

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Tüskevár Közös Önkormányzati Hivatal



Tartalomjegyzék

Az Informatikai Biztonsági Szabályzat célja és hatálya.....	6
Személyi hatálya.....	6
Tárgyi hatálya.....	6
Szerepkörök, feladatok, felelőségek.....	6
Jegyző, a szervezet vezetője.....	6
Eljárásrendek	9
Szerepkörök	9
Tevékenységek.....	9
Hivatalrendszer belső együttműködése	10
Az Informatikai biztonsági szabályzat kialakítása a 41/2015. (VII. 15.) BM rendeletben megfogalmazottak szerint	10
Szervezeti szintű alapfeladatok adminisztratív védelmi intézkedés alapján az érintett szervezet.....	10
Az informatikai biztonsági szabályzatban meg kell határozni.....	10
További alapvető elvárások	10
Az informatikai biztonsági szabályzat elsősorban a következő elektronikus információs rendszerbiztonsággal kapcsolatos területeket szabályozza	10
Osztályba sorolás követelményei.....	11
Az ASP rendszerhez csatlakozás	12
Az infrastruktúra felállításának főbb feladatai	12
IT biztonsági feltételek megteremtése.....	12
Fizikai biztonság megteremtése ASP-ben.....	12
Örzés, védelem.....	13
Humán erőforrás az ASP-ben.....	13
Oktatás, képzés az ASP-ben.....	14
ASP jogosultság kezelés	14
ASP rendszerbe történő belépés, autentikáció.....	14
Csatlakozó önkormányzatok kliens oldali biztonsága.....	15
Munkaállomásra vonatkozó biztonsági elvárások	17
Rosszindulatú kódok elleni védelem.....	18
A vírusvédelmi eljárások követelményei.....	18
Hálózatbiztonság	18
Hálózat védelme	18
Informatikai határvédelem, tűzfal	19
1. Mobil eszközök használata.....	19
Osztályba sorolás eredménye, besorolási nyilatkozat.....	19
Adminisztratív Védelmi Intézkedések.....	20

Szervezeti szintű alapfeladatok	20
Informatikai biztonsági szabályzat	20
Az elektronikus információs rendszerek biztonságáért felelős személy	21
Intézkedési terv és mérőföldkövei	21
Az elektronikus információs rendszerek nyilvántartása	21
Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás	21
Kockázatelemzés	22
Kockázatelemzési és kockázatkezelési eljárásrend	22
Biztonsági osztályba sorolás	22
Kockázatelemzés	22
Rendszer és szolgáltatás beszerzés	22
Külső elektronikus információs rendszerek szolgáltatásai	22
Üzletmenet- (ügymenet-) folytonosság tervezése	23
Üzletmenet-folytonosságra vonatkozó eljárásrend	23
Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre	23
Az elektronikus információs rendszer mentései	24
Az elektronikus információs rendszer helyreállítása és újraindítása	24
Emberi tényezőket figyelembe vevő – személy – biztonság	24
Eljárás jogviszony megszűnésekor	24
Fegyelmi intézkedések	25
Viselkedési szabályok az interneten	25
Tudatosság és képzés	25
Képzési eljárásrend	25
Biztonságtudatossági képzés	26
Fizikai Védelmi Intézkedések	26
Fizikai és környezeti védelem	26
Fizikai védelmi eljárásrend	26
Fizikai belépési engedélyek	26
A fizikai belépés ellenőrzése	27
Logikai Védelmi Intézkedések	27
Általános védelmi intézkedések	27
Engedélyezés	27
Személybiztonság	27
Tervezés	28
Rendszerbiztonsági terv	28

Cselekvési terv.....	28
Személyi biztonság.....	29
Rendszer és szolgáltatás beszerzés	29
A rendszer fejlesztési életciklusa	29
Konfigurációkezelés	30
Konfigurációkezelési eljárásrend.....	30
Alapkonfiguráció	30
Elektronikus információs rendszerelem leltár.....	30
A szoftverhasználat korlátozásai.....	30
A felhasználó által telepített szoftverek.....	30
Karbantartás	31
Rendszer karbantartási eljárásrend.....	31
Rendszeres karbantartás	31
Adathordozók védelme	31
Adathordozók védelmére vonatkozó eljárásrend.....	31
Hozzáférés az adathordozókhoz.....	31
Adathordozók törlése	32
Adathordozók használata	32
Azonosítás és hitelesítés.....	32
Azonosítási és hitelesítési eljárásrend	32
Azonosítás és hitelesítés (szervezetten belüli felhasználók)	32
Azonosító kezelés.....	32
A hitelesítésre szolgáló eszközök kezelése	32
A hitelesítésre szolgáló eszköz visszacsatolása	33
Azonosítás és hitelesítés (szervezetten kívüli felhasználók)	33
Hozzáférés ellenőrzése	33
Hozzáférés ellenőrzési eljárásrend.....	33
Felhasználói fiókok kezelése	33
Hozzáférés ellenőrzés érvényesítése.....	34
Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek	34
Külső elektronikus információs rendszerek használata.....	34
Nyilvánosan elérhető tartalom	34
Rendszer- és információsértetlenség	35
Rendszer- és információsértetlenségére vonatkozó eljárásrend	35
Hibajavítás	35

Kártékony kódok elleni védelem.....	35
Az elektronikus információs rendszer felügyelete	36
A kimeneti információ kezelése és megőrzése.....	36
Naplózás és elszámoltathatóság	36
Naplózási eljárásrend.....	36
Naplózható események	36
Naplóbejegyzések tartalma	36
Időbélyegek	36
A napló információk védelme.....	37
A naplóbejegyzések megőrzése	37
Naplógenerálás	37
Rendszer- és kommunikációvédelem.....	37
Rendszer- és kommunikációvédelmi eljárásrend	37
A határok védelme.....	37
Alapfogalmak.....	38
Mellékletek:.....	42

Az Informatikai Biztonsági Szabályzat célja és hatálya

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, valamint 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 értelmében az állami és önkormányzati szervezeteknek rendelkezniük kell Informatikai Biztonsági Szabályzattal.

A szabályzat kialakításánál az említett jogszabályokon túl figyelembe kell venni az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendeletet, valamint a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI 30. § (1) bekezdésében kapott felhatalmazás alapján a(z) Tüskevári Közös Önkormányzati Hivatal (továbbiakban: Hivatal) informatikai biztonsági szabályzatát az alábbiakban határozza meg.

Személyi hatálya

Az Informatikai Biztonsági Szabályzat kiterjed a **Közös Önkormányzati Hivatal** köztisztviselőire, ügyintézőire, a hivatal valamennyi munkatársára, valamint azokra a személyekre, akik részt vesznek az önkormányzatnál keletkező, tárolt, illetve továbbított adatok kezelésében.

Tárgyi hatálya

Az Informatikai Biztonsági Szabályzat kiterjed a **Közös Önkormányzati Hivatal**nál kezelt, keletkezett információkra, az informatikai rendszerben üzemeltetett valamennyi hardver és szoftver elemekre, amely felhasználja, feldolgozza, felügyeli, ellenőrzi, tárolja, továbbítja az önkormányzatnál keletkező, illetve felhasznált adatokat. Kiterjed továbbá a rendszerelemek dokumentációira.

Szerepkörök, feladatok, felelősségek

Az informatikai biztonság megfelelő kialakításának egyik követelménye a biztonsággal kapcsolatos szerepkörök szétválasztása.

Az önkormányzat minden munkatársa, szerződésben lévő informatikai alvállalkozója és természetes személy köteles az Informatikai Biztonsági Szabályzat előírásait betartani.

Az SZMSZ-ben rögzített beosztások és felelősségi körök figyelembevételével javasolt az önkormányzatok informatikai biztonsági szerepkörök meghatározása.

Az alábbi részben a jogszabály által kötelezően meghatározott feladatok és felelősök felsorolása található.

Jegyző, a szervezet vezetője

Az állami és önkormányzati szervek elektronikus információbiztonságáról 2013. évi L. törvény alapján:

„11. § (1) A szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről a következők szerint:

- a) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
- b) biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,
- c) az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,
- f) meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,
- g) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,
- h) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
- i) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
- j) 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,
- k) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködött vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
- l) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködött vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
- m) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,
- n) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

12. § A szervezet vezetője köteles együttműködni a hatósággal. Ennek során:

- a) a 11. § (1) bekezdés c) pontjában meghatározott, az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt,
- b) a szervezet informatikai biztonsági szabályzatát tájékoztatás céljából megküldi,
- c) az ellenőrzés lefolytatásához szükséges feltételeket biztosítja a hatóság részére."

Elektronikus információs rendszer biztonságáért felelős személy

Az állami és önkormányzati szervek elektronikus információbiztonságáról 2013. évi L. törvény alapján:

„13. § (1) Az elektronikus információs rendszer biztonságáért felelős személy feladata ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést.

(2) Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:

- a) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,

- b) elvégzi vagy irányítja az a) pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
- c) előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
- d) előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,
- e) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,
- f) kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.
- (3) Az elektronikus információs rendszer biztonságáért felelős személy e törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet.
- (4) 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.
- (5) Az elektronikus információs rendszer biztonságáért felelős személy biztosítja az e törvényben meghatározott követelmények teljesülését
- a) a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők,
- b) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők e törvény hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.
- (6) Az elektronikus információs rendszer biztonságáért felelős személy e törvény szerinti feladatai és felelőssége az (5) bekezdés szerinti esetekben más személyre nem átruházható.
- (7) Az elektronikus információs rendszer biztonságáért felelős személy jogosult az (5) bekezdés szerinti közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelés alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.
- (8) A szervezetenél csak olyan személy végezheti az elektronikus információs rendszer biztonságáért felelős személy feladatait, aki büntetlen előéletű, rendelkezik a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel.
- (9) A büntetlen előélet követelményének való megfelelést az elektronikus információs rendszer biztonságáért felelős személy a szervezettel fennálló jogviszonya keletkezését megelőzően köteles igazolni. A szervezet az elektronikus információs rendszer biztonságáért felelős személyt kötelezheti, hogy a szervezettel fennálló jogviszonya alatt a büntetlen előélet követelményének való megfelelést igazolja.
- (10) Nem kell a (8) bekezdés szerinti képzettséget megszereznie annak a személynek, aki rendelkezik a külön jogszabályban meghatározott, akkreditált nemzetközi képzettséggel vagy e szakterületen szerzett 5 év szakmai gyakorlattal.
- (11) Az elektronikus információs rendszer biztonságáért felelős személy és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában

részt vevő személyek miniszteri rendeletben meghatározott rendszeres szakmai képzésen, továbbképzésen vesznek részt.”

Eljárásrendek

A jogszabálynak történő megfelelés alapján az Informatikai Biztonsági Szabályzat mellet a szervezetnek rendelkeznie kell eljárásrendekkel. Az elektronikus információs rendszer legmagasabb osztályba sorolt értékéhez tartozó eljárásrendek listája az alábbi:

- Kockázatelemzési és kockázatkezelési eljárásrend
- Beszerzési eljárásrend
- Üzletmenet folytonosságra vonatkozó eljárásrend
- Biztonsági eseménykezelési eljárásrend
- Személybiztonsági eljárásrend
- Képzési eljárásrend
- Fizikai védelmi eljárásrend
- Biztonságelemzési eljárásrend
- Konfigurációkezelési eljárásrend
- Rendszer karbantartási eljárásrend
- Adathordozók védelmére vonatkozó eljárásrend
- Azonosítási és hitelesítési eljárásrend
- Hozzáférés ellenőrzési eljárásrend
- Rendszer és információ sértetlenségre vonatkozó eljárásrend
- Naplózási eljárásrend
- Rendszer- és kommunikáció védelmi eljárásrend

Szerepkörök

A Polgármesteri hivatal a részletes hivatali szerepköröket a Szervezeti és Működési Szabályzatban rögzítette.

Polgármesteri hivatal (képviselő testület, jegyző, polgármester): az Informatikabiztonsági feladatokkal kapcsolatban kitűzi a célokat, programokat, stratégiát, politikát határoz meg, felügyeli ezek megvalósulását, forrást biztosít a megvalósításokhoz.

Informatikai referens: az informatikabiztonsággal kapcsolatban szervezi, és szakmai kompetenciájának megfelelően végrehajtja a Polgármesteri hivatal által meghatározott politikát, célokat, stratégiát. Kapcsolatot tart és felügyeli a feladatok végrehajtásával megbízott személyt, vagy személyeket.

Informatikabiztonsági felelős- az a szakember, aki szakmailag kompetens és ellátja az informatikabiztonsággal kapcsolatos törvényi feladatokat.

Beosztottak, alkalmazottak, köztisztviselők: végrehajtják és betartják az utasításokat, szabályokat. Magatartásukkal segítik a hatékony és biztonságos informatikabiztonság megteremtését.

Tevékenységek

A polgármesteri hivatal a tv.-ben meghatározott alaptevékenységét a Szervezeti és Működési Szabályzatban rögzítette.

Hivatalrendszer belső együttműködése

A polgármesteri hivatal a belső együttműködését a Szervezeti és Működési Szabályzatban rögzítette.

Az Informatikai biztonsági szabályzat kialakítása a 41/2015. (VII. 15.) BM rendeletben megfogalmazottak szerint

Szervezeti szintű alapfeladatok adminisztratív védelmi intézkedés alapján az érintett szervezet

megfogalmazza, és az érintett szervezetre érvényes követelmények szerint **dokumentálja**, valamint az érintett szervezeten belül **kihirdeti** az informatikai biztonsági szabályzatot, más belső szabályozásában, vagy magában az informatikai biztonsági szabályzatban **meghatározza** az informatikai biztonsági szabályzat **felülvizsgálatának és frissítésének gyakoriságát**, gondoskodik arról, hogy az informatikai biztonsági szabályzat **jogosulatlanok számára ne legyen megismerhető**, módosítható.

Az informatikai biztonsági szabályzatban meg kell határozni

- a **célokat**, a szabályzat **tárgyi és személyi** (a szervezet jellegétől függően területi) **hatályát**,
- az elektronikus információbiztonsággal kapcsolatos **szerepköröket**,
- a szerepkörhöz rendelt **tevékenységet**,
- a tevékenységhez kapcsolódó **felelősséget**,
- az információbiztonság szervezetrendszerének **belső együttműködését**.

További alapvető elvárások

Rögzíteni kell:

- a biztonsági osztályba sorolás eredményét a szervezet informatikai biztonsági szabályzatában,
- a kockázatelemzések eredményét az informatikai biztonsági szabályzatban, kockázatelemzési jelentésben, vagy a kockázatelemzési eljárásrendben előírt dokumentumban,
- a kockázatelemzési eljárásrendnek megfelelően, meg kell ismertetni a kockázatelemzés eredményét az érintettekkel.

Az informatikai biztonsági szabályzat elsősorban a következő elektronikus információs rendszerbiztonsággal kapcsolatos területeket szabályozza

- kockázatelemzés (amely szorosan kapcsolódik a biztonsági osztályba és biztonsági szintbe soroláshoz),
- biztonsági helyzet-, és eseményértékelés eljárási rendje,
- az elektronikus információs rendszer (ideértve ezek elemeit is) és információtechnológiai szolgáltatás beszerzés (amennyiben az érintett szervezet ilyet végez, vagy végezhet),
- biztonsággal kapcsolatos tervezés (például: beszerzés, fejlesztés, eljárásrendek kialakítását),
- fizikai és környezeti védelem szabályai, jellemzői,

- az emberi erőforrásokban rejlő veszélyek megakadályozása (pl.: személyzeti felvételi-és kilépési eljárás során követendő szabályok, munkavégzésre irányuló szerződésben a személyes kötelek rögzítése, a felelősség érvényesítése, stb.),
- az informatikai biztonság tudatosítására irányuló tevékenység és képzés az érintett szervezet összes közszolgálati, vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottainak, munkavállalóinak, megbízottjainak tekintetében,
- az érintett szervezetnél alkalmazott elektronikus információs rendszerek biztonsági beállításával kapcsolatos feladatok, elvárások, jogok (amennyiben az érintett szervezetnél ez értelmezhető),
- üzlet-, ügy- vagy üzemmenet folytonosság tervezése (így különösen a rendszerleállítás során a kézi eljárásokra történő átállás, visszaállás az elektronikus rendszerre, adatok pótlása, stb.),
- az elektronikus információs rendszerek karbantartásának rendje,
- az adathordozók fizikai és logikai védelmének szabályozása,
- az elektronikus információs rendszerhez való hozzáférés során követendő azonosítási és hitelesítési eljárás, és a hozzáférési szabályok betartásának ellenőrzése,
- amennyiben az érintett szervezetnek erre lehetősége van, a rendszerek használatáról szóló rendszerbejegyzések értékelése, az értékelés eredményétől függő eljárások meghatározása,
- az adatok mentésének, archiválásának rendje,
- a biztonsági események - ideértve az adatok sérülését is - bekövetkeztekor követendő eljárás, ideértve a helyreállítást,
- az elektronikus információs rendszerhez jogosultsággal (vagy jogosultság nélkül fizikailag) hozzáférő, nem az érintett szervezet tagjainak tevékenységét szabályozó (karbantartók, magán-, vagy polgári jogi szerződés alapján az érintett szervezet számára feladatokat végrehajtók), az elektronikus információbiztonságot érintő, szerződéskötés során érvényesítendő követelmények,
- az informatikai biztonsági szabályzat tartalmazza az érintett szervezet elvárt biztonsági szintjét, valamint az érintett szervezet egyes elektronikus információs rendszereinek elvárt biztonsági osztályát.

Osztályba sorolás követelményei

Technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelmények a 41/2015. (VII. 15.) BM rendelet alapján történik meg:

- az elektronikus információs rendszerek biztonsági osztályba sorolása a rendelet 1. melléklet alapján,
- az elektronikus információs rendszerrel rendelkező szervezetek vagy szervezeti egységek biztonsági szintbe sorolása a rendelet 2. melléklet szerint,
- az elvégzett besorolás alapján az elektronikus információs rendszerrel rendelkező szervezet a rendelet 3. mellékletben meghatározott, az elektronikus információs rendszerére érvényes biztonsági osztályhoz rendelt követelményeket a rendelet 4. mellékletben meghatározott módon teljesíti.

Informatikai Biztonsági Szabályzat kialakításához ASP specifikus irányelvek

Az ASP rendszerhez csatlakozás

A 257/2016. (VIII. 31.) Korm. rendelet 2. melléklete tartalmazza a minimumkövetelményekhez tartozó megfelelés elvárását. Ez alapján ki lehet alakítani azt az informatikai infrastruktúra környezetet, amellyel biztosított az ASP rendszerhez történő csatlakozás a következők alapján.

Az informatikai környezet fő komponensei:

- Munkaállomások beüzemelés
- Nyomtatók üzembe állítása
- Hálózati aktív eszközök beüzemelése, hálózat kiépítése
- Vírusvédelmi rendszer beüzemelése
- Tűzfal beüzemelése
- Internetkapcsolat üzembe állítása

Az infrastruktúra felállításának főbb feladatai

Tenant létrehozása a Keretrendszerben (ASP. KERET), Tenant adminisztrátor felvétele a Keretrendszerben (ASP.KERET).

Adatbázisok létrehozása a Gazdálkodási (ASP. GAZD) és szakrendszerben.

Tenant felhasználók felvétele és szerepkörök összerendelése a Keretrendszerben (ASP. KERET).

Tanúsítványok elkészítése és hozzárendelése.

Tanúsítványok kiosztása önkormányzati felhasználók között.

IT biztonsági feltételek megteremtése

- Önkormányzati biztonsági szint meghatározása.
- A meghatározott biztonsági szinthez kapcsolódó védelmi intézkedések biztosítása.
- Információbiztonsági szabályozások kialakítása, szükség szerinti módosítása, jóváhagyása, kihirdetése.
- Biztonsági auditra való felkészülés.
- ASP-vel kapcsolatos audit tevékenység csak a Hatóság írásbeli engedélyével végezhető el. Erről az önkormányzat tájékoztatást ad a Magyar Államkincstár részére.
- ASP rendszeren külsős Fél, szervezet nem végezhet sérülékenységi vizsgálatot a Hatóság írásbeli engedélye nélkül. Ezen vizsgálati tényről az önkormányzat tájékoztatást ad a Magyar Államkincstár részére.

Fizikai biztonság megteremtése ASP-ben

A fizikai biztonság meghatározásánál az ASP-t futtató objektum tekintetében, amennyiben az önkormányzati hivatal teheti, szükséges biztonsági zónákat kijelölni, melyet minden esetben az önkormányzati hivatali szervezet határoz meg saját eljárásrendjében, az alábbi javaslatok figyelembevételével:

- Az épület földrajzi elhelyezkedését. Lehetőleg a bejutás ellenőrzött legyen.
- Az épület építészeti, épületgépészeti adottságait.
- Ügyfélforgalom mértékét.
- ASP felhasználóknak nyújtott szolgáltatásokat.
- Az információk osztályozása, minősítését.

Őrzés, védelem

A törekedni kell az élő erős őrzés megvalósítására. Ha megvan a lehetőség, akkor szabályzatban szükséges rögzíteni az őrszolgálat működési rendjét, az incidenskezelés folyamatát.

Az önkormányzati hivatalok ASP-t is futtató helységeibe a bejutás ellenőrzötnen kell, hogy megtörténjen, az ellenőrzésről lehetőség szerint beléptető rendszer gondoskodik.

Lehetőséghez képest legyen kialakítva az objektum védelme beléptető, behatolás védelmi, tűzjelző és video-megfigyelő rendszerrel. A biztonsági rendszerek adatai legyenek archiválva, akár több hónapra visszamenőleg megőrizve a hazai jogszabályokat figyelembe véve.

Földszinti ablakokon lehetőség szerint vasrács védjen az illetéktelen behatolástól. Az informatikai biztonsági felelős rendszeresen (pl. félévente) ellenőrzést hajtson végre, az eredményt jegyzőkönyvbe rögzítse. A jegyzőkönyvet az ASP Szolgáltatási szerződésben megjelölt fél kérésére, illetve a Hatóság felszólítására betekintésre adja át.

Amennyiben az önkormányzat „méretéből” adódóan nem rendelkezik a fentebb leírtakkal, az önkormányzati hivatalnak fejlesztési terv keretében, azonnali hatállyal törekednie kell, hogy meg tudjon valósulni a jogszabályban is megfogalmazott fizikai biztonság. A fizikai biztonság meglétét mind a Hatóság, mind a Magyar Államkincstár ellenőrizheti.

A fizikai biztonságnak meg kell felelnie a jogszabályi elvárásoknak.

Humán erőforrás az ASP-ben

Az ASP rendszereket használó önkormányzati hivatal szervezeti egység vezetőjének a felelőssége, hogy meghatározza az egyes, ASP szakrendszer munkakörökhöz tartozó felelősségeket és feladatokat.

Alkalmasság vizsgálat:

- Az önkormányzati hivatal humánpolitikai szervezet vezetőjének a felelőssége, hogy foglalkoztatás előtt a betöltendő ASP rendszerhez kapcsolódó munkakör kockázataival arányos mértékű megfelelési vizsgálatot végezzen el a foglalkoztatni kívánt munkatárs vonatkozásában.
- A kockázattal arányos mértékben mérlegelni kell a foglalkoztatni kívánt személy egyéni tulajdonságait is (pl. megbízhatóság, felelősségtudat, elkötelezettség, terhelhetőség, koncentrálóképeség stb.).
- Meg kell győződni arról, hogy a foglalkoztatni kívánt személy rendelkezik a munka elvégzéséhez szükséges végzettséggel, tapasztalatokkal.
- Az informatikai biztonsági szakterület vezetőjének felelőssége, hogy az informatika külsős felek által, a szerződött feladatok végrehajtására kijelölt személyek a munkavégzés kockázataival arányos mértékben átvilágításra kerüljenek.
- A humánpolitikai szakterület vezetőjének a felelőssége, hogy a foglalkoztatás alkalmával az önkormányzati hivatal munkaköri leírásban rögzítse a kockázatokkal arányosan a titoktartás követelményeit (ASP titoktartási nyilatkozat, mely korábban megküldésre került) és a foglalkoztatás egyéb kikötéseit.

- Az önkormányzati hivatal jogi szakterület vezetőjének felelőssége, hogy a szerződő felek a szerződésben rögzítsék a kockázatokkal arányosan a titoktartás követelményeit és az együttműködés egyéb kikötéseit.
- A humánerőforrás fentebb leírt pontjai nem lehetnek ellentmondásban az önkormányzati hivatal hatályos Informatikai Biztonsági Szabályzatával.

Oktatás, képzés az ASP-ben

Az önkormányzati munkatársaknak ASP oktatáson kell részt venni, amely alapján a rendszert az elvárásoknak megfelelően, önállóan is használni tudják. Az informatikai biztonsági képzés az Informatikai Biztonsági Felelős feladata, mely rögzítésre került a hatályos Informatikai Biztonsági Szabályzatban. Az oktatás folyamatát a képzési eljárásrendnek kell szabályoznia. A Hatóság és a Magyar Államkincstár jogosult a képzési dokumentációk megtekintésére.

ASP jogosultság kezelés

A szerződésben meghatározott tenant adminisztrátorok rendszerbe történő „felvitelét” az ASP Központ végzi el az önkormányzat által megküldött adatlap alapján.

- A privilegizált joggal rendelkező felhasználók a munkatársaik részére további jogosultságot osztanak. Ezt a tevékenységet az önkormányzati jegyző felelősségi és hatáskörébe tartozóan tudják elvégezni.
- Egy önkormányzati fióknál (tenantnál) minimum egy felhasználó karbantartónak szükséges „lenni”, ezt a rendszer figyelni (pl.: nem lehet zárolni, vagy elvenni tőle a jogot, ha csak egyedüli felhasználó karbantartó a tenantnál).
- A rendszer használata során elvárt, hogy a privilegizált joggal rendelkező munkatársak a privilegizált jog használatát munkavégzésükhöz csak indokolt esetben használják.
- A privilegizált joghoz tartozó bejelentkezési azonosítót zárt borítékban, biztonságosan zárható helyen kell tárolni.

A tenant adminisztrátor feladatai:

- új felhasználók (userek) rögzítése,
- meglévő felhasználók adatainak módosítása,
- felhasználók zárolása (szükség szerint),
- felhasználói jogosultságok (szerepkörök) kiosztása,
- felhasználói jogosultságok módosítása, megvonása,
- helyettesítések beállítása, eltávolítása,
- felhasználói csoportok létrehozása, módosítása, törlése (ugyanazon szerepkörök kiosztása több felhasználónak),
- üzleti napló megtekintése (a rendszerben történő változásokat lehet lekérdezni, követni).

ASP rendszerbe történő belépés, autentikáció

A Belügyminisztérium – az Igazságügyi Minisztérium és a Nemzeti Adatvédelmi és Információszabadság hatóság bevonásával – megvizsgálta azt a kérdést, hogy az elektronikus személyi igazolvány (eSZIG) felhasználása az ASP rendszerbe történő

azonosításra ütközik-e valamely jogszabályba, illetve szükséges-e az önkormányzat alkalmazásában álló közzolgálati tisztviselők jogszabályi kötelezése az eSZIG kiváltására. Ez nem ütközik jogszabályba.

Az ASP elsődleges autentikációs eszköze az eSZIG. A használatához javasolt kártyaolvasók hatóság által bevizsgált és elfogadott eszközök.

Az ASP eSZIG-gel történő azonosítás során személyes adatahoz az ASP rendszer nem fér hozzá. Belépéskor ugyanis az e-személyi érvényességét közvetlenül a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatalának (a továbbiakban: KEKKH) szervere ellenőrzi. A KEKKH szervere az ASP rendszernek egy ún. hash-kódot (RID) ad vissza, mely azonos okmány esetén mindig ugyanaz, de ez a kód nem fejthető vissza személyes adattá. Az ASP rendszer ehhez az anonim hash-kódhoz rendeli a felhasználót.

Az elektronikus személyigazolvánnyal történő autentikáció során a következő szabályzókra kell megkülönböztetett módon figyelni:

- Minden ASP rendszert használó munkatárnak rendelkeznie kell eSZIG-el.
- Az eSZIG használatához szükséges a kártyaolvasó számítógépre történő telepítése.
- Az ASP rendszerbe történő sikeres beléptetés érdekében a Keretrendszerbe rögzített felhasználói fiók és az eSZIG összerendelése szükséges.
- A személyi igazolvány kártyát csak a tulajdonosa használhatja, azt ASP rendszer autentikációs folyamat céljából másnak átadni tilos.
- Az hivatal vezetőjének a Jegyzőnek gondoskodnia kell arról, hogy a kérdéses kártya hiánya esetén az ASP rendszerbe történő ideiglenes bejelentkezés lehetősége biztosított legyen. Az ehhez tartozó szabályrendszer kialakítása elengedhetetlen.

Csatlakozó önkormányzatok kliens oldali biztonsága

Az ASP kapcsán kiemelten kell kezelni a csatlakozó önkormányzatokkal kapcsolatos biztonsági kockázatokat. A csatlakozó önkormányzatok a saját infrastruktúrájukat fogják használni az alkalmazások igénybevétele során, így a kliens rendszerek biztonsága nagymértékben befolyásolja a teljes ASP rendszer biztonságát.

Fontos az ASP rendszerbe olyan kikerülhetetlen biztonsági megoldásokat beépíteni, ami szűkíti a felhasználók biztonságra kockázatos tevékenységének lehetőségét.

Az csatlakozó önkormányzatok tekintetében a lehetséges fenyegetettségek, sebezhetőségek, valamint ezek megelőzésére alkalmazható intézkedések az alábbiak pl.:

Elem	Fenyegetések, veszélyek, sebezhetőségek	Védelem
ASP rendszer önkormányzati, végponti állomásai	Érzékeny adatok ellopása, adatfájlok törlése, ellopása, módosítása.	Hozzáférés védelem beállítása.
	Rosszindulatú program (vírus, trójai faló, stb.) bejuttatása a rendszerbe.	Vírusvédelmi rendszer alkalmazása.
	Vírus, trójai faló, féreg aktiválódása, pl. e-mail csatolmány megnyitásakor.	Vírusvédelmi rendszer alkalmazása.

Elem	Fenyegetések, veszélyek, sebezhetőségek	Védelem
	Végrehajtható programok, script-ek (Java Applet, JavaScript, VB Script, CGI, stb.) letöltése, pl. az állomás DoS támadásra való felhasználására a felhasználó tudtán kívül.	Böngésző biztonsági beállítása.
	Web és alkalmazásba csomagolt ActiveX objektumok, amelyek a programozó szándékától függően a legkülönbözőbb károkat (gépleállítás, konfiguráció feltérképezés, monitor/billentyűzet elvétel, stb.) okozhatják.	Böngésző biztonsági beállítása.
	Ismeretlen forrásból érkező e-mailek és azok csatolmányainak megnyitása.	Vírusvédelmi rendszer alkalmazása, felhasználó oktatása.
	Az Internet böngészőkben meglévő biztonsági „lyukak” megszüntetésére szolgáló javító programok letöltésének elmulasztása. A biztonsági „lyukak” kihasználásával elérhetők a végponti felhasználó érzékeny adatai (jelszó, az állomás konfigurációja, fájl nevek, fájl struktúra, a meglátogatott weblapok címei, stb.).	Legújabb verziók, frissítések telepítése.
	A munkaállomásra letöltött adatlapok (kérdőív, adatszolgáltató formanyomtatvány, stb.) programhibái. A szolgáltatott adatok rejtjelezés nélküli elküldése.	Csak megbízható forrásból származó program használata.
	Vírusvédelmi program frissítésének elmulasztása.	Rendszeres, automatikus frissítés.
	Az igénybevett szolgáltatás letagadása.	Naplózás.
	A munkaállomás ellopása.	Követelményrendszer szerinti fizikai biztonság kialakítása.
	Mobil eszköz ellopása	Az előírt fizikai védelmi eszközök alkalmazása. Követelményrendszer szerinti hozzáférés-védelem és rejtjelezés alkalmazása.
Internet	A felhasználó login adatainak (felhasználói-azonosító, jelszó) lehallgatása, ezek segítségével a felhasználó megismerésének.	Rejtjelezett adatátviteli csatorna használata.
	Érzékeny adatok lehallgatása.	Rejtjelezett adatátviteli csatorna használata.
	Adatok lehallgatás és továbbítása megváltoztatott tartalommal elleni védelme.	Hozzáférés-vezérlés kialakítása. Rejtjelezett adatátviteli csatorna. Egyszer használatos jelszó.

Elem	Fenyegetések, veszélyek, sebezhetőségek	Védelem
	E-mail-ek, elektronikus dokumentumok eltérítése.	Hozzáférés-vezérlés kialakítása.
Tűzfal	Tűzfal-biztonságpolitika hiánya vagy hiányos volta.	Tűzfal-biztonságpolitika elkészítése, vagy aktualizálása.
	Ad hoc vagy nem a biztonságpolitikának megfelelő biztonsági beállítás, vagy üzemeltetés.	Biztonsági beállítások rendszeres ellenőrzése, naplózás, riasztás.
	Portok letapogatása.	Tűzfal biztonsági beállítása.
	IP cím megszemélyesítés, a támadó a védett hálózaton működő számítógép (pl. szerver) IP címét megszerezve egy belső munkaállomást „szimulálva” a tűzfalon keresztül fér hozzá a szerveren levő adatállományokhoz.	Megfelelő hálózati biztonságpolitika, architektúra terv kialakítása.
	Visszaélés, forrás útvonalválasztással. A támadó a védett belső hálózat felépítésének ismeretében a saját gépében meghatározott útvonallal és belső IP címmel belső gépet „játszik el” és fér hozzá az útvonal végén levő belső géphez.	Megfelelő hálózati biztonságpolitika, architektúra terv kialakítása. Hálózati végpont IP címhez, MAC címhez kötése.
	Szerver típus specifikus biztonsági lyukak az operációs rendszerben. Az aktuális javító- és szerviz csomagok telepítésének elmulasztása.	Operációs rendszerek biztonsági frissítéseinek folyamatos figyelése, végrehajtása.
	A tűzfal távoli, pl. Interneten keresztül történő adminisztrálása.	Tűzfal adminisztrálása csak védett hálózatról, vagy konzolról.
	Vírusvédelmi programok frissítésének elmulasztása.	Vírusvédelmi rendszer folyamatos frissítése.
	Hiányos biztonsági naplózás. A biztonsági naplók értékelésének elmulasztása vagy rendszertelensége.	Minden jelentős biztonsági esemény naplózása, naplózott események folyamatos értékelése.
	Hiányos fizikai biztonság.	Követelményrendszer szerinti fizikai biztonság kialakítása.

Munkaállomásra vonatkozó biztonsági elvárások

Az ASP rendszerhez csatlakozó eszközök karbantartásáról, változáskövetéséről gondoskodni kell a következők figyelembevételével:

- A folyamatot változáskövetési eljárásrendbe szükséges megfogalmazni.
- A munkaállomásokon legyen telepítve vírusvédelmi program, a legfrissebb vírus definíciós adatállománnyal. A végpontvédelem tartalmazzon e-mail (csatolmány) védelmet is.
- A munkaállomáson legyen megoldott a böngésző megfelelő biztonsági beállítása.
- Javasolt a tervszerű beavatkozásokhoz karbantartási időablak kijelölése.

- A munkaállomások programfrissítése elvárt, különös tekintettel a legfrissebben kiadott security patch komponensekre.
- A telepítő programok, a licenz azonosítók zárható helyen legyenek tárolva.
A munkaállomások elhelyezésénél gondot kell fordítani:
- A készülékek olyan módon legyenek a hivatalban elhelyezve, hogy azokat az ügyfelek ne tudják elérni.
- A monitor kijelzési képét az ügyfelek ne tudják elolvasni.
- Ideiglenesen magára hagyott készülékek zárolása, képernyővédő aktiválása legyen megoldott.
- Munkaidő végén a munkaállomások kikapcsolása történjen meg.
Az ASP központhoz csatlakoztatott infrastruktúra elemekre értelmezve javasolt:
- a naplóinformációinak a védelme,
- hiba esetén a naplóbejegyzések elemzése,
- a rendszer hozzáférés ellenőrzése.

Rosszindulatú kódok elleni védelem

Az ASP rendszerhez történő csatlakozás során elvárás, hogy az önkormányzatok a csatlakozó eszközök vírusvédelmét saját hatáskörben valósítsák meg.

A vírusvédelmi eljárások követelményei

- Meg kell határozni a vírusfertőzés megelőzésére vonatkozó szabályokat.
- Például: Működő vírusvédelmi rendszer nélkül munkaállomást, laptopot, számítógépes hálózatot nem szabad üzemeltetni. Továbbá a vírusvédelmi program vírus definíciós állományit a legfrissebb állapotba kell tartani.
- A teendőket rögzíteni kell vírusfertőzés esetén.
- Vírustámadás esetén szükség szerint a vírusriadó elrendelése.
- Sérülés, vírusfertőzés után az elvárt helyreállítási eljárások meghatározása.

Hálózatbiztonság

Hálózat védelme

Az informatikai biztonságra és hálózati elérésre vonatkozó minimális és ajánlott feltételek megfogalmazása során az internet eléréshez és a hálózat kiépítéséhez, bővítéséhez szükséges eszközök meghatározásra kerültek, pl. router, switch, tűzfal.

A rendszer üzemeltetésével kapcsolatos elvárások:

- A menedzselhető hálózati aktív eszköz tekintetében az eszköz gyári, alapértelmezett bejelentkezési azonosítói (név, password) kerüljenek megváltoztatásra. Legyen megoldott az azonosítók zárt borítékban, és biztonságosan zárható helyen történő tárolása. Csak előre kijelölt, privilegizált felhasználóknak legyen lehetősége bejelentkezni a kérdéses eszközökbe.
- A hálózati végpontok védelme legyen megoldva. A lehetőségek figyelembevétele mellett pl. port security, esetleg 802.1x szabványnak megfelelően.
- Az eszközök hálózatba történő illesztéséről készüljön dokumentáció.
- Az eszközök firmware frissítése a legutolsó stabil változatnak megfelelően történjen meg.

- A menedzselhető eszközök legfrissebb konfigurációja legyen elmentve és zárható helyen tárolva.

Informatikai határvédelem, tűzfal

- A szervezet internethez való csatlakoztatása a központi tűzfalon keresztül történjen meg.
- A tűzfal szabályok dokumentálása és azok zárható helyen történő tárolása legyen biztosítva.

A tűzfal szabályok módosítása a kijelölt felelős előzetes, írásbeli engedélye alapján történhessen meg.

1. Mobil eszközök használata

Az informatikai biztonság megfelelő megteremtés és szinten tartása miatt külön gondoskodni kell a mobil eszközök használatainak a szabályozásáról. Ehhez javasolt szempontok a következők:

- A mobil eszközök használatát minden esetben előzetes jegyzői engedélyezésnek kell megelőznie.
- A mobil eszközök (pl. notebook) használatára a munkaadásokra vonatkozó szabályok is legyenek érvényesek.
- Ki kell dolgozni a mobil informatikai eszközök igénylésének, kiadásának, visszavételének, nyilvántartásának üzemeltetésének a folyamatait.
- Továbbá azokat a szabályokat, amelyek az eszközök hivatalon kívüli kivételére, az eszközök javítására, esetleges elvesztésére, vagy a selejtezésére vonatkoznak.

Osztályba sorolás eredménye, besorolási nyilatkozat

Tüskevári Közös Önkormányzati Hivatal nyilatkozatban rögzíti, hogy a 2017.08 hó időszakban külsős szakember által egy kockázatértékelés során végzett L_2013 tv. – nek való megfelelés vizsgálatának eredményeként a Hivatal biztonsági szintje:

Önkormányzati Információs Rendszer 2-es (azaz kettős) besorolású

Indoklás:

- A **szervezet által működtetett** és kockázatértékelés során vizsgált elektronikus információs rendszer (**Önkormányzati Információs Rendszer**) nem magasabb a 2-es biztonsági osztálynál. Az **ASP specifikus rendszerek nem a szervezet által működtetett rendszerek.**
- Hivatalunkban az elektronikus információs rendszerek biztonságához kapcsolódó eljárások teljes kialakítására törekszünk, de ehhez belső forrásból sem megfelelő szaktudás, sem megfelelő eszközrendszer nem áll még rendelkezésünkre.
- Hivatalunkban az információs rendszerek biztonságával kapcsolatos felelősségeket és feladatokat egy, az elektronikus információs rendszer biztonságáért felelős, irányítási jogkörében korlátozott személyhez rendeltük hozzá.
- Hivatalunkban az elektronikus információs rendszerek és szolgáltatások nyilvántartása nem teljes körű.
- Hivatalunkban az adathordozók nyilvántartása, kezelése, törlése nem teljes körű.

- Hivatalunkban az elektronikus információs rendszerek biztonsági felügyelete nem automatizált.
- Hivatalunkban az elektronikus információs rendszerek előállítanak a biztonságra vonatkozó információkat, de azokat a szervezet nem elemzi.
- A hiányosságok pótlására Hivatalunk intézkedési tervet fog készíteni, melyhez határidőket és felelős személyeket fog hozzárendelni.

Az elektronikus információs rendszerek osztályba sorolásának az eredményét az Informatikai Biztonsági Szabályzatban rögzíteni kell. Jelen esetben ennek az értéke a következő:

Szakrendszer	Biztonsági osztály
Adó rendszer ASP	4
Keretrendszer ASP	4
Gazdálkodási rendszer ASP	3
Önkormányzati Információs Rendszer	2

Az informatikai biztonsági szabályzat elsősorban a következő, az érvényes rendeletben meghatározott elektronikus információs rendszerbiztonsággal kapcsolatos területeket szabályozza:

Adminisztratív Védelmi Intézkedések

Szervezeti szintű alapfeladatok

Informatikai biztonsági szabályzat

A Hivatal megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az informatikai biztonsági szabályzatát. Az informatikai biztonsági szabályzat a Hivatal, vezető testülete hagyja jóvá.

Az informatikai biztonsági szabályzatát szükség szerint, de legalább évente egyszer az informatika biztonsági rendszer felülvizsgálata során (belső audit) a Hivatal felülvizsgálja, szükség szerint módosítja. Az informatikabiztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor az informatikai biztonsági szabályzatot újra vizsgálja, szükség szerinti módosítja. A Hivatal az „informatikai biztonsági jelentésben” rögzíti az érintett hivatal elvárt biztonsági szintjét, valamint az érintett hivatal egyes elektronikus információs rendszereinek elvárt biztonsági osztályát.

A Hivatal a részletes informatikai biztonsági szabályzat egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban (*Informatikai Biztonsági Szabályzat*) kezeli.

Az elektronikus információs rendszerek biztonságáért felelős személy

A Hivatal vezetője az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg (külsős alvállalkozó), aki: ellátja az állami és hivatali szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott feladatokat. A Hivatal vezetője gondoskodik (alvállalkozó esetén szerződésben elvárja) a biztonságért felelős személy képzettségéről az idevonatkozó rendeletnek megfelelően.

Intézkedési terv és mérföldkövei

A Hivatal vezetése intézkedési tervet készít az elektronikus információbiztonsági stratégia megvalósításához az ide vonatkozó törvényben meghatározott határidőkkel, és ebben mérföldköveket határoz meg. Az így elkészített intézkedési tervet meghatározott időnként felülvizsgálja és karbantartja a kockázatkezelési stratégia és a kockázatokra adott válaszok, tevékenységek prioritása alapján. Ha az adott elektronikus információs rendszerre vonatkozó biztonsági osztály meghatározásánál (belső vagy külső vizsgálat során) hiányosságot állapítanak meg, vagy a meghatározott biztonsági szint alacsonyabb, mint az érintett hivatalra érvényes szint, akkor a Hivatal vezetése a vizsgálatot követő 90 napon belül felülvizsgálatot készít a hiányosság megszüntetése érdekében.

A Hivatal a részletes intézkedési tervet egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban (*Informatikai Biztonsági Stratégia*) kezeli.

Az elektronikus információs rendszerek nyilvántartása

A Hivatal az elektronikus információs rendszereiről, minden rendszerre nézve nyilvántartást vezet, azt szükség szerint aktualizálja. A nyilvántartás tartalmazza:

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

A Hivatal az elektronikus rendszerek nyilvántartását egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban kezeli.

Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás

A Hivatal vezetése megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információbiztonsággal kapcsolatos (ideértve a rendszer- és felhasználói, külső és belső hozzáférési) engedélyezési eljárási folyamatokat. Felügyeli az elektronikus információs rendszer és környezet biztonsági állapotát, meghatározza az információbiztonsággal összefüggő szerepköröket és felelősségeket, kijelöli az ezeket betöltő személyeket, integrálja az elektronikus információbiztonsági engedélyezési folyamatokat a Hivatali szintű kockázatkezelési eljárásba, összhangban az informatikai biztonsági szabállyal.

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

- a) emberi, fizikai és logikai erőforrásra,
- b) eljárási és védelmi szintre és folyamatra

Kockázatelemzés

Kockázatelemzési és kockázatkezelési eljárásrend

A Hivatal vezetése megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a kockázatelemzési eljárásrendet, mely a kockázatelemzési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő.

Biztonsági osztályba sorolás

A Hivatal jogszabályban meghatározott szempontok alapján megvizsgálja (alvállalkozó igénybevétele esetén megvizsgáltatja) elektronikus információs rendszereit, és a 3.1.1.7 pont szerinti nyilvántartás alapján meghatározza, hogy azok melyik biztonsági osztályba sorolandók.

A Hivatal vezetése jóváhagyja a biztonsági osztályba sorolást, és dokumentumban (*Informatikai Biztonsági Szabályzat*) rögzíti annak eredményét.

A biztonsági osztályba sorolást az elektronikus információs rendszereket érintő változások után ismételten elvégzi.

Kockázatelemzés

A Hivatal végrehajtja a biztonsági kockázatelemzéseket és rögzíti azok eredményét (*a NEIH módszertani segédletben*). A kockázatkezelési szabályzatnak megfelelően felülvizsgálja a kockázatelemzések eredményét és megismerteti a kockázatelemzés eredményét az érintettekkel.

Amikor változás áll be az elektronikus információs rendszerben vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését), továbbá olyan körülmények esetén, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát, ismételt kockázatelemzést hajt végre a Hivatal.

A Hivatal gondoskodik arról, hogy a kockázatelemzési eredmények a jogosulatlanok számára ne legyenek hozzáférhetőek, megismerhetőek. A kockázatelemzési eredményeket bizalmasan kezeli.

Rendszer és szolgáltatás beszerzés

Külső elektronikus információs rendszerek szolgáltatásai

A Hivatal:

- a) szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján általa igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek az érintett Hivatal elektronikus információbiztonsági követelményeinek;

- b) meghatározza és dokumentáltatja az érintett Hivatal felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban;
- c) külső és belső ellenőrzési eszközökkel ellenőrizteti, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

Üzletmenet- (ügymenet-) folytonosság tervezése

Üzletmenet-folytonosságra vonatkozó eljárásrend

Az információk védelmének és a megfelelő rendelkezésre állásának biztosítása érdekében a Hivatal az alábbi elvárásokat fogalmazza meg az üzletmenet-folytonossági tervekkel szemben:

- a) biztosítsák, hogy a kockázatok esetleges bekövetkezésekor a szolgáltatás kiesés ne legyen nagyobb a tervezetnél (ne sérüljön az SLA);
- b) adjanak megfelelő alapot a kockázatok csökkentésére irányuló hatékony intézkedések végrehajtásához és eredményességük nyomon követéséhez;
- c) határozzák meg azokat az intézkedéseket, amelyek ahhoz szükségesek, hogy a Hivatal folyamatos működése biztosítva legyen;
- d) határozzák meg azokat az intézkedéseket, feladatokat, melyeket az esetleges folytonosság megszakadásra felkészülésként, illetve bekövetkezésekor a kár enyhítéseként, illetve a helyreállítáért kell tenni;
- e) biztosítsák, hogy az üzletmenet-folytonosság és a szolgáltatások rendelkezésre állása személyes felelősséghez köthető legyen;
- f) illeszkedjenek a Hivatal közép és hosszú távú stratégiáihoz és céljaihoz;

Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

A Hivatal vezetése által az elektronikus információs rendszerekhez készített rendszerbiztonsági terveknek tartalmazniuk kell az adott elektronikus rendszer (szolgáltatás) üzletmenet-folytonossági tervét is, amely:

- a) összhangban áll az Informatikai Biztonságpolitikával és a Biztonságtervezési Eljárásrenddel, valamint igazodik a szervezet felépítéséhez és architektúrájához;
- b) összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével;
- c) meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszerhez kapcsolódó üzletmenet-folytonossági tervet;
- d) az elektronikus információs rendszer vagy a működtetési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálja az üzletmenet-folytonossági tervet;
- e) tájékoztatja az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, személyeket és Hivatali egységeket;
- f) gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető, módosítható;
- g) meghatározza az alapfeladatokat (a biztosítandó szolgáltatásokat és azok elvárt szolgáltatási szintjét [angolul SLA]) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;
- h) rendelkezik a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről;

- i) jelöli a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket;
- j) fenntartja a Hivatal által előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is;
- k) kidolgozza a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

A Hivatal az elektronikus információbiztonsággal kapcsolatos üzletmenet-folytonossági terveket rendszerenként külön dokumentumban (*Rendszerbiztonsági terv*) és mellékleteiben kezeli.

Az elektronikus információs rendszer mentései

A Hivatal a rendszerbiztonsági és üzletmenet-folytonossági elvárásokkal összhangban:

- a) meghatározott gyakorisággal mentést végez az elektronikus információs rendszerben tárolt felhasználószintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;
- b) meghatározott gyakorisággal elmenti az elektronikus információs rendszerben tárolt rendszerszintű információkat, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;
- c) meghatározott gyakorisággal elmenti az elektronikus információs rendszer dokumentációját, köztük a biztonságra vonatkozókat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;
- d) megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen.

A Hivatal az információs rendszerek mentésével kapcsolatos elvárásait (mentések gyakorisága a tolerálható adatvesztés függvényében, elvárt helyreállítási idő, megőrzési idő, offsite példányok, stb.) rendszerenként külön dokumentumban (*Mentési Napló*) és mellékleteiben kezeli.

Az elektronikus információs rendszer helyreállítása és újraindítása

A Hivatal gondoskodik az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.

A Hivatal az elektronikus információbiztonsággal kapcsolatos helyreállítási szabályokat, valamint az elektronikus információs rendszer helyreállításának, újraindításának menetét az érintett rendszerre vonatkozó dokumentumban és mellékleteiben kezeli.

Emberi tényezőket figyelembe vevő – személy – biztonság

Eljárás jogviszony megszűnésekor

A Hivatal:

- a) megszünteti, vagy visszaveszi a személy egyéni hitelesítő eszközeit;
- b) tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető a jogviszony megszűnése után is fennálló kötelezettségekről;

- c) visszaveszi az érintett hivatal elektronikus információs rendszerével kapcsolatos, tulajdonát képező összes eszközt;
- d) megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és a Hivatali információkhoz;
- e) az általa meghatározott módon a jogviszony megszűnéséről értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket;
- f) a jogviszonyt megszüntető személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik;
- g) a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását megelőzi.

Fegyelmi intézkedések

A Hivatal fenntartja magának a jogot, hogy a jelen IBSZ-t megsértőkkel szemben eljárjon. Az eljárást a Hivatal jegyzője vagy az IT referens kezdeményezheti. A kezdeményezést a Hivatal vezetője felülvizsgálja, a szükséges intézkedéseket elrendelheti. Az IBSZ megsértése esetén az intézmény megvonhatja a hálózat, illetve a gépek használatának jogát határozott időre, vagy határozatlan időre, visszavonásig.

Ha az IBSZ megsértése kismértékű, vagy nem tekinthető szándékosnak, akkor az elkövetőt írásban figyelmeztetni kell. A figyelmeztetés utáni ismételt elkövetést szándékosnak kell tekinteni. Különösen súlyos esetben, illetve szándékosság esetén a rendszergazdák a használati jogot megvonhatják és az IBSZ megsértője a teljes információs rendszerből kitiltható. Ha szükséges, az intézmény fegyelmi eljárást, polgári jogi pert is indíthat. Amennyiben az elkövetett vétség a Büntető Törvénykönyv szerint bűncselekménynek minősül, a Hivatal vezetője köteles a szabályszegővel szemben feljelentést tenni, és a rendelkezésre álló bizonyítékokat az eljáró hatóságok részére átadni.

Viselkedési szabályok az interneten

A Hivatal:

- a) tiltja és számon kéri a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzétételét;
- b) tiltja a belső szabályzatában meghatározott, interneten megvalósuló tevékenységeket (pl.: chat, fájlcsere, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták, stb.);
- c) tilthatja a közösségi oldalak használatát, magánpostafiók elérését, és más, a Hivataltól idegen tevékenységet.

A Hivatal az elektronikus információbiztonsággal kapcsolatos engedélyezési és hozzáférési szabályokat egy külön dokumentumban (*Engedélyezési és jogosultsági szabályzat*) kezeli.

Tudatosság és képzés

Képzési eljárásrend

A Hivatal rendszeres képzésben részesíti az információs rendszer felhasználóit. A képzések gyakoriságát az információs rendszerek változásainak és egyéb igényeknek

a figyelembevételével kell meghatározni, de évente legalább egyszer továbbképzésen kell részt vennie minden munkavállalónak. A szervezetbe újonnan belépő munkavállalókat a lehető leghamarabb alapképzésben kell részesíteni.

A Hivatal vezetése:

- a) felelős a képzési kritériumok meghatározásáért
- b) biztosítja a képzéshez a szükséges erőforrásokat
- c) gondoskodik a képzések fontosságának tudatosításáról a teljes szervezetben

Az IT referens:

- a) felelős a képzési rendszer kialakításáért, fenntartásáért
- b) felelős a szükséges oktatások megtartásáért, megtartatásáért

A munkatársak:

- a) felelősek a képzési előírások betartásáért, a képzések során leadott anyagok elsajátításáért

Biztonságtudatossági képzés

A Hivatal annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára:

- a) az új felhasználók kezdeti képzésének részeként;
- b) amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;
- c) a Hivatal vezetése által meghatározott gyakorisággal, de minimum évente egyszer

Fizikai Védelmi Intézkedések

Fizikai és környezeti védelem

Fizikai védelmi eljárásrend

A Hivatal azon helyiségeibe, ahol információs rendszerek (pl. szerverek) vagy rendszerelemek (pl. számítógépek) találhatóak, vagy ahonnan bármilyen jellegű hozzáférés lehetséges a rendszerekhez vagy rendszerelemekhez, csak az arra jogosultak léphetnek be, meghatározott szabályok szerint.

A szabályok és korlátozások nem vonatkoznak a létesítmény bárki által szabadon látogatható vagy igénybe vehető helyiségeire.

Fizikai belépési engedélyek

A Hivatal:

- a) összeállítja, jóváhagyja és kezeli az elektronikus információs rendszereknek helyt adó létesítményekbe belépésre jogosultak listáját;
- b) a belépési jogosultságot igazoló dokumentumokat (pl. kitűzők, azonosító kártyák, intelligens kártyák) bocsát ki a belépéshez a belépni szándékozó részére;
- c) rendszeresen felülvizsgálja a belépésre jogosult személyek listáját;

- d) eltávolítja a belépésre jogosult személyek listájáról azokat, akiknek a belépése nem indokolt;
- e) intézkedik a b) pont szerinti dokumentumok visszavonása, érvénytelenítése, törlése, megsemmisítése iránt.

A fizikai belépés ellenőrzése

A Hivatal:

- a) kizárólag a szervezet által meghatározott be-, és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést;
- b) naplózza a fizikai belépéseket;
- c) ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket;
- d) kíséri a létesítménybe ad-hoc belépésre jogosultakat és figyelemmel követi a tevékenységüket;
- e) megóvjaa a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző eszközt;
- f) nyilvántartást vezet a fizikai belépést ellenőrző eszközről;
- g) meghatározott rendszerességgel változtatja meg a hozzáférési kódokat és kulcsokat, vagy azonnal, ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az adott személy elveszti a belépési jogosultságát;
- h) az egyéni belépési engedélyeket a belépési pontokon ellenőrzi;
- i) a kijelölt pontokon való átjutást felügyeli a szervezet által meghatározott fizikai belépést ellenőrző rendszerrel, vagy eszközzel;
- j) felhívja a szervezet tagjainak figyelmét a rendellenességek jelentésére.

Logikai Védelmi Intézkedések

Általános védelmi intézkedések

Engedélyezés

Az érintett szervezet megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információbiztonsággal kapcsolatos (ideértve a rendszer- és felhasználói, külső és belső hozzáférési) engedélyezési eljárási folyamatokat; felügyeli az elektronikus információs rendszer és környezet biztonsági állapotát; meghatározza az információbiztonsággal összefüggő szerepköröket és felelősségi köröket, kijelöli az ezeket betöltő személyeket; integrálja az elektronikus információbiztonsági engedélyezési folyamatokat a szervezeti szintű kockázatkezelési eljárásba, összhangban az informatikai biztonsági szabályzattal.

Személybiztonság

Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed az érintett szervezet teljes személyi állományára, valamint minden olyan természetes személyre, aki az érintett szervezet elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem az érintett szervezet tagja, a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell, mint kötelezettséget érvényesíteni

(ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).

Tervezés

Rendszerbiztonsági terv

A Hivatal vezetése az elektronikus információs rendszereihez rendszerbiztonsági tervet készített, amely:

- a) összhangban áll az Informatikai Biztonságpolitikával és a Biztonságtervezési Eljárásrenddel, valamint igazodik a szervezet felépítéséhez és architektúrájához,
- b) meghatározza az elektronikus információs rendszer hatókörét, alapfeladatait (biztosítandó szolgáltatásait és azok elvárt szolgáltatási szintjeit [angolul SLA]), biztonságkritikus elemeit és alapfunkcióit;
- c) meghatározza az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát;
- d) meghatározza az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait;
- e) a vonatkozó rendszerdokumentáció keretében foglalja az elektronikus információs rendszer biztonsági követelményeit (naplózás, mentés és helyreállítás, üzletmenet-folytonosság);
- f) meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és azok bővítését, végrehajtja a jogszabály szerinti biztonsági feladatokat;
- g) gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és szerepkörökben dolgozók megismerjék (ideértve annak változásait is);
- h) belső szabályozásában, vagy a rendszerbiztonsági tervben meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszer rendszerbiztonsági tervét (belső audit);
- i) frissíti a rendszerbiztonsági tervet az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások, és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén;
- j) elvégzi a szükséges belső egyeztetéseket;
- k) gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

Kivételek

Ha egy adott információs rendszer jelentősége nem indokolja, vagy a különböző jogi, szabályozási, vagy üzemeltetési körülmények nem teszik lehetővé, a Hivatal vezetése eltekint a rendszerbiztonsági terv megkövetelésétől.

Cselekvési terv

Az érintett szervezet cselekvési tervet készít, ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg;

- a) a cselekvési tervben dokumentálja a megállapított hiányosságok javítására, valamint az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányuló tervezett tevékenységeit;

- b) frissíti a meglévő cselekvési tervet az érintett szervezet által meghatározott gyakorisággal a biztonsági értékelések, biztonsági hatáselemzések és a folyamatos felügyelet eredményei alapján.

Személyi biztonság

A Hivatal:

- a) megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat a rájuk vonatkozó szabályokat, felelősségüket az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet;
- b) Az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja;
- c) meghatározott gyakorisággal felülvizsgálja és frissíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat a rájuk vonatkozó szabályokat, felelősségüket az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet a viselkedési szabályok betartását;
- d) gondoskodik arról, hogy a c) pont szerinti változás esetén a hozzáféréssel rendelkezők tekintetében a b) pont szerinti eljárás megtörténjen;
- e) meghatározza az érintett szervezeten kívüli irányban megvalósuló követelményeket;

A Hivatal az elektronikus információbiztonsággal kapcsolatos engedélyezési és hozzáférési szabályokat egy külön dokumentumban (*Engedélyezési és jogosultsági szabályzat*) kezeli.

Rendszer és szolgáltatás beszerzés

A rendszer fejlesztési életciklusa

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

A Hivatal a fejlesztési életciklus egészére meghatározza és dokumentáltatja az információbiztonsági szerepköröket és felelősségeket.

A Hivatal meghatározza és a Hivatalra érvényes szabályok szerint kijelöli az információbiztonsági szerepköröket betöltő, felelős személyeket.

A rendszer életciklus szakaszai a következők:

- a) követelmény meghatározás;
- b) fejlesztés vagy beszerzés;
- c) megvalósítás vagy értékelés;
- d) üzemeltetés és fenntartás;
- e) kivonás (archiválás, megsemmisítés).

Konfigurációkezelés

Konfigurációkezelési eljárásrend

A konfigurációkezelés célja az informatikai infrastruktúra adatainak kézben tartása, az egyes komponensek beazonosítása, figyelemmel követése és karbantartása. A szolgáltatásokról, a szoftver és hardver konfigurációkról és azok dokumentációjáról központilag tárol információkat így segíti az incidensfelügyeletet, problémakezelést, változáskezelést és a verziókövetést.

Alapkonfiguráció

Azon információs rendszereknél, ahol indokolt és technikailag lehetséges, a Hivatal egy-egy alapkonfigurációt fejleszt ki, dokumentáltatja és karbantartatja azt, valamint leltárba foglalja a rendszer lényeges elemeit.

Elektronikus információs rendszerelem leltár

A Hivatal leltárt készít az elektronikus információs rendszer elemeiről, amit naprakészen tart annak érdekében, hogy:

- a) pontosan tükrözze az elektronikus információs rendszer aktuális állapotát,
- b) az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet, valamint azok licenceit tartalmazza;
- c) legyen kellően részletes a nyomkövetéshez és a jelentéskészítéshez.

A szoftverhasználat korlátozásai

A Hivatal:

- a) kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak és a szerzői jogi, vagy más jogszabályoknak;
- b) a másolatok, megosztások ellenőrzésére nyomon követi a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát;
- c) ellenőrzi és dokumentálja az állomány megosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.

A Hivatal az elektronikus információbiztonsággal, rendszer- és szoftverhasználattal kapcsolatos szabályait egy külön dokumentumban (*Engedélyezési és jogosultsági szabályzat*) kezeli.

A felhasználó által telepített szoftverek

A Hivatal információs rendszereire, valamint azok számítógépeire és egyéb komponenseire csak a rendszergazdák telepíthetnek szoftvereket, valamint azok rendszerszintű beállításait is csak ők (vagy az általuk megbízott külsős szakértők) jogosultak megváltoztatni.

Karbantartás

Rendszer karbantartási eljárásrend

A Hivatal vezetése megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a rendszer karbantartási eljárásrendet, mely a rendszer karbantartási kezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

A Hivatal az elektronikus információbiztonsággal kapcsolatos karbantartási szabályokat egy külön dokumentumban (*Beszerezési és Karbantartási Szabályzat*) kezeli.

Rendszeres karbantartás

A Hivatal által megbízott személyek vagy vállalkozók:

- a) a karbantartásokat és javításokat ütemezetten hajtja végre, dokumentáltatja és felülvizsgáltatja a karbantartásokról és javításokról készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és a Hivatal követelményeinek megfelelően;
- b) jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban;
- c) az ezért felelős személyek jóváhagyásához köti az elektronikus információs rendszer vagy a rendszerelemek kiszállítását a Hivatali létesítményből;
- d) az elszállítás előtt minden adatot és információt – mentést követően – töröl a berendezésről;
- e) ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat;
- f) csatolja a meghatározott, karbantartással kapcsolatos információkat a karbantartási nyilvántartáshoz.

A Hivatal az elektronikus információbiztonsággal kapcsolatos karbantartási szabályokat egy külön dokumentumban (*Beszerezési és Karbantartási Szabályzat*) kezeli.

Adathordozók védelme

Adathordozók védelmére vonatkozó eljárásrend

Az adathordozónak minősülő olyan eszközök (pl. floppy, CD, USB eszközök, külső merevlemezek, stb.) kezelésének általános irányelvei:

- a) minél nagyobb mértékben járuljon hozzá az adathordozók kezeléséből eredő kockázatok csökkentéséhez;
- b) tegye lehetővé valamennyi, a tevékenységet érintő adathordozók kezelésével kapcsolatos fenyegető esemény azonosítását;

Hozzáférés az adathordozókhoz

A Hivatal dokumentálja az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, valamint jogosítványuk tartalmát, időtartamát.

Adathordozók törlése

A Hivatal a helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal törli az elektronikus információs rendszer meghatározott adathordozóit a leselejtezés, a hivatali ellenőrzés megszűnte, vagy újrafelhasználásra való kibocsátás előtt. A törlési mechanizmusokat az információ minősítési kategóriájával arányos erősségnek és sértetlenségnek megfelelően alkalmazza.

Adathordozók használata

A Hivatal engedélyezi az adathordozók használatát, és dokumentálja az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, valamint jogosítványuk tartalmát, időtartamát.

Azonosítás és hitelesítés

Azonosítási és hitelesítési eljárásrend

A Hivatal vezetése megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az azonosítási és hitelesítésre vonatkozó eljárásrendet, mely az azonosítási és hitelesítési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

A Hivatal az elektronikus információbiztonsággal kapcsolatos engedélyezési és hozzáférési szabályokat egy külön dokumentumban *(Engedélyezési és jogosultsági szabályzat)* kezeli.

Azonosítás és hitelesítés (szervezeten belüli felhasználók)

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

Azonosító kezelés

A Hivatal:

- a) az egyéni-, csoport-, szerepkör- vagy eszközazonosítók kijelölését a Hivatal által meghatározott személyek vagy szerepkörök jogosultságához köti;
- b) hozzárendeli az azonosítót a kívánt egyénhez, csoporthoz, szerepkörhöz vagy eszközhöz;
- c) meghatározott időtartamig megakadályozza az azonosítók ismételt felhasználását;
- d) meghatározott időtartamú inaktivitás esetén letiltja az azonosítót.

A hitelesítésre szolgáló eszközök kezelése

A Hivatal vezetése által kijelölt személy:

- a) ellenőrzi a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát;
- b) meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;
- c) biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;
- d) dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket;

- e) megváltoztatja a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az elektronikus információs rendszer telepítése során;
- f) meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit;
- g) a hitelesítésre szolgáló eszköz típusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket;
- h) megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;
- i) megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét;
- j) lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.

A hitelesítésre szolgáló eszköz visszacsatolása

Az elektronikus információs rendszer fedett visszacsatolást biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.

Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

A szervezet jelenleg egyik rendszeréhez sem biztosít hozzáférést külső felhasználók számára.

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti az érintett hivatalon kívüli felhasználókat és tevékenységüket.

Hitelesítés szolgáltatók tanúsítványának elfogadása

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

Hozzáférés ellenőrzése

Hozzáférés ellenőrzési eljárásrend

A Hivatal vezetése megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a hozzáférés ellenőrzési eljárásrendet, mely a hozzáférés ellenőrzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

A Hivatal az elektronikus információbiztonsággal kapcsolatos engedélyezési és hozzáférési szabályokat egy külön dokumentumban (*Engedélyezési és jogosultsági szabályzat*) kezeli.

Felhasználói fiókok kezelése

A Hivatal:

- a) meghatározza és azonosítja az elektronikus információs rendszer felhasználói fiókjait és ezek típusait;
- b) kijelöli a felhasználói fiókok fiókkezelőit;
- c) kialakítja a csoport- és szerepkör tagsági feltételeket;

- d) meghatározza az elektronikus információs rendszer jogosult felhasználóit, a csoport- és szerepkör tagságot és a hozzáférési jogosultságokat, valamint (szükség esetén) az egyes felhasználói fiókok további jellemzőit;
- e) létrehozza, engedélyezi, módosítja, letiltja és eltávolítja a felhasználói fiókokat a meghatározott eljárásokkal vagy feltételekkel összhangban;
- f) ellenőrzi a felhasználói fiókok használatát;

...értesíti a fiókkezelőket, ha:

- a) a felhasználói fiókokra már nincsen szükség;
- b) a felhasználók kiléptek vagy áthelyezésre kerültek;
- c) az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak;

...feljogosít az elektronikus információs rendszerhez való hozzáférésre:

- a) az érvényes hozzáférési engedély,
- b) a tervezett rendszerhasználat,
- c) az alapfeladatok és funkcióik alapján;

A Hivatal meghatározott gyakorisággal felülvizsgálja a felhasználói fiókokat, a fiókkezelési követelményekkel való összhangot.

A megbízott személy kialakít egy folyamatot a megosztott vagy csoport felhasználói fiókokhoz tartozó hitelesítő eszközök, adatok újra kibocsátására (ha ilyen alkalmaznak), a csoport tagjainak változása esetére.

Hozzáférés ellenőrzés érvényesítése

Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

Nincsenek olyan felhasználói tevékenységek, melyeket az elektronikus információs rendszerben azonosítás vagy hitelesítés nélkül végre lehetne hajtani.

Külső elektronikus információs rendszerek használata

A Hivatal meghatározza, hogy:

- a) milyen feltételek és szabályok betartása mellett jogosult a felhasználó egy külső rendszerből hozzáférni az elektronikus információs rendszerhez;
- b) külső elektronikus információs rendszerek segítségével hogyan jogosult a felhasználó feldolgozni, tárolni vagy továbbítani a Hivatal által ellenőrzött információkat.

Nyilvánosan elérhető tartalom

A Hivatal:

- a) kijelöli azokat a személyeket, akik jogosultak a nyilvánosan hozzáférhető elektronikus információs rendszeren az érintett Hivataltól kapcsolatos bármely információ közzétételére;
- b) a kijelölt személyeket képzésben részesíti annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános információkat;

- c) közzététel előtt átvizsgálja a javasolt tartalmat;
- d) meghatározott gyakorisággal átvizsgálja a nyilvánosan hozzáférhető elektronikus információs rendszertartalmat a nem nyilvános információk tekintetében és eltávolítja azokat.

Rendszer- és információsértetlenség

Rendszer- és információsértetlenségére vonatkozó eljárásrend

A rendszer- és információsértetlenség megvalósítása során a Hivatal az informatikai biztonságpolitikában meghatározott célok és követelmények szerint jár el, valamint alkalmazza a biztonságtervezési eljárásrendben foglaltakat.

A fentiekén túlmenően – de azokkal összhangban – a Hivatal az alábbi követelményeket fogalmazza meg a rendszerek és információk sértetlenségének megőrzése érdekében:

Hibajavítás

A Hivatal:

- a) azonosítja, belső eljárásrendje alapján jelenti és kijavítja, vagy kijavíttatja az elektronikus információs rendszer hibáit;
- b) telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket a szervezet feladatellátásának hatékonysága, az előre nem látható következmények szempontjából;
- c) a biztonságkritikus szoftvereket frissítésük kiadását követő 1 hónapon belül telepíti, vagy telepítteti;
- d) beépíti a hibajavítást a konfigurációkezelési folyamatba.

Kártékony kódok elleni védelem

A Hivatal:

- a) az elektronikus információs rendszerét annak belépési és kilépési pontjain védi a kártékony kódok ellen, felderíti és megsemmisíti azokat.
- b) frissíti a kártékony kódok elleni védelmi mechanizmusokat a konfigurációkezelési szabályaival és eljárásaival összhangban minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg;

...konfigurálja a kártékony kódok elleni védelmi mechanizmusokat úgy, hogy a védelem eszköze:

- a) rendszeres ellenőrzéseket hajt végre az elektronikus információs rendszeren és végrehajtja a külső forrásokból származó fájlok valós idejű ellenőrzését a végpontokon a hálózati belépési, vagy kilépési pontokon a biztonsági szabályzatnak megfelelően, amikor a fájlokat letöltik, megnyitják, vagy elindítják;
- b) a kártékony kód észlelése esetén blokkolja vagy karanténba helyezi azt; és riassza a rendszeradminisztrátort és az érintett Hivatal által meghatározott további személy(ek)e)t;
- c) ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az elektronikus információs rendszer rendelkezésre állására.

Az elektronikus információs rendszer felügyelete

A Hivatal:

- a) felügyeli az elektronikus információs rendszert, hogy észlelje a kibertámadásokat, vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat;
- b) azonosítja az elektronikus információs rendszer jogosulatlan használatát;
- c) felügyeleti eszközöket alkalmaz a meghatározott alapvető információk gyűjtésére és a rendszer ad hoc területeire a potenciálisan fontos, speciális típusú tranzakcióknak a nyomon követésére;
- d) védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;
- e) erősíti az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelet észlel;
- f) meghatározott gyakorisággal biztosítja az elektronikus információs rendszer felügyeleti információkat a meghatározott személyeknek vagy szerepköröknek.

A kimeneti információ kezelése és megőrzése

A Hivatal az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

Naplózás és elszámoltathatóság

Naplózási eljárásrend

A Hivatal az elektronikus információbiztonsággal kapcsolatos naplózási szabályokat rendszerenként külön dokumentumban (*Rendszerbiztonsági terv*) és mellékleteiben határozza meg, az alábbi általános követelmények figyelembevételével:

Naplózható események

A Hivatal az érintett elektronikus információs rendszerre vonatkozó rendszerbiztonsági tervben:

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

Naplóbejegyzések tartalma

Az elektronikus információs rendszer a naplóbejegyzésekből gyűjt elegendő információt ahhoz, hogy ki lehessen mutatni, milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

Időbélyegek

Az elektronikus információs rendszer belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához. Időbélyegeket rögzít a

naplóbejegyzésekben a koordinált világidőhöz – úgynevezett UTC – vagy a Greenwichi középidejűhöz – úgynevezett GMT – rendelhető módon, megfelelően a Hivatal által meghatározott időmérési pontosságnak.

Szinkronizálás

Az elektronikus információs rendszer meghatározott gyakorisággal összehasonlítja a belső rendszerórát egy hiteles külső időforrással, és ha az időeltérés nagyobb, mint a meghatározott időtartam, szinkronizálja a belső rendszerórát a hiteles külső időforrással.

A napló információk védelme

Az elektronikus információs rendszer megvédi a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

A naplóbejegyzések megőrzése

A Hivatal a naplóbejegyzéseket meghatározott – a jogszabályi és az érintett szervezet belüli információ megőrzési követelményeknek megfelelő – időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

Naplógenerálás

Az elektronikus információs rendszer:

- a) biztosítja a naplóbejegyzés generálási lehetőségét a 3.3.8.2 pontban meghatározott, naplózható eseményekre;
- b) lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az elektronikus információs rendszer egyes elemeire;
- c) naplóbejegyzéseket állít elő a 3.3.8.2 pont szerinti eseményekre, a 3.3.8.3 pontban meghatározott tartalommal.

Rendszer- és kommunikációvédelem

Rendszer- és kommunikációvédelmi eljárásrend

A rendszer- és kommunikációvédelem megvalósítása során a Hivatal az informatikai biztonságpolitikában meghatározott célok és követelmények szerint jár el, valamint alkalmazza a biztonságtervezési eljárásrendben foglaltakat.

A fentieken túlmenően – de azokkal összhangban – a Hivatal az alábbi követelményeket fogalmazza meg a rendszer- és kommunikációvédelem érdekében:

A határok védelme

Az elektronikus információs rendszer:

- a) felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt;
- b) a nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a Hivatal belső hálózatától;
- c) csak a Hivatal biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeket keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.

Alapfogalmak

1. *adat*: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;
2. *adatifeldolgozás*: az adatkezeléshez kapcsolódó technikai feladatok elvégzése;
3. *adatifeldolgozó*: az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az adatkezelő részére adatfeldolgozást végez;
4. *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, valamint az adatok további felhasználásának megakadályozása;
5. *adatkezelő*: az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az adatkezelést végzi;
6. *adminisztratív védelem*: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás;
7. *auditálás*: előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;
8. *bizalmasság*: az elektronikus információs 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;
9. *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 bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;
10. *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;
11. *biztonsági osztály*: az elektronikus információs rendszer védelmének elvárt erőssége;
12. *biztonsági osztályba sorolás*: a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;
13. *biztonsági szint*: a Hivatal felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;
14. *biztonsági szintbe sorolás*: a Hivatal felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

15. *elektronikus információs rendszer biztonsága*: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;
16. *életciklus*: az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;
17. *észlelés*: a biztonsági esemény bekövetkezésének felismerése;
18. *felhasználó*: egy adott elektronikus információs rendszert igénybe vevők köre;
19. *fenyegetés*: olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;
20. *fizikai védelem*: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek 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, klimatizálás és a tűzvédelem;
21. *folytonos védelem*: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;
22. *globális kibertér*: a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese;
23. *informatikai biztonságpolitika*: a biztonsági célok, alapelvek és a Hivatal vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására;
24. *informatikai biztonsági stratégia*: az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere;
25. *információ*: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti;
26. *kiberbiztonság*: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez;
27. *kibervédelem*: a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését;
28. *kockázat*: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;

29. *kockázatelemzés*: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;
30. *kockázatkezelés*: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;
31. *kockázatokkal arányos védelem*: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;
32. *korai figyelmeztetés*: valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;
33. *létfontosságú információs rendszerelem*: az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené;
34. *logikai védelem*: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;
35. *magyar kibertér*: a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve Magyarország érintett benne;
36. *megelőzés*: a fenyegetés hatása bekövetkezésének elkerülése;
37. *reagálás*: a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;
38. *rendelkezésre állás*: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;
39. *sértetlenség*: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;
40. *sérülékenység*: az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;
41. *sérülékenység vizsgálat*: az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;
42. *számítógépes incidenskezelő központ*: az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint

kritikus információs infrastruktúrák védelmére szakosodott hivatalokban tagsággal és akkreditációval rendelkezik [(európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)];

43. *Hivatal*: az adatkezelést vagy adatfeldolgozást végző jogi személy, valamint jogi személyiséggel nem rendelkező gazdasági társaság, egyéni vállalkozó;

44. *teljes körű védelem*: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;

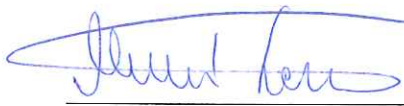
45. *üzemeltető*: az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős;

46. *védelmi feladatok*: megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés;

47. *zárt célú elektronikus információs rendszer*: jogszabályban meghatározott elkülönült nemzetbiztonsági, honvédelmi, rendészeti, igazságszolgáltatási, külügyi feladatokat ellátó elektronikus információs, informatikai vagy hírközlési rendszer;

48. *zárt védelem*: az összes számításba vehető fenyegetést figyelembe vevő védelem.

Tüskevár, 2017. december 1.



Polgármester





Jegyző



IBSZ-01

MEGISMÉRÉSI NYILATKOZAT

Az informatikai biztonsági szabályzatában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

[illegible]

IBSZ-01

MEGISMÉRÉSI NYILATKOZAT

Az informatikai biztonsági szabályzatában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

[illegible]

IBSZ-01

MEGISMÉRÉSI NYILATKOZAT

Az informatikai biztonsági szabályzatában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

[illegible]

IBSZ-01

MEGISMERÉSI NYILATKOZAT

Az informatikai biztonsági szabályzatában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

[illegible]

IBSZ-01

MEGISMERÉSI NYILATKOZAT

Az informatikai biztonsági szabályzatában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

[illegible]

IBSZ-01

MEGISMERÉSI NYILATKOZAT

Az informatikai biztonsági szabályzatában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

[illegible]

IBSZ-01

MEGISMERÉSI NYILATKOZAT

Az informatikai biztonsági szabályzatában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

[illegible]