Tájékoztatás az önkormányzati ASP rendszerekhez csatlakozáshoz megvalósítandó informatikai biztonsági követelményekről

Verziószám: 2.0

Kiadás dátuma: 2018. 06. 18.

Tartalom

Informatikai biztonsági követelmények

Célok és kötelességek

Az ASP Központ a legfrissebb verziójú „Tájékoztatás az önkormányzati ASP rendszerekhez csatlakozáshoz megvalósítandó informatikai biztonsági követelményekről" című dokumentumot (továbbiakban: Tájékoztató) kiadja, és azt elhelyezi az ASP Tájékoztatási Portálon, amely bármely Önkormányzati Hivatal, vagy Közös önkormányzati Hivatal (továbbiakban: Hivatal) számára elérhető. A csatlakozott Hivatalnak **kötelessége** a legújabb verziójú Tájékoztató szerint frissíteni az Informatikai Biztonsági Szabályzatát (a továbbiakban: IBSZ).

A Tájékoztató alapvető célja, hogy az önkormányzati ASP-ben elérhető szolgáltatások használata, alkalmazása során biztosítsa az informatikai biztonsági előírások és elvárások megvalósulását. A Tájékoztató – a Hivatal **hatályos, kihirdetett IBSZ-évelegyütt** – elő kell, hogy mozdítsa az informatikai és kommunikációs eszközök előírásoknak megfelelő és biztonságos használatát, ezzel támogatva, hogy a Hivatal által kezelt információvagyon sértetlensége, bizalmassága és rendelkezésre állása a kapcsolódó **jogszabályokban** megfogalmazottak szerint biztosított legyen.

Az önkormányzati ASP rendszer szakrendszereinek biztonsági osztályba sorolását a Magyar Államkincstártól a Hivatal egy későbbi időpontban kapja meg (a Hivataloknak az önkormányzati ASP szakrendszereit nem kell biztonsági osztályba sorolni). Jelen dokumentum Védelmi intézkedések fejezetében felsorolt adminisztratív, fizikai és logikai védelmi intézkedések megvalósítása a Hivatalok számára kötelező, a hiányosságok kezelésére Cselekvési tervet kell készíteni, melyet a kitöltött „Osztályba sorolás és védelmi intézkedés" (továbbiakban: OVI) táblázattal együtt kell a Nemzeti Kibervédelmi Intézet (korábban: NEIH, továbbiakban: Hatóság) számára megküldeni. Az OVI táblázatban csak a jelen dokumentumban felsorolt követelményeket kell megjeleníteni, hogy teljesül-e az elvárás, vagy nem. Az OVI táblázat további pontjait a Hivatalnak nem kell kitölteni.

Csatlakozó önkormányzatok biztonsága

Az önkormányzati ASP rendszer kapcsán kiemelten kell kezelni a Hivatallal kapcsolatos biztonsági kockázatokat. A Hivatal a saját infrastruktúráját fogja használni az ASP rendszer és alkalmazások igénybe vétele során, így a kliens oldali rendszerek biztonsága nagymértékben befolyásolja a teljes önkormányzati ASP rendszer biztonságát.

A Hivatal számára általános szerződési feltételek szerint egységes biztonsági megfelelőség van előírva, amely minimalizálja a kliens oldali kockázatokat.

Szükséges meghatározni ASP-ben a jogosítások kérdését, és a fluktuáció miatt a felhasználók jogosításának időszakos, Hivatali szintű ellenőrzését és esetleges korrekcióját.

Interfészes csatlakozás feltétele az önkormányzati ASP-hez

Azon interfésszel csatlakozó Hivatalok, amelyek az ASP.ADÓ szakrendszerhez külön interfészes külső szakrendszerrel kapcsolódnak (pl. iratkezelő rendszer), abban az esetben a külső rendszernek (pl. iratkezelő rendszer) meg kell felelnie az ASP biztonsággal kapcsolatos elvárásainak.

További biztonsági követelmények

- Az ASP Központtól kapott szoftveres tanúsítvány és annak jelszava nem adható át az ASP Központ által nem feljogosított személynek.
- Az önkormányzati ASP rendszerben csak a „257/2016. (VIII. 31.) Korm. rendelet az önkormányzati ASP rendszerről" jogszabályban említett szereplők végeznek, illetve végeztetnek központilag fejlesztői, üzemeltetői, működtetői tevékenységet. Bárminemű fejlesztői tevékenységet az ASP Központ vezetője engedélyez írásban.
- Az önkormányzati ASP rendszerben tesztelést végezni csak az idézett Korm. rendeletben meghatározott felek jogosultak.
- A tenant adminisztrátornak törekednie kell a legkisebb jogosultság kiosztásához a felhasználók körében. A jogosultságok kiosztásánál javasolt figyelembe venni a szervezeti és működési szabályzatot, amely nem kerülhet ellentmondásba sem a Hivatali IBSZ-szel, sem e Tájékoztatóval. Az ASP Központ egy esetleges biztonsági incidens során a tenant adminisztrátoroknak privilégiumokkal járó jogosultság- kiosztását számon kérheti. Biztonsági audit során, ha az indokoltnál magasabb hozzáférés állapítható meg egyes felhasználók esetében, annak oka jegyzőkönyvben kell, hogy szerepeljen. Általánosságban megállapítható, hogy a jogosultságok kiosztója is felelőssé tehető a gondatlanságból bekövetkezett biztonsági események kapcsán. Biztonsági incidensek esetén a Hivatal IBSZ-e szerint kell eljárni (dokumentálás, eljárások, ellenőrzés, utóvizsgálat stb.), azonban az önkormányzati ASP-t ért incidensek észlelését jelenteni kell az ASP Központ felé is a Kormányzati Eseménykezelő Központ mellett (utóbbi esetén az észlelés nem feltétlenül jelentkezik a Hivataloknál, de kizárni sem lehet). A jelentés nem tartalmazhat olyan szenzitív adatot (pl. személyes adatot), elemeket, amelyet harmadik fél nem ismerhet meg . Az incidens nem feltétlenül a kliens oldali eszközön jelentkezett, még ha azt az ASP rendszer felhasználója úgy véli, emiatt fontos az eszkalálás. Ennek bejelentési felülete

a hibabejelentő rendszer. Az ASP Központ a bejelentéseket fogadja, továbbítja az illetékes terület felé és a jogszabály szerinti lépéseket megteszi. A Hivatalnak további kötelezettségei is vannak biztonsági incidensek kapcsán (pl. Kormányzati Eseménykezelő Központtal történő kapcsolatfelvétel), melyet a jogszabályok részleteznek.

- Ha az önkormányzati ASP-t üzemeltetői, működtetői oldalon éri biztonsági incidens, az ASP Központnak kötelessége értesítést elhelyeznie a Tájékoztatási Portál nyilvánosság elöl elzárt felületén, megjelenítve a lehetséges elhárítási határidőt, illetve a keretrendszer elérhetősége esetén, a keretrendszer felületén is megjeleníteni ezeket az információkat. Ebben az esetben az üzemeltető szervezet veszi fel a kapcsolatot a jogszabályban megjelölt Hatósággal.
- A Korm. rendelet szerinti üzemeltető és működtető felek a Hatóság kérésére, utasítására is leállíthatják az önkormányzati ASP rendszert, vagy annak bizonyos elemeit (pl. kibertámadás esetén). Ebben az esetben az ASP Központ tájékoztatása addig nem fog megtörténni, amíg az incidens kiváltója, okozója, felderítése akadályokba ütközhet, azaz a Hatóság írásbeli engedélyezéséig.

A Hivatalok feladata a fentiek alapján, hogy ASP-t megjelenítsék az IBSZ-ükben, jelen Tájékoztató **nem váltja ki** ezt az elvárást.

Az IBSZ-nek hatályosnak, szervezeten belül kihirdetettnek kell lennie, és korábban megküldésre kellett kerülnie a Hatóságnak, a Hivatal saját elektronikus információs rendszereinek biztonsági osztályba sorolásával, illetve a Hivatal biztonsági szintjével. Mind a biztonsági osztálynak, mind a biztonsági szintnek szerepelnie kell a hatályos IBSZ-ben.
A jogszabály elvárja az önkormányzati ASP-hez történő csatlakozás után az IBSZ és az eljárásrendek esetleges felülvizsgálatát, ismételt kihirdetését, ahol az értelmezhető.

Elvárások az ASP rendszer igénybevételével kapcsolatban

- A Hivatalokra vonatkozó biztonsági intézkedések megvalósulását kell a Hatóság által biztosított OVI űrlapon megküldeni a Hatóság részére,
- ha a biztonsági intézkedések megvalósításában hiányosságok vannak, akkor **Cselekvési tervet** kell készíteni, amelyet az OVI táblázattal együtt kell a Hatóság részére megküldeni (felelős és határidők megjelölésével),
- ASP.ADÓ szakrendszerhez történő külső interfészes csatlakozás (pl iratkezelő rendszer) esetén a Magyar Államkincstár nem engedélyezi az ASP szakrendszerek bármelyikéhez történő csatlakozást, ha a Hivatal által csatlakoztatni kívánt rendszer biztonsági elvárásai nem felelnek meg ASP biztonsági elvárásainak! Az interfész kialakítása minden esetben a Hivatal feladata! A csatlakozás időpontjáig teljesíteni kell az ASP központ által előírt biztonsági szintet.

Védelmi intézkedések

A védelmi intézkedések megvalósulásának jelentős részét az ASP Központ biztosítja. Tekintettel azonban arra, hogy az adatkezelés a Hivatal helyszínein, a Hivatal munkavállalói és szerződött partnerei által is megvalósul, így biztonsági elvárások egy része a Hivatal hatáskörébe tartozik.
Az alábbi felsorolásban szerepelnek a védelmi intézkedések a működtető és üzemeltető szervezet biztonsági elvárásai a Hivatal irányába, az önkormányzati ASP rendszer használatát illetően. Az elvárásokat a Hivatalnak teljesítenie kell, azok megvalósulását hatósági ellenőrzés folyamán be kell tudni mutatni.
A felsorolás tartalma változhat, melyről az ASP Központ értesítést küld levelezés útján, valamint a Tájékoztató portálon.

Adminisztratív védelmi intézkedések

1. Szervezeti szintű alapfeladatok

1.1. Informatikai biztonsági szabályzat

- 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.

1.1.1. 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.

1.1.2. 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 (ha 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 kötelmek 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 (ha az érintett szervezetnél ez értelmezhető);
- üzlet-, ügy- vagy üzemmenet folytonosság tervezése (így különösen a rendszerleállás 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;
- ha 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.

1.2. Az elektronikus információs rendszerek biztonságáért felelős személy

Az érintett szervezet vezetője az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg, aki ellátja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 13. §-ában meghatározott feladatokat.

1.3. Az intézkedési terv és mérföldkövei

Amennyiben nem valósul meg minden védelmi intézkedés jelen listából, abban az esetben a Hivatalnak intézkedési tervet és ahhoz illeszkedő mérföldköveket kell meghatároznia az alábbiak alapján:

- intézkedési tervet készít, ebben mérföldköveket határoz meg;
- meghatározott időnként felülvizsgálja és karbantartja az intézkedési tervet:
  - a kockázatkezelési stratégia és a kockázatokra adott válasz tevékenységek prioritása alapján;
  - ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni, a hiányosság megszüntetése érdekében;
  - ha a meghatározott biztonsági szint alacsonyabb, mint az érintett szervezetre érvényes szint, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni, az előírt biztonsági szint elérése érdekében.
- folyamatosan aktualizálja a nyilvántartást.

1.4. Az elektronikus információs rendszerek nyilvántartása

Az érintett szervezet:

- elektronikus információs rendszereiről nyilvántartást vezet;
- folyamatosan aktualizálja a nyilvántartást.

A nyilvántartás minden rendszerre nézve tartalmazza:

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

1.5. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás

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

- emberi, fizikai és logikai erőforrásra
- eljárási és védelmi követelményszintre és folyamatra.

2. Kockázatelemzés

2.1. Kockázatelemzési és kockázatkezelési eljárásrend

Az érintett szervezet:

- megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a kockázatelemzési és kockázatkezelési eljárásrendet, mely a kockázatelemzési és kockázatkezelési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
- belső szabályozásában, vagy magában a kockázatelemzési és kockázatkezelési eljárásrendről szóló dokumentumban meghatározza a kockázatelemzési és kockázatkezelési eljárásrend felülvizsgálatának és frissítésének gyakoriságát.

Az eljárásrend kiterjed:

- a lehetséges kockázatok felmérésére;
- a kockázatok kezelésének felelősségére
- a kockázatok kezelésének elvárt minőségére.

2.2. Biztonsági osztályba sorolás

Az érintett szervezet:

- jogszabályban meghatározott szempontok alapján megvizsgálja elektronikus információs rendszereit, és az 1.4. pont szerinti nyilvántartás alapján meghatározza, hogy azok melyik biztonsági osztályba sorolandók;
- vezetője jóváhagyja a biztonsági osztályba sorolást;
- rögzíti a biztonsági osztályba sorolás eredményét a szervezet informatikai biztonsági szabályzatában.

Elvárás:

- a biztonsági osztályba sorolást az elektronikus információs rendszereket érintő változások után ismételten el kell végezni;
- kapcsolódást kell biztosítani az 1.3. pontban foglalt intézkedési tervhez és mérföldköveihez.

2.3. Kockázatelemzés

Az érintett szervezet:

- végrehajtja a biztonsági kockázatelemzéseket;
- rögzíti a kockázatelemzések eredményét az informatikai biztonsági szabályzatban, kockázatelemzési jelentésben, vagy a kockázatelemzési

eljárásrendben előírt dokumentumban;

- a kockázatelemzési eljárásrendnek megfelelően felülvizsgálja a kockázatelemzések eredményét;
- a kockázatelemzési eljárásrendnek megfelelően, vagy az 1.1. pont szerinti informatikai biztonsági szabályzata keretében 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;
- gondoskodik arról, hogy a kockázatelemzési eredmények a jogosulatlanok számára ne legyenek megismerhetők.

3. Rendszer és szolgáltatás beszerzés

3.1. Beszerzési eljárásrend

Az érintett szervezet:

- megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a beszerzési eljárásrendet, mely az érintett szervezet elektronikus információs rendszerére, az ezekhez kapcsolódó szolgáltatások és információs rendszer biztonsági eszközök beszerzésére vonatkozó szabályait fogalmazza meg (akár az általános beszerzési szabályzat részeként), és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
- a beszerzési eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a beszerzési eljárásrendet.

3.2. Erőforrás igény felmérés

Az érintett szervezet:

- az elektronikus információs rendszerre és annak szolgáltatásaira vonatkozó biztonsági követelmények teljesítése érdekében meghatározza, és dokumentálja, valamint biztosítja az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges erőforrásokat, a beruházás tervezés részeként;
- elkülönítetten kezeli az elektronikus információs rendszerek biztonságát beruházás tervezési dokumentumaiban.

3.3. Beszerzések

3.3.1. Az érintett szervezet az elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben szerződéses követelményként meghatározza:

- a funkcionális biztonsági követelményeket;
- a garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint);
- a biztonsággal kapcsolatos dokumentációs követelményeket;
- a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket;
- az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.

3.3.2. A védelem szempontjainak érvényesítése a beszerzés során

- Az érintett szervezet védi az elektronikus információs rendszert, rendszerelemet vagy rendszerszolgáltatást a beszerzés, vagy a beszerzett eszköz beillesztéséből adódó kockázatok ellen.
- Az érintett szervezet szerződéses követelményként meghatározza a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak a leírását.

4. Üzletmenet (ügymenet) folytonosság tervezése

4.1. Üzletmenet folytonosságra vonatkozó eljárásrend

Az érintett szervezet:

- megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül az érintett személyi kör részére kihirdeti az elektronikus információs rendszerre vonatkozó eljárásrendet, mely az üzletmenet-folytonosságra vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
- az üzletmenet-folytonossági tervben, vagy más szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti az üzletmenet-folytonosságra vonatkozó eljárásrendet.

4.2. Üzletmenet folytonossági terv informatikai erőforrás kiesésekre

Az érintett szervezet:

- megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kizárólag a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyek és szervezeti egységek számára kihirdeti az elektronikus információs rendszerekre vonatkozó üzletmenet-folytonossági tervet;

- összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével;
- meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszerhez kapcsolódó üzletmenet-folytonossági tervet;
- 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;
- tájékoztatja az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket;
- gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető, módosítható;
- meghatározza az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;
- rendelkezik a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről;
- jelöli a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket;
- fenntartja a szervezet által előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is;
- kidolgozza a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

4.3. Kritikus rendszerelemek meghatározása

Meg kell határozni az elektronikus információs rendszer alapfunkcióit támogató kritikus rendszerelemeket.

4.4. A folyamatos működésre felkészítő képzés

Az érintett szervezet az elektronikus információs rendszer folyamatos működésére felkészítő képzést tart a felhasználóknak, szerepkörüknek és felelősségüknek megfelelően:

- szerepkörbe vagy felelősségbe kerülésüket követő meghatározott időn belül;
- meghatározott gyakorisággal, vagy amikor az elektronikus információs rendszer változásai ezt szükségessé teszik.

4.5. Üzletmenet folytonosság elérhetőség

A biztonsági tárolási helyszínhez történő hozzáférés érdekében - meghatározott körzetre kiterjedő rombolás vagy katasztrófa esetére - vészhelyzeti eljárásokat kell kidolgozni.

4.6. Infokommunikációs szolgáltatások

Az érintett szervezet - a Nemzeti Távközlési Gerinchálózatra csatlakozó elektronikus információs rendszerek kivételével - tartalék infokommunikációs szolgáltatásokat létesít, erre vonatkozóan olyan megállapodásokat köt, amelyek lehetővé teszik az elektronikus információs rendszer alapfunkciói, vagy meghatározott műveletek számára azok meghatározott időtartamon belüli újrakezdését, ha az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a tartalék feldolgozási vagy tárolási helyszínen.

Szolgáltatás-prioritási rendelkezések

Ha az elsődleges és a tartalék infokommunikációs szolgáltatások nyújtására szerződés keretében kerül sor, az tartalmazza a szolgáltatás-prioritási rendelkezéseket, a szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási idő célokkal) összhangban.

5. Emberi tényezőket figyelembe vevő - személy – biztonság

5.1. Személybiztonsági eljárásrend

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 jelen fejezet szerinti elvárásokat 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).

5.2. Munkakörök, feladatok biztonsági szempontú besorolása

Az érintett szervezet:

- minden érintett szervezeti munkakört, vagy érintett szervezethez kapcsolódó feladatot biztonsági szempontból besorol;
- felméri a nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat;
- rendszeresen felülvizsgálja és frissíti a munkakörök és feladatok biztonság szempontú besorolását.

5.3. A személyek ellenőrzése

Az érintett szervezet:

- az elektronikus információs rendszerhez való hozzáférési jogosultság megadása előtt ellenőrzi, hogy az érintett személy az (5.2. első két alpont) pontok szerinti besorolásnak megfelelő feltételekkel rendelkezik-e;
- az (5.2. pont első két alpont) szerinti munkaköröket betöltő vagy feladatokat ellátó személyek tekintetében kezdeményezi a nemzetbiztonsági szolgálatokról szóló törvényben meghatározott nemzetbiztonsági ellenőrzést;
- folyamatosan ellenőrzi e pont szerinti feltételek fennállását.

5.4. Eljárás a jogviszony megszűnésekor

Az érintett szervezet:

- belső szabályozásban meghatározott időpontban megszünteti a hozzáférési jogosultságot az elektronikus információs rendszerhez;
- megszünteti vagy visszaveszi a személy egyéni hitelesítő eszközeit;
- tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről;
- visszaveszi az érintett szervezet elektronikus információs rendszerével kapcsolatos, tulajdonát képező összes eszközt;
- megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz;
- az általa meghatározott módon a jogviszony megszűnéséről értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket;
- a jogviszonyt megszüntető személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik;
- a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását megelőzi.

5.5. Az áthelyezések, átirányítások és kirendelések kezelése

Az érintett szervezet:

- szükség esetén elvégzi az 5.3. pontban foglalt, a személyek ellenőrzésére vonatkozó eljárást;
- logikai és fizikai hozzáférést engedélyez az újonnan használni kívánt elektronikus információs rendszerhez;
- szükség esetén elvégzi az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását vagy megszüntetését;
- az általa meghatározott módon a jogviszony változásáról értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket.

5.6. Az érintett szervezettel szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények

Az érintett szervezet:

- a külső szervezettel kötött megállapodásban, szerződésben megköveteli, hogy a külső szervezet határozza meg az érintett szervezettel kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is;
- szerződéses kötelezettségként megköveteli, hogy a szerződő fél feleljen meg az érintett szervezet által meghatározott személybiztonsági követelményeknek;
- a szerződő féltől megköveteli, hogy dokumentálja a személybiztonsági követelményeket;
- előírja, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik az érintett szervezet elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést az érintett szervezetnek;
- folyamatosan ellenőrzi a szerződő féltől személybiztonsági követelményeknek való megfelelését.

5.7. Fegyelmi intézkedések

Az érintett szervezet:

- belső eljárási rendje szerint fegyelmi eljárást kezdeményez az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben;
- ha az elektronikus információbiztonsági szabályokat nem az érintett szervezet személyi állományába tartozó személy sérti meg, érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések fennállásának lehetőségét, szükség szerint bevezeti ezeket az eljárásokat.

5.8. Belső egyeztetés

Az érintett szervezet tervezi és egyezteti az elektronikus információs rendszer biztonságát érintő tevékenységeit, hogy csökkentse annak a nem érintett szervezeti egységeire gyakorolt hatását.

5.9. Viselkedési szabályok az interneten

Az érintett szervezet:

- tiltja és számon kéri a szervezettel kapcsolatos információk nyilvános internetes oldalakon való illegális közzétételét;
- tiltja a belső szabályzatában meghatározott, interneten megvalósuló tevékenységet (pl.: chat, fájlcsere, képernyőmegosztás, felhőszolgáltatás, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták, stb.);

- tilthatja a közösségi oldalak használatát, magánpostafiók elérését, és más, a szervezettől idegen tevékenységet.

6. Tudatosság és képzés

6.1. Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és az e célt szolgáló ágazati szervezetekkel.

6.2. Képzési eljárásrend

Az érintett szervezet:

- megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a képzési eljárásrendet, mely a képzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
- a képzési eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a képzési eljárásrendet.

6.3. Biztonság tudatosság képzés

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

- az új felhasználók kezdeti képzésének részeként
- amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;
- az érintett szervezet által meghatározott gyakorisággal.

6.4. Belső fenyegetés

A biztonságtudatossági képzés az érintett személyeket készítse fel a belső fenyegetések felismerésére, és tudatosítsa jelentési kötelezettségüket.

6.5. Szerepkör, vagy feladat alapú biztonsági képzés

Az érintett szervezet szerepkör, vagy feladat alapú biztonsági képzést nyújt az egyes szerepkörök szerinti, azért felelős személyeknek:

- az elektronikus információs rendszerhez való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően;
- amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;
- az érintett szervezet által meghatározott rendszerességgel.

6.6. A biztonsági képzésre vonatkozó dokumentációk

Az érintett szervezet:

- dokumentálja a biztonságtudatosságra vonatkozó alap-, és szerepkör alapú biztonsági képzéseket;

- a képzésen résztvevőkkel a képzés megtörténtét elismerteti, és ezt a dokumentumot megőrzi.

Fizikai védelmi intézkedések

7. Fizikai védelmi eljárásrend

Jelen fejezet alkalmazása során figyelemmel kell lenni a más jogszabályban meghatározott tűz-, és személyvédelmi, valamint a személyes adatok kezelésére vonatkozó rendelkezésekre, valamint arra, hogy e fejezet rendelkezései az adott létesítmény bárki által szabadon látogatható, vagy igénybe vehető területeire nem vonatkoznak.

Az érintett szervezet:

- megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információs rendszerek szempontjából érintett létesítményekre vagy helyiségekre érvényes fizikai védelmi eljárásrendet, amely az érintett szervezet elektronikus információbiztonsági vagy egyéb szabályzatának részét képező fizikai védelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
- a fizikai védelmi eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a fizikai védelmi eljárásrendet.

7.1. Fizikai belépési engedélyek

Az érintett szervezet:

- összeállítja, jóváhagyja, és kezeli az elektronikus információs rendszereknek helyt adó létesítményekbe belépésre jogosultak listáját;
- belépési jogosultságot igazoló dokumentumokat (pl. kitűzők, azonosító kártyák, intelligens kártyák) bocsát ki a belépéshez a belépni szándékozó részére;
- rendszeresen felülvizsgálja a belépésre jogosult személyek listáját;
- eltávolítja a belépésre jogosult személyek listájáról azokat, akik a belépésre már nem jogosultak;
- intézkedik az e felsorolás 2. pont szerinti dokumentum visszavonása, érvénytelenítése, törlése, megsemmisítése iránt.

7.2. A fizikai belépés ellenőrzése

Az érintett szervezet:

- kizárólag az érintett szervezet által meghatározott be-, és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést;

- ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket;
- kíséri a létesítménybe ad-hoc belépésre jogosultakat, és figyelemmel követi a tevékenységüket;
- megóvja a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző eszközt;
- nyilvántartást vezet a fizikai belépést ellenőrző eszközről;
- 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;
- az egyéni belépési engedélyeket a belépési pontokon ellenőrzi;
- a kijelölt pontokon való átjutást felügyeli a szervezet által meghatározott fizikai belépést ellenőrző rendszerrel vagy eszközzel;
- felhívja a szervezet tagjainak figyelmét a rendellenességek jelentésére.

7.3. Hozzáférés az adatátviteli eszközökhöz és csatornákhoz

Az érintett szervezet az általa meghatározott biztonsági védelemmel ellenőrzi az elektronikus információs rendszer adatátviteli eszközeinek és kapcsolódási pontjainak helyt adó helyiségekbe történő fizikai belépést.

7.4. A kimeneti eszközök hozzáférés ellenőrzése

Az érintett szervezet ellenőrzi az elektronikus információs rendszer kimeneti eszközeihez való fizikai hozzáférést annak érdekében, hogy jogosulatlan személyek ne férjenek azokhoz hozzá.

7.5. A fizikai hozzáférések felügyelete

Az érintett szervezet ellenőrzi az elektronikus információs rendszereknek helyt adó létesítményekbe történt fizikai hozzáféréseket annak érdekében, hogy észlelje a fizikai biztonsági eseményt és reagáljon arra.

7.6. Behatolás riasztás, felügyeleti berendezések

Az érintett szervezet rendszeresen átvizsgálja a fizikai hozzáférésekről készült naplókat.

7.7. A látogatók ellenőrzése

Az érintett szervezet meghatározott ideig megőrzi az elektronikus információs rendszereknek helyt adó létesítményekbe történt látogatói belépésekről szóló információkat.

7.8. Áramellátó berendezések és kábelezés

Az érintett szervezet védi az elektronikus információs rendszert árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben.

7.9. Tűzvédelem

Az érintett szervezet az elektronikus információs rendszerek számára független áramellátással támogatott észlelő, az informatikai eszközökhöz megfelelő tűzelfojtó berendezéseket alkalmaz, és tart karban.

7.10. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem

Az érintett szervezet védi az elektronikus információs rendszert a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzárószelepek hozzáférhetőek, és megfelelően működnek, valamint a kulcsszemélyek számára ismertek.

7.11. Be- és kiszállítás

Az érintett szervezet engedélyezi, vagy tiltja, továbbá figyeli és ellenőrzi a létesítménybe bevitt, onnan kivitt információs rendszerelemeket, és nyilvántartást vezet ezekről.

7.12. Az elektronikus információs rendszer elemeinek elhelyezése

Az érintett szervezet úgy helyezi el az elektronikus információs rendszer elemeit, hogy a legkisebb mértékre csökkentse a szervezet által meghatározott fizikai és környezeti veszélyekből adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét.

7.13. Karbantartók

Az érintett szervezet:

- kialakít egy folyamatot a karbantartók munkavégzési engedélyének kezelésére, és nyilvántartást vezet a karbantartó szervezetekről vagy személyekről;
- megköveteli a hozzáférési jogosultság igazolását az elektronikus információs rendszeren karbantartást végzőktől;
- felhatalmazást ad a szervezethez tartozó, a kívánt hozzáférési jogosultságokkal és műszaki szakértelemmel rendelkező személyeknek arra, hogy felügyeljék a kívánt jogosultságokkal nem rendelkező személyek karbantartási tevékenységeit.

7.14. Időben történő javítás

Az érintett szervezet karbantartási támogatást szerez be a meghatározott elektronikus információs rendszerelemekhez.

Logikai védelmi intézkedések

8. Általános védelmi intézkedések

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.

8.1. Az elektronikus információs rendszer kapcsolódásai

Az érintett szervezet:

- szabályozza, és belső engedélyhez kötheti az elektronikus információs rendszerének kapcsolódását más elektronikus információs rendszerekhez;
- dokumentálja az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.

8.2. Belső rendszer kapcsolatok

Az érintett szervezet belső engedélyhez köti az elektronikus információs rendszereinek összekapcsolását.

8.3. Külső kapcsolódásokra vonatkozó korlátozások

Az érintett szervezet a külső elektronikus információs rendszerekhez való kapcsolódásokhoz az informatikai biztonsági szabályzatában szabályrendszert állít fel, és alkalmaz, amelynek eredménye lehet az összes kapcsolat engedélyezése vagy tiltása, meghatározott kapcsolatok engedélyezése, meghatározott kapcsolatok tiltása.

8.4. 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).

9. Tervezés

9.1. Cselekvési terv

Az érintett szervezetnek cselekvési tervet kell készíteni, amennyiben nem felel meg a szervezet jelen dokumentáció bármely pontja kapcsán az elvárásoknak:

- cselekvési tervet készít, ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg;
- a cselekvési tervben dokumentálja a megállapított hiányosságok javítására, valamint az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányuló tervezett tevékenységeit;
- frissíti a meglévő cselekvési tervet az érintett szervezet által meghatározott gyakorisággal a biztonsági értékelések, biztonsági hatáselemzések és a folyamatos felügyelet eredményei alapján.

9.2. Személyi biztonság

Az érintett szervezet:

- megfogalmazza, és az érintett szervezetre 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;
- 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;
- 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;
- gondoskodik arról, hogy az előző bekezdés szerinti változás esetén a hozzáféréssel rendelkezők tekintetében a második bekezdés szerinti eljárás megtörténjen;
- meghatározza az érintett szervezeten kívüli irányban megvalósuló követelményeket.

10. Konfigurációkezelés

10.1. Konfigurációkezelési eljárásrend

Az érintett szervezet:

- megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a konfigurációkezelési eljárásrendet, mely a konfigurációkezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
- a fizikai védelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a konfigurációkezelési eljárásrendet.

10.2. Legszűkebb funkcionalitás

Az érintett szervezet:

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

10.3. Duplikálás elleni védelem

Az érintett szervezet ellenőrzi, hogy az elektronikus információs rendszer hatókörén belüli elemek nincsenek-e felvéve más elektronikus információs rendszerek leltárában.

10.4. A szoftver használat korlátozásai

Az érintett szervezet:

- kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak;
- a másolatok, megosztások ellenőrzésére nyomon követi a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát;
- 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.

10.5. A felhasználó által telepített szoftverek

Az érintett szervezet:

- megfogalmazza az elektronikus információs rendszer vonatkozásában, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti azokat a szabályokat, amelyek meghatározzák a szoftverek felhasználó általi telepítési lehetőségét;
- érvényesíti a szoftvertelepítésre vonatkozó szabályokat az érintett szervezet által meghatározott módszerek szerint;

- meghatározott gyakorisággal ellenőrzi a szabályok betartását.

11. Karbantartás

11.1. Rendszer karbantartási eljárásrend

Az érintett szervezet:

- megfogalmazza, és az érintett szervezetre 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 fizikai védelmi eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a rendszer karbantartási eljárásrendet.

11.2. Adathordozó ellenőrzés

Az érintett szervezet ellenőrzi a diagnosztikai és teszt programokat tartalmazó adathordozókat a kártékony kódok tekintetében, mielőtt azt az elektronikus információs rendszerben használnák.

11.3. Távoli karbantartás

Az érintett szervezet:

- jóváhagyja, nyomon követi és ellenőrzi a távoli karbantartási és diagnosztikai tevékenységeket;
- akkor engedélyezi a távoli karbantartási és diagnosztikai eszközök használatát, ha az összhangban áll az informatikai biztonsági szabályzattal, és dokumentálva van az elektronikus információs rendszer rendszerbiztonsági tervében;
- hitelesítéseket alkalmaz a távoli karbantartási és diagnosztikai munkaszakaszok létrehozásánál;
- nyilvántartást vezet a távoli karbantartási és diagnosztikai tevékenységekről;
- lezárja a munkaszakaszt és a hálózati kapcsolatokat, amikor a távoli karbantartás befejeződik.

12. Adathordozók védelme

12.1. Adathordozók védelmére vonatkozó eljárásrend

Az érintett szervezet:

- megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az adathordozók védelmére vonatkozó eljárásrendet, mely az adathordozókra vonatkozó védelmi szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;

- az adathordozók védelmére vonatkozó eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti az adathordozók védelmére vonatkozó eljárásrendet.

12.2. Hozzáférés az adathordozókhoz

Az érintett szervezet az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, jogosítványuk tartalmát meghatározza.

12.3. Adathordozók tárolása

Az érintett szervezet:

- fizikailag ellenőrzi és biztonságosan tárolja az adathordozókat, az arra engedélyezett vagy kijelölt helyen;
- védi az elektronikus információs rendszer adathordozóit mindaddig, amíg az adathordozókat jóváhagyott eszközökkel, technikákkal és eljárásokkal nem semmisítik meg, vagy nem törlik.

12.4. Adathordozók szállítása

Az érintett szervezet:

- meghatározott biztonsági óvintézkedésekkel védi és ellenőrzi az elektronikus információs rendszer adathordozóit az ellenőrzött területeken kívüli szállítás folyamán;
- biztosítja az adathordozók elszámoltathatóságát az ellenőrzött területeken kívüli szállítás folyamán;
- dokumentálja az adathordozók szállításával kapcsolatos tevékenységeket;
- korlátozza az adathordozók szállításával kapcsolatos tevékenységeket az arra jogosult személyekre.

12.5. Kriptográfiai védelem

Kriptográfiai mechanizmusokat kell alkalmazni a digitális adathordozókon tárolt információk bizalmasságának és sértetlenségének a védelmére az ellenőrzött területeken kívüli szállítás, használat folyamán (hordozható adattároló, pl. okostelefon, laptop, pendrive stb.).

12.6. Adathordozók törlése

Az érintett szervezet:

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

12.7. Adathordozók használata

Az érintett szervezet engedélyezi, korlátozza, vagy tiltja egyes, vagy bármely adathordozó típusok használatát a meghatározott elektronikus információs rendszereken vagy rendszerelemeken működő biztonsági intézkedések használatával.

12.8. Ismeretlen tulajdonos

Az érintett szervezet megtiltja az olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek tulajdonosa nem azonosítható.

13. Azonosítás és hitelesítés

13.1. Azonosítási és hitelesítési eljárásrend

Az érintett szervezet:

- 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;
- az azonosítási és hitelesítésre vonatkozó eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti az azonosítási és hitelesítésre vonatkozó eljárásrendet.

13.2. Azonosító kezelés

Az érintett szervezet:

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

13.3. A hitelesítésre szolgáló eszközök kezelése

Az érintett szervezet, amennyiben a szervezet felhasználója nem elektronikus személyazonosító okmánnyal hitelesíti magát:

- ellenőrzi a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát.
- meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;
- biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;
- dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket;
- megváltoztatja a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az elektronikus információs rendszer telepítése során;

- meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit;
- a hitelesítésre szolgáló eszköz típusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket;
- megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;
- megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét;
- lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.

13.4. Jelszó (tudás) alapú hitelesítés

Az érintett szervezet a jelszavakat nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hasító érték tárolást), és nem továbbítja;

13.5. Birtoklás alapú hitelesítés

Az érintett szervezet:

- az elektronikus információs rendszer hardver token alapú hitelesítése esetén olyan mechanizmusokat alkalmaz, amely megfelel az érintett szervezet által meghatározott minőségi követelményeknek, vagy
- az elektronikus információs rendszer nyilvános kulcsú infrastruktúra alapú hitelesítés esetén összekapcsolja a hitelesített azonosságot az egyéni vagy csoport fiókkal.

13.6. Személyes vagy megbízható harmadik fél általi regisztráció

Az érintett szervezet meghatározott hitelesítő eszköz átvételéhez megkövetel egy olyan regisztrációs eljárást, melyet meghatározott regisztrációs szervezet folytat le az érintett szervezet által meghatározott személyek vagy szerepkörök jóváhagyása mellett.

14. Hozzáférés ellenőrzése

14.1. Hozzáférés ellenőrzési eljárásrend

Az érintett szervezet:

- megfogalmazza, és az érintett szervezetre 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 hozzáférés védelmére vonatkozó eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a hozzáférések védelmére vonatkozó eljárásrendet.

14.2. Felhasználói fiókok kezelése

Az érintett szervezet:

- meghatározza és azonosítja az elektronikus információs rendszer felhasználói

fiókjait és ezek típusait;
- kijelöli a felhasználói fiókok fiókkezelőit;
- kialakítja a csoport- és szerepkör tagsági feltételeket;
- 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;
- létrehozza, engedélyezi, módosítja, letiltja, és eltávolítja a felhasználói fiókokat a meghatározott eljárásokkal vagy feltételekkel összhangban;
- ellenőrzi a felhasználói fiókok használatát;
- értesíti a fiókkezelőket, ha:
  - a felhasználói fiókokra már nincsen szükség,
  - a felhasználók kiléptek vagy áthelyezésre kerültek,
  - az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak;
- feljogosít az elektronikus információs rendszerhez való hozzáférésre:
  - az érvényes hozzáférési engedély,
  - a tervezett rendszerhasználat,
  - az alapfeladatok és funkcióik alapján;
- meghatározott gyakorisággal felülvizsgálja a felhasználói fiókokat, a fiókkezelési követelményekkel való összhangot;
- kialakít egy folyamatot a megosztott vagy csoport felhasználói fiókokhoz tartozó hitelesítő eszközök vagy adatok újra kibocsátására (ha ilyet alkalmaznak), a csoport tagjainak változása esetére.

14.3. A felelősségek szétválasztása

Az érintett szervezet:
- szétválasztja az egyéni felelősségeket;
- dokumentálja az egyéni felelősségek szétválasztását;
- meghatározza az elektronikus információs rendszer hozzáférés jogosultságait az egyéni felelősségek szétválasztása érdekében.

14.4. Legkisebb jogosultság elve

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

14.5. Jogosult hozzáférés a biztonsági funkciókhoz

Az érintett szervezet hozzáférési jogosultságokat biztosít a meghatározott biztonsági funkciókhoz és biztonságkritikus információkhoz.

14.6. Nem privilegizált hozzáférés a biztonsági funkciókhoz

Az érintett szervezet kötelezővé teszi, hogy a szervezet meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal

rendelkező felhasználói a nem biztonsági funkciók használatához nem a különleges jogosultsághoz kötött - úgynevezett privilegizált - fiókjukat vagy szerepkörüket használják.

14.7. Privilegizált fiókok

Az érintett szervezet az elektronikus információs rendszer privilegizált fiókjait meghatározott személyekre vagy szerepkörökre korlátozza.

14.8. A munkaszakasz zárolása

Az érintett szervezet:

- meghatározott időtartamú inaktivitás után, vagy a felhasználó erre irányuló lépése esetén a munkaszakasz zárolásával megakadályozza az elektronikus információs rendszerhez való további hozzáférést;
- megtartja a munkaszakasz zárolását mindaddig, amíg a felhasználó a megfelelő eljárások alkalmazásával nem azonosítja és hitelesíti magát újra.

14.9. Képernyőtakarás

A munkaszakasz zárolásakor a képernyőn korábban látható információt egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel - ami a záró személy nevét is tartalmazhatja - kell eltakarni.

14.10. A munkaszakasz lezárása

Az elektronikus információs rendszer automatikusan lezárja a munkaszakaszt az érintett szervezet által meghatározott feltételek vagy munkaszakasz szétkapcsolást igénylő események megtörténte után.

14.11. Vezeték nélküli hozzáférés

Az érintett szervezet:

- belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki a vezeték nélküli technológiák kapcsán;
- engedélyezési eljárást folytat le a vezeték nélküli hozzáférés feltételeként.

14.12. Mobil eszközök hozzáférés ellenőrzése

Az érintett szervezet:

- belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki az általa ellenőrzött mobil eszközökre;
- engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást.

14.13. Titkosítás

Az érintett szervezet teljes eszköztitkosítást, tároló alapú titkosítást, vagy más technológiai eljárást alkalmaz az általa meghatározott mobil eszközökön tárolt információk bizalmasságának és sértetlenségének a védelmére, vagy az információk hozzáférhetetlenné tételére.

14.14. Külső elektronikus információs rendszerek használata

Az érintett szervezet:

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

14.15. Korlátozott használat

Az érintett szervezet csak abban az esetben engedélyezi jogosult felhasználóknak egy külső elektronikus információs rendszer felhasználását az elektronikus információs rendszerhez való hozzáférésre, az által ellenőrzött információk feldolgozására, tárolására vagy továbbítására, ha:

- előzetesen ellenőrzi a szükséges biztonsági intézkedések meglétét a külső rendszeren saját szabályzóinak megfelelő módon; vagy
- jóváhagyott kapcsolat van az elektronikus információs rendszerek között, vagy megállapodás született a külső elektronikus információs rendszert befogadó szervezettel.

14.16. Hordozható adattároló eszközök

Az érintett szervezet korlátozza vagy megtiltja az ellenőrzött hordozható tárolóeszközök használatát külső elektronikus információs rendszerben is jogosultsággal rendelkező személyek számára.

14.17. Információ megosztás

Az érintett szervezet:

- elősegíti az információmegosztást azzal, hogy engedélyezi a jogosult felhasználóknak eldönteni, hogy a megosztásban résztvevő partnerhez rendelt jogosultságok megfelelnek-e az információra vonatkozó hozzáférési korlátozásoknak, olyan meghatározott információmegosztási körülmények esetén, amikor felhasználói megítélés szóba jöhet;
- automatizált mechanizmusokat vagy kézi folyamatokat alkalmaz arra, hogy segítséget nyújtson a felhasználóknak az információmegosztási vagy együttműködési döntések meghozatalában.

14.18. Nyilvánosan elérhető tartalom

Az érintett szervezet:

- kijelöli azokat a személyeket, akik jogosultak a nyilvánosan hozzáférhető elektronikus információs rendszeren az érintett szervezettel kapcsolatos bármely információ közzétételére;
- az előző pont szerinti kijelölt személyeket képzésben részesíti annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak

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

15. Rendszer és információ sértetlenség

15.1. Rendszer és információ sértetlenségre vonatkozó eljárásrend

Az érintett szervezet:
- megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a rendszer- és információsértetlenségre vonatkozó eljárásrendet, mely a szervezet informatikai biztonsági szabályzatának részét képező, rendszer- és információsértetlenségre vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
- a rendszer- és információsértetlenségre vonatkozó eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja, és frissíti a rendszer- és információsértetlenségre vonatkozó eljárásrendet.

15.2. Hibajavítás

Az érintett szervezet:
- azonosítja, belső eljárásrendje alapján jelenti és kijavítja vagy kijavíttatja az elektronikus információs rendszer hibáit;
- telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket az érintett szervezet feladatellátásának hatékonysága, a szóba jöhető következmények szempontjából;
- a biztonságkritikus szoftvereket a frissítésük kiadását követő meghatározott időtartamon belül telepíti vagy telepítteti;
- beépíti a hibajavítást a konfigurációkezelési folyamatba.

15.3. Kártékony kódok elleni védelem

Az érintett szervezet:
- az elektronikus információs rendszerét annak belépési és kilépési pontjain védi a kártékony kódok ellen, felderíti és megsemmisíti azokat;
- 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:

- rendszeres ellenőrzéseket hajtson végre az elektronikus információs rendszeren, és hajtsa végre 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,
- a kártékony kód észlelése esetén blokkolja vagy helyezze karanténba azt, és riassza a rendszeradminisztrátort és az érintett szervezet által meghatározott további személy(eke)t;

- ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az elektronikus információs rendszer rendelkezésre állására.

15.4. Automatikus frissítés

Az elektronikus információs rendszer automatikusan frissíti a kártékony kódok elleni védelmi mechanizmusokat.

15.5. Az elektronikus információs rendszer felügyelete

Az érintett szervezet:

- 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;
- azonosítja az elektronikus információs rendszer jogosulatlan használatát;
- felügyeleti eszközöket alkalmaz a meghatározott alapvető információk gyűjtésére, és a rendszer ad hoc területeire a potenciálisan fontos, speciális típusú tranzakcióknak a nyomon követésére;
- védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;
- erősíti az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelet észlel;
- meghatározott gyakorisággal biztosítja az elektronikus információs rendszer felügyeleti információkat a meghatározott személyeknek vagy szerepköröknek.

15.6. Biztonsági riasztások és tájékoztatások

Az érintett szervezet:

- folyamatosan figyeli a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;
- folyamatosan figyelemmel kíséri a Nemzeti Elektronikus Információbiztonsági Hatóságtól érkező értesítéseket;
- szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki;

- a belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez;
- kialakítja és működteti a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, és kapcsolatot tart az érintett, külön jogszabályban meghatározott szervekkel;
- megfelelő ellenintézkedéseket és válaszlépéseket tesz.

15.7. Bemeneti információ ellenőrzés

Az elektronikus információs rendszer ellenőrzi a meghatározott információ belépési pontok érvényességét.

15.8. A kimeneti információ kezelése és megőrzése

Az érintett szervezet az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

Jogszabályi hivatkozások

- Az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet
- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
- 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.