenység vizsgálatokat és egyéb rendszerteszteléseket megelőzően egyeztetni kell a különböző szervezeti egységekkel annak érdekében, hogy azok végrehajtása a lehető legkisebb hatással legyenek a hivatali folyamatokra.)

X.2 Rendszerbiztonsági terv

A Kormányhivatal felelős szervezeti egységeinek az általa üzemeltetett elektronikus információs rendszerekhez Rendszerbiztonsági Terveket kell készítenie a *Rendszerbiztonsági Terv sablonban* (*6. számú függelék*) rögzített tartalommal és struktúrában. A rendszerbiztonsági terv részben vagy egészében helyettesíthető az adott elektronikus információs rendszer rendszerdokumentációjának biztonsági fejezetével is, amennyiben az tartalmilag is megfelel az elvárásoknak.

A Rendszerbiztonsági tervek készítésébe az érintett szervezeti egységek vezetőit is be kell vonni. A továbbiakban a Rendszerbiztonsági terveket csak az érintettek ismerhetik meg.

Az elektronikus információs rendszerek rendszerbiztonsági terveit a változáskezelés folyamat részeként folyamatosan naprakészen kell tartani, mely az informatikai feladatellátásért felelős szervezeti egység feladata és az informatikai feladatok ellátásáért felelős vezető felelőssége.

X.3 Felhasználókkal szembeni elvárások

A Kormányhivatalnak elvárásokat és szabályokat, valamint felelősségeket kell megfogalmaznia külön-külön minden elektronikus információs rendszeréhez, melynek megismeréséről és elfogadásáról az első jogosultságigénylés alkalmával írásban kell nyilatkoztatni a rendszer minden – hivatali és külsős –

felhasználóját. A már jogosultsággal rendelkező belső felhasználók esetében az elvárások és szabályok változását követően kell mielőbb pótolni az írásos nyilatkozatot.

A felhasználókkal szembeni elvárásokat és a rájuk vonatkozó szabályokat, illetve felelősségüket a tartalmazó dokumentum információs rendszerenkénti előállítása az informatikai feladatellátásáért felelős szervezeti egység feladata és az **Informatikai feladatok ellátásáért felelős vezető** felelőssége. A feladat elvégzésében segítséget kérhetnek az **Informatikai biztonsági felelőstől** és az elektronikus információbiztonsági feladatok ellátásában közreműködő személyektől, valamint az érintett szervezeti egység vezetőjétől, továbbá – konzultációs céllal – bevonhatók a jogi, valamint a humánpolitikai feladatokat ellátó szervezeti egységek munkatársai is.

Indokolt esetben – de legalább évente egyszer – az informatikai feladatellátásáért felelős szervezeti egység – **informatikai feladatok ellátásáért felelős vezető** által – kijelölt munkatársának felül kell vizsgálnia a személyekkel, felhasználókkal szembeni elvárásokat tartalmazó dokumentumot, melynek – amennyiben történt benne változás – újbóli elfogadásáról ismét nyilatkoztatni kell minden belső felhasználót.

XI. Informatikai biztonság értékelése és mérése

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
A biztonságértékelés és mérés rendszerének kialakítása, működtetése	IBF	IBF	NE, HVRA, HRA, VRA, IÜR, IÜFV, IBM, DP	IFEFV, KMB
A biztonságértékelés és mérés rendszerének kialakításához, működtetéséhez szükséges technikai feltételek biztosítása	IÜFV, IFEFV	IFEFV	NE, HVRA, HRA, VRA, IÜR, IÜFV, IBM, IBF, DP	KMB

Annak érdekében, hogy az informatikai biztonsági hiányosságok azonosításra és mielőbbi javításra kerülhessenek, a Kormányhivatalnál ki kell alakítani, valamint folyamatosan működtetni kell a biztonságértékelés és mérés rendszerét.

A biztonságértékelés és mérés rendszerének kialakításáért valamint annak folyamatos működtetéséért az **Informatikai biztonsági felelős** a felelős, az ehhez szükséges technikai feltételek biztosításáért az **Informatikai feladatok ellátásáért felelős vezető** a felelős.

Az informatikai biztonság értékelésére és mérésére vonatkozó további részletes követelményeket és eljárásokat, továbbá szabályokat a *Biztonságelemzési eljárásrend* tartalmazza.

XI.1 Biztonsági osztály szerinti követelmények

Az elektronikus információs rendszerek vonatkozásában kialakítandó biztonságértékelési és mérési megoldásoknak az alábbi biztonsági osztályok szerint növekvő és egymásra épülő elvárásoknak kell megfelelni:

- 3-as biztonsági osztály: Biztonságértékelés és mérés feltételrendszerének kialakítása, biztonsági értékelés és mérés végrehajtása, Sérülékenységvizsgálat
    - Éves biztonságértékelési terv készítése.
    - Biztonságértékelés elvégzése.
    - Sérülékenységvizsgálatok technikai feltételeinek megteremtése.
    - A sérülékenységvizsgálatok lefolytatását végző hatósággal történő együttműködés megszervezése.
    - Sérülékenységvizsgálatok elvégeztetése vagy sérülékenységi teszteszköz bevezetése és használata:
        - Internet felől elérhető rendszerek esetén: az **Informatikai biztonsági felelős** által előre ütemezetten vagy a rendszerek jelentősebb változása esetén
        - Internet felől nem elérhető rendszerek esetén: az **Informatikai biztonsági felelős** által előre ütemezetten vagy a rendszerek jelentősebb változása esetén.
- 4-es biztonsági osztály: 3-as osztály + Speciális értékelések elvégzése (szükség szerint)
    - Egyedi fejlesztésű szoftverelemek forráskód elemzése (szükség szerint).
    - Social engineering típusú értékelések elvégzése/elvégeztetése (szükség szerint).

XI.2 Általános követelmények

- A Kormányhivatalnál az elektronikus információs rendszerek és a működési környezetek védelmi intézkedéseinek vonatkozásában kontrollálni kell a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelően történő működését. Ezen értékelésekre, elemzésekre a megfelelő szerződéses és biztonsági előírások betartásával, a szükséges szakértelemmel és tanúsítványokkal rendelkező külső független értékelők vagy értékelő csoportok is bevonhatók az **Informatikai biztonsági felelős** javaslatára, a **Kormánymegbízott** jóváhagyásával.
- Az **Informatikai biztonsági felelősnek** éves biztonságértékelési tervet kell készítenie, melyben meg kell határoznia, hogy a biztonsági értékelés mely elektronikus információs rendszerekre terjedjen ki és az egyes rendszerek viszonylatában mikor kerüljön végrehajtásra.
- A – biztonságértékelési terv alapján elvégzett – biztonságértékelés eredményéről összefoglaló jelentést kell készíteni és eljuttatni az **Informatikai feladatok ellátásáért felelős vezető** és a **Kormánymegbízott** számára.
- A Kormányhivatalnak ki kell fejlesztenie és felügyelnie kell az elektronikus információs rendszerei biztonsági mérésének rendszerét.

Sérülékenységvizsgálat:

- A Kormányhivatal felügyelete, irányítása alatt álló – Internet felől elérhető – elektronikus információs rendszerekre vonatkozóan technikai szintű auditot az **Informatikai biztonsági felelős** által előre ütemezetten, Internet felől nem elérhető rendszerek esetén az **Informatikai**

biztonsági felelős által előre ütemezetten, a fenyegetettségek felmérésével egy időben kell igényelni a jogszabályban kijelölt szervezettől. Ennek a végrehajtásért az **Informatikai biztonsági felelős**, a technikai feltételek biztosításáért az **Informatikai feladatok ellátásáért felelős vezető** a felelős.

Sérülékenységi teszteszköz:

- A Kormányhivatal lehetőségeihez mérten, amennyiben a sérülékenységvizsgálathoz teszteszközt kell használni, a teszteszköz kiválasztásakor ügyelnie kell arra, hogy az eszköz sérülékenység feltáró képessége könnyen bővíthető legyen az ismertté vált újabb sérülékenységekkel, ahogy azok megjelennek.
- A Kormányhivatal felügyelete, irányítása alatt álló elektronikus információs rendszerek aktuális sérülékenységeiről az **Informatikai biztonsági felelős** által előre ütemezetten információt kell beszerezni és ez alapján vizsgálni kell a szervezett kitettségét. Szükség esetén intézkedni kell a kapcsolódó kockázatok elfogadható mértékűre csökkentéséről.
- A sérülékenységvizsgálat során használt szoftver (amennyiben ilyen rendelkezésre áll) adatbázisát minden új vizsgálat megkezdése előtt frissíteni kell. Ezzel biztosítható, hogy a szoftver képes legyen a legutóbb megismert sérülékenységek felismerésére.

Feltárt sérülékenységek kezelése:

- Sérülékenység azonosítást követően az **Informatikai biztonsági felelős** meghatározza annak kockázati szintjét és a kívánt intézkedést.
- A sérülékenységek menedzselését mindig a nagyobb kockázatú rendszerekkel kell kezdeni.
- Az intézkedések végrehajtása során a változáskezelési eljárásokat vagy biztonsági incidenskezelési eljárásokat kell követni, a feltárt sérülékenység súlyosságának megfelelően.
- Amennyiben egy sérülékenység kijavítására elérhető javítócsomag, úgy a javítócsomag telepítéséből adódó és magának a sérülékenységnek a kockázatait össze kell hasonlítani. Javítócsomagokat telepítés előtt meg kell vizsgálni és tesztelni kell a súlyos mellékhatások elkerülése céljából. A hibajavításokra vonatkozó részletes követelményeket és szabályokat a *Rendszer- és információsértetlenségi eljárásrend* tartalmazza.
- Amennyiben egy sérülékenység javítására nem érhető el javítócsomag, úgy egyéb korrektív kontrolokat kell alkalmazni.
- A sérülékenységek kezelése során végzett tevékenységeket dokumentálni kell.
- A sérülékenység kezelő folyamat hatékonyságát rendszeresen felül kell vizsgálni és értékelni kell azt.

XII. Rendszer és szolgáltatás beszerzés

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
Beszerzések során a biztonsági elvárások	IBF	KMB	IFEFV, IÜFV, IIFFV, AFV	-

ellenőrzése				

A Kormányhivatalnak az informatikai beszerzések során az informatikai biztonsági követelményeket már az életciklus tervezési, fejlesztési, beszerzési szakaszában figyelembe kell venni és folyamatosan nyomon kell követni.

A beszerzések feltételrendszerének kialakításáért a **Kormánymegbízott** a felelős.

A Kormányhivatal olyan eljárást alakít ki, mely biztosítja, hogy az **Informatikai biztonsági felelős** a beszerzési követelményeket már a beszerzés kezdetén érvényesíteni tudja.

A Kormányhivatal az általa kialakítandó beszerzési eljárásban a biztonsági osztályoknak megfelelően a szállítók számára is meghatározza az Ibtv. szerinti követelményeket.

A rendszer és szolgáltatás beszerzésekre, valamint a fejlesztésekre vonatkozó részletes informatikai biztonsági követelményeket és szabályokat az *Informatikai beszerzési eljárásrend* és az *Alkalmazásfejlesztési szabályzat* tartalmazza.

XII.1 Biztonsági osztály szerinti követelmények

Az elektronikus információs rendszerek vonatkozásában a beszerzések során az alábbi biztonsági osztályok szerint növekvő és egymásra épülő elvárásoknak kell megfelelni:

- 2-es biztonsági osztálytól: Külső üzemeltetésű EIR-ek szolgáltatásainak ellenőrzése
- 3-as biztonsági osztály: 2-es osztály + Beszerzési eljárásrend, erőforrás igények felmérése és biztosítása, szerződéses követelmények, saját üzemeltetésű EIR-ek dokumentációi (admin, user kézikönyvek), folyamatos ellenőrzés
- 4-es biztonsági osztály: 3-as osztály + Védelem szempontjainak érvényesítése, védelmi intézkedések dokumentációja, a funkciók, protokollok, szolgáltatások előzetes meghatározása, független értékelők alkalmazása a beszerzés biztonsági szempontú teljesülésének ellenőrzésére

XII.1.1 Általános követelmények

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 **Informatikai biztonsági felelősnek** kell ellenőrizni.

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:

- elvárt biztonsági osztályt, funkcionális biztonsági követelményeket;
- a garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint);
- a biztonsággal kapcsolatos dokumentációs követelményeket;

- a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket;
- az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.

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 informatikai biztonsági követelményeinek.

Figyelemmel kell kísérni az elektronikus információs rendszerek biztonsági elemeinek megbízhatóságát és teljesítményét.

XIII. Adathordozók védelme

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
Az adathordozók megfelelő fizikai és logikai védelme feltételrendszerének kialakítása	IFEFV, IÜFV, IIFFV, AFV	IFEFV	IBF	FŐIG/IG

Az elektronikus információs rendszerekben és a szervezetnél használt adathordozóknak és mobil eszközöknek a bizalmassága, sértetlensége és rendelkezésre állása érdekében biztosítani kell az adathordozók és mobil eszközök megfelelő fizikai és logikai védelmét.
Az adathordozók és mobil eszközök megfelelő fizikai és logikai védelme feltételrendszerének kialakításáért az **Informatikai feladatok ellátásáért felelős vezető** a felelős.
Az adathordozók és mobil eszközök védelmére vonatkozó további részletes követelményeket és eljárásokat, továbbá szabályokat az *Adathordozók és mobil eszközök védelmére vonatkozó eljárásrend* tartalmazza.

XIII.1 Biztonsági osztály szerinti követelmények

Az elektronikus információs rendszerek vonatkozásában az adathordozók és mobil eszközök védelmére vonatkozó eljárásoknak az alábbi biztonsági osztályok szerint növekvő és egymásra épülő elvárásoknak kell megfelelni:

- 2-es biztonsági osztály: Adathordozókhoz való hozzáférés és adathordozók használati szabályainak kialakítása, adathordozók biztonságos törlése
    - Adathordozók és mobil eszközök igénylésének, kiadásának és visszavételének valamint nyilvántartásának szabályozott működtetése.
    - Adathordozók biztonságos törlésének végrehajtása.
- 4-es biztonsági osztály: 2-es osztály + Adathordozók címkézése, biztonságos tárolása és szállítása, kriptográfiai védelme, Az ismeretlen tulajdonosú adathordozók használatának tiltása:
    - Adathordozók USB porton keresztüli csatlakoztatásának kontrollálása.

- Adathordozók biztonságos tárolása és szállítása.
- Adathordozók titkosítása (az ellenőrzött területeken kívüli szállítás folyamán).

3-as szervezeti szinttől kezdődően: Mobileszköz menedzsment (MDM) alkalmazásának kialakítása szükséges.

XIII.1.1 Általános követelmények

A Kormányhivatalnál az adathordozók és mobil eszközök védelmére vonatkozó eljárások során legalább a következőket kell teljesíteni:

- Az adathordozók tartalmát az *Adathordozók és mobil eszközök védelmére vonatkozó eljárásrend* *Adathordozók biztonságos törlése* című fejezetének előírásai szerinti törölni kell, amennyiben:
  - az adathordozó tartalmára már nincs szükség;
  - az adathordozó kikerül a Kormányhivatal tulajdonából;
  - az adathordozó karbantartás céljából átadásra kerül külső fél (személy vagy szervezet) számára;
  - az adathordozó újrafelhasználásra kerül;
  - az adathordozó selejtezésre kerül.

XIII.2 Adathordozók és mobil eszközök igénylése, kiadása és visszavétele, valamint nyilvántartása

A Kormányhivatali munkavégzéshez adathordozót és mobil eszközt a felhasználók számára az adott **Szervezeti egység vezetője / Adatgazda** igényelhet, a *7. számú függelék* kitöltésével. Az igénylés teljesítéséhez az **Informatikai feladatok ellátásáért felelős vezető** jóváhagyása szükséges. Cserélhető adathordozó igénylése kizárólag indokolt esetben hagyható jóvá.

Az adathordozó és mobil eszköz igényléseket indoklással együtt a Helpdesk bejelentő felületen keresztül kell benyújtani.

Minden egyes kiadott adathordozóról és mobil eszközről nyilvántartást kell vezetni, továbbá az eszközök visszavétele esetén ennek tényét a kapcsolódó nyilvántartásban rögzíteni kell. A *8. számú függelékben* rögzített nyilvántartások vezetése az **Informatikai feladatok ellátásáért felelős vezető** felelőssége.

Az adathordozók és mobil eszközök igénylésével, kiadásával és visszavételével, valamint nyilvántartásával kapcsolatos részletes eljárásokat az *Adathordozók és mobil eszközök védelmére vonatkozó eljárásrend* tartalmazza.

XIII.3 Adathordozók használata

XIII.3.1 Általános használati szabályok

A Kormányhivatalnál kizárólag a Kormányhivatal tulajdonába tartozó adathordozók használata engedélyezett, saját tulajdonú adathordozók használata és a számítógépekhez vagy egyéb kormányhivatali eszközökhöz való csatlakoztatása szigorúan tilos.

Az adathordozók használatának feltétele az Informatikai feladatok ellátásáért felelős szervezeti egység által biztosított vírusvédelmi eszközzel való folyamatos ellenőrzés.

Cserélhető adathordozók esetében az adathordozót átvevő (használó) személy felel az adathordozón lévő információk kitudódása és illetéktelen kézbe kerülése esetén az okozott károkért.

Az adathordozók kizárólag munkavégzés céljából használhatóak, a Kormányhivatal tevékenységének végzéséhez. A felhasználók munkájához nem kapcsolódó adatok tárolása, illetve az adathordozók magáncélú felhasználása nem engedélyezett.

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 *Mentési és archiválási eljárásrendben* meghatározott gyakoriság alapján. A munkaállomás helyi meghajtóin tárolt adatok bizalmasságáért, sértetlenségéért és rendelkezésre állásáért a felhasználó tartozik felelősséggel.

A Kormányhivatalon kívül történő eszközhasználat esetén az adathordozókon tárolt adatokat, dokumentumokat a lehető leghamarabb fel kell másolni a megfelelő hálózati meghajtóra, ezután az adathordozóról pedig törölni kell azokat.

Az adathordozók Kormányhivatal telephelyein kívülre vitele esetére a következő eljárások vonatkoznak:

- Adathordozó csak engedéllyel vihető ki a Kormányhivatal telephelyein kívülre, melyet a szervezeti egység vezető engedélyez;
- A telephelyen kívülre történő szállítás esetén az adathordozó biztonságáért a szállítást végző felel;
- Az adathordozón tárolt adatok biztonsági osztályához tartozó előírásokat minden esetben be kell tartani;
- A telephelyen kívülre történő szállítás során betartandó előírásokról részletesen az *Adathordozók és mobil eszközök védelmére vonatkozó eljárásrend Kormányhivatal által ellenőrzött területeken kívüli szállítás* című fejezete rendelkezik.

Az ismeretlen (nem egyértelműen beazonosítható) tulajdonosú adathordozók használata tilos. Ilyen esetben a talált adathordozót nem szabad a számítógépekhez csatlakoztatni vagy mások számára továbbadni. Az **Informatikai biztonsági felelős** felé haladéktalanul jelenteni kell a megtalálás tényét és át kell adni számára a megtalált adathordozót.

Az **Informatikai biztonsági felelős** a talált adathordozót és a Kormányhivatalba kerülésének módját a *Biztonsági esemény és incidenskezelési eljárásrend* előírásai szerint egyedileg megvizsgálja, vagy megvizsgáltatja elszeparált környezetben (szükség esetén külső szakértők bevonásával), majd a vizsgálat lezárását követően az incidensről jelentést készít.

XIII.4 Mobil eszközök használata

XIII.4.1 Általános használati szabályok

Hivatali munkavégzéshez kapcsolódó adatkezelésre saját tulajdonú mobil eszköz kizárólag eseti engedély alapján használható a Kormányhivatalnál. Ebben az esetben a felhasználó felelőssége az eszközön tárolt adatok védelmének biztosítása.

A hivatali mobil eszközt átvevő (használó) személy felel az eszközön lévő információk kitudódása és illetéktelen kézbe kerülése esetén az okozott károkért.

A hivatali mobil eszközt kizárólag az eszközt átvevő kormányhivatali munkatárs használhatja, azt nem adhatja át másnak használatra.

A szervezeten kívüli használat esetén a mobil eszközt nem lehet felügyelet nélkül hagyni, valamint látható helyen hagyni (otthoni munkavégzés esetén vagy szállodában zárt szekrényben vagy széfben kell tárolni). Amennyiben másképpen nem biztosítható az eszköz megfelelő védelme, a dolgozónak magával kell vinnie az eszközt.

A mobil eszközök használata során ügyelni kell arra, hogy harmadik fél ne tekinthessen bele az eszköz megjelenítő felületébe.

A mobil eszközök képernyőjét zárolni kell használatukat követően.

XIII.4.2 Mobil eszközök védelmére vonatkozó további intézkedések

Mobileszköz menedzsment (MDM) alkalmazását ki kell alakítani a Kormányhivatalnál és a hivatali okostelefonok távolról való zárolását és tartalmuknak törlését biztosítani kell. Ennek megvalósítása az **IT üzemeltetésért felelős vezető** felelőssége.

XIII.5 Adathordozók biztonságos tárolása

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
Adathordozók biztonságos tárolása	Felhasználó, IÜR	IFEFV	IBF	-
Adathordozók másodpéldányainak megfelelő elhelyezése	IÜR	FVFV	IÜFV	FVFV

A nem beépített adathordozókat a napi munkavégzés befejezését követően – amennyiben lehetséges – 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).

A tárolás során a gyártói előírásokat be kell tartani, és a gyártó által előírt megfelelő környezeti paramétereket biztosítani kell.

Amennyiben az adathordozókon levő jelölések valamilyen okból kifolyólag már nem olvashatóak (például lekopott vagy megrongálódott a jelölés), vagy esetleg a megjelölést egyéb okból változtatni szükséges (például az adathordozó terjesztési korlátozásának megváltozása miatt), az adathordozó használójának ezt a tényt jelentenie kell az Informatikai feladatok ellátásáért felelős szervezeti egység felé, melynek a feladatra kijelölt munkatársai a szükséges intézkedésekről gondoskodnak.

XIV. Hozzáférés-felügyelet

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
Azonosítás	üzemeltetésért felelős szervezeti egység	IFEFV	IBF	-
Hitelesítés	felhasználó, üzemeltetésért felelős szervezeti egység	IFEFV	IBF	-
Engedélyezés	üzemeltetésért felelős szervezeti egység, érintett szervezeti egység vezetője	SZEV/AG	IBF	-
Felügyelet	felhasználó, üzemeltetésért felelős szervezeti egység	IFEFV	IBF	-

XIV.1 Azonosítás

XIV.1.1 Felhasználói fiókok

Az elektronikus információs rendszereknek minden belső és külső felhasználót egyedileg kell azonosítaniuk annak érdekében, hogy:

- minden, egy adott időpontban végzett tevékenység összerendelhető legyen egy természetes személlyel;
- az összerendelés egyértelmű, megváltoztathatatlan, később is visszakereshető legyen.

A beépített (ún. built-in) fiókokat (Guest, Admin, root stb.) is vagy nevesíteni kell –átnevezéssel–, vagy le kell tiltani. Amennyiben erre nincs mód, úgy technikai fiókként kell kezelni azokat.

Korábban már felhasznált azonosítókat a megszüntetésüktől számított 12 hónapig nem lehet ismételten kiadni, vagy egyéb módon használatba venni.

XIV.1.2 Privilegizált fiókok

A privilegizált funkciók eléréséhez erre a célra dedikált –szintén nevesített– fiókokat kell létrehozni az információs rendszerekben. A privilegizált – kiemelt jogosultságú – fiókokat egységes névkonvenció alapján kell elnevezni, mely alapján megkülönböztethetőek az általános – felhasználói – fiókoktól.
A privilegizált fiókokkal általános – nem rendszergazdai – tevékenységet végezni tilos!
Az **Informatikai biztonsági felelőst** tájékoztatni kell minden privilegizált jogosultságigénylésről, mely folyamatban felülbírálati jogkörrel rendelkezik.

Minden más követelmény megegyezik a felhasználói fiókoknál ismertetettekkel.

XIV.1.3 Technikai fiókok

A nem nevesített –technikai vagy szolgáltatás– fiókot (illetve azok kezelését) nem személyhez, hanem szervezeti egységhez kell rendelni, mely esetben mindig az adott szervezeti egység vezetője felelős a fiókért és annak használatával elvégzett módosításokért.

Technikai fiók a jogosultsági szintjétől függően lehet felhasználói vagy privilegizált.

XIV.2 Hitelesítés

A Kormányhivatal tulajdonában vagy használatában lévő valamennyi elektronikus információs rendszer esetében az azonosítást legalább egy hitelesítő mechanizmussal is ki kell egészíteni. A hitelesítés mechanizmus általános módszere a felhasználói azonosítóhoz tartozó jelszó alkalmazása.

XIV.2.1 Felhasználói fiókok jelszavai

A jelszavakkal kapcsolatos minimális elvárások –melyeknél csak szigorúbbakat szabad alkalmazni– minden hivatalon belül használt rendszer esetében:

- a jelszavak hossza legalább 14 karakter kell, hogy legyen;
- sem részben, sem egészében nem tartalmazhatja a fiókazonosítót;
- az alábbi négyféle karaktertípus közül legalább kettőt tartalmaznia kell:
  - kisbetű (a..z)
  - nagybetű (A..Z)
  - számjegy (0..9)
- a jelszavakat legalább 90 naponként meg kell változtatni;
- az új jelszónak legalább egy karakterében különböznie kell a legutóbb használt 10 bármelyikétől;
- A jelszó minimális élettartama 1 nap.

A kezdeti jelszót az első belépéskor meg kell változtatni, továbbá a jelszavak bizalmasságát minden felhasználónak meg kell őriznie, azokat más személy tudomására hozni szigorúan tilos! A jelszavakat azok kompromitálódása – vagy annak gyanúja – esetén haladéktalanul meg kell változtatni, vagy a hozzá kapcsolódó fiókot le kell tiltatni.

XIV.2.2 Privilegizált fiókok jelszavai

A privilegizált –kiemelt jogosultságú– fiókok jelszavaira vonatkozó követelmények az alábbiak szerint szigorodnak a felhasználói fiókoknál már ismertetetteken túlmenően, illetve azokkal együtt értelmezve:

- a jelszavak hossza legalább 16 karakter kell, hogy legyen;
- az alábbi négyféle karaktertípus közül legalább hármat kell tartalmaznia:
  - kisbetű (a..z)
  - nagybetű (A..Z)
  - számjegy (0..9)

Minden más követelmény és eljárás megegyezik a felhasználói fiókok jelszavainál ismertetettekkel.

XIV.2.3 Technikai fiókok jelszavai

A nem nevesített – technikai vagy szolgáltatás – fiókok jelszavát csak lezárt borítékban páncélszekrénybe elzárva vagy jelszókezelő rendszerben lehet tárolni, és az ahhoz való hozzáféréseket dokumentálni kell.
Továbbá a nem nevesített –technikai vagy szolgáltatás– fiókokhoz tartozó jelszavakkal kapcsolatos követelmények –legyenek azok felhasználói vagy privilegizált fiókok– az alábbiak szerint módosulnak:

- a jelszavak hossza legalább 16 karakter kell, hogy legyen;
- a technikai fiókok jelszavát minden megismerést követően, vagy minimum kétévente egyszer meg kell változtatni, és ismételten el kell zárni azt borítékba vagy felvinni a jelszókezelő rendszerbe.

A fenti módosítások együttesen értelmezendők és alkalmazandók a felhasználói vagy privilegizált fiókok jelszavaira vonatkozó követelményekkel és eljárásokkal (függően attól, hogy az adott technikai fiók felhasználóinak vagy privilegizáltnak minősül-e).

Azon rendszerek esetében, amelyeknél a fenti szabályozást nem lehet érvényesíteni, az adott alkalmazás maximális biztonsági lehetőségeit kihasználva kell a jelszavak erősségét beállítani, és törekedni kell az alkalmazás megfelelő módosítására, cseréjére.

XIV.2.4 Többtényezős hitelesítés

Azon információs rendszerek esetében, melyek biztonsági osztályba sorolása ezt megköveteli, a Kormányhivatal többtényezős hitelesítést alkalmaz. A többtényezős hitelesítéssel és a hitelesítő eszközök vagy tanúsítványok kezelésével kapcsolatos követelményeket és eljárásokat az *Azonosítási és hitelesítési eljárásrendnek*, a műszaki megvalósítás dokumentálását pedig a *Rendszerbiztonsági tervnek* kell tartalmaznia.

XIV.3 Engedélyezés

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

- emberi, fizikai és logikai erőforrásra;

- eljárási és védelmi követelményszintre és folyamatra.

XIV.3.1 Legkisebb jogosultság elve

A felhasználók csak a számukra kijelölt feladatok végrehajtásához szükséges és elégséges jogosultságokat kaphatják meg az információkhoz és a rendszer erőforrásaihoz való logikai hozzáférés során, a *Hozzáférés ellenőrzési eljárásrendben* foglaltakkal összhangban.

XIV.3.2 Jogosultságok felülvizsgálata

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.

XIV.4 Felügyelet

XIV.4.1 Sikertelen hitelesítési kísérletek

Öt 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 munkatársai oldhatják fel.

Valós fenyegetés vagy egymás utáni többszöri zárolás esetén haladéktalanul értesíteni kell az **Informatikai biztonsági felelőst**!

XIV.4.2 Inaktív fiókok nyomon követése

Azokat a fiókokat, melyekbe az alábbiakban meghatározott ideje nem jelentkeztek be sikeresen, felül kell vizsgálni és szükség szerint gondoskodni azok letiltásáról és deaktiválásáról:

- nem technikai fiókok esetében: 30 nap;
- technikai fiókok esetében: 180 nap.

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.

XV. Rendszerüzemeltetés

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
A konfigurációkezelés feltételrendszerének kialakítása	IFEFV, IÜFV, IIFFV, AFV	IFEFV	IBF	FŐIG/IG
Hibajavítás (patch management) feltételrendszerének kialakításáért	IFEFV, IÜFV, IIFFV, AFV	IFEFV	IBF	FŐIG/IG
Határvédelem és rendszerfelügyelet kialakítása	IFEFV, IÜFV, IIFFV, AFV	IFEFV	IBF	FŐIG/IG
Vírusvédelmi rendszer kialakítása	IFEFV, IÜFV, IIFFV, AFV	IFEFV	IBF	FŐIG/IG
A mentés, archiválás és visszatöltés tervezése és elvégzése	IFEFV, IÜFV, IIFFV, AFV	IFEFV	IBF	FŐIG/IG
A naplózási környezet feltételrendszerének kialakítása	IFEFV, IÜFV, IIFFV, AFV	IFEFV	IBF	FŐIG/IG

XV.1 Konfigurációkezelés

A Kormányhivatalnak biztosítania kell, hogy jogosulatlanul és kontroll nélküli konfiguráció ne működhessen a szervezetekben. A változáskezelés kontrollált folyamat legyen, csak megfelelő folyamatok mentén kerülhessen be új konfiguráció az éles rendszerekbe, a jogosulatlanul betöltött konfigurációk időben észlelhetőek legyenek.

A konfigurációkezelés feltételrendszerének kialakításáért az **Informatikai feladatok ellátásáért felelős vezető** a felelős.

A konfigurációkezelésre vonatkozó részletes követelményeket és szabályokat a *Konfigurációkezelési eljárásrend*, a változásokkal kapcsolatos folyamatokat és teendőket az *Informatikai üzemeltetési eljárásrend* tartalmazza.

XV.1.1 Biztonsági osztály szerinti követelmények

Az elektronikus információs rendszerek vonatkozásában kialakítandó konfigurációkezelési megoldásoknak az alábbi biztonsági osztályok szerint növekvő és egymásra épülő elvárásoknak kell megfelelni:

- 2-es biztonsági osztály: Alapkonfiguráció és elektronikus információs rendszerelem leltár kialakítása,

- 3-as biztonsági osztály: 2-es osztály + Szükséges szolgáltatások meghatározása és átvizsgálása,
- 4-es biztonsági osztály: 3-as osztály + Biztonsági konfiguráció kialakítása, Elektronikus nyilvántartás kialakítása,
    - Konfigurációs elemek automatikus felderítése (autodiscovery)
    - Konfigurációs elemek és kapcsolataik elektronikus nyilvántartása (CMDB).

XV.1.1.1 Általános követelmények

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 erre való visszatérés. Az egyes elektronikus információs rendszerek alapkonfigurációit a Rendszerbiztonsági tervekben kell dokumentálni (melyek korábbi verzióit szintúgy meg kell őrizni változatlan formában).
Az elektronikus információs rendszerek elemeiről leltárt kell vezetni, melynek tartalmát folyamatosan naprakészen kell tartani.

XV.2 Hibajavítás (Patch management)

A hibajavítást (vagy más néven patch-menedzsmentet) úgy kell kialakítani a Kormányhivatal által alkalmazott informatikai rendszerek vonatkozásában, hogy az informatikai feladatokat ellátó szervezeti egységek munkatársai a lehető leghamarabb informálódjanak a legújabb sérülékenységekről, és képesek legyenek azokat a lehető legrövidebb időn belül kezelni.

A patch-menedzsment feltételrendszerének kialakításáért az **Informatikai feladatok ellátásáért felelős vezető** a felelős.
A hibajavításokra vonatkozó részletes követelményeket és szabályokat a *Rendszer- és információsértetlenségi eljárásrend* tartalmazza.

XV.2.1 Általános követelmények

A sérülékenységek kezelésének három leggyakoribb módja:

- az eszköz vagy szoftver gyártója által kiadott javító/biztonsági patch-ek telepítésével,
- a konfigurációs beállítások módosításával vagy javításával,
- valamilyen kerülő megoldás (workaround) alkalmazásával (pl. egyes funkciók letiltásával).

A gyártók által kiadott javítások (patch-ek) telepítését rendszeresen el kell végezni minden informatikai eszközön és szoftveren, maximum az alábbi határidők szerint:

Patch gyártó általi besorolása	Informatikai eszköz/szoftver jellege	A telepítés határideje
biztonsági, kritikus besorolással	kiszolgálók és infrastruktúra eszközök	2 hét
	kliens gépek (desktopok és laptopok)	3 hét
	egyéb eszközök (pl. nyomtatók)	4 hét
biztonsági (de nem kritikus)	kiszolgálók és infrastruktúra eszközök	1 hónap
	kliens gépek (desktopok és laptopok)	2 hónap
	egyéb eszközök (pl. nyomtatók)	2 hónap
kritikus (de nem biztonsági)	kiszolgálók és infrastruktúra eszközök	1 hónap
	kliens gépek (desktopok és laptopok)	2 hónap
	egyéb eszközök (pl. nyomtatók)	2 hónap
minden egyéb javítás, frissítés	kiszolgálók és infrastruktúra eszközök	3 hónap
	kliens gépek (desktopok és laptopok)	3 hónap
	egyéb eszközök (pl. nyomtatók)	6 hónap

Kiszolgálóknak és infrastruktúra eszközöknek minősülnek az alábbiak is:

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

XV.3 Karbantartás

Feladat	Felelős(ök)	Számon kérhető	Konzulens(ek)	Tájékoztatandó(k)
A karbantartások feltételrendszerének kialakítása és a karbantartások, javítások végrehajtása (informatikai eszközök tekintetében)	IFEFV, IÜFV, IIFFV, AFV Vállalkozó/ Szolgáltató	IFEFV	IBF	FŐIG/IG
A karbantartások feltételrendszerének kialakítása és a karbantartások, javítások végrehajtása (fizikai védelmet biztosító eszközök, berendezések tekintetében)	FVFV, Vállalkozó/ Szolgáltató	FVFV	IBF	FŐIG/IG

Az elektronikus információs rendszerek és rendszerelemek megfelelő működése érdekében rendszeres karbantartásokat kell végezni.

Az informatikai eszközök tekintetében a karbantartások feltételrendszerének kialakításáért és a karbantartási, javítási tevékenységek végrehajtásáért az **Informatikai feladatok ellátásáért felelős vezető** a felelős.
A fizikai védelmet biztosító eszközök, berendezések tekintetében (ideértve a tűzoltó- vagy klíma berendezéseket is) a karbantartások feltételrendszerének kialakításáért és a karbantartási, javítási tevékenységek végrehajtásáért az **Fizikai védelemért felelős vezető** a felelős.
A rendszerek és rendszerelemek karbantartására vonatkozó további részletes követelményeket és eljárásokat, továbbá szabályokat a *Rendszer karbantartási eljárásrend* tartalmazza.

XV.3.1 Biztonsági osztály szerinti követelmények

Az elektronikus információs rendszerek vonatkozásában a karbantartási eljárásoknak az alábbi biztonsági osztályok szerint növekvő és egymásra épülő elvárásoknak kell megfelelni:

- 2-es biztonsági osztály: Rendszeres karbantartások megtervezése és végrehajtása
    - Éves karbantartási terv
    - Rendszeres karbantartások és javítások végrehajtása
- 4-es biztonsági osztály: 2-es osztály + Karbantartási eszközök jóváhagyása, nyilvántartása, ellenőrzése, valamint a diagnosztikai és teszt programokat tartalmazó adathordozók ellenőrzése, Távoli karbantartások jóváhagyása, nyomon követése és ellenőrzése

XV.3.2 Általános követelmények

A Kormányhivatalnál a karbantartások és javítások során legalább a következőket kell teljesíteni:

- A karbantartásokat előre meg kell tervezni, amely az informatikai eszközök tekintetében az **IT üzemeltetésért felelős vezető** feladata, aki ennek céljából éves *karbantartási tervet* készít, a karbantartási ablakok előzetes meghatározásával együtt. A karbantartási ablakok idejét az adott **Szervezeti egység vezetővel / Adatgazdával** egyeztetni kell, és ez alapján előzetesen tájékoztatni kell a felhasználókat. Továbbá a terven felül minimum 2 héttel lehet előre nem tervezett karbantartási ablakot kérni. A karbantartási tervet az **Informatikai feladatok ellátásáért felelős vezető** hagyja jóvá. A fizikai védelmet biztosító eszközök, berendezések esetében a **Fizikai védelemért felelős vezető** felelőssége az eszközök és berendezések karbantartási tervének elkészítése.
- 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 értesíteni kell. A felhasználók időben történő értesítése az **IT üzemeltetésért felelős vezető** felelőssége.
- A karbantartásokat és javításokat a szállító vagy a gyártó által előírt módon, ütemezetten kell végrehajtani, és dokumentálni kell valamint felülvizsgálni a karbantartásokról és javításokról készült feljegyzéseket. Az egyes karbantartást igénylő elemek karbantartásának megtörténtéért és ennek dokumentálásáért az **Infrastruktúra üzemeltetési rendszergazdák** felelősek. A dokumentálás megtörténtét az **Informatikai biztonsági felelősnek** szúrópróbaszerűen ellenőriznie kell.

- Amennyiben egy elektronikus információs rendszer vagy annak egy vagy több elemének karbantartása vagy javítása azt igényli, hogy kiszállítsák a szervezetből, akkor azt az **Informatikai feladatok ellátásáért felelős vezetőnek** 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.
- 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 – az *Adathordozók és mobil eszközök védelmére vonatkozó eljárásrend Adathordozók biztonságos törlése* című fejezetének előírásai szerinti – visszaállíthatatlan törlése után lehetséges. Amennyiben ilyen esetben az adathordozó kivétele vagy visszaállíthatatlan törlése sem végrehajtható, úgy az eszköz kiszállítását kizárólag – az **Informatikai feladatok ellátásáért felelős vezető** jóváhagyásán felül – az **Informatikai biztonsági felelős** és a **Szervezeti egység vezető / Adatgazda** jóváhagyásával lehet végrehajtani.
- A kiszállítást megelőző vizsgálatok és tevékenységek végrehajtásáért, és azok dokumentálásáért az **IT üzemeltetésért felelős vezető** a felelős.
- A karbantartások, javítások elvégzését követően meg kell győződni az eszköz megfelelő működéséről és a *Rendszer karbantartási eljárásrend* szerinti biztonsági ellenőrzésnek kell alávetni.

XV.4 Vírusvédelem

A Kormányhivatal egészére kiterjedő, folyamatos vírusvédelem és rendszeres vírusellenőrzés biztosítása érdekében automatikus frissítésű, 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.
A vírusvédelmi rendszer kialakításáért az **Informatikai feladatok ellátásáért felelős vezető** a felelős.
A vírusvédelemre vonatkozó további részletes követelményeket és szabályokat a *Rendszer- és információsértetlenségi eljárásrend* tartalmazza.

XV.4.1 Általános követelmények

- A vírusvédelmi feladatok elvégzéséhez olyan vírusvédelmi programokkal kell rendelkezni a Kormányhivatalnak, amely(ek) segítségével az előforduló összes platform ellenőrizhető, és ezeknek a programoknak a vírusdefiníciós állományait rendszeresen frissíteni kell.
- A munkaállomásokon, a szervereken központi felügyeleti rendszert kell alkalmazni.
- A számítógépeken hetente legalább egyszer teljes körű vírusellenőrzést kell végezni előre ütemezett módon, automatikusan.
- A szervereken és munkaállomásokon a valósidejű 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.

- Vírusvédelem nélkül sem hálózati, sem önálló munkaállomás, sem -hordozható számítógép és mobil eszköz nem üzemeltethető.
- A jogosultságok kialakításánál figyelembe kell venni, hogy a felhasználók nem állíthatják le a gépükön futó vírusvédelmi szoftvert, és nem változtathatják meg annak beállításait.
- A vírusvédelmi alkalmazásnak minden esetben rezidensként (minden írást és olvasást ellenőrizve) kell futnia a memóriában.

XV.5 Mentés

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.
A mentés, archiválás és visszatöltés tervezésének és üzemeltetésének kialakításáért az **Informatikai feladatok ellátásáért felelős vezető** a felelős.
A mentésre és archiválásra vonatkozó további részletes követelményeket és eljárásokat, továbbá szabályokat a *Mentési és archiválási eljárásrend* tartalmazza.

XV.5.1 Biztonsági osztály szerinti követelmények

Az elektronikus információs rendszerek vonatkozásában a kialakítandó mentési megoldásoknak az alábbi biztonsági osztályok szerint növekvő és egymásra épülő elvárásoknak kell megfelelni:

- 2-es biztonsági osztály: Biztonsági mentés, archiválás és visszatöltés tervezése, elvégzése
    - Minimum mentési gyakoriság:
        - napi mentés
        - heti mentés
        - havi mentés
- 4-es biztonsági osztály: 2-es osztály + Biztonsági tárolási helyszín, megbízhatósági és sértetlenségi teszt
    - Minimum mentési gyakoriság:
        - RPO (maximálisan tolerált adatvesztés mértéke) érték szerint, napon belüli mentés
        - napi mentés
        - heti mentés
        - havi mentés

XV.5.1.1 Általános követelmények

Biztonsági mentéseknek kell készülniük:

- az online elérhető (éles, tartalék, fejlesztői) adatbázisokról és fájlrendszer könyvtárakról,
- az offline elérhető (archivált) adatbázisokról és fájlrendszer könyvtárakról,

- szoftverek telepítőkészletéről.

A mentés, archiválás, visszatöltés megfelelőségéhez biztosítani kell:

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

XV.5.1.2 Mentés, archiválás és visszatöltés tervezési követelményei

A mentések paramétereinek meghatározásához alkalmazandó irányelvek:

- A mentések tervezése, a visszaállási pontok kialakítása során figyelembe kell venni a rendelkezésre állási elvárások által rögzített, maximálisan megengedett kiesési időket.
- A mentés rendjét a Mentési és archiválási eljárásrend tartalmazza.
- A mentést követően biztosítani kell egy példány off-line - rendszertől függetlenített - elhelyezését, a sikeres mentést követő 1 napon belül.

Az archiválások paramétereinek meghatározásához alkalmazandó irányelvek:

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

Gondoskodni kell a mentett és archív állományok adatainak (archivált rendszerek) visszaolvasásához, visszatöltéséhez szükséges berendezés mindenkori rendelkezésre állásáról.

XV.5.1.3 Mentések, archiválások elvégzésének követelményei

A mentések, archiválások elvégzése során végrehajtandó feladatok:

- Változásmenedzsment (elektronikus információs rendszer szinten, tartalomváltozás, médiaváltozás, eszközváltozás, infrastruktúra átszervezés, bővítés):
    - 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.
    - Abban az esetben, ha a programverzió változtatása adatkonvertálással is jár, akkor a telepítés előtt soron kívül el kell végezni az adatok mentését.
- Mentések felügyelete
    - Automatikus mentésekről értesítést kell küldeni, hiba esetén a **Mentésért felelős rendszeradminisztrátornak** felül kell vizsgálnia a mentési jobot és szükség esetén el kell végeznie manuálisan a mentést.

XV.6 Naplózás

Az elektronikus információs rendszerekben kezelt adatokhoz való hozzáférések nyomonkövethetősége, a rendszerek jogosulatlan használatának és a bekövetkezett problémák azonosítása érdekében az eseményeket naplózni kell.

A naplózási környezet feltételrendszerének kialakításáért az **Informatikai feladatok ellátásáért felelős vezető** a felelős.

A naplózásra vonatkozó további részletes követelményeket és eljárásokat, továbbá szabályokat a *Naplózási eljárásrend* tartalmazza.

XV.6.1 Biztonsági osztály szerinti követelmények

Az elektronikus információs rendszerek vonatkozásában kialakítandó naplózási megoldásoknak az alábbi biztonsági osztályok szerint növekvő és egymásra épülő elvárásoknak kell megfelelni:

- 2-es biztonsági osztály: Naplóesemények gyűjtése, időszinkronizáció, naplóvédelem:
    - Forrásrendszeri naplógyűjtés;
    - Naplóállományok formátuma: emberi feldolgozásra alkalmas formátum;
    - Megőrzési ciklus: minimum 7 nap (biztosítani kell, hogy a ciklus vége előtt a tárhely ne teljen be vagy ne íródjon felül).
- 3-as biztonsági osztály: 2-es osztály + Naplóesemények értékelése:
    - Gyanús események vizsgálata: havonta;
    - Naplóállományok alapján generált riasztások ellenőrzési gyakorisága: naponta;
    - Megőrzési ciklus: minimum 1 hónap.
- 4-es biztonsági osztály: 3-as osztály + Korrelációs elemzés, automatikus feldolgozás, hiteles naplótárolás:
    - Központi naplógyűjtés;
    - Naplóállományok formátuma: gépi feldolgozásra alkalmas formátum;
    - Központi értékelő és riasztási rendszer (SIEM);
    - Megőrzési ciklus: minimum 1 év.

XV.6.1.1 Általános követelmények

A Kormányhivatalnál kialakított naplózásnak legalább a következőket kell teljesítenie az elektronikus információs rendszerekben:

- 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.
- A különböző elektronikus információs rendszerek naplóállományainak egységes értelmezhetősége érdekében olyan naplózási architektúrát kell kialakítani, ami biztosítja, hogy:
    - ahol csak technikailag lehetséges, a naplózás szerveroldalon történjen,
    - automatikus mechanizmus gondoskodjon az egyes rendszerek, eszközök rendszerórájának szinkronizálásáról.

- 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.
- Az eseménynaplók és az azok kezeléséhez kapcsolódó biztonsági naplók tárolását a következő szempontok figyelembe vételével kell megoldani:
    - a naplóadatokat időpecséttel kell ellátni,
    - a naplóadatoknak sértetlenül rendelkezésre kell állniuk az esetleges elévülési időn belül,
    - biztosítani kell, hogy az adatokban keletkezésük után változtatást már ne lehessen végrehajtani,
    - az adatok bizalmasságára tekintettel, az adatok nem juthatnak illetéktelenek kezébe.
- Mind a rendszergazdai tevékenységet, mind a biztonsági eseményeket nyomon kell követni az egyes elektronikus információs rendszerekben.
- Gondoskodni kell a naplóállományok rendszeres mentéséről vagy redundáns storage-on való tárolásáról és rendszeres felülvizsgálatáról.
- A kiemelt jogosultságokkal bíró felhasználók ne tudjanak nyomtalanul módosítani a naplózási beállításokon.
- A naplóállományoknak az alábbi információkat kell minimálisan tartalmazni:
    - felhasználó azonosítója;
    - számítógép azonosítója vagy pontos helye;
    - a használt hálózati cím;
    - a bekövetkezett esemény pontos dátuma és ideje (rögzíteni, hogy a naplózás UTC vagy helyi idő alapján történik);
    - a bekövetkezett esemény részletei;
    - a (fel)használt szoftvert/alkalmazást.
- A naplózó rendszernek az alábbi típusú események rögzítésére kell kiterjedniük:
    - rendszerindításokat, -leállításokat;
    - rendszerriasztásokat, meghibásodási jelentéseket;
    - a rendszerben fellépő hibákat;
    - felhasználók felvételét, törlését, felfüggesztését, jogosultságának módosítását;
    - a felhasználó bejelentkezést vagy sikertelen bejelentkezési kísérleteket;
    - naplózási funkciók indítását és leállítását;
    - naplóállomány létrehozását, törlését (külön jegyzőkönyvben rögzítve);
    - a rendszerdátum, -idő megváltoztatását;
    - szoftverkonfiguráció megváltozását;
    - nyilvános hálózaton keresztüli kapcsolatnál létrehozást és bontást; ellenoldali fél adatait; forgalom jellege; továbbított vagy fogadott állomány neveit, elérési útvonalát;
    - kijelentkezéseket;

- tűzfal/IPS/terheléselosztó rendszereken átmenő forgalmat;
- programleállásokat;
- az azonosítási és a hitelesítési mechanizmus használatát;
- személyi műveleteket, amelyek a rendszer biztonságát érintik.

XV.7 Határvédelem és rendszerfelügyelet

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

A kormányhivatali rendszerek rendelkezésre állásának és az adatforgalom bizalmasságának és sértetlenségének biztosítása érdekében külső és belső határvédelmi eszközöket és megoldásokat kell alkalmazni.

A határvédelem és rendszerfelügyelet kialakításáért és működtetéséért az **Informatikai feladatok ellátásáért felelős vezető** a felelős.

A határvédelemre és a rendszerfelügyeletre vonatkozó további részletes követelményeket és szabályokat a *Rendszer- és kommunikációvédelmi eljárásrend* tartalmazza.

XV.7.1 Biztonsági osztály szerinti követelmények

Az elektronikus információs rendszerek vonatkozásában kialakítandó határvédelmi és rendszerfelügyeleti megoldásoknak az alábbi biztonsági osztályok szerint növekvő és egymásra épülő elvárásoknak kell megfelelni:

- 2-es biztonsági osztály:
  - Menedzselhető, biztonságos hálózati architektúra kialakítása;
    - Védett zónák kialakítása (DMZ, VPN);
    - Tűzfalak használata;
    - Behatolás elleni védelem.
  - Rendszerfelügyeleti rendszer:
    - Riasztások figyelése, kezelése: napi 8 órában.
- 3-as biztonsági osztály: 2-es osztály + Túlterhelés elleni védelem
  - DoS/DDoS védelem kialakítása az Internet eléréssel rendelkező rendszerek esetén.
- 4-es biztonsági osztály: 3-as osztály +
  - Rendszerfelügyeleti rendszer:
    - Riasztások figyelése: napi 24 órában;
    - Automatizált eseményfigyelés: valós időben (SIEM).

XV.7.1.1 Általános követelmények

A kialakítandó határvédelmi és rendszerfelügyeleti megoldások kialakítása során legalább az alábbiakat kell teljesíteni az elektronikus információs rendszerekben:

- A Kormányhivatal számítógépes hálózatára tilos olyan munkaállomást csatlakoztatni, amely:
    - nem bizalmas hálózati kapcsolattal is rendelkezik,
    - nem tagja a Kormányhivatal kontrollált munkakörnyezetének (címtár, tartomány).
- A Kormányhivatal számára bizalmas hálózati kapcsolatnak számít a belső számítógépes hálózat, minden egyéb hálózat nem bizalmas hálózatnak számít, olyannak, amelyről azt kell feltételezni, hogy veszélyt jelent a Kormányhivatal informatikai biztonsága számára.
- A Kormányhivatalnak a kontrollok hatékonyabb működtetése érdekében a külső kapcsolatai számát a szükséges minimumra kell korlátozni.
- Tűzfalak használata
    - Minden hálózati forgalom a külső és belső hálózati szegmens között a tűzfalon keresztül kell, hogy haladjon, a tűzfalakat oly módon kell beállítani, hogy védve legyenek minden nem engedélyezett, elektronikus vagy fizikai hozzáféréstől.
    - A tűzfalaknak mindig dedikált gépen kell futniuk és azon más szolgáltatás vagy belső információ nem lehet, vagy appliance-t kell használni.
    - A tűzfalaknak naplózniuk kell minden gyanús és tiltott tevékenységet.
- Az informatikai rendszert központi behatolás-detektáló és megelőző rendszer (IDS/IPS) kialakításával kell védeni. Az IDS/IPS eszközök esetében a központi szolgáltató határvédelmi rendszereire kell támaszkodni, azok hiánya esetén saját eszközöket kell alkalmazni.
- Az informatikai rendszer kritikus elemeit, illetve biztonsági eszközeit folyamatosan monitorozni kell. A monitorozásnak minimálisan az alábbi témákra kell kiterjednie:
    - Határvédelmi incidensek, és hálózati illegális tevékenység;
    - Vírusvédelmi incidensek;
    - Jogosultság kezelési incidensek;
    - Mentési feladatok sikeres/sikertelen végrehajtása;
    - Külső beszállítók és szolgáltatók felhasználóinak tevékenységei, távoli elérések naplózása;
    - Rendszergazdák tevékenységei;
    - Biztonsági riasztórendszerek naplózása.

XV.8 Adatátvitel bizalmassága és sértetlensége

Az elektronikus információs rendszernek védenie kell a továbbított információk bizalmasságát és sértetlenségét, ezért olyan adatátviteli protokollt kell az érintett szervezetnek használnia, amely képes biztosítani az adatátvitel bizalmasságát és sértetlenségét, ezért megfelelő védelmi mechanizmust kell kialakítani az adatátvitel során.

Az adatátvitel bizalmasságának, sértetlenségének kialakításáért az **Informatikai feladatok ellátásáért felelős vezető** a felelős.

Az adatátvitel bizalmasságára, sértetlenségére vonatkozó további részletes követelményeket és szabályokat a *Rendszer- és kommunikációvédelmi eljárásrend* tartalmazza.

XV.8.1 Biztonsági osztály szerinti követelmények

Az elektronikus információs rendszerek vonatkozásában az adatátvitel bizalmasságára, sértetlenségére vonatkozó védelmi mechanizmusoknak az alábbi biztonsági osztályok szerint növekvő és egymásra épülő elvárásoknak kell megfelelni:

- 2-es biztonsági osztály: Kriptográfiai kulcsokra vonatkozó eljárásrend, Elkülönített folyamatok, Távoli felügyelet létesítésének kontrollja;
- 3-as biztonsági osztály: Biztonságos név/cím feloldó szolgáltatások, Architektúra és tartalékok név/cím feloldási szolgáltatás esetén;
- 4-es biztonsági osztály: Mobilkód korlátozása, Nyilvános kulcsú infrastruktúra tanúsítványok, Munkaszakaszok hitelességének biztosítása.

XV.8.1.1 Általános követelmények

A titkosított adathoz csak az arra jogosult – utólag is ellenőrizhető módon – férhet hozzá. Az információ integritása védelmében titkosítási módszereket kell alkalmazni. Ennek érdekében az elektronikusan tárolt információt át kell alakítani úgy, hogy az ahhoz hozzáférők meghatározott kulcs, illetve kód ismerete nélkül ne tudják az adatot megfejteni – kinyerni annak információ tartalmát. A módszernek meg kell valósítania, hogy harmadik személy az adatátviteli vagy adattároló eszközhöz való hozzáférése esetén ne jusson hozzá az információhoz.

A Kormányhivatal elektronikus információs rendszereinek tekintetében az alábbi kriptográfiai megoldások alkalmazhatók:

- blokk-titkosításra: AES-128, AES-192, AES-256 (DES, 3DES algoritmus már nem!)
- kulcscsere folyamatnál (key agreement):
    - Diffie-Hellman (DH);
    - Menezes-Qu_Vanstone (MQV).
- kulcscsomagolásnál (key wrapping):
    - AES;
    - három-kulcsos TDEA algoritmusok.
- kulcsgenerálásához (Key Derivation Function – KDF): HMAC alapú megoldás.
- Lenyomatoló (hash) függvények előállítása:
    - SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256);
    - SHA-3 (SHA3-224, SHA3-256, SHA3-384, SHA3-512);
    - (SHA-1 és korábbi (pl. MD4, MD5) hash függvények (pl. jelszó tárolásra) már nem használható.).
- Üzenet autentikációs kód (Message Authentication Code – MAC):
    - HMAC (hash alapú): minimum 112 bit hosszúságú kulcs;
    - CMAC és DMAC (blokk-titkosítás alapú): AES alkalmazása.

A Kormányhivatal elektronikus információs rendszereinek meg kell gátolnia a személyes kommunikációhoz használt számítástechnikai perifériák (pl. kamerák, mikrofonok, asztal megosztás; távoli informatikai felügyelet) automatikus távoli aktiválását.

A távoli felügyelet létesítésének szabályai:

- a távolról menedzselt munkaállomást használó felhasználó részére biztosítani kell a kapcsolat engedélyezésének lehetőségét;
- a távolról menedzselt munkaállomást használó felhasználónak lehetőség szerint úgy kell átadnia a képernyőjét a távoli felügyeletet végző számára, hogy személyes adatot ne jelenítsen meg;
- a munkavégzés képernyőn történő nyomon követhetőségét biztosítani kell a távolról menedzselt munkaállomást használó felhasználó részére;
- a felhasználó számára egyértelműen megállapíthatónak kell lennie, hogy a munkaállomása távolról menedzselt állapotban van-e.

XV.9 Elektronikus információs rendszer kapcsolódásai

3-as vagy magasabb informatikai biztonsági osztályú rendszerek összekapcsolása esetén a következő szabályok betartását kell szem előtt tartani:

- Azonos informatikai biztonsági besorolású rendszerek esetén a **Szervezeti egység vezető / Adatgazda** jóváhagyása szükséges, és az összekapcsolás folyamatát, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát dokumentálni kell.
- Alacsonyabb informatikai biztonsági besorolású rendszerek csatlakoztatása esetén a **Szervezeti egység vezető / Adatgazda** és az **Informatikai biztonsági felelős** együttes jóváhagyása szükséges. Az adatkapcsolat megvalósítása során, amennyiben kétirányú adattovábbítás valósul meg, az adatcserében résztvevő rendszerelemeket a magasabb biztonsági besorolású rendszer hardening előírásai szerint kell konfigurálni.

XVI. A Szabályzatban használt fogalmak, meghatározások

Fogalom	Meghatározás
Adat	az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;
Adatgazda	annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik;
Adathordozó	az adatok tárolására, megőrzésére szolgáló, beépített vagy cserélhető eszközök összefoglaló neve;
Adatkezelés	az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése;
Adatkezelő	az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;
Adatvagyon	adatok, szellemi, erkölcsi javak összessége;
Auditálás	előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;
Bizalmasság	az informatikai rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról; lefedi a tárolt, feldolgozás alatt álló, illetve ideiglenes állapotban, átmeneti helyen előforduló, átviteli csatornán megjelenő adatokat
Biztonság	A rendszer tulajdonsága. Sokkal több, mint mechanizmusok vagy funkciók adott készlete. Az IT biztonság egyrészt rendszer tulajdonság, valamint mechanizmusok összessége, melyek lefedik mind logikailag, mind fizikailag a teljes rendszert.
Biztonsági esemény	nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ

Fogalom	Meghatározás
	bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;
Biztonsági esemény kezelése	az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;
Biztonsági osztály	az informatikai rendszer védelmének elvárt erőssége;
Biztonsági osztályba sorolás	a kockázatok alapján az informatikai rendszer védelme elvárt erősségének meghatározása;
Biztonsági szint	a szervezet felkészültsége a jogszabályokban meghatározott biztonsági feladatok kezelésére;
Biztonsági szintbe sorolás	a szervezet felkészültségének meghatározása a jogszabályokban meghatározott biztonsági feladatok kezelésére;
CMDB (Konfigurációkezelési adatbázis)	Az az adatbázis, amelyet a konfigurációrekordok tárolására használnak a teljes életciklusukon keresztül.
Disaster Recovery Plan (DRP)	Tevékenységek és programok, amelyekkel a szervezet visszatérhet egy elfogadott állapotba. A képesség arra, hogy egy szolgáltatás megszakadására választ lehessen adni a katasztrófa utáni helyreállítási terv (DRP) megvalósításával, hogy a szervezet kritikus folyamatait visszaállítsák.
Elektronikus információs rendszer (EIR)	az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese. Egy elektronikus információs rendszernek kell tekinteni az adott adatgazda által, adott cél érdekében az adatok, információk kezelésére használt eszközök, eljárások, valamint az ezeket kezelő személyek együttesét;
Életciklus	az informatikai rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;
Észlelés	a biztonsági esemény bekövetkezésének felismerése;
Felhasználó	egy adott informatikai rendszert igénybe vevők köre;
Fenyegetés	olyan lehetséges művelet vagy esemény, amely sértheti az informatikai rendszer vagy az informatikai rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az informatikai rendszer védettségét, biztonságát;
Fizikai védelem	a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek

Fogalom	Meghatározás
	fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klímatizálás és a tűzvédelem;
Hálózat	számítógépek (vagy általánosabban elektronikus információs rendszerek) összekapcsolása, és az összekapcsolt rendszerek legkülönbözőbb komponensei közötti adatcserét megvalósító logikai és fizikai eszközök összessége;
Hozzáférés	olyan eljárás, amely valamely elektronikus információs rendszer használója számára – jogosultságának függvényében – meghatározott célra, helyen és időben elérhetővé teszi az elektronikus információs rendszer erőforrásait, elérhetővé tesz a rendszerben adatokként tárolt információkat;
Infokommunikáció	Az infokommunikáció az Európai Unió hivatalos szóhasználatában az információ technológia és az elektronikus hírközlés konvergenciáját, integrálódását fejezi ki. Infokommunikáció alatt mindazon eszközöket, technológiákat és alkalmazásokat, illetve azok használatát kell érteni, amelyek az egyén, a vállalkozás és az állam szintjén egyaránt értelmezhető minőség-, hatékonyság- és eredményesség javulást eredményeznek.
Információ	bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret;
IT-kockázat	az a tiszta kihatás, mely az alábbiakból tevődik össze: (1) annak valószínűsége, hogy egy adott veszélyforrás kihasznál vagy kivált valamely sebezhetőséget a rendszerben, és (2) ennek bekövetkezésekor a kihatások, következmények. Az IT-vel kapcsolatos kockázatok jogi kötelezettségekből vagy a szervezet feladatait/céljait fenyegető veszteségekből származnak, melyek főbb okai: a) információk jogosulatlan (rosszindulatú, nem-rosszindulatú vagy véletlen) megismerése (felfedése), módosítása vagy megsemmisítése b) nem rosszindulatú hibák és mulasztások c) IT folyamatok megszakadása természeti katasztrófák vagy emberi vétség miatt gondatlan, hibás kezelés az IT műveletek és implementáció során
Garancia	A megbízhatóság alapja, hogy a négy biztonsági cél (integritás, rendelkezésre állás, bizalmasság és elszámoltathatóság) megfelelően kielégítésre kerül egy adott implementációban. A "megfelelően kielégítésre kerül" az alábbiakat öleli át: (1) a funkcionalitások helyesen

Fogalom	Meghatározás
	hajtódnak végre, (2) elegendő védelmet építettek a rendszerbe a nem szándékos (felhasználói vagy szoftver) hibák ellen, és (3) a rendszer a megkívánt szinten ellenáll a szándékos behatolási kísérleteknek illetve biztonsági funkciókat kikerülni akaró támadásoknak.
Katasztrófa elhárítás	Aktivitások és programok, amelyekkel a szervezet visszatérhet egy elfogadott állapotba. A képesség arra, hogy egy szolgáltatás megszakadására választ lehessen adni a katasztrófa utáni helyreállítási terv (DRP) megvalósításával, hogy a szervezet kritikus üzleti folyamatait visszaállítsák.
Kockázat	a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;
Kockázatelemzés	az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;
Mentési job	ütemezett mentési feladat.
Mobil eszköz	olyan kisméretű hordozható számítástechnikai eszköz, amely vezeték nélküli adattovábbításra képes, cserélhető vagy beépített adathordozóval és önálló áramforrással rendelkezik. Ilyen eszköz az okostelefon, tablet, PDA, ebook-olvasó stb.
Reagálás	a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;
Rendelkezésre állás	annak biztosítása, hogy az informatikai rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatók legyenek;
Sebezhetőség	a rendszer biztonsági követelményeiben, tervezésében, implementációjában vagy üzemeltetésében fellelhető olyan gyengeség, mely véletlenül kiváltható vagy szándékosan vissza lehet vele élni, és a rendszer biztonsági politikájának megsértését vonja maga után;
Sértetlenség	az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az adat az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az informatikai rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az informatikai rendszer eleme rendeltetésének megfelelően használható;
Sérülékenység	az informatikai rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;

Fogalom	Meghatározás
Sérülékenység vizsgálat	az informatikai rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;
Változáskezelés	az Informatikai szervezeti egység(ek) az informatikai rendszeren bekövetkező változások engedélyezési, végrehajtási, felügyeleti és értékelési tevékenységeinek ellátásához változáskezelési rendszert üzemeltet(nek), amelynek célja a változtatással összefüggő incidensek bekövetkezésének megelőzése és a módosítások kockázatának csökkentése, ezen keresztül az alkalmazások rendelkezésre állásának emelése, a folyamat dokumentálása és mérése;
Veszély (fenyegetés)	egy veszélyforrás lehetősége arra, hogy véletlenül vagy szándékosan kiváltson, kihasználjon egy adott sebezhetőséget;
Veszélyforrás	vagy (1) szándék és módszer, mellyel egy sebezhetőséget szándékosan ki akarnak használni, vagy (2) helyzet és módszer, amely véletlenül kiválthat egy sebezhetőséget;
Védelmi feladatok	megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés;

XVII. Jogszabályi háttér

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)
- 41/2015. (VII.15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.
- 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról.
- 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről.
- 38/2011. (III. 22.) Korm. Rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról.
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról.
- 270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről.
- 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól.

XVIII. Függelékek jegyzéke

Sorszám:	Megnevezés:
1. számú függelék	Biztonsági osztályba és biztonsági szintbe sorolás
2. számú függelék	Felhasználói Felelősségvállalási Nyilatkozat
3. számú függelék	Biztonsági események bejelentési elérhetőségei
4. számú függelék	Titoktartási nyilatkozat (Külső, Belső)

Sorszám:	Megnevezés:
5. számú függelék	Szerverszoba követelmények
6. számú függelék	Rendszerbiztonsági Terv sablon
7. számú függelék	Informatikai eszköz igénylési és átadás-átvételi űrlap
8. számú függelék	Adathordozók és mobil eszközök nyilvántartása
9. számú függelék	Jogosultságigénylő űrlap

XIX. Záró rendelkezések

A szabályzat 2019. június 1. napján lép hatályba.

Veszprém, 2019. május 24.

Takács szabolcs
Kormánymegbízott

Veszprém Megyei Kormányhivatal 2.

Jóváhagyom:

Budapest, 2019. 05. hó 31. nap

Tuzson Bence
Államtitkár

Miniszterelnökség 6.