**Kormányzati Személyügyi Döntéstámogató Rendszer**

**Rendszerbiztonsági Specifikáció**

A Kormányzati Személyügyi Döntéstámogató Rendszer Ibtv. szerinti rendszer biztonsági osztályba sorolása:

Bizalmasság: 4

Sértetlenség: 4

Rendelkezésre állás: 4

Eredő osztály: 4

Az osztályba-sorolást, az adatkezeléshez tartozó adatkezelői / adatgazdai hatáselemzést eredményeként kapta meg a BM IHÁT/IBO. Ezen adatok ismeretében készült el a Kormányzati Személyügyi Döntéstámogató Rendszer Rendszerbiztonsági Specifikációja.

A Rendszerbiztonsági terv elkészítésekor az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) és a 41/2015. (VII. 15.) BM végrehajtási rendeletének figyelembevétele szükséges. Jelen dokumentum a jelzett jogszabályok szerinti biztonsági specifikációt tartalmazza, mely a 4-es osztályhoz tartozó kritériumok leválogatásával és konkrét feladattá formálásával készült.

**Adminisztratív védelmi intézkedések**

**3.1.3.1. 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.

**3.1.3.2. 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.

**3.1.3.3. Beszerzések**

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 garanciaszintet);
* a biztonsággal kapcsolatos dokumentációs követelményeket;
* a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket;
* az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.

**3.1.3.3.2 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.

**3.1.3.3.3. A védelmi intézkedések terv-, és megvalósítási dokumentációi**

Az érintett szervezet szerződéses követelményként meghatározza a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések terv- és megvalósítási dokumentációit, köztük a biztonsággal kapcsolatos külső rendszer interfészek leírását, a magas és alacsony szintű biztonsági tervet, - ha azzal a szállító rendelkezik - a forráskódot és futtatókörnyezetet.

**3.1.3.3.4 Funkciók - protokollok - szolgáltatások**

Az érintett szervezet szerződéses rendelkezésként megköveteli a fejlesztőtől, szállítótól, hogy már a fejlesztési életciklus korai szakaszában meghatározza a használatra tervezett funkciókat, protokollokat és szolgáltatásokat.

**3.1.3.4. Az elektronikus információs rendszerre vonatkozó dokumentáció**

Az érintett szervezet, ha hatókörébe tartozik, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely tartalmazza:

* a rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését,
* a biztonsági funkciók hatékony alkalmazását és fenntartását,
* a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket.
* Az érintett szervezet megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amely tartalmazza:
* a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját,
* a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit,
* a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához,
* gondoskodik arról, hogy az információs rendszerre vonatkozó - különösen az adminisztrátori és fejlesztői - dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható,
* gondoskodik a dokumentációknak az érintett szervezet által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről.

**3.1.3.5. Biztonságtervezési elvek**

Az érintett szervezet biztonságtervezési elveket dolgoz ki és alkalmaz az elektronikus információs rendszer specifikációjának meghatározása, tervezése, fejlesztése, kivitelezése és módosítása során.

**3.1.3.6. Külső elektronikus információs rendszerek szolgáltatásai**

Az érintett szervezet szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján általa igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek az érintett szervezet elektronikus információbiztonsági követelményeinek, továbbá meghatározza és dokumentálja az érintett szervezet felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban, külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

**3.1.3.3.7. Független értékelők**

Az érintett szervezet független értékelőket vagy értékelő csoportokat alkalmaz a védelmi intézkedések értékelésére.

**3.1.3.8. Folyamatos ellenőrzés**

Az érintett szervezet folyamatba épített ellenőrzést vagy ellenőrzési tervet hajt végre, amely tartalmazza:

* az ellenőrizendő területeket,
* az ellenőrzések, valamint az ellenőrzéseket támogató értékelések gyakoriságát,
* az érintett szervezet ellenőrzési stratégiájához illeszkedő folyamatos biztonsági értékeléseket,
* a mérőszámok megfelelőségét,
* az értékelések és az ellenőrzések által generált biztonsággal kapcsolatos adatok összehasonlító elemzését,
* az érintett szervezet reagálását a biztonsággal kapcsolatos adatok elemzésének eredményére,
* az érintett szervezet döntését arról, hogy milyen gyakorisággal kell az elemzési adatokat általa meghatározott személyi- és szerepkörökkel megismertetni (ideértve azok változásait is).

**3.1.4.1 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.

**3.1.4.2. 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.

**3.1.4.2.2. Egyeztetés**

Az üzletmenet-folytonossági tervet egyeztetni kell a kapcsolódó, hasonló tervekért felelős szervezeti egységekkel.

**3.1.4.2.3. Alapfunkciók újraindítása**

Meg kell határozni az alapfunkciók újrakezdésének időpontját az üzletmenet-folytonossági terv aktiválását követőn.

**3.1.4.2.4. Kritikus rendszerelemek meghatározása**

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

**3.1.4.3. 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.

**3.1.4.4. Az üzletmenet-folytonossági terv tesztelése**

Az érintett szervezet:

* meghatározott gyakorisággal és meghatározott teszteken keresztül vizsgálja az elektronikus információs rendszerre vonatkozó üzletmenet-folytonossági tervet a terv hatékonyságának és az érintett szervezet felkészültségének a felmérése céljából,
* értékeli az üzletmenet-folytonossági terv tesztelési eredményeit,
* az értékelés alapján szükség esetén javítja a tervet, a javításokkal kapcsolatban az üzletmenet-folytonossági tervre vonatkozó általános eljárási szabályok szerint jár el,
* az üzletmenet-folytonossági terv tesztelését a kapcsolódó tervekért felelős szervezeti egységekkel egyeztetni kell,
* az üzletmenet folytonossági tervet a tartalék feldolgozási helyszínen is tesztelni kell, hogy az érintett szervezet megismerje az adottságokat és az elérhető erőforrásokat, valamint értékelje a tartalék feldolgozási helyszín képességeit a folyamatos működés támogatására.

**3.1.4.5. Biztonsági tárolási helyszín**

Az érintett szervezet kijelöl egy biztonsági tárolási helyszínt, ahol az elektronikus információs rendszer mentéseinek másodlatát az elsődleges helyszínnel azonos módon, és biztonsági feltételek mellett tárolja. A biztonsági tárolási helyszínnek el kell különülni az elsődleges tárolás helyszínétől, az azonos veszélyektől való érzékenység csökkentése érdekében. A biztonsági tárolási helyszínhez történő hozzáférés érdekében - meghatározott körzetre kiterjedő rombolás vagy katasztrófa esetére - vészhelyzeti eljárásokat kell kidolgozni.

**3.1.4.6. Tartalék feldolgozási helyszín**

Az érintett szervezet:

* kijelöl egy tartalék feldolgozási helyszínt azért, hogy ha az elsődleges feldolgozási képesség nem áll rendelkezésére, elektronikus információs rendszere előre meghatározott műveleteit, előre meghatározott időn belül - összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal - a tartalék helyszínen újra kezdhesse, vagy folytathassa,
* biztosítja, hogy a működés újrakezdéséhez, vagy folytatásához szükséges eszközök és feltételek a tartalék feldolgozási helyszínen, vagy meghatározott időn belül rendelkezésre álljanak,
* biztosítja, hogy a tartalék feldolgozási helyszín informatikai biztonsági intézkedései egyenértékűek legyenek az elsődleges helyszínen alkalmazottakkal.

**3.1.4.7. 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.

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.

Olyan tartalék infokommunikációs szolgáltatásokat kell igénybe venni, melyek csökkentik az elsődleges infokommunikációs szolgáltatásokkal közös hibalehetőségek valószínűségét (pl. alternatív technológiára épülnek).

**3.1.4.8. Az elektronikus információs rendszer mentései**

Az érintett szervezet meghatározott gyakorisággal mentést végez az elektronikus információs rendszerben tárolt felhasználószintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal továbbá meghatározott gyakorisággal elmenti az elektronikus információs rendszerben tárolt rendszerszintű információkat, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal. Továbbá az érintett szervezet meghatározott gyakorisággal elmenti az elektronikus információs rendszer dokumentációját, köztük a biztonságra vonatkozókat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal és megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen. Meghatározott gyakorisággal tesztelni kell a mentett információkat, az adathordozók megbízhatóságának és az információ sértetlenségének a garantálása érdekében.

**3.1.4.9. Az elektronikus információs rendszer helyreállítása és újraindítása**

Az érintett szervezet gondoskodik az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően. valamint a tranzakció alapú elektronikus információs rendszerek esetén tranzakció helyreállítást hajt végre.

**3.1.5.1. Biztonsági eseménykezelési eljárásrend**

Az érintett szervezet eseménykezelési eljárást dolgoz ki a biztonsági eseményekre, amelyek magukban foglalják az előkészületet, az észlelést, a vizsgálatot, az elszigetelést, a megszüntetést és a helyreállítást. Az érintett szervezet egyezteti az eseménykezelési eljárásokat az üzletmenet-folytonossági tervéhez tartozó tevékenységekkel:

* az eseménykezelési tevékenységekből levont tanulságokat beépíti az eseménykezelési eljárásokba,
* az eseménykezelési tevékenységekből levont tanulságokat beépíti a fejlesztési és üzemeltetési eljárásokba, elvárásokba,
* az eseménykezelési tevékenységekből levont tanulságokat beépíti a továbbképzésekbe és tesztelésekbe.

**3.1.5.4. A biztonsági események figyelése**

Az érintett szervezet nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági eseményeit.

**3.1.5.6. A biztonsági események jelentése**

Az érintett szervezet:

* mindenkitől, aki az elektronikus információs rendszerrel, vagy azok elhelyezésére szolgáló objektummal kapcsolatban áll megköveteli, hogy jelentsék a biztonsági esemény bekövetkeztét, vagy ha erre utaló jelet, vagy veszélyhelyzetet észlelnek valamint jogszabályban meghatározottak szerint jelenti a biztonsági eseményekre vonatkozó információkat az elektronikus információs rendszerek biztonságának felügyeletét ellátó szerveknek,
* automatizált mechanizmusokat alkalmaz, hogy segítse a biztonsági események jelentését,
* tanácsadást és támogatást nyújt az elektronikus információs rendszer felhasználóinak a biztonsági események kezeléséhez és jelentéséhez,
* automatizált mechanizmusokat alkalmaz, hogy növelje a biztonsági események kezelésével kapcsolatos információk és a támogatás rendelkezésre állását.

**3.1.5.7. Segítségnyújtás a biztonsági események kezeléséhez**

Az érintett szervezet tanácsadást és támogatást nyújt az elektronikus információs rendszer felhasználóinak a biztonsági események kezeléséhez és jelentéséhez valamint automatizált támogatási mechanizmusokat alkalmaz, hogy növelje a biztonsági események kezelésével kapcsolatos információk és a támogatás rendelkezésre állását.

**3.1.5.8. Biztonsági eseménykezelési terv**

Az érintett szervezet kidolgozza a biztonsági eseménykezelési tervet, amely:

* az érintett szervezet számára iránymutatást ad a biztonsági esemény kezelési módjaira,
* ismerteti a biztonsági eseménykezelési lehetőségek struktúráját és szervezetét,
* átfogó megközelítést nyújt arról, hogy a biztonsági eseménykezelési lehetőségek hogyan illeszkednek az általános szervezetbe,
* kielégíti az érintett szervezet feladatkörével, méretével, szervezeti felépítésével és funkcióival kapcsolatos egyedi igényeit,
* meghatározza a bejelentésköteles biztonsági eseményeket,
* meghatározza és folyamatosan pontosítja a biztonsági események kiértékelésének, kategorizálásának (súlyosság, stb.) kritériumrendszerét,
* támogatást ad a biztonsági eseménykezelési lehetőségek belső mérésére,
* meghatározza azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására,
* kihirdeti és tudomásul veteti a biztonsági eseménykezelési tervet a biztonsági eseményeket kezelő (névvel és/vagy szerepkörrel azonosított) személyeknek és szervezeti egységeknek,
* meghatározott gyakorisággal felülvizsgálja a biztonsági eseménykezelési tervet,
* frissíti a biztonsági eseménykezelési tervet, figyelembe véve az elektronikus információs rendszer és a szervezet változásait vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat,
* a biztonsági eseménykezelési terv változásait ismerteti az érintettekkel,
* gondoskodik arról, hogy a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető, módosítható.

**3.1.5.9. Képzés a biztonsági események kezelésére**

Az érintett szervezet biztonsági eseménykezelési képzést biztosít az elektronikus információs rendszer felhasználóinak a számukra kijelölt szerepkörökkel és felelősségekkel összhangban. Az érintett szervezet a képzést a biztonsági eseménykezelési szerepkör vagy felelősség kijelölését követő, meghatározott időtartamon belül, vagy amikor ezt az elektronikus információs rendszer változásai megkívánják, vagy meghatározott gyakorisággal tartja. Az érintett szervezet meghatározott gyakorisággal teszteli az elektronikus információs rendszerre vonatkozó biztonsági eseménykezelési képességeket előre kidolgozott tesztek felhasználásával, annak érdekében, hogy meghatározza a biztonsági eseménykezelés hatékonyságát, és dokumentálja az eredményeket valamint egyezteti a biztonsági eseménykezelés tesztelését a kapcsolódó tervekért (pl. üzletmenet-folytonossági terv és katasztrófaelhárítási terv) felelős szervezeti egységekkel.

**3.1.6.1. 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).

**3.1.6.2. 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.

**3.1.6.3. A személyek ellenőrzése**

Az érintett szervezet az elektronikus információs rendszerhez való hozzáférési jogosultság megadása előtt ellenőrzi, hogy az érintett személy a munkakörök, feladatok biztonsági szempontú besorolásnak megfelelő feltételekkel rendelkezik-e. A biztonsági szempontok szerint besorolt munkaköröket, feladatokat betöltő vagy feladatokat ellátó személyek tekintetében kezdeményezi a nemzetbiztonsági szolgálatokról szóló törvényben meghatározott nemzetbiztonsági ellenőrzést. Az érintett szervezet folyamatosan ellenőrzi a személyek ellenőrzéséről szóló feltételek fennállását.

**3.1.6.4 Eljárás a jogviszony megszűnésekor**

Az érintett szervezet a belső szabályozásban meghatározott időpontban megszünteti a hozzáférési jogosultságot az elektronikus információs rendszerhez, tehát:

* 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.

**3.1.6.5. Az áthelyezések, átirányítások és kirendelések kezelése**

Az érintett szervezet szükség esetén elvégzi a „A személyek ellenőrzése” pontban foglalt, a személyek ellenőrzésére vonatkozó eljárást mielőtt logikai és fizikai hozzáférést engedélyez az újonnan használni kívánt elektronikus információs rendszerhez.

Az érintett szervezet szükség esetén elvégzi az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását vagy megszüntetését. Az érintett szervezet az általa meghatározott módon a jogviszony változásáról értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket.

**3.1.6.6. 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.

Az érintett szervezet szerződéses kötelezettségként megköveteli, hogy a szerződő fél feleljen meg az érintett szervezet által meghatározott személybiztonsági követelményeknek. Az érintett szervezet a szerződő féltől megköveteli, hogy dokumentálja a személybiztonsági követelményeket.

Az érintett szervezet 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 az soron kívül küldjön értesítést az érintett szervezetnek.

Az érintett szervezet folyamatosan ellenőrzi a szerződő féltől személybiztonsági követelményeknek való megfelelését.

**3.1.6.7. Fegyelmi intézkedések**

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

**3.1.6.8. 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.

**3.1.6.9. Viselkedési szabályok az interneten**

Az érintett szervezet tiltja és számon kéri:

* a szervezettel kapcsolatos információk nyilvános internetes oldalakon való illegális közzétételét,
* a belső szabályzatában meghatározott, interneten megvalósuló tevékenységet (pl.: chat, fájlcsere, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták, stb.),
* a közösségi oldalak használatát, magánpostafiók elérését, és más, a szervezettől idegen tevékenységet.

**3.1.7.1. Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és az e célt szolgáló ágazati szervezetekkel**

Az érintett szervezet kapcsolatot alakít ki és tart fenn az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével:

* az elektronikus információs rendszerhez hozzáféréssel rendelkező személyek folyamatos:oktatásának, képzésének elősegítése,
* az ajánlott elektronikus információbiztonsági eljárások, technikák és technológiák naprakészen tartása,
* a fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információk megosztása,

**3.1.7.2. 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. Az érintett szervezet a képzési eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a képzési eljárásrendet.

**3.1.7.3. 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.

**3.1.7.4. Belső fenyegetés**

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

**3.1.7.5. 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.

**3.1.7.6. 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.

**3.2.1.11. Vészvilágítás**

Az érintett szervezet egy automatikus vészvilágítási rendszert alkalmaz és tart karban, amely áramszünet esetén aktiválódik, és amely biztosítja a vészkijáratokat és a menekülési útvonalakat.

**Fizikai védelmi intézkedések**

**3.2.1.2. Fizikai védelmi eljárásrend**

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.

**3.2.1.3. 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 a belépési jogosultságot igazoló dokumentum visszavonása, érvénytelenítése, törlése, megsemmisítése iránt.

**3.2.1.4. A fizikai belépés ellenőrzése**

Az érintett szervezet:

* kizárólag a szervezet által meghatározott be-, és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést,
* naplózza a fizikai belépéseket, 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.

**3.2.1.5. 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.

**3.2.1.6. 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.

**3.2.1.7. 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,
* rendszeresen átvizsgálja a fizikai hozzáférésekről készült naplókat,
* azonnal átvizsgálja a fizikai hozzáférésekről készült naplókat, ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak,
* összehangolja a biztonsági események kezelését, valamint a napló átvizsgálások eredményét.

**3.2.1.7.2. Behatolás riasztás, felügyeleti berendezések**

Az érintett szervezet felügyeli a fizikai behatolás riasztásokat és a felügyeleti berendezéseket.

**3.2.1.8. A látogatók ellenőrzése**

Az érintett szervezet:

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

**3.2.1.9. Áramellátó berendezések és kábelezés**

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

**3.2.1.9.1. Tartalék áramellátás**

Az érintett szervezet az elsődleges áramforrás kiesése esetére, a tevékenységhez méretezett, rövid ideig működőképes szünetmentes áramellátást biztosít az elektronikus információs rendszer szabályos leállításához vagy a hosszútávú tartalék áramellátásra történő átkapcsoláshoz.

**3.2.1.10. Vészkikapcsolás**

Az érintett szervezet:

* lehetőséget biztosít az elektronikus információs rendszer vagy egyedi rendszerelemek áramellátásának kikapcsolására vészhelyzetben,
* gondoskodik a vészkikapcsoló berendezések biztonságos és könnyű megközelíthetőségéről,
* megakadályozza a jogosulatlan vészkikapcsolást.

**3.2.1.11. Vészvilágítás**

Az érintett szervezet egy automatikus vészvilágítási rendszert alkalmaz és tart karban, amely áramszünet esetén aktiválódik, és amely biztosítja a vészkijáratokat és a menekülési útvonalakat.

**3.2.1.12. Tűzvédelem**

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

**3.2.1.12.2. Automatikus tűzelfojtás**

Az érintett szervezet a személyzet által folyamatosan nem felügyelt elektronikus információs rendszerek számára automatikus tűzelfojtási képességet biztosít.

**3.2.1.13. Hőmérséklet és páratartalom ellenőrzés**

Az érintett szervezet az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl adatközpont, szerver szoba, központi gépterem) az erőforrások biztonságos működéséhez szükséges szinten tartja a hőmérsékletet és páratartalmat. Az érintett szervezet az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl adatközpont, szerver szoba, központi gépterem) figyeli a hőmérséklet és páratartalom szintjét.

**3.2.1.14. 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. Az érintett szervezet az informatikai erőforrásokat koncentráltan tartalmazó helyiségek tervezése (pl adatközpont, szerver szoba, központi gépterem) során biztosítja, hogy az a víz-, és más hasonló kártól védett legyen, akár csővezetékek kiváltásával, áthelyezésével is.

**3.2.1.15. Be- és kiszállítás**

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

**3.2.1.16. 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.

**3.2.1.17. Ellenőrzés**

Az érintett szervezet ellenőrzi a karbantartó személyzet által a létesítménybe hozott karbantartási eszközöket, a nem megfelelő vagy jogosulatlan módosítások megakadályozása érdekében.

**3.2.1.19. 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.

**3.2.1.19.3. Időben történő javítás**

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

**Logikai védelmi intézkedések**

**3.3.1. 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, amelyben:

* 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.

**3.3.1.2. Az elektronikus információbiztonsággal kapcsolatos engedélyezés** kiterjed minden, az érintett szervezet hatókörébe tartozó emberi, fizikai és logikai erőforrásra valamint az eljárási és védelmi szintre és folyamatra.

**3.3.1.3. Az elektronikus információs rendszer kapcsolódásai**

Az érintett szervezet a belső rendszer kapcsolatok

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

**3.3.1.3.3. Az érintett szervezet külső kapcsolódásokra vonatkozó korlátozásai**

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.

**3.3.1.4. 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).

**3.3.2.1. Biztonságtervezési szabályzat**

Az érintett szervezet megfogalmazza, az érintett szervezetre érvényes követelmények szerint dokumentálja, és a munka- és feladatkörük miatt érintettek számára kihirdeti a biztonságtervezési szabályzatot, amely tartalmazza a biztonságtervezési eljárás folyamatait, valamint biztosítja annak ellenőrzését valamint felügyeli az elektronikus információs rendszer és környezet biztonsági állapotát.

**3.3.2.2. Rendszerbiztonsági terv**

Az érintett szervezet, ha az elektronikus információs rendszer tervezése a hatókörébe tartozik, az elektronikus információs rendszerhez rendszerbiztonsági tervet készít, amely:

* összhangban áll szervezeti felépítésével vagy szervezeti szintű architektúrájával,
* meghatározza az elektronikus információs rendszer hatókörét, alapfeladatait (biztosítandó szolgáltatásait), biztonságkritikus elemeit és alapfunkcióit,
* meghatározza az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát,
* meghatározza az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait,
* a vonatkozó rendszerdokumentáció keretébe foglalja az elektronikus információs rendszer biztonsági követelményeit,
* meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedés bővítéseket, végrehajtja a jogszabály szerinti biztonsági feladatokat,
* gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és szerepkörökben dolgozók megismerjék (ideértve annak változásait is),
* belső szabályozásában, vagy a rendszerbiztonsági tervben meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszer rendszerbiztonsági tervét,
* 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,
* elvégzi a szükséges belső egyeztetéseket,
* gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

**3.3.2.3. Cselekvési terv**

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

**3.3.2.4. 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 valamint meghatározza az érintett szervezeten kívüli irányban megvalósuló követelményeket.

**3.3.2.5. Információbiztonsági architektúra leírás**

Az érintett szervezet (ha a hatókörébe tartozik, és ha más dokumentumban nem kerül meghatározásra, vagy azokból nem következik):

* elkészíti az elektronikus információs rendszer információbiztonsági architektúra leírását,
* az általános architektúrájában bekövetkezett változtatásokra reagálva felülvizsgálja, és frissíti az információbiztonsági architektúra leírást,
* biztosítja, hogy az információbiztonsági architektúra leírásban tervezett változtatás tükröződjön a rendszerbiztonsági tervben és a beszerzésekben.

**3.3.2.5.2. Az információbiztonsági architektúra leírás:**

* összegzi az elektronikus információs rendszer bizalmasságának, sértetlenségének és rendelkezésre állásának védelmét szolgáló filozófiát, követelményeket és megközelítést,
* megfogalmazza, hogy az információbiztonsági architektúra miként illeszkedik a szervezet általános architektúrájába, és hogyan támogatja azt,
* leírja a külső szolgáltatásokkal kapcsolatos információbiztonsági feltételezéseket és függőségeket.

**3.3.3.2. A rendszer fejlesztési életciklusa**

Az érintett szervezet elektronikus információs rendszereinek teljes életútján, azok minden életciklusában figyelemmel kíséri informatikai biztonsági helyzetüket. A fejlesztési életciklus egészére meghatározza és dokumentálja az információbiztonsági szerepköröket és felelősségeket, valamint meghatározza, és a szervezetre érvényes szabályok szerint kijelöli az információbiztonsági szerepköröket betöltő, felelős személyeket. A rendszer életciklus szakaszai a következők: követelmény meghatározás, fejlesztés vagy beszerzés, megvalósítás vagy értékelés, üzemeltetés és fenntartás, kivonás (archiválás, megsemmisítés).

**3.3.3.3. Funkciók, portok, protokollok, szolgáltatások**

Az érintett szervezet megköveteli, hogy a szolgáltató meghatározza a szolgáltatások igénybevételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat.

**3.3.3.4. Fejlesztői változáskövetés**

Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:

* vezesse végig a változtatásokat az elektronikus információs rendszer, rendszerelem vagy rendszer szolgáltatás tervezése, fejlesztése, megvalósítása, üzemeltetése során,
* dokumentálja, kezelje, és ellenőrizze a változtatásokat, biztosítsa ezek sértetlenségét,
* csak a jóváhagyott változtatásokat hajtsa végre az elektronikus információs rendszeren, rendszerelemen vagy rendszerszolgáltatáson,
* dokumentálja a jóváhagyott változtatásokat és ezek lehetséges biztonsági hatásait,
* kövesse nyomon az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás biztonsági hibáit és azok javításait, továbbá jelentse észrevételeit az érintett szervezet által meghatározott személyeknek.

**3.3.3.5. Fejlesztői biztonsági tesztelés**

Az érintett szervezet megköveteli, hogy az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője:

* készítsen biztonságértékelési tervet, és hajtsa végre az abban foglaltakat,
* hajtson végre (a fejlesztéshez illeszkedő módon) egység-, integrációs-, rendszer-, vagy regressziós tesztelést, és ezt értékelje ki az érintett szervezet által meghatározott lefedettség és mélység mellett,
* dokumentálja, hogy végrehajtotta a biztonságértékelési tervben foglaltakat, és ismertesse a biztonsági tesztelés és értékelés eredményeit,
* javítsa ki a biztonsági tesztelés és értékelés során feltárt hiányosságokat.

**3.3.4.1. Biztonságelemzési eljárásrend**

Az érintett szervezet:

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

**3.3.4.2. Biztonsági értékelések**

Az érintett szervezet:

* biztonságértékelési tervet készít,
* meghatározott gyakorisággal értékeli az elektronikus információs rendszer és működési környezete védelmi intézkedéseit, kontrollálja a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelő működését,
* elkészíti a biztonságértékelés eredményét összefoglaló jelentést,
* gondoskodik a biztonságértékelés eredményét összefoglaló jelentésnek az érintett szervezet által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismeréséről.

**3.3.4.2.2. A biztonsági értékelés tartalmazza:**

* az értékelendő (adminisztratív, fizikai és logikai) védelmi intézkedéseket,
* a biztonsági ellenőrzések eredményességét meghatározó eljárásrendeket,
* 3.3.4.2.2.3. az értékelési környezetet, az értékelő csoportot, az értékelés célját, az értékelést végzők feladatát.

**3.3.4.3. Speciális értékelés**

Az érintett szervezet a védelmi intézkedések értékelése keretében bejelentés mellett, vagy bejelentés nélkül sérülékenységvizsgálatot, rosszhiszemű felhasználó tesztet, belső fenyegetettség értékelést, a biztonságkritikus egyedi fejlesztésű szoftverelemek forráskód elemzését, az érintett szervezet által meghatározott egyéb biztonsági értékeléseket végeztet.

**3.3.4.4. A biztonsági teljesítmény mérése**

Az érintett szervezet kifejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét.

3.3.5. Tesztelés, képzés és felügyelet

Az érintett szervezet, ha ez hatókörébe tartozik, megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint kihirdeti az elektronikus információs rendszer tesztelésével, képzésével és felügyeletével kapcsolatos eljárásokat, amelyek támogatják a tesztelési, képzési és felügyeleti tevékenységek:

* fejlesztését és fenntartását,
* folyamatos időbeni végrehajtását,
* felülvizsgálja a tesztelési, képzési és ellenőrzési terveket a kockázatkezelési stratégia és a lehetséges, vagy bekövetkezett biztonsági események súlya alapján.

**3.3.5.2. A biztonsági teljesítmény mérése**

Az érintett szervezet kifejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét.

**3.3.5.3. Sérülékenység teszt**

Az érintett szervezet:

* az elektronikus információs rendszerei és alkalmazásai tekintetében sérülékenység tesztet végez, ha azt az elektronikus információs rendszerfejlesztési, üzemeltetési és használati körülményei lehetővé teszik,
* meghatározott gyakorisággal, vagy véletlenszerűen, valamint olyan esetben, amikor új lehetséges sérülékenység merül fel az elektronikus információs rendszerrel vagy alkalmazásaival kapcsolatban, megismétli a sérülékenység tesztet,
* a sérülékenység tesztet sérülékenységvizsgálati eszközök és technikák alkalmazásával, vagy külső szervezet bevonásával azon elektronikus információs rendszerek tekintetében végzi el, amelyek az érintett szervezet felügyelete, irányítása alatt állnak,
* kimutatást készít a feltárt hibákról, valamint a nem megfelelő konfigurációs beállításokról,
* végrehajtja az ellenőrzési listákat és tesztelési eljárásokat,
* felméri a sérülékenység lehetséges hatásait,
* elemzi a sérülékenység teszt eredményét,
* megosztja a sérülékenység teszt eredményét a szervezet által meghatározott személyekkel és szerepkörökkel.

**3.3.5.3.2. Frissítési képesség**

Az érintett szervezet olyan sérülékenységi teszteszközt alkalmaz, melynek sérülékenység feltáró képessége könnyen bővíthető az ismertté váló sérülékenységekkel.

**3.3.5.3.3. Frissítés időközönként, új vizsgálat előtt vagy új sérülékenység feltárását követően**

Az érintett szervezet az elektronikus információs rendszerre vizsgált sérülékenység körét aktualizálja az új tesztet megelőzően, vagy a sérülékenység feltárását követően azonnal.

**3.3.5.3.4. Privilegizált hozzáférés**

Az elektronikus információs rendszer különleges jogosultsághoz kötött - úgynevezett privilegizált - hozzáférést biztosít az érintett szervezet által kijelölt rendszerelemekhez a sérülékenység teszt végrehajtásához.

**3.3.5.3.5. Felfedhető információk**

Az érintett szervezet meghatározza, hogy egy támadó milyen információkat képes elérni az elektronikus információs rendszerben, és ennek elhárítására javításokat hajt végre.

**3.3.6.1. 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. Az érintett szervezet a fizikai védelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a konfigurációkezelési eljárásrendet.

**3.3.6.2. Alapkonfiguráció**

Az érintett szervezet az elektronikus információs rendszereihez egy-egy alapkonfigurációt fejleszt ki, dokumentálja és karbantartja ezt, valamint leltárba foglalja a rendszer lényeges elemeit.

**3.3.6.2.2. Áttekintések és frissítések**

Az alapkonfiguráció frissítését az elektronikus információs rendszerelemek telepítésének és frissítéseinek szerves részeként kell elvégezni.

**3.3.6.2.3. Korábbi konfigurációk megőrzése**

Változatlan állapotban meg kell őrizni az elektronikus információs rendszer alapkonfigurációját és annak további verzióit, hogy szükség esetén lehetővé váljon az erre való visszatérés.

**3.3.6.2.4. Magas kockázatú területek konfigurálása**

Biztonsági szempontokból meghatározott módon konfigurált elektronikus információs rendszerelemeket vagy eszközöket kell biztosítani azon személyek számára, akik az elektronikus információs rendszert külső helyszínen használják.

**3.3.6.3. A konfigurációváltozások felügyelete (változáskezelés)**

Az érintett szervezet:

* meghatározza a változáskezelési felügyelet alá eső változástípusokat,
* meghatározza az egyes változástípusok esetén a változáskezelési vizsgálat kötelező és nem kötelező elemeit, előfeltételeit (csatolt dokumentációk, teszt jegyzőkönyvek, stb.),
* megvizsgálja a változáskezelési felügyelet elé terjesztett, javasolt változtatásokat, majd kockázatelemzés alapján jóváhagyja vagy elutasítja azokat,
* dokumentálja az elektronikus információs rendszerben történt változtatásokra vonatkozó döntéseket,
* megvalósítja a jóváhagyott változtatásokat az elektronikus információs rendszerben,
* visszakereshetően megőrzi az elektronikus információs rendszerben megvalósított változtatások dokumentumait, részletes leírását,
* auditálja és felülvizsgálja a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységeket.

**3.3.6.3.2. Előzetes tesztelés és megerősítés**

A konfiguráció megváltoztatása előtt az új verziót tesztelni kell, ezután dönteni kell annak megfelelőségéről, továbbá dokumentálni kell az elektronikus információs rendszer változtatásait az éles rendszerben történő megvalósítása előtt.

**3.3.6.4. Biztonsági hatásvizsgálat**

Az érintett szervezet megvizsgálja az elektronikus információs rendszerben tervezett változtatásoknak az információbiztonságra való hatását, még a változtatások megvalósítása előtt.

**3.3.6.5. A változtatásokra vonatkozó hozzáférés korlátozások**

Az érintett szervezet az elektronikus információs rendszerre vonatkozóan szabályozásában meghatározza a változtatásokhoz való hozzáférési jogosultságot, dokumentálja a hozzáférési jogosultságokat, jóváhagyja azokat, fizikai és logikai hozzáférés korlátozásokat alkalmaz az elektronikus információs rendszer változtatásaival kapcsolatban.

**3.3.6.6. Konfigurációs beállítások**

Az érintett szervezet:

* meghatározza a működési követelményeknek még megfelelő, de biztonsági szempontból a lehető leginkább korlátozott módon - a "szükséges minimum" elv alapján - az elektronikus információs rendszerben használt információtechnológiai termékekre kötelező konfigurációs beállítást, és ezt ellenőrzési listaként dokumentálja,
* elvégzi a konfigurációs beállításokat az elektronikus információs rendszer valamennyi elemében,
* a meghatározott elemek konfigurációs beállításaiban azonosít, dokumentál és jóváhagy minden eltérést,
* figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait, az érintett szervezet belső szabályzataival és eljárásaival összhangban.

**3.3.6.7. 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.

**3.3.6.7.2. Rendszeres felülvizsgálat**

Az érintett szervezet meghatározott gyakorisággal átvizsgálja az elektronikus információs rendszert, meghatározza és kizárja, vagy letiltja a szükségtelen vagy nem biztonságos funkciókat, portokat, protokollokat és szolgáltatásokat. Az érintett szervezetnek a szoftver használatra meghatározott szabályzatainak vagy a szoftver használatára vonatkozó feltételeinek és kikötéseinek megfelelően az elektronikus információs rendszer megakadályozza a tiltott programok futtatását.

**3.3.6.7.3. Nem futtatható szoftverek**

Az érintett szervezet meghatározza, rendszeresen felülvizsgálja és frissíti az elektronikus információs rendszerben nem futtatható (tiltott, úgynevezett feketelistás) szoftverek listáját, és megtiltja ezek futtatását.

**3.3.6.8. Elektronikus információs rendszerelem leltár**

Az érintett szervezet leltárt készít az elektronikus információs rendszer elemeiről, valamint meghatározott gyakorisággal felülvizsgálja és frissíti az elektronikus információs rendszerelem leltárt továbbá gondoskodik arról, hogy a leltár:

* pontosan tükrözze az elektronikus információs rendszer aktuális állapotát,
* az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet tartalmazza,
* legyen kellően részletes a nyomkövetéshez és a jelentéskészítéshez,
* az érintett szervezet az elektronikus információs rendszerelem leltárt frissíti az egyes rendszerelemek telepítésének, eltávolításának, frissítésének időpontjában,
* automatizált mechanizmusok biztosítják, hogy a szervezet által meghatározott gyakorisággal a jogosulatlan hardver-, szoftver- és firmware elemek észlelése megtörténjen,
* a jogosulatlan elemek észlelése esetén le kell tiltani az ilyen elemek általi hálózati hozzáférést, el kell őket különíteni, és értesíteni kell az illetékes személyeket,
* az érintett szervezet ellenőrzi, hogy az elektronikus információs rendszer hatókörén belüli elemek nincsenek-e felvéve más elektronikus információs rendszerek leltárában.

**3.3.6.9. Konfigurációkezelési terv**

Az érintett szervezet:

* kialakít, dokumentál és végrehajt egy, az elektronikus információs rendszerre vonatkozó konfigurációkezelési tervet, mely figyelembe veszi a szerepköröket, felelősségeket, konfigurációkezelési folyamatokat és eljárásokat,
* bevezet egy folyamatot a konfigurációelemek azonosítására a rendszer-fejlesztési életciklus folyamán és a konfigurációelemek konfigurációjának kezelésére,
* meghatározza az elektronikus információs rendszer konfigurációelemeit, és a konfigurációelemeket a konfigurációkezelés alá helyezi,
* védi a konfigurációkezelési tervet a jogosulatlan felfedéssel és módosítással szemben.

**3.3.6.10. A szoftverhasználat 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 továbbá 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.

**3.3.6.11. 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 továbbá meghatározott gyakorisággal ellenőrzi a szabályok betartását.

**3.3.7.1.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.

**3.3.7.2. Rendszeres karbantartás**

Az érintett szervezet a karbantartásokat és javításokat ütemezetten hajtja végre, dokumentálja és felülvizsgálja a karbantartásokról és javításokról készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és a szervezeti követelményeknek megfelelően:

* 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,
* az ezért felelős személyek jóváhagyásához köti az elektronikus információs rendszer vagy a rendszerelemek kiszállítását a szervezeti létesítményből,
* az elszállítás előtt minden adatot és információt - mentést követően - töröl a berendezésről,
* ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat,
* csatolja a meghatározott, karbantartással kapcsolatos információkat a karbantartási nyilvántartáshoz.

**3.3.7.3. Karbantartási eszközök**

Az érintett szervezet az elektronikus információs rendszer vonatkozásában jóváhagyja, nyilvántartja, és ellenőrzi az elektronikus információs rendszer karbantartási eszközeit.

**3.3.7.4. Adathordozó ellenőrzése**

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

**3.3.7.4. 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.

**3.3.8.1. 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.

**3.3.8.2. Hozzáférés az adathordozókhoz**

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

**3.3.8.3. Adathordozók címkézése**

Az érintett szervezet megjelöli az elektronikus információs rendszer adathordozóit, jelezve az információra vonatkozó terjesztési korlátozásokat, kezelési figyelmeztetéseket és a megfelelő biztonsági jelzéseket, ha ezek rendelkezésre állnak.

**3.3.8.4. 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.

**3.3.8.5. 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.

**3.3.8.5.2. Kriptográfiai védelem**

Kriptográfiai mechanizmusokat kell alkalmazni a digitális adathordozókon tárolt információk bizalmasságának és sértetlenségének a védelmére az ellenőrzött területeken kívüli szállítás folyamán.

**3.3.8.6. 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.

**3.3.8.7. 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.

**3.3.8.7.2. Ismeretlen tulajdonos**

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

**3.3.9.1. 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.

**3.3.9.2. Azonosítás és hitelesítés**

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

**3.3.9.2.2. Hálózati hozzáférés privilegizált fiókokhoz**

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a különleges jogosultsághoz kötött - úgynevezett privilegizált - felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

**3.3.9.2.3. Hálózati hozzáférés nem privilegizált fiókokhoz**

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a nem privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

**3.3.9.2.4. Helyi hozzáférés privilegizált fiókokhoz**

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a privilegizált felhasználói fiókokhoz való helyi hozzáféréshez.

**3.3.9.2.5. Visszajátszás-védelem**

Az elektronikus információs rendszer visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

**3.3.9.2.6. Távoli hozzáférés - külön eszköz**

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a felhasználói fiókokhoz való távoli hozzáféréshez, és az egyik hozzáférést megelőző tényező egy, az elektronikus információs rendszertől elkülönülő olyan eszköz, amelyen a meghatározott biztonsági követelmények teljesülnek.

**3.3.9.2.7. Helyi hozzáférés nem privilegizált fiókokhoz**

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a nem privilegizált felhasználói fiókokhoz való helyi hozzáféréshez.

**3.3.9.2.8. Visszajátszás ellen védett hálózati hozzáférés nem privilegizált fiókokhoz**

Az elektronikus információs rendszer visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a nem privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

**3.3.9.3. Eszközök azonosítása és hitelesítése**

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a meghatározott eszközöket, vagy eszköz típusokat mielőtt helyi vagy távoli hálózati kapcsolatot létesítene velük.

**3.3.9.4. 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.

**3.3.9.5. A hitelesítésre szolgáló eszközök kezelése**

Az érintett szervezet:

* 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.

**3.3.9.5.2. Jelszó (tudás) alapú hitelesítés**

Az érintett szervezet:

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

**3.3.9.5.3. Birtoklás alapú hitelesítés**

Az érintett szervezet:

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:

* ellenőrzi a tanúsítványokat egy elfogadott megbízható pontig tartó tanúsítványlánc felépítésével és ellenőrzésével, beleértve a tanúsítvány állapot információ ellenőrzését is,
* kikényszeríti a megfelelő magánkulcshoz való jogosult hozzáférést,
* megvalósítja a visszavonási adatok helyi tárolását a tanúsítványlánc felépítésének és ellenőrzésének támogatására arra az esetre, amikor a visszavonási információk a hálózaton keresztül nem elérhetők.

**3.3.9.5.4. Tulajdonság alapú hitelesítés**

Az érintett szervezet a felhasználó egyedi azonosítást lehetővé tevő tulajdonságai alapján végzi el az azonosítást.

**3.3.9.5.5. 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.

**3.3.9.6. 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.

**3.3.9.7. Hitelesítés kriptográfiai modul esetén**

Az elektronikus információs rendszer egy adott kriptográfiai modulhoz való hitelesítésre olyan mechanizmusokat használ, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának.

**3.3.9.8. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)**

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

**3.3.9.8.2. Hitelesítésszolgáltatók tanúsítványának elfogadása**

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

**3.3.9.4. Azonosító kezelés**

Az érintett szervezet az egyéni-, csoport-, szerepkör- vagy eszközazonosítók kijelölését a szervezet által meghatározott személyek vagy szerepkörök jogosultságához köti, továbbá:

* hozzárendeli az azonosítót a kívánt egyénhez, csoporthoz, szerepkörhöz vagy eszközhöz,
* meghatározott időtartamig megakadályozza az azonosítók ismételt felhasználását,
* meghatározott időtartamú inaktivitás esetén letiltja az azonosítót.

**3.3.9.5. A hitelesítésre szolgáló eszközök kezelése**

Az érintett szervezet 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,
* valamint lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.

**3.3.9.6. 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.

**3.3.9.8. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)**

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

**3.3.9.8.2. Hitelesítésszolgáltatók tanúsítványának elfogadása**

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

**3.3.10.1. 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.

**3.3.10.2. Felhasználói fiókok kezelése**

Az érintett szervezet meghatározza és azonosítja az elektronikus információs rendszer felhasználói fiókjait és ezek típusait; továbbá:

* 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.

**3.3.10.2.2. Automatikus kezelés**

Az elektronikus információs rendszer automatizált mechanizmusokat alkalmaz az elektronikus információs rendszer fiókjainak kezeléséhez.

**3.3.10.2.3. Ideiglenes fiókok eltávolítása**

Meghatározott időtartam letelte után az elektronikus információs rendszer automatikusan eltávolítja vagy letiltja az ideiglenes vagy kényszerhelyzetben létrehozott felhasználói fiókokat vagy egyes kijelölt felhasználói fiók típusokat.

**3.3.10.2.4. Inaktív fiókok letiltása**

Az elektronikus információs rendszer automatikusan letiltja az inaktív fiókokat meghatározott időtartam letelte után.

**3.3.10.2.5. Automatikus naplózás**

Az elektronikus információs rendszer automatikusan naplózza a fiókok létrehozásával, módosításával, engedélyezésével, letiltásával és eltávolításával kapcsolatos tevékenységeket, és értesíti ezekről a meghatározott személyeket vagy szerepköröket.

**3.3.10.3. Hozzáférés ellenőrzés érvényesítése**

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

**3.3.10.4. Információáramlás ellenőrzés érvényesítése**

Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat a rendszeren belüli és a kapcsolódó rendszerek közötti információáramlás ellenőrzéséhez az érintett szervezet által meghatározott információáramlás ellenőrzési szabályoknak megfelelően.

**3.3.10.5. 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.

**3.3.10.6. 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.

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

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.

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

Privilegizált funkciók használatának naplózása: Az elektronikus információs rendszer naplózza a privilegizált funkciók végrehajtását.

Privilegizált funkciók tiltása nem privilegizált felhasználóknak: Az elektronikus információs rendszer megakadályozza, hogy a nem privilegizált felhasználók privilegizált funkciókat hajtsanak végre, ideértve a biztonsági ellenintézkedések kikapcsolását, megkerülését, vagy megváltoztatását.

**3.3.10.7. Sikertelen bejelentkezési kísérletek**

Az elektronikus információs rendszer:

* az érintett szervezet által meghatározott esetszám korlátot alkalmaz a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire,
* ha a sikertelen bejelentkezési kísérletekre felállított esetszám korlátot a felhasználó túllépi, automatikusan zárolja a felhasználói fiókot, vagy csomópontot meghatározott időtartamig, vagy meghatározott módon késlelteti a következő bejelentkezési kísérletet.

**3.3.10.8. A rendszerhasználat jelzése**

Az érintett szervezet az elektronikus információs rendszer felhasználásával az érintett szervezet által meghatározott rendszer használatra vonatkozó figyelmeztető üzenetet vagy jelzést küld a felhasználó számára a rendszerhez való hozzáférés engedélyezése előtt, mely jelzi, hogy:

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

Az elektronikus információs rendszer a figyelmeztető üzenetet vagy jelzést mindaddig a képernyőn tartja, amíg a felhasználó közvetlen műveletet nem végez az elektronikus információs rendszerbe való bejelentkezéshez vagy további rendszer hozzáféréshez.

Az elektronikus információs rendszer a nyilvánosan elérhető rendszerek esetén:

* kijelzi a rendszer használat feltételeit, mielőtt további hozzáférést biztosít,
* ha felügyelet, adatrögzítés vagy naplózás történik, kijelzi, hogy ezek megfelelnek az adatvédelmi szabályoknak,
* leírást biztosít a rendszer engedélyezett felhasználásáról.

**3.3.10.10. 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.

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

**3.3.10.11. A munkaszakasz lezárása**

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

**3.3.10.12. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek**

Az érintett szervezet:

* kijelöli azokat a felhasználói tevékenységeket, amelyeket az elektronikus információs rendszerben azonosítás vagy hitelesítés nélkül is végre lehet hajtani;
* dokumentálja és indokolja a rendszerbiztonsági tervben, vagy más szabályzatban az azonosítás vagy hitelesítés nélkül is végrehajtható felhasználói tevékenységeket.

3.3.10.13. Távoli hozzáférés

Az érintett szervezet:

* kidolgozza és dokumentálja minden engedélyezett távoli hozzáférés típusra a felhasználásra vonatkozó korlátozásokat, a konfigurálási vagy a kapcsolódási követelményeket és a megvalósítási útmutatókat,
* engedélyezési eljárást folytat le az elektronikus információs rendszerhez történő távoli hozzáférés feltételeként.

**3.3.10.13.2. Ellenőrzés**

Az elektronikus információs rendszer figyeli és ellenőrzi a távoli hozzáféréseket.

**3.3.10.13.3. Titkosítás**

Kriptográfiai mechanizmusokat kell alkalmazni a távoli hozzáférés munkaszakaszok bizalmasságának és sértetlenségének a védelmére.

**3.3.10.13.4. Hozzáférés ellenőrzési pontok**

Minden távoli hozzáférést felügyelt hozzáférés ellenőrzési ponton keresztül kell irányítani az elektronikus információs rendszerben.

**3.3.10.13.5. Privilegizált parancsok elérése**

Az érintett szervezet:

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

**3.3.10.14. 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.

**3.3.10.12. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek**

Az érintett szervezet kijelöli azokat a felhasználói tevékenységeket, amelyeket az elektronikus információs rendszerben azonosítás vagy hitelesítés nélkül is végre lehet hajtani valamint dokumentálja és indokolja a rendszerbiztonsági tervben, vagy más szabályzatban az azonosítás vagy hitelesítés nélkül is végrehajtható felhasználói tevékenységeket.

**3.3.10.13. Távoli hozzáférés**

Az érintett szervezet kidolgozza és dokumentálja minden engedélyezett távoli hozzáférés típusra a felhasználásra vonatkozó korlátozásokat, a konfigurálási vagy a kapcsolódási követelményeket és a megvalósítási útmutatókat. Az érintett szervezet engedélyezési eljárást folytat le az elektronikus információs rendszerhez történő távoli hozzáférés feltételeként.

**3.3.10.14. 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, valamint engedélyezési eljárást folytat le a vezeték nélküli hozzáférés feltételeként.

**3.3.10.15. 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, illetve engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást.

**3.3.10.15.2. 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.

**3.3.10.16. 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 továbbá meghatározza, hogy külső elektronikus információs rendszerek segítségével hogyan jogosult a felhasználó feldolgozni, tárolni vagy továbbítani az érintett szervezet által ellenőrzött információkat.

**3.3.10.16.2. 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.

**3.3.10.16.3. Hordozható adattároló eszközök**

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

**3.3.10.17. Információmegosztás**

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.

**3.3.10.18. 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 a kijelölt személyeket képzésben részesíti annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános információkat. Az érintett szervezet a közzététel előtt átvizsgálja a javasolt tartalmat valamint meghatározott gyakorisággal átvizsgálja a nyilvánosan hozzáférhető elektronikus információs rendszertartalmat a nem nyilvános információk tekintetében, és eltávolítja azokat.

**3.3.11.2. Rendszer- és információsértetlenségre 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.

**3.3.11.3. 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.

**3.3.11.3.2. Automatizált hibajavítási állapot**

Az érintett szervezet automatizált mechanizmusokat alkalmaz az elektronikus információs rendszer elemei hibajavítási állapotának meghatározására.

**3.3.11.4. Kártékony kódok elleni védelem**

Az érintett szervezet azelektronikus 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.

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

**3.3.11.5. 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.

**3.3.11.5.2. Automatizálás**

Automatizált eszközöket kell alkalmazni az események közel valós idejű vizsgálatának támogatására.

**3.3.11.5.3. Felügyelet**

Az elektronikus információs rendszer felügyelje a beérkező és kimenő adatforgalmat a szokatlan vagy jogosulatlan tevékenységekre vagy körülményre tekintettel.

**3.3.11.5.4. Riasztás**

Az elektronikus információs rendszer riassza az érintett szervezet illetékes személyeit, csoportjait, amikor veszélyeztetés vagy lehetséges veszélyeztetés előre meghatározott jeleit észleli.

**3.3.11.6. 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.

**3.3.11.8. Szoftver- és információsértetlenség**

Az érintett szervezet sértetlenség ellenőrző eszközt alkalmaz a szoftverek és információk jogosulatlan módosításának észlelésére.

**3.3.11.9. Kéretlen üzenetek elleni védelem**

Az érintett szervezet:

* kéretlen üzenetek - úgynevezett levélszemét - elleni védelmet valósít meg az elektronikus információs rendszer belépési és kilépési pontjain, a levélszemét észlelése és kiszűrése érdekében,
* új verziók elérhetővé válásakor frissíti a levélszemét elleni védelmi mechanizmusokat, összhangban a konfigurációkezelési szabályzattal és eljárásrenddel.

**3.3.11.9.2. Központi kezelés**

Az érintett szervezet központi beállításokkal irányítja a levélszemét elleni védelmet.

**3.3.11.9.3. Frissítés**

Az elektronikus információs rendszer automatikusan frissíti a levélszemét elleni védelmi mechanizmusokat azok újabb verzióival.

**3.3.11.10. Bemeneti információ ellenőrzés**

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

**3.3.11.11. Hibakezelés**

Az elektronikus információs rendszer:

* hibajelzéseket generál a hibajavításhoz szükséges információkat biztosítva, ugyanakkor nem nyújt semmi olyan információt, amelyet a támadók kihasználhatnak,
* a hibajelzéseket kizárólag a meghatározott személyek vagy szerepkörök számára teszi elérhetővé.

**3.3.11.12. 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.

**3.3.12.1. Naplózási eljárásrend**

Az érintett szervezet megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül a szabályozásában meghatározott személyek vagy szerepkörök számára kihirdeti a naplózási eljárásrendet, mely a naplózásra és elszámoltathatóságra vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő. A naplózásra és elszámoltathatóságra vonatkozó eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja, és frissíti a naplózási eljárásrendet.

**3.3.12.2. Naplózható események**

Az érintett szervezet meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét valamint egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő szervezeti egységgel, hogy növelje a kölcsönös támogatást, és hogy iránymutatással segítse a naplózható események kiválasztását. Megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

**3.3.12.3. Naplóbejegyzések tartalma**

Az elektronikus információs rendszer a naplóbejegyzésekben gyűjtsön be elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele. Az elektronikus információs rendszer a naplóbejegyzésekben további, az érintett szervezet által meghatározott kiegészítő, részletesebb információkat is rögzít.

**3.3.12.4. Napló tárkapacitás**

Az érintett szervezet a naplózásra elegendő méretű tárkapacitást biztosít, a biztonsági osztályba sorolásból következő naplózási funkciók figyelembevételével.

**3.3.12.5. Naplózási hiba kezelése**

Az elektronikus információs rendszer naplózási hiba esetén riasztást küld a meghatározott személyeknek vagy szerepköröknek, aki elvégzi a meghatározott végrehajtandó tevékenységeket, így például a rendszer leállítását, a legrégebbi naplóbejegyzések felülírását, a naplózási folyamat leállítását.

**3.3.12.6. Naplóvizsgálat és jelentéskészítés**

Az érintett szervezet rendszeresen felülvizsgálja és elemzi a naplóbejegyzéseket nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából, illetve jelenti ezeket a meghatározott személyeknek vagy szerepköröknek. Az érintett szervezet automatikus mechanizmusokat használ a naplóbejegyzések vizsgálatának, elemzésének és jelentésének átfogó folyamattá integrálására, amely a veszélyes, vagy tiltott tevékenységekre és történésekre reagál. Az érintett szervezet megvizsgálja és összefüggésbe hozza a különböző adattárakban található naplóbejegyzéseket, a teljes érintett szervezetre kiterjedő helyzetfelmérés érdekében.

**3.3.12.7. Naplócsökkentés és jelentéskészítés**

Az elektronikus információs rendszer:

* lehetőséget biztosít naplócsökkentésre és jelentés készítésére, amely támogatja az igény esetén végzendő naplóáttekintési, naplóvizsgálati és jelentéskészítési követelményeket és a biztonsági eseményeket követő tényfeltáró vizsgálatait,
* nem változtathatja meg a naplóbejegyzések eredeti tartalmát és időrendjét.

**3.3.12.7.2. Automatikus feldolgozás**

Az elektronikus információs rendszer biztosítja, hogy a fontos naplóbejegyzéseket automatikusan fel lehessen dolgozni.

**3.3.12.8. Időbélyegek**

Az elektronikus információs rendszer a belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához. Időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz - úgynevezett UTC - vagy a Greenwichi középidőhöz - úgynevezett GMT - rendelhető módon, megfelelve az érintett szervezet által meghatározott időmérési pontosságnak. Az elektronikus információs rendszer meghatározott gyakorisággal összehasonlítja a belső rendszerórákat egy hiteles külső időforrással, és ha az időeltérés nagyobb, mint a meghatározott időtartam, szinkronizálja a belső rendszerórákat a hiteles külső időforrással.

**3.3.12.9. A naplóinformációk védelme**

Az elektronikus információs rendszer megvédi a naplóinformációt és a napló kezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben. A naplófunkciók kezelésére csak az érintett szervezet által meghatározott, privilegizált felhasználók jogosultak.

**3.3.12.11. A naplóbejegyzések megőrzése**

Az érintett szervezet a naplóbejegyzéseket meghatározott - a jogszabályi és az érintett szervezeten belüli információ megőrzési követelményeknek megfelelő - időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

**3.3.12.12. Naplógenerálás**

Az elektronikus információs rendszer:

* biztosítja a naplóbejegyzés generálási lehetőségét a naplózandó valamint a naplózható események tekintetében,
* lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az elektronikus információs rendszer egyes elemeire, naplóbejegyzéseket állít elő meghatározott tartalommal.

**3.3.13.1. Rendszer- és kommunikációvédelmi eljárásrend**

Az érintett szervezet megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belüli szabályozásában meghatározott személyek vagy szerepkörök számára kihirdeti a rendszer- és kommunikációvédelmi eljárásrendet, mely a rendszer- és kommunikációvédelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. A rendszer- és kommunikációvédelmi eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja, és frissíti a rendszer- és kommunikációvédelmére vonatkozó eljárásrendet.

**3.3.13.2. Alkalmazás szétválasztás**

Az elektronikus információs rendszer elkülöníti a felhasználók által elérhető funkcionalitást (beleértve a felhasználói felület szolgáltatásokat) az elektronikus információs rendszer irányítási funkcionalitásától.

**3.3.13.4. Információmaradványok**

Az elektronikus információs rendszer meggátolja a megosztott rendszererőforrások útján történő jogosulatlan vagy véletlen információáramlást.

**3.3.13.5. Túlterhelés - szolgáltatás megtagadás alapú támadás - elleni védelem**

Az elektronikus információs rendszer véd a túlterheléses (úgynevezett szolgáltatás megtagadás) jellegű támadásokkal szemben, vagy korlátozza azok kihatásait a megtagadás jellegű támadások listája alapján, a meghatározott biztonsági intézkedések bevezetésével.

**3.3.13.6. A határok védelme**

Az elektronikus információs rendszer:

* felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt,
* a nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól,
* csak az érintett szervezet biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.

**3.3.13.6.2. Hozzáférési pontok**

Az érintett szervezet korlátozza az elektronikus információs rendszer külső hálózati kapcsolatainak a számát.

**3.3.13.6.3. Külső kommunikációs szolgáltatások**

Az érintett szervezet:

* felügyelt interfészt működtet minden külső infokommunikációs szolgáltatáshoz,
* minden felügyelt interfészhez forgalomáramlási szabályokat alakít ki,
* védi az összes interfésznél az átvitelre kerülő információk bizalmasságát és sértetlenségét,
* dokumentál minden kivételt a forgalomáramlási szabályok alól, a kivételt alátámasztó alapfeladattal és az igényelt kivétel időtartamával együtt,
* meghatározott gyakorisággal áttekinti a forgalomáramlási szabályok alóli kivételeket, és eltávolítja azokat a kivételeket, amelyeket közvetlen alapfeladat már nem indokol.

**3.3.13.6.4. Alapeseti visszautasítás**

Az elektronikus információs rendszer a felügyelt kapcsolódási pontjain tilt, és csak kivételként engedélyez hálózati forgalmat.

**3.3.13.6.5. Távoli készülékek megosztott csatornahasználatának tiltása**

A távoli készülékkel kapcsolatban álló elektronikus információs rendszer meggátolja, hogy a készülék egyidejűleg helyi kapcsolatokat létesítsen a rendszerrel.

**3.3.13.7. Az adatátvitel bizalmassága**

Az elektronikus információs rendszer védje meg a továbbított információk bizalmasságát.

**3.3.13.7.2. Kriptográfiai vagy egyéb védelem**

Az elektronikus információs rendszer kriptográfiai mechanizmusokat alkalmaz az adatátvitel során az információk jogosulatlan felfedése ellen, kivéve, ha az átvitel más, az érintett szervezet által meghatározott alternatív fizikai ellenintézkedéssel védett.

**3.3.13.8. Az adatátvitel sértetlensége**

Az elektronikus információs rendszer megvédi a továbbított információk sértetlenségét.

Kriptográfiai vagy egyéb védelem: az elektronikus információs rendszer kriptográfiai mechanizmusokat alkalmaz az adatátvitel során az információk megváltozásának észlelésére, ha az átvitel nincsen más alternatív fizikai intézkedésekkel védve.

**3.3.13.9. A hálózati kapcsolat megszakítása**

Az elektronikus információs rendszer megszakítja a hálózati kapcsolatot egy munkaszakaszra épülő kétirányú adatcsere befejezésekor, meghatározott időtartamú inaktivitás után.

**3.3.13.10. Kriptográfiai kulcs előállítása és kezelése**

Az érintett szervezet előállítja és kezeli az elektronikus információs rendszerben alkalmazott kriptográfiához szükséges kriptográfiai kulcsokat a kulcsok előállítására, szétosztására, tárolására, hozzáférésére és megsemmisítésére vonatkozó belső szabályozásnak megfelelően.

**3.3.13.11. Kriptográfiai védelem**

Az elektronikus információs rendszer szabványos, egyéb jogszabályokban biztonságosnak minősített kriptográfiai műveleteket valósít meg.

**3.3.13.12. Együttműködésen alapuló számítástechnikai eszközök**

Az elektronikus információs rendszer meggátolja az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha az érintett szervezet engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.

**3.3.13.13. Nyilvános kulcsú infrastruktúra tanúsítványok**

Az érintett szervezet nyilvános kulcsú tanúsítványokat állít ki a belső hitelesítési rend szerint, vagy a nyilvános kulcsú tanúsítványokat beszerzi a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatótól.

**3.3.13.14. Mobilkód korlátozása**

Az érintett szervezet:

* meghatározza az elfogadható és a nem elfogadható mobilkódokat és mobilkód technológiákat,
* használati korlátozásokat vezet be vagy megvalósítási útmutatót bocsát ki az elfogadható mobilkódokra és mobilkód technológiákra,
* engedélyezi, felügyeli és ellenőrzi a mobilkódok használatát az elektronikus információs rendszeren belül.

**3.3.13.15. Elektronikus információs rendszeren keresztüli hangátvitel (úgynevezett VoIP)**

Az érintett szervezet:

* használati korlátozásokat vezet be vagy megvalósítási útmutatót ad a VoIP technológiákhoz, felmérve a rosszindulatú használat esetén az elektronikus információs rendszerben okozható károkat,
* engedélyezi, felügyeli, és ellenőrzi a VoIP használatát az elektronikus információs rendszeren belül.

**3.3.13.16. Biztonságos név/cím feloldó szolgáltatások (úgynevezett hiteles forrás)**

Az elektronikus információs rendszer a név/cím feloldási kérésekre a hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozó kiegészítő adatokat is biztosít, és ha egy elosztott, hierarchikus névtár részeként működik, akkor jelzi az utódtartományok biztonsági állapotát is, és (ha azok támogatják a biztonságos feloldási szolgáltatásokat) hitelesíti az utód- és elődtartományok közötti bizalmi láncot.

**3.3.13.17. Biztonságos név/cím feloldó szolgáltatás** (úgynevezett rekurzív vagy gyorsító tárat használó feloldás)

Az elektronikus információs rendszer eredethitelesítést és adatsértetlenség ellenőrzést kér és hajt végre a hiteles forrásból származó név/cím feloldó válaszokra.

**3.3.13.18. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén**

Azok az elektronikus információs rendszerek, amelyek együttesen biztosítanak név/cím feloldási szolgáltatást egy szervezet számára, hibatűrők és belső/külső szerepkör szétválasztást valósítanak meg.

**3.3.13.19. Munkaszakasz hitelessége**

Az elektronikus információs rendszer védje meg a munkaszakaszok hitelességét.

**3.3.13.21. A maradvány információ védelme**

Az elektronikus információs rendszer védi az érintett szervezet által meghatározott maradvány információk (pl.: átmeneti fájlok) bizalmasságát, sértetlenségét.

**3.3.13.22. A folyamatok elkülönítése**

Az elektronikus információs rendszer elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára.