BAJAI
SZENT RÓKUS
KÓRHÁZ
1795

Bajai Szent Rókus Kórház
6500 Baja, Rókus u. 10.
Tel.: 79/422-233, Fax: 79/425-575

MŰKÖDÉSI SZABÁLYZAT

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

TARTALOM

1. ÁLTALÁNOS RENDELKEZÉS

1.1 A szabályzat célja

A szabályzat célja meghatározni a Bajai Szent Rókus Kórház (a továbbiakban: BSZRK) informatikai biztonsággal kapcsolatban támasztott elvárásait és az egyes információbiztonsági területeken elvégezni a szükséges feladatokat, ellenőrzéseket annak érdekében, hogy a BSZRK informatikai infrastruktúrája, elektronikus információs rendszerei (a továbbiakban EIR) és rendszerelemei, valamint az azokban tárolt, kezelt adat, információ bizalmassága, integritása és rendelkezésre állása megfelelő szintű legyen.

A BSZRK döntése alapján a BSZRK-nak Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 7/2024. (VI. 24.) MK rendeletben meghatározott jelentős szintnek megfelelő védelmi osztály követelményeit kell teljesítenie, és ezzel összhangban a BSZRK EIR-einek biztonsági osztályát is e rendelet alapján kell meghatározni.

1.2 A szabályzat hatálya

1.2.1 Szervezeti hatály

A szabályzat szervezeti hatálya a BSZRK valamennyi szervezeti egységére kiterjed.

1.2.2 Személyi hatály

A szabályzat személyi hatálya a BSZRK-val jogviszonyban álló természetes és jogi személyekre terjed ki; különösen azokra, akik kapcsolatba kerülnek, vagy kapcsolatba szándékoznak kerülni a BSZRK informatikai architektúrájával, EIR-ivel (használják, fejlesztik, telepítik, üzemeltetik, javítják stb. azokat), így:

- a BSZRK által foglalkoztatottakra,
- a BSZRK-val szerződéses kapcsolatban álló természetes és jogi személyekre,
- illetve az BSZRK informatikai rendszereihez hozzáférő személyekre (például az ellenőrző hatóságok képviselői).

A szabályzatban megadott szervezeti egységek és szerepkörök rövidítése a következő:

- Főigazgató: továbbiakban: FI
- Orvos-igazgató (Főigazgató-helyettes): továbbiakban: FIH
- Gazdasági igazgató: továbbiakban: GI,
- Intézeti jogász: IJ
- Munkaügyi csoport: MO
- Munkaügyi csoport koordinátor: MOV
- Informatikai Csoport: továbbiakban: ICS,
- Informatikai csoport koordinátor: továbbiakban: ICSV,
- Elektronikus információbiztonsági felelős: továbbiakban: IBF
- Belső ellenőr: továbbiakban: BE
- Adatvédelmi tisztviselő: továbbiakban: DPO,

Ahol a szabályzatban szervezeti vezető (pl. ICSV) került meghatározásra felelősként, feladat végrehajtójaként, közreműködőként stb., ott a vezető külön jelzés nélkül is delegálhatja a feladatot, annak végrehajtását, közreműködést az általa irányított foglalkoztatottak vagy külső támogatók számára (amennyiben a velük kötött szerződés és a BSZRK erőforrásai erre lehetőséget adnak)

1.2.3 Tárgyi hatály

A szabályzat tárgyi hatálya kiterjed a BSZRK informatikai architektúrájára, EIR-eire, beleértve az azokat alkotó

- környezeti infrastruktúra elemeire,
- hardver elemekre, készülékekre, berendezésekre, eszközökre és azok beállításaira,
- szoftver elemekre és azok beállításaira,
- dokumentáció elemekre,

valamint az BSZRK informatikai architektúrájában, EIR-eiben kezelt adatokkal összefüggésben használt bármilyen adatrögzítésre, tárolásra, feldolgozásra vagy továbbításra képes EIR-re és ezek működési környezetére.

A tárgyi hatály kiterjed továbbá az ezen rendszerek működéséhez alkalmazott szoftverekre, illetve az ezekkel rögzített, tárolt, feldolgozott vagy továbbított adatokra és információkra.

1.2.4 Területi hatály

A szabályzat területi hatálya kiterjed a BSZRK székhelyére, telephelyére, valamint valamennyi földrajzi lokációra, ahol a BSZRK informatikai architektúrája, EIR-ei használatra kerülnek.

1.2.5 Időbeli hatály

A szabályzat az aláírás napján lép hatályba, és határozatlan időre kerül kiadásra. A szabályzat kiadását követően bevezetett rendszereknek, telepített informatikai rendszerelemeknek, végrehajtott beállításoknak, kialakított folyamatoknak a szabályzatban elvárt követelményeknek a bevezetés, telepítés, beállítás, kialakítás idején (azaz üzembe állításkor) meg kell felelniük. A szabályzat kiadása idején üzemelő rendszerek, rendszerelemek, alkalmazott beállítások és folyamatok megfelelőségét a szabályzat kiadását követő fél éven belül az adott rendszerért, rendszerelemért, beállításért, folyamatért felelős informatikusnak fel kell mérnie és a nem megfelelésről tájékoztatnia kell az ICSV-t és az IBF-et, akik a nem megfelelések kezelésére intézkedési tervet készítenek a szabályzat kiadását követő hat hónapon belül.

A szabályzat kiadását követő két éven belül meg kell szüntetni a nem megfelelőségeket, vagy (kockázatértékelést és kockázatkezelő intézkedések bevezetését követően) az FI által elfogadni azokat.

A szabályzatban előírt dokumentumokat, nyilvántartásokat, cselekvési terveket a szabályzat kiadását követő fél éven belül kell elkészítenie az adott feladat felelősének.

1.3 A szabályzat felülvizsgálata

A szabályzatot legalább évente egy alkalommal felül kell vizsgálni.

A szabályzat módosítására van szükség, ha a BSZRK, vagy a BSZRK informatikai architektúrájának, EIR-einek működését meghatározó jogszabályi környezetben jelentős változások következnek be.

A szabályzat eseti módosítása szükséges, ha a benne szereplő adatok megváltoztak, vagy ha a szabályzat olyan kisebb mértékű kiegészítésre szorul, amely nem érinti az aktuális biztonsági követelményeket.

A szabályzat eseti módosítását, felülvizsgálatát a FI, FIH, GI, IJ, ICSV és az IBF kezdeményezheti.

A szabályzat felülvizsgálatát az IBF koordinálja, akit ebben a tevékenységében az ICSV támogat.

A szabályzat függelékeinek módosítása nem eredményezi a szabályzat módosítását, azok önállóan módosíthatók.

1.4 Hatásköri és Illetékességi szabályok

A szabályzat belső használatú dokumentum: a BSZRK által foglalkoztatottak, illetve egyéb érintettek (a BSZRK-val szerződéses kapcsolatban álló természetes és jogi személyek, más Szervezetek képviseletében az BSZRK által kontrollált területen tartózkodó személyek) megismerhetik és kezelhetik, de illetéktelenekneknek nem adhatják tovább és tartalmát illetéktelenekkel nem oszthatják meg.

A BSZRK valamennyi foglalkoztatottja és szerződött partnere köteles végrehajtani a számára kötelező feladatokat, és kerülni a szabályzatban számára tiltott tevékenységeket.

A BSZRK valamennyi foglalkoztatottja és szerződött partnere köteles támogatni a szabályzatban meghatározott ellenőrzéseket és az azokat végző személyeket.

1.5 Kapcsolódó dokumentumok

2024. évi LXIX. törvény

418/2024. (XII. 23.) Korm. rendelet

7/2024. (VI. 24.) MK rendelet

2023. évi CIII. törvény

(EU) 2019/881 európai parlamenti és tanácsi rendelet

339/93/EGK rendelet

765/2008/EK

(EU) 2021/241 európai parlamenti és tanácsi rendelet

(EU) 2021/1060 európai parlamenti és tanácsi rendelet

1025/2012/EU rendelet

(EU) 2022/2555 európai parlamenti és tanácsi irányelv

(EU) 2019/1150 európai parlamenti és tanácsi rendelet

1025/2012/EU rendelet

Polgári Törvénykönyvről szóló törvény

2. ALAPFOGALMAK

2024. évi LXIX. törvény definiált a szabályzatban használt fogalmak:

adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;

adatfeldolgozás: az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;

adatfeldolgozó: az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;

adatkezelés: az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;

adatkezelő: az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;

adatkicserélő szolgáltatás: az elektronikus hírközlésről szóló törvény szerinti fogalom;

adatközponti szolgáltatás: olyan szolgáltatás, amely központosított elhelyezést, összeköttetést és működést biztosít adattároló, -feldolgozó és -továbbító információtechnológiai és hálózati berendezések számára, ideértve az energiaellátást és környezeti felügyeletet biztosító létesítményeket és infrastruktúrát is;

adatosztályozás: a szervezet által az elektronikus információs rendszerben kezelt adatok és információk biztonsági besorolása azok bizalmasságának, sértetlenségének és rendelkezésre állásának szempontjából;

ágazaton belüli kiberbiztonsági incidenskezelő központ: olyan kiberbiztonsági incidenskezelő központ, amelyet az e törvény hatálya alá tartozó egy vagy több, egy ágazathoz tartozó szervezet az ágazaton belül meghatározott szakterületen előforduló kiberbiztonsági incidenseinek a központosított és egységes kezelése érdekében üzemeltet;

auditor: az e törvény szerinti kiberbiztonsági audittevékenység végzésére jogosult, független gazdálkodó szervezet;

behatolásvizsgálat: olyan sérülékenységvizsgálati módszer, amelynek során az IKT-rendszer, valamint az elektronikus információs rendszer gyenge pontjainak feltárására és kihasználhatóságának ellenőrzésére kerül sor a biztonsági intézkedések elleni rosszindulatú támadások szimulációjával;

belső informatikai biztonsági vizsgálat: olyan sérülékenységvizsgálati módszer, amelynek során az informatikai rendszer sérülékenységvizsgálata a belső hálózati végpontról közvetlenül történik, vagy a belső hálózatban használt eszköz, vagy rendszerelem vizsgálata kerül végrehajtásra;

bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

bizalmi szolgáltatás: a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

bizalmi szolgáltató: a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége;

biztonsági osztályba sorolás: a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;

digitális szolgáltatás: a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

DNS: hierarchikusan felépülő elnevezési rendszer, más néven doménnévrendszer, amely lehetővé teszi az internetes szolgáltatások és erőforrások azonosítását, lehetővé téve a végfelhasználók eszközei számára az internetes útvonal-meghatározási és összekapcsolási szolgáltatások igénybevételét e szolgáltatások és erőforrások elérése érdekében;

DNS-szolgáltató: olyan szervezet, amely a következő szolgáltatások valamelyikét nyújtja a szervezeten kívüli más szervezet vagy személy részére:

- *autoritatív DNS-szolgáltatás*: a doménnév – doménnév-regisztrációt végző szolgáltató által kezelt – adatainak lekérdezését közvetlenül lehetővé tevő szolgáltatás, amely a legfelső szintű doménnév-nyilvántartó szolgáltatás része,

- *rekurzív DNS-szolgáltatás*: olyan DNS-szolgáltatás, amely a felhasználók doménnév-lekérdezéseit a megfelelő autoritatív DNS-szolgáltatókhoz továbbítja a hierarchikusan felépülő doménnévrendszerben és az autoritatív DNS-szolgáltató által a lekérdezésre adott válaszokat továbbítja a felhasználó részére,

- *DNS-gyorsítótárazás*: a doménnév-lekérdezésre adott válaszok átmeneti tárolása és a felhasználói lekérdezéseknek a tárolt doménnévadatok alapján történő kiszolgálása,

doménnév: az internetes kommunikációhoz használt IP-cím alfanumerikus karakterekből álló megfelelője,

doménnév-regisztrációt végző szolgáltató: a legfelső szintű doménnév-nyilvántartó által felhatalmazott szolgáltató, amely jogosult domén regisztrálására;

elektronikus hírközlési szolgáltató: az elektronikus hírközlésről szóló törvény szerinti fogalom;

elektronikus információs rendszer:

- az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlési hálózat,

- minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi, ideértve a kiber-fizikai rendszereket, vagy

- korábbi alpontokban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;

elektronikus információs rendszer biztonsága: az elektronikus információs rendszerek azon képessége, hogy adott bizonyossággal ellenálljanak minden olyan eseménynek, amely veszélyeztetheti a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát;

életciklus: az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;

esemény: az elektronikus információs rendszerben bekövetkezett állapotváltozás;

felhőszolgáltatás: olyan digitális szolgáltatás, amely önkiszolgáló módon történő hálózati hozzáférést tesz lehetővé igény szerint méretezhető, megosztott fizikai vagy virtuális erőforrások rugalmas készletéhez;

felhőszolgáltató: felhőalapú számítástechnikai szolgáltatást nyújtó szervezet;

használatbavétel: az elektronikus információs rendszer adatokkal való feltöltése és rendeltetésszerű használatának megkezdése;

ideiglenes hozzáférhetetlenné tétel: az elektronikus adathoz való hozzáférés ideiglenes megakadályozása;

jelentős kiberbiztonsági incidens:

- a közvetlenül alkalmazandó európai uniós jogi aktusban ekként meghatározott kiberbiztonsági incidens,
- közvetlenül alkalmazandó európai uniós jogi aktus hiányában az olyan kiberbiztonsági incidens, amely
- a szervezet üzleti szolgáltatásának vagy a szervezet által nyújtott szolgáltatásnak legalább 5%-os csökkenésével vagy a szervezet éves bevételének legalább 5%-os kiesésével jár vagy fenyeget;
- súlyos működési zavart okoz vagy képes okozni a szolgáltatásokban, vagy pénzügyi vagy reputációs veszteséget okoz vagy képes okozni a kiberbiztonsági incidens által érintett szervezetnek vagy személynek; vagy
- jelentős vagyoni vagy nem vagyoni kár okozásával más természetes vagy jogi személyeket érintett, vagy képes érinteni;

jelentős kiberfenyegetés: olyan kiberfenyegetés, amelyről – technikai jellemzői alapján – feltételezhető, hogy jelentős vagyoni vagy nem vagyoni hátrányt vagy kárt okozva súlyos hatást gyakorolhat egy szervezet elektronikus információs rendszereire vagy a szervezet szolgáltatásainak felhasználóira;

képviselő: Magyarországon letelepedett minden olyan természetes vagy jogi személy, akit vagy amelyet kifejezetten kijelöltek arra, hogy valamely, Magyarországon nem letelepedett szervezet nevében eljárjon, és akihez vagy amelyhez a kiberbiztonsági hatóság, vagy a kiberbiztonsági incidenskezelő központ az adott szervezet helyett fordulhat;

kiberbiztonság: az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 1. pontjában meghatározott fogalom;

kiberbiztonsági audit: az elektronikus információs rendszerek biztonsági osztályba sorolása, valamint a biztonsági osztályba sorolás szerinti védelmi intézkedések megfelelőségének ellenőrzése;

kiberbiztonsági hatóság: a Kormány rendeletében kijelölt nemzeti kiberbiztonsági hatóság;

kiberbiztonsági incidens: olyan esemény, amely veszélyezteti az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát;

kiberbiztonsági incidenskezelés: minden olyan tevékenység és eljárás, amelynek célja a kiberbiztonsági incidens megelőzése, észlelése, elemzése és elszigetelése vagy a kiberbiztonsági incidensre való reagálás és a kiberbiztonsági incidenst követően a működés helyreállítása;

kiberbiztonsági incidenskezelő központ: a Kormány rendeletében kijelölt szerv;

kiberbiztonsági incidensközeli helyzet: olyan esemény, amely veszélyeztethette volna az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát, de amelynek bekövetkezését sikerült megakadályozni, vagy amely nem következett be;

kiberfenyegetés: az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 8. pontjában meghatározott fogalom;

kiber-fizikai rendszer: olyan programozható elektronikus információs rendszerek, amelyek kölcsönhatásba lépnek a fizikai környezettel vagy kezelik a fizikai környezettel kölcsönhatásba lépő eszközöket. Ezek az elektronikus információs rendszerek közvetlenül fizikai változást érzékelnek vagy idéznek elő az eszközök, folyamatok és események megfigyelésével vagy vezérlésével;

kihelyezett (irányított) infokommunikációs biztonsági szolgáltatást nyújtó szolgáltató: olyan kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató, amely a kiberbiztonsági kockázatok kezelését végzi vagy azzal összefüggő szolgáltatást nyújt;

kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató: olyan szervezet, amely az IKT-termék, hálózat, infrastruktúra, alkalmazás vagy bármely más elektronikus információs rendszer telepítésével, kezelésével, üzemeltetésével vagy karbantartásával kapcsolatos szolgáltatásokat nyújt a szolgáltatást igénybe vevő telephelyén vagy távolról;

kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának, bekövetkezési valószínűségének és az ez által okozott kár nagyságának a függvénye;

kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének, fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;

kockázatkezelés: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása és az intézkedések végrehajtása;

kockázatmenedzsment keretrendszer: olyan strukturált, ugyanakkor rugalmas megközelítés és szervezeti folyamatok összessége, amely integrálja a kiberbiztonsággal kapcsolatos kockázatkezelési tevékenységeket a rendszerfejlesztési életciklusban a kockázatokkal arányos védelmi intézkedések azonosításán, bevezetésén, értékelésén, működtetésén és nyomon követésén keresztül az új és már

használatban lévő rendszerek fenyegetettségeinek folyamatos felderítése, és kockázatainak hatékony kezelése érdekében;

közösségimédia-szolgáltatási platform: olyan platform, amely lehetővé teszi a végfelhasználók számára, hogy több eszközön keresztül kapcsolódjanak, tartalmakat osszanak meg, fedezzenek fel és kommunikáljanak egymással;

központi szolgáltatás: a központi szolgáltató által kötelezően vagy egyedi igény alapján biztosítandó szolgáltatás;

központi szolgáltató: olyan szervezet, amely állami és önkormányzati feladatot ellátó szervezet részére jogszabály alapján kizárólagos joggal nyújt informatikai és elektronikus hírközlési szolgáltatást;

legfelső szintű doménnév-nyilvántartó: olyan szervezet, amelyre egy meghatározott legfelső szintű domént bíztak és amely felelős egyrészt a legfelső szintű domén kezeléséért – ideértve a legfelső szintű domén alatti doménnevek nyilvántartásba vételét –, másrészt a legfelső szintű domén technikai üzemeltetéséért, amely magában foglalja a névszervereinek üzemeltetését, adatbázisainak karbantartását és a legfelső szintű doménzónafájlok elosztását a névszerverek között, függetlenül attól, hogy ezeknek az üzemeltetési tevékenységeknek bármelyikét maga a szervezet végzi vagy azokat kiszervezi, kivéve azokat az eseteket, amikor a legfelső szintű doménneveket a nyilvántartó kizárólag saját használatra veszi igénybe;

megfelelőségértékelés: az az értékelési eljárás, amely bizonyítja, hogy egy IKT-termékkel, IKT-folyamattal, IKT-szolgáltatással kapcsolatos, meghatározott követelmények teljesültek;

megfelelőségértékelő szervezet: a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről szóló, 2008. július 9-i 765/2008/EK európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom;

megfelelőségi nyilatkozat: a gyártó vagy a szolgáltató által kiállított dokumentum, amely igazolja, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat esetében értékelték, hogy az megfelel-e valamely nemzeti kiberbiztonsági tanúsítási rendszer biztonsági követelményeinek;

megfelelőségi önértékelés: az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom;

mérföldkő: az európai uniós forrásból finanszírozott központi rendszer fejlesztése esetén a Helyreállítási és Rezilienciaépítési Eszköz létrehozásáról szóló, 2021. február 12-i (EU) 2021/241 európai parlamenti és tanácsi rendelet 2. cikk 4. pontja és az Európai Regionális Fejlesztési Alapra, az Európai Szociális Alap Pluszra, a Kohéziós Alapra, az Igazságos Átmenet Alapra és az Európai Tengerügyi, Halászati és Akvakultúra-alapra vonatkozó közös rendelkezések, valamint az előbbiekre és a Menekültügyi, Migrációs és Integrációs Alapra, a Belső Biztonsági Alapra és a határigazgatás és a vízumpolitika pénzügyi támogatására szolgáló eszközre vonatkozó pénzügyi szabályok megállapításáról szóló, 2021. június 24-i (EU) 2021/1060 európai parlamenti és tanácsi rendelet 2. cikk 4. pontja szerinti, valamint a fejlesztésekre irányuló egyéb projektek esetén a projektben meghatározott fogalom;

minősített bizalmi szolgáltatás: a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

minősített bizalmi szolgáltató: a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

műszaki előírás: az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről szóló, 2012. október 25-i 1025/2012/EU európai parlamenti és tanácsi rendelet (a továbbiakban: 1025/2012/EU rendelet) 2. cikk 4. pontjában meghatározott fogalom;

műveleti célú elektronikus információs rendszer:

- a rendvédelmi szervek és a nemzetbiztonsági szolgálatok számára törvényben meghatározott közbiztonsági, nemzetbiztonsági feladatok ellátása érdekében használt elektronikus információs rendszer és

- a honvédségi szervezetek által, a törvényben meghatározott katonai műveleti feladatok – így különösen közvetlen művelettámogatás, -tervezés, -vezetés, helyzetkövetés – ellátása érdekében használt elektronikus információs rendszer;

nagyszabású kiberbiztonsági incidens: olyan kiberbiztonsági incidens, amely olyan mértékű zavart okoz, amely meghaladja Magyarországnak az arra való reagálási képességét, vagy amely Magyarországra és legalább még egy másik országra jelentős hatást gyakorol;

nem privát felhőszolgáltatás: olyan szolgáltató által nyújtott felhőszolgáltatás, amelyet a szolgáltató bárki számára elérhető módon vagy kizárólag a szervezetek egy meghatározott köre számára nyújt;

nemzeti kiberbiztonsági incidenskezelő központ: az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, kiberbiztonsági incidensekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal rendelkezik [európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)];

nemzeti kiberbiztonsági stratégia: a kiberbiztonság területén követendő stratégiai célokat és prioritásokat, valamint a megvalósításukhoz szükséges irányítási intézkedéseket meghatározó dokumentum;

nemzeti kiberbiztonsági tanúsítvány: olyan független harmadik fél által kiállított dokumentum, amely igazolja, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat esetében értékelték, hogy az megfelel-e valamely nemzeti kiberbiztonsági tanúsítási rendszer biztonsági követelményeinek;

nemzeti válságkezelési terv: az (EU) 2022/2555 európai parlamenti és tanácsi irányelv alapján a nagyszabású kiberbiztonsági események és válságok elhárítására szolgáló nemzeti terv, amely meghatározza a nagyszabású kiberbiztonsági események és válságok kezelésének célkitűzéseit és szabályait;

online keresőprogram: az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról szóló, 2019. június 20-i (EU) 2019/1150 európai parlamenti és tanácsi rendelet 2. cikk 5. pontjában meghatározott fogalom;

online piactér: olyan szolgáltatás, amely a kereskedő által vagy a kereskedő nevében működtetett szoftvert, többek között weboldalt, valamely weboldal egy részét vagy valamely alkalmazást használ, és amelynek révén a fogyasztók távollevők közötti szerződést köthetnek más kereskedőkkel vagy fogyasztókkal;

regisztrált felhasználói jogosultság: a biztonsági vizsgálatot végző személy számára a sérülékenységvizsgálat elvégzése érdekében célzottan létrehozott felhasználói jogosultság;

rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;

sebezhetőség: IKT-termék, -szolgáltatás, -folyamat gyengesége, érzékenysége vagy hiányossága, amelynek kihasználása veszélyezteti vagy sérti az IKT-termék, -szolgáltatás, -folyamat bizalmasságát, sértetlenségét vagy rendelkezésre állását;

sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik, azaz hiteles, valamint a származás ellenőrizhetőségét, bizonyosságát, azaz letagadhatatlanságát is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

sérülékenység: az elektronikus információs rendszer gyengesége, érzékenysége vagy hiányossága, amelynek kihasználása veszélyezteti vagy sérti egy elektronikus információs rendszer bizalmasságát, sértetlenségét vagy rendelkezésre állását;

sérülékenységkezelési terv: a sérülékenységek megszüntetésére irányuló tervdokumentum;

sérülékenységvizsgálat: sérülékenységmenedzsment eszköz vagy módszer, amely során informatikai rendszerek, hardverek és szoftverek biztonsági szempontból történő átvizsgálása zajlik, az ellenőrzést automatizált eszközökkel és közvetlen, szakértő által végzett vizsgálatokkal hajtják végre;

szabvány: az 1025/2012/EU rendelet 2. cikk 1. pontjában meghatározott fogalom;

szervezet: állami szerv vagy állami szervezet, a Polgári Törvénykönyvről szóló törvény szerinti jogi személy, jogi személyiség nélküli szervezet;

támogató rendszer: a szervezet alapfeladatainak ellátásában közvetlenül nem részt vevő elektronikus információs rendszer, amely szükséges azon rendszerek működéséhez, amelyek alapfeladatot látnak el;

tanúsítás: független harmadik fél által végzett megfelelőségértékelési tevékenység;

tartalomszolgáltató hálózat szolgáltatója: a digitális tartalmak és szolgáltatások széles körű, akadálymentes és gyors rendelkezésre állását biztosító, földrajzilag elosztott szerverek hálózatának szolgáltatója;

távoli sérülékenységvizsgálat: olyan sérülékenységvizsgálat, amelynek során

- az elektronikus információs rendszer internet felőli, külső sérülékenységvizsgálatára kerül sor, amelynek keretében az interneten fellelhető, nyilvános adatbázisokban való szabad keresés, célzott

információgyűjtés, valamint az elérhető számítógépek szolgáltatásai sebezhetőségének feltérképezése történik,

- automatizált és kézi vizsgálatok útján kerülnek feltárásra a webes alkalmazások sérülékenységei, vagy

- a vezeték nélküli hozzáférési és kapcsolódási pontok keresése, feltérképezése, titkosítási eljárások elemzése, titkosítási kulcsok visszafejthetőségének ellenőrzése célszoftverek és kézi vizsgálat útján történik;

továbbfejlesztés: az érintett, már működő elektronikus információs rendszer olyan mértékű fejlesztése, amely funkcionalitásának érdemi megváltozásával jár, vagy védelmének elvárt erősségére hatással van;

üzemeltetési kiberbiztonsági incidens: olyan kiberbiztonsági incidens, amely az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált, vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását nem szándékoltan csökkenti vagy megszünteti;

üzemeltető: az a természetes személy, jogi személy, jogi személyiség nélküli szervezet vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős;

zárt, teljes körű, folytonos és a kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme,

- amely az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósul,

- amely az elektronikus információs rendszer valamennyi elemére kiterjed,

- amely az összes számításba vehető fenyegetést, veszélyt figyelembe veszi, valamint

- amelynek költségei arányosak a fenyegetések által okozható károk értékével.

3. INFORMÁCIÓBIZTONSÁGI ELVÁRÁSOK

3.1 Szervezet szintű elvárások

3.1.1 Alapfeladatok

3.1.1.1 Informatikai biztonsági szabályzat

A BSZRK informatikai biztonsági szabályzatát ki kell hirdetni és elérhetővé kell tenni a szabályzat „1.2.2 Személyi hatály" fejezetében meghatározott személyek számára.

A szabályzatot és a benne előírt dokumentumokat, nyilvántartásokat a BSZRK belső szabályzó dokumentumai számára kialakított elektronikus tárhelyen kell tárolni. A tárhely rendelkezésre állását, az ott tárolt dokumentumok illetéktelen hozzáférés és módosítás, valamint törlés elleni védelmét megfelelően biztosítani szükséges.

A szabályzatban említett nem publikus dokumentumokhoz, nyilvántartásokhoz, függelékekhez (átfogóan: tartalomhoz) az alábbi személyek férhetnek hozzá:

- FI,
- ÁFIH,
- ICSV,
- IJ,
- IBF,
- BE (ellenőrzés tárgyához kötötten),
- aki a tartalmat előállítja (az általa előállított tartalom esetében),
- aki a tartalomban szereplő adat, információ felhasználására kötelezett (az adott tartalom vonatkozásában).

3.1.1.2 Az elektronikus információs rendszerek biztonságáért felelős személy

A BSZRK-nak ki kell neveznie, meg kell bíznia az BSZRK EIR biztonságáért felelős személyt (információbiztonsági felelőst, vagy IBF-et), aki ellátja az 418/2024. (XII. 23.) Korm. rendelet 12. §-ában, valamint az ebben a szabályzatban meghatározott feladatokat.

3.1.1.3 Információbiztonságot érintő erőforrások

A BSZRK-nak biztosítania kell az eme dokumentumban meghatározott információbiztonsági célok végrehajtásához és fejlesztéséhez szükséges erőforrásokat. A kiberbiztonsági ráfordításokat a hatályos törvényeknek, végrehajtási rendeleteknek, irányelveknek, szabályozásoknak, szabványoknak és ajánlásoknak megfelelően dokumentálni kell. Ez kiterjed az éves költségvetésre, beruházási kérelmekre és a közbeszerzésekre.

3.1.1.4 Az intézkedési terv és mérföldkövei

A BSZRK-nak a 7/2024. (VI. 24.) MK rendelet 1. melléklete alapján, valamint az NKI által kibocsátott érvényes OVI táblázatok alapján fel kell mérnie és a nem publikus EIR Rendszerbiztonsági tervben rögzítenie kell az EIR-einek biztonsági osztályát. A felmérést az IBF koordinálja, akit ebben a tevékenységben az ICSV támogat.

Amennyiben a felmérés a célként megadott biztonsági osztályra érvényes (az ebben a szabályzatban meghatározott) követelményekhez képest hiányosságot állapít meg, a felmérést követő 90 napon belül intézkedési tervet kell készíteni az azonosított hiányosságok megszüntetése érdekében. (A „M4.3.12. Elvárt intézkedés tervezése (intézkedési terv)" mellékletben lévő minta szerint)

Az intézkedési terv készítése az ICSV feladata, akit ebben a tevékenységében az IBF támogat.

Az intézkedési tervben egzakt intézkedéseket és hozzájuk határidőket, valamint felelősöket kell meghatározni.

Az intézkedési tervben meghatározott intézkedéseket végre kell hajtani és a végrehajtást az intézkedési tervben haladéktalanul dokumentálni kell, amelyeknek felelőse az adott intézkedéshez az intézkedési tervben meghatározott felelős.

Az intézkedési tervet legalább évente felül kell vizsgálni és aktualizálni kell (a BSZRK kockázatkezelési stratégiája és a kockázatokra adott válasz tevékenységek prioritása alapján). A felülvizsgálatot az IBF koordinálja, akit ebben a tevékenységben az ICSV támogat.

Az ebben a pontban meghatározott feladatok végrehajtásáról az IBF rendszeresen, de legalább évente köteles beszámolni az FI-nek.

3.1.1.5 Az elektronikus információs rendszerek nyilvántartása

A BSZRK EIR-eiről nyilvántartást kell vezetni (az EIR Rendszerbiztonsági tervekben és a központi leltározó rendszerben) és a nyilvántartást rendszeresen (de legalább negyedévente) aktualizálni szükséges.

A nyilvántartás vezetése és aktualizálása az ICSV feladata.

A nyilvántartásnak minden rendszerre nézve tartalmaznia kell:

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

3.1.1.6 Biztonsági teljesítmény mérése

A BSZRK EIR-i biztonsági teljesítményét mérőszámok és mutatók segítségével határozza meg és követi nyomon, amikről az adott EIR Rendszerbiztonsági terve vagy annak melléklete ír bővebben annak vonatkozásában.

A teljesítmény mérésnek a következőket figyelembe kell venni:

- az adott rendszer állapota és annak változás
- az adott rendszer kiberbiztonsági rezilienciája
- a szervezet eseményekre adott válaszának reakcióideje

A biztonsági teljesítmény mérések eredményéről legalább negyedévente jelentést kell készíteni, ami az ICSV feladata, akit ebben a tevékenységében az IBF támogat.

A biztonsági teljesítmény mérés rendszerét legalább évente egyszer felül kell vizsgálni és szükség szerint frissíteni, ami ez IBF feladata.

3.1.1.7 Szervezeti architektúra

A BSZRK a biztonsági követelményeket szervezeti szinten a „Szervezeti szintű elvárások" pontban határozza meg, melyek az egész szervezetre vonatkoznak.

Az EIR szintű biztonsági követelményeket a „Rendszer szintű elvárások" pontban határozza meg, melyek hatása csak az adott EIR-re, rendszerelemekre és az ahhoz köthető személyekre és szervezetekre terjed ki. Erről részletesebben az adott EIR rendszerbiztonsági terve ír.

3.1.1.8 A szervezet működése szempontjából kritikus infrastruktúra biztonsági terve

A BSZRK kidolgozza a kritikus infrastruktúra és kulcsfontosságú erőforrások biztonsági tervet, amiben azonosítja és rangsorolja a BSZRK működésében kritikus szerepet betöltő infrastruktúrákat és

erőforrásokat és azok védelmére tervet készít. (lásd a „Kritikus infrastruktúra biztonsági terve" külön álló dokumentum)

A biztonsági terve elkészítését az ICSV végzi, akit ebben a tevékenységében az IBF támogat.

A biztonsági tervet legalább évente egyszer felül kell vizsgálni és szükség szerint frissíteni, ami ez IBF feladata.

3.1.1.9 Kockázatmenedzsment stratégia

A BSZRK kockázatmenedzsment stratégiát alakít ki melynek részletei a „4.3 KOCKKÁZATMENEDZSMENT KERETRENDSZER" mellékletben és „3.2.7 Kockázatkezelés" fejezetben kerülnek kifejtésre.

3.1.1.10 Engedélyezési folyamatok meghatározása

A BSZRK engedélyezési folyamataira és azok felelőseire a „3.2.3 Értékelés, Engedélyezés és Monitorozás" fejezet tér ki részletesebben.

3.1.1.11 Szervezeti működés és üzleti folyamatok meghatározása

A BSZRK az üzleti folyamatok, az információbiztonság és az azok kockázatokra gyakorolt hatása alapján határozza meg szervezeti céljait és az azokból eredendő információvédelmi igényeket.

A szervezeti célokat és információvédelmi igényeket rendszeresen, de legalább évente felül kell vizsgálni.

3.1.1.12 Biztonsági személyzet képzése

A BSZRK a biztonsági személyek képzését és fejlesztését célzó programot dolgoz ki. Valamint a „3.1.2.3 Szerepkör alapú biztonsági képzés" pont szerint képzést biztosít számukra a feladataik ellátásához.

3.1.1.13 Tesztelés, képzés és felügyelet

A BSZRK kidolgoz egy folyamatot, amely biztosítja, hogy a BSZRK EIR-ekhez kapcsolódó biztonsági tesztelések, képzések és felügyeleti tevékenységek elvégzésére vonatkozó szervezeti tervek megfelelő fejlesztés és karbantartás mellett folyamatosan végrehajtásra kerüljenek és a tervek összhangban vannak a szervezeti kockázatmenedzsment stratégiával és a kockázatkezelési intézkedésekre vonatkozó, az egész szervezetre kiterjedő prioritásokkal.

3.1.1.14 Szakmai csoportokkal és közösségekkel való kapcsolattartás

A BSZRK a következő szempontok szerint;

- meghatározott személyek biztonsági oktatása és képzése;
- naprakész információk, ajánlott biztonsági gyakorlatok, technikák és technológiák beszerzése;
- biztonsági eseményekkel, sérülékenységekkel és fenyegetésekkel kapcsolatos információk megosztása;

kapcsolatot alakít ki kiberbiztonsággal kapcsolatban lévő szakmai csoportokkal.

3.1.1.15 Fenyegetettség tudatosító program

A BSZRK fenyegetésekkel szembeni tudatosító programot vezet be, amihez a BSZRK-on belüli és a szakmai csoportoktól/közösségektől származó információkat oszt meg, ezzel elősegítve a fenyegetések felismerését.

3.1.1.16 Kockázatmenedzsment keretrendszer

A „4.3 KOCKKÁZATMENEDZSMENT KERETRENDSZER" és „3.2.7 Kockázatkezelés" szerint összegyűjtött információk szerint a BSZRK azonosítja és dokumentálja;

- - a kockázatelemzést, kockázatkezelést és a kockázatok felügyeletét érintő feltételezéseit;
- - a kockázatelemzést, kockázatkezelést és a kockázatok felügyeletét érintő megkötéseit;
- - a kockázatmenedzsment során figyelembe vett prioritásokat és kompromisszumokat;
- - a szervezet kockázattűrő képességét.

A folyamat során keletkezett dokumentumokat el kell juttatni az IBSZ-hez, aki az általa kapott információk és a BSZK-ban bekövetkezett szervezeti változások tükrében rendszeresen, de legalább évente felülvizsgálja a kockázatmenedzsment keretrendszer szempontrendszerét.

3.1.1.17 Kockázatkezelésért felelős szerepkörök

A BSZRK kockázatkezelésért felelős személyt nevez ki, akinek a feladata a BSZRK információbiztonsági irányítási folyamatainak összehangolása a BSZRK más stratégiai, működési és költségvetés-tervezési folyamataival.

A BSZRK kockázati vezetőt nevez ki, akinek a feladata a kockázatok szervezeti szintű áttekintésének és elemzésének, valamint a kockázatmenedzsment szervezeten belüli egységes működésének biztosítása.

3.1.1.18 Ellátási lánc kockázatmenedzsment stratégiája

A BSZRK ellátási lánc kockázatmenedzsment stratégiát alakít ki melynek részletei a „3.1.9 Ellátási Lánc kockázatkezelés" fejezetben kerülnek kifejtésre.

A BSZRK továbbá a kockázatmenedzsment stratégia keretében azonosítja, rangsorolja és értékeli azokat a beszállítókat, amelyek a szervezet EIR-ei és rendszerelemei működése szempontjából kritikus technológiákat, termékeket és szolgáltatásokat szállítanak a szervezet alapvető feladatainak ellátásához.

A BSZRK ellátási lánc kockázatmenedzsment stratégiája minden szervezeti egységre érvényes.

Az ellátási lánc kockázatmenedzsment stratégiát az IBF éves rendszerességgel felülvizsgálja és szüksége esetén frissíti.

3.1.1.19 Folyamatos felügyeleti stratégia

A BSZRK folyamatos felügyeleti stratégiát és programot dolgoz ki, aminek célja a szervezet biztonsági állapotának nyomon követése.

A BSZRK alapfeladatainak ellátásához szükséges szolgáltatásokhoz támasztott teljesítménymutatókat és az azokról készített hatékonyság-értékelés gyakoriságát a „Informatikai alapfeladatok" külön álló dokumentumban határozza meg.

A BSZRK a folyamatos felügyelet teljesítménymutatóinak alakulását folyamatosan nyomon követi és a hatékonyság-értékelés eredményinek tükrében válaszlépéseket kell tenni.

Az EIR-ek biztonsági állapotáról az IBF éves rendszerességgel beszámolót készít a FI számára.

3.1.2 Tudatosság és Képzés

3.1.2.1 Eljárásrend

A BSZRK-nak meg kell fogalmaznia, dokumentálnia és ki kell hirdetni a BSZRK-n belül a képzési eljárásrendet, majd ezt legalább éves gyakorisággal felül kell vizsgálja és frissíteni kell.

A feladatot a MO-nek kell végeznie.

Az ebben a pontban felsorolt követelményeket a BSZRK belső képzési szabályzatában is meg lehet határozni, ki lehet hirdetni.

A képzés anyagát legalább évi rendszerességgel felül kell vizsgálni és frissíteni kell, hogy az általa biztosított ismeretek naprakészek maradjanak és a belső és külső biztonsági eseményekből levont tanulságok is integrálásra kerüljenek.

Ezt az ICSV végzi, akit ebben a tevékenységében az IBF támogat.

3.1.2.2 Biztonság tudatosság képzés

A BSZRK-nak annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést kell szerveznie az elektronikus információs rendszer felhasználói számára

- az új felhasználók kezdeti képzésének részeként; valamint
- amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi; de
- legalább évente egy alkalommal.

A képzésen átadott ismeretnek gyakorlatcentrikusnak kell lennie, amelynek keretében az elvárásokon túl be kell mutatni az elvárások hátterét (indokát), az elvárásoknak való megfelelés módját és a nem megfelelés következményeit is, valamint kiemelt módon ki kell térni a szervezeten belüli fenyegetésekre, és a pszichológiai manipuláció és adatgyűjtés jeleinek felismerésére.

3.1.2.3 Szerepkör alapú biztonsági képzés

A BSZRK-nak munkakör, vagy feladat alapú biztonsági képzést kell nyújtania az egyes munkakörök szerint, az adott munkakört betöltő személyeknek

- az EIR-hez való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően;
- amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi; de
- legalább évente egy alkalommal

A biztonsági képzés anyagában fel kell használni a belső és külső biztonsági eseményekből levont tanulságokat.

3.1.2.4 A biztonsági képzésre vonatkozó dokumentációk

A BSZRK-nak dokumentálnia kell a biztonságtudatosságra vonatkozó alap-, és szerepkör alapú biztonsági képzéseket, és az azokon való részvételt.

A képzésen résztvevőkkel a képzés megtörténtét el kell ismertetni, és ezt a dokumentumot meg kell őrizni a foglalkoztatott kilépését követő év végéig, vagy külső érintettnél a kapcsolódó szerződés megszűnésétől számított 8 évig.

A megőrzés foglalkoztatott esetében a MO, külső érintett esetében a IJ feladata.

3.1.3 Biztonsági események kezelése

3.1.3.1 Eljárásrend

Az eljárásrendet rendszeresen, de legalább évente felül kell vizsgálni, aktualizálni kell. A felülvizsgálat és aktualizálás az ICSV feladata, amit az IBF ellenőriz.

3.1.3.2 Képzés a biztonsági események kezelésére

A BSZRK-nak biztonsági eseménykezelési képzést kell biztosítania az elektronikus információs rendszer felhasználói számára, a nekik kijelölt szerepkörökkel és felelősségekkel összhangban.

A képzést a biztonsági eseménykezelési szerepkör vagy felelősség kijelölését követő legalább egy éven belül, vagy amikor ezt az elektronikus információs rendszer változásai megkívánják, és azt követően évente kell megtartani.

A képzés anyagát az ICSV, biztonsági eseményt követően vagy legalább kétévente köteles felülvizsgálni és frissíteni.

3.1.3.3 Biztonsági események kezelésének tesztelése

A BSZRK a szervezet biztonsági esemény kezelési képességeinek felmérésére teszteket alkalmaz. Ezzel meghatározva a képzések hatékonyságát, a potenciális gyengeségeket és a hiányosságokat. A tesztekbe a biztonsági esemény kezelési tervben meghatározott kapcsolódó tervek felelőseivel is egyeztetni kell a tesztelés idejéről, módszereiről és eszközeiről.

A teszteléshez felhasználható módszerek:

- ellenőrzőlisták
- teljes tesztelés
- tervek strukturált átnézése
- szimulációk

A tesztelést és annak kiértékelését az IBF végzi éves rendszerességgel, az abban érintett szervezetek bevonásával.

A tesztelés eredményeit fel kell használni a szervezet biztonsági eseménykezelési képességeinek javítására.

3.1.3.4 A biztonsági események kezelése

A BSZRK szempontjából biztonsági eseménynek számít valamennyi olyan tett, cselekedet vagy történés, vagy azok elmaradása, amely a BSZRK EIR-einek az elvárt rendelkezésre állását, integritását vagy bizalmasságát kedvezőtlenül befolyásolja.

A BSZRK EIR-eit érintő biztonsági eseményeket ebben a szabályzatban leírt módon kell kezelni, beleértve az előkészületet, az észlelést, a vizsgálatot, az elszigetelést, a megszüntetést és a helyreállítást.

A biztonsági események kezelése során elsősorban az alábbi eseménytípusokra kell felkészülni:

- az elektronikus információs rendszer szokásostól eltérő/hibás működése,
- az elektronikus információs rendszer lassulása/leállása
- az elektronikus információs rendszer hardverhibája,
- az elektronikus információs rendszer nem megfelelő módosítása/beállítása
- igénybe vett szolgáltatás szokásostól eltérő/hibás működése,
- igénybe vett szolgáltatás lassulása/leállása,
- elektronikus információs rendszerelem (hardver) elvesztése, sérülése, megsemmisülése,
- elektronikus információs rendszerben tárolt adat nem kívánt létrehozása/módosítása/törlése
- a szabályzatoknak vagy irányelveknek való nem megfelelés;
- a fizikai és környezeti biztonsági rendelkezések megsértése;
- kártékony kód általi fertőzés;
- véletlen, illetve nem szándékos emberi hibák;
- hozzáférési előírások megsértése;
- a nem teljes vagy nem pontos működési adatokból eredő hibák;
- a bizalmasság és sértetlenség megsértése;
- szándékos adatmódosítás vagy törlés;
- más személy felhasználói adatainak használata

A biztonsági események kezelésére megfelelő mértékben fel kell készülni. A racionálisan előre tervezhető lépéseket az ICSV koordinálásával előzetesen meg kell határozni (részletesebben lásd a „3.1.3 Biztonsági események kezelése" fejezetben).

Az események kezelésekor a lehető leghamarabb mérséklő intézkedésnek kell születnie.

Az eseménykezelés során elsődleges cél a szokásos szolgáltatás lehető leggyorsabb helyreállítása és a szakmai folyamatokra gyakorolt káros hatás minimalizálása.

Az eseményt az azt észlelőnek haladéktalanul jelezni kell az ICSV és az IBF felé. A jelentési kötelezettség elmaradása, vagy késlekedés a jelentéssel szankciókat vonhat maga után.

Amennyiben az eseményt vélhetően külső, illetéktelen beavatkozás, vagy vírustámadás okozta, az érintett információs rendszer(eleme)t le kell választani a hálózat(ok)ról, szükség esetén ki kell kapcsolni. Ilyen esetekben fokozottan figyelni kell, hogy hordozható adathordozó se maradjon kívülről elérhető.

A meghibásodott eszközben használt adathordozók kizárólag biztonsági ellenőrzést követően használhatók más számítógépekben.

A beérkezett bejelentés alapján az ICSV feladata az esemény kivizsgálásának és dokumentálásának koordinálása. Az ICSV a tervezett és végrehajtott lépésekről az IBF-et tájékoztatni köteles.

Amennyiben az IBF szükségesnek tartja, a kivizsgálásba közvetlenül is bekapcsolódhat, további vizsgálati irányokat és lépéseket határozhat meg. A kivizsgálást olyan időtávon belül kell megtenni, amely biztosítja, hogy az esemény hatása előre valószínűsíthetően ne befolyásolja a BSZRK informatikai infrastruktúrájának és a benne kezelt adatoknak a zártságát, integritását és rendelkezésre állását.

Az eseményből levont tanulságok alapján az ICSV-nek és az IBF-nek javaslatot kell tennie, hogy az esemény ismételt előfordulási esélye csökkenjen, illetve az okozott kár mérsékeltebb legyen.

Az ICSV feladata ezenkívül a biztonsági események kezelési eljárásait összehangolni az üzletmenetfolytonossági tervhez (lásd részletesebben a „3.2.5.2 Üzletmenet-folytonossági terv" pontban) tartozó tevékenységekkel; illetve a biztonsági események kezelési tevékenységekből levont tanulságokat beépíteni az eseménykezelési eljárásokba, a fejlesztési és üzemeltetési eljárásokba, elvárásokba, továbbképzésekbe és tesztelésbe.

Az ebben a pontban leírtakat rendszeresen, de legalább évente a ICSV-nek felül kell vizsgálni és frissíteni kell.

Az eseménykezelési tervvel kapcsolatban ebben és a kapcsolódó további pontokban előírtakat az eseménykezelési tervben (lásd „4.3 KOCKKÁZATMENEDZSMENT KERETRENDSZER" függelék) kell pontosan meghatározni (felelősök, időtartamok, folyamatok stb.).

A BSZRK a biztonsági eseményekkel kapcsolatos folyamatokat automatikus módszerekkel is támogatja.

3.1.3.5 A biztonsági események nyomonkövetése

A BSZRK EIR-eit érintő biztonsági eseményeket nyomon kell követni és dokumentálni kell.

A dokumentálást az egyes információs rendszereknek automatikusan kell végezniük, amennyiben az esemény jellege és a naplózási beállítások ezt lehetővé teszik; egyébként a dokumentálást és nyomkövetést az adott elektronikus információs rendszer üzemeltetőjének kell elvégeznie.

3.1.3.6 A biztonsági események jelentése

A felhasználók kötelessége, hogy a közvetlen felettesük és az informatikai Help Desk felé jelentsék a biztonsági esemény bekövetkeztét, vagy ha erre utaló jelet, vagy veszélyhelyzetet észlelnek.

A biztonsági eseményre vonatkozó jelentési kötelezettség elmulasztása szankciókat vonhat maga után (beleértve a munkajogi intézkedéseket is).

A biztonsági eseményekre vonatkozó információkat az IBF feladata jelenteni a jogszabályban meghatározottak szerint, az EIR-ek biztonságának felügyeletét ellátó szerveknek (amennyiben az esemény jelentési kötelezettséggel jár).

A BSZRK a biztonsági események bejelentését automatikus módszerekkel is támogatja.

3.1.3.7 Segítségnyújtás a biztonsági események kezeléséhez

Az elektronikus információs rendszer felhasználóinak a biztonsági események kezeléséhez és jelentéséhez az ICS munkatársai támogatást nyújtanak.

A BSZRK a biztonsági események kezelését automatikus módszerekkel is támogatja.

3.1.3.8 Biztonsági eseménykezelési terv

A BSZRK a foglalkoztatottjai és partnerei számára a biztonsági események kezelési módjaira iránymutatást adó biztonsági eseménykezelési terve a „4.4 BIZTONSÁGI ESEMÉNYKEZELÉSI TERV" függelékben található. A tervet az ICSV dolgozza ki, az IBF pedig legalább éves rendszerességgel ellenőrzi azt.

A biztonsági eseménykezelési terv ismerteti a biztonsági eseménykezelési lehetőségek struktúráját, valamint bemutatja, hogy a biztonsági eseménykezelési lehetőségek hogyan illeszkednek az BSZRK működésébe.

A biztonsági eseménykezelési tervben meg kell határozni

- a bejelentés-köteles biztonsági eseményeket,
- folyamatosan pontosítani kell a biztonsági események kiértékelésének, kategorizálásának (súlyosság stb.) kritériumrendszerét,
- támogatást kell adni a biztonsági eseménykezelési lehetőségek belső mérésére (összhangban a „3.1.1.13 Tesztelés, képzés és felügyelet" pontban és a „3.1.3.3 Biztonsági események kezelésének tesztelése" pontban leírtakkal),
- meg kell határozni azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására.

A biztonsági eseménykezelési tervet

- ki kell hirdetni és tudomásul kell vetetni a biztonsági eseményeket kezelő (névvel és/vagy szerepkörrel azonosított) személyeknek és szervezeti egységeknek;
- meghatározott gyakorisággal, de legalább évente felül kell vizsgálni, frissíteni kell az EIR és a BSZRK változásait vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat figyelembe véve.

A biztonsági eseménykezelési terv változásait ismertetni kell a tervet megismerni jogosultak számára, egyben gondoskodni kell arról, hogy a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető, módosítható.

3.1.4 Karbantartás

3.1.4.1 Eljárásrend

A BSZRK informatikai infrastruktúrájának, informatikai rendszerelemeinek karbantartása kapcsán az ebben a pontban megadott eljárásrendet kell alkalmazni.

A karbantartási eljárásrendet rendszeresen, de legalább évente felül kell vizsgálni, aktualizálni kell. A felülvizsgálat és aktualizálás az ICSV feladata.

A rendszerkarbantartással kapcsolatos elvárások teljesülését az ICSV koordinálja.

A felülvizsgálat megtörténtét és megfelelőségét, valamint az elvárások teljesülését az IBF ellenőrzi, legalább éves rendszerességgel.

3.1.4.2 Szabályozott karbantartás

A BSZRK informatikai infrastruktúrájának és rendszerelemeinek megfelelő rendelkezésre állása, folyamatos használhatósága érdekében azokat rendszeresen és tervezetten karban kell tartani.

A karbantartásokat a jogszabályi előírások, szállítói/gyártói ajánlások, belső utasítások és szakmai legjobb gyakorlat szerint kell tervezni és végrehajtani.

A karbantartásokat és javításokat lehetőleg előre megtervezett időpontban és módon kell végrehajtani, amelyhez az ICSV éves karbantartási tervet készít, az ütemezésbe a szakmai területek képviselőit is bevonva.

Ha a BSZRK a karbantartást belső erőforrással nem tudja elvégezni, az ICSV feladata kezdeményezni az BSZRK vezetésénél külső támogató szervezet/szakember megbízását.

Karbantartási tevékenységet csak olyan külső támogató végezhet, amely/aki érvényes szerződéssel vagy megbízással rendelkezik, adathordozóval is kapcsolatos karbantartás esetén pedig aláírta a BSZRK által készített titoktartási nyilatkozatot és dokumentált formában megismerte a BSZRK vonatkozó információbiztonsági előírásait.

A karbantartást végző külső támogatókról nyilvántartás kell vezetni, melynek minimálisan a következőket tartalmaznia:

- szervezet megnevezése,
- szerződésszám,
- szerződés időtartama,
- szerződéses kapcsolattartó neve, elérhetősége,
- karbantartást végzők neve, elérhetősége
- szerződés tárgya, hatálya (mely rendszerelemre terjed ki).

Külső támogató munkavégzése esetén az ICSV feladata kijelölni azt a foglalkoztatott szakembert, akinek folyamatos felügyeletet kell biztosítania a karbantartás során és őt előre tájékoztatni a karbantartás várható jellegzetességeiről, valamint a karbantartást végző személyekről.

A külső támogatóval kötött szerződésbe kell foglalni, hogy a karbantartást felügyelők jogosultak kérni a karbantartást végző személy személyazonosságának igazolását, illetve, hogy a karbantartást végző személynek kötelessége a felszólításra a szükséges iratokat bemutatni.

A karbantartási tevékenységet az ICSV előzetes jóváhagyásával szabad elkezdeni.

A karbantartást az ICSV vagy általa kijelölt szakember által folyamatosan felügyelni kell, függetlenül attól, hogy azt a helyszínen vagy távolról végzik.

Amennyiben a karbantartáshoz szükséges az EIR vagy a rendszerelemek kiszállítása a BSZRK által kontrollált területről, a kiszállítást előzetesen, írásban engedélyezni szükséges. Az engedélyt az ICSV adhatja meg.

Az EIR vagy a rendszerelemek kiszállítása előtt azokról valamennyi adatot és információt- ellenőrzött, sikeres mentést követően - visszaállíthatatlan módon törölni kell (a „ 3.1.5.6 Adathordozók törlése" pontban megfelelően).

Az elvégzett karbantartás után az eszköz és a karbantartás jellegétől függő funkcionális és biztonsági teszteket kell végezni, melynek eredményét rögzíteni kell a karbantartási dokumentációban. Sikertelen teszt esetén az eszköz nem helyezhető újra éles üzembe. Az eseményt jelezni kell az ICSV felé, aki dönt a további intézkedésekről.

A tervezett és végrehajtott karbantartásokat megfelelően dokumentálni kell, legalább az alábbiakat rögzítve:

- az elvégzett karbantartás leírása,
- az érintett rendszerelem, eszköz megnevezése és azonosítója,
- a karbantartás engedélyezője,
- a karbantartás elvégzője,
- a karbantartás dátuma,
- leállási idő (ha volt ilyen),
- karbantartást követő tesztelés eredménye,
- karbantartó neve, beosztása és aláírása,
- karbantartást felügyelő neve, beosztása és aláírása,
- tesztelő, átvevő neve, beosztása és aláírása.

3.1.4.3 Karbantartási eszközök

A BSZRK nyilvántartást vezet az EIR-ek karbantartásához az ICSV által jóváhagyott eszközökről, valamint ellenőrzi, hogy a karbantartáshoz valóban csak az engedélyezett eszközöket használják.

Adathordozók esetében az EIR-hez való kapcsolást megelőzően diagnosztikai programokkal ellenőrzi kell, hogy azok nem tartalmaznak káros kódot.

Az elszállítandó karbantartó eszközök esetében meg kell győződni arról, hogy azok nem tartalmazzanak szervezeti információkat és amennyiben korábban tartalmaztak, az megfelelő módon meg lett semmisítve.

Amennyiben ez nem teljesül, a BSZRK-nak meg kell akadályoznia az eszköz elszállítását vagy azt az ICSV-nek külön engedélyeznie kell.

3.1.4.4 Távoli karbantartás

A BSZRK lehetőséget biztosít arra, hogy az ICSV jóváhagyásával, az EIR-en távoli karbantartásai és diagnosztikai tevékenységet végezzenek, amennyiben ez megfelel a karbantartási szabályzatnak.

Távoli karbantartás esetén az EIR elérését erős hitelesítési eljárással kell biztosítani. A befejezte után pedig az erre a célra használt hálózati kapcsolatokat és munkaszakaszokat meg kell szüntetni.

3.1.4.5 Karbantartó személyek

A BSZRK biztosítja, hogy az EIR karbantartását végző személyek rendelkezzenek a karbantartáshoz szükséges megfelelő hozzáférési jogosultságokkal és azokról nyilvántartást vezet.

Az EIR-en kiséret nélkül karbantartást végző személyek esetén ellenőrizni kell azok hozzáférési jogosultságait.

A szükséges hozzáférési jogokkal nem rendelkező karbantartók tevékenységét a BSZRK megfelelő műszaki szakértelemmel rendelkező foglalkoztatottjának felügyelnie kell.

Az ICSV-nek joga van ideiglenes hozzáférési jogosultság biztosítására.

3.1.4.6 Kellő időben történő karbantartás

A BSZRK biztosítja, hogy a karbantartásokat a jogszabályi előírások, szállítói/gyártói ajánlások, belső utasítások és szakmai legjobb gyakorlat szerint kellő időn belül megtörténjenek.

Ennek pontos menetét az egyes EIR-ek Rendszerbiztonsági Tervei részletezik.

3.1.5 Adathordozók védelme

3.1.5.1 Eljárásrend

Az eljárásrendet rendszeresen, de legalább évente felül kell vizsgálni, aktualizálni kell. A felülvizsgálat és aktualizálás az ICSV feladata.

Az adathordozók védelmével kapcsolatos elvárások teljesülését az IBF feladata legalább évente ellenőrizni.

A BSZRK informatikai infrastruktúrájában, illetve a BSZRK által kontrollált adatok tárolására kizárólag a BSZRK tulajdonában lévő, regisztrált adathordozót lehet használni.

A BSZRK-ban adathordozók beszerzésére kizárólag az ICS jogosult.

A foglalkoztatottak adathordozó iránti igényüket az érintett szervezeti egység vezetőjének írásban kell jeleznie az ICSV felé, aki az igényt elbírálja, és engedélyezés esetén intézkedik az adathordozó beszerzése, kiosztása érdekében.

Az adathordozó átadását és átvételét dokumentálni szükséges, legalább az alábbi adatokat rögzítve:

- adathordozó típusa, jellemzője és gyári azonosítója,
- adathordozót átadó személy neve és beosztása,
- adathordozó átvevő (a későbbiekben azt használó felelős megőrző) személy neve és beosztása,
- átadás helye, ideje,
- átadó és átvevő aláírása.

A BSZRK adathordozóin csak a BSZRK által jóváhagyott, az adathordozó felelős megőrzőjének feladatainak végrehajtásához szükséges adat tárolható.

Jogsértő, vagy magánjellegű adat, információ a BSZRK tulajdonát képező adathordozón nem tárolható.

A BSZRK az adathordozók használatát hardver, illetve szoftver úton korlátozhatja, szabályozhatja.

Az adathordozó megfelelő használatát a BSZRK előzetes értesítés nélkül figyelheti, monitorozhatja.

A BSZRK központi informatikai infrastruktúrájából bármilyen adatot, bármely okból (otthoni munkavégzés stb.) CD/DVD-n, elektronikus levélben vagy egyéb más módon (USB kulcson stb.) kijuttatni csak az érintett adatgazda előzetes, írásos engedélyével szabad.

3.1.5.2 Hozzáférés az adathordozókhoz

A BSZRK által birtokolt/kontrollált adathordozókhoz hozzáférés általánosságban az alábbi személyek részére, az alább meghatározott módon, mértékben engedélyezett:

Adathordozó	Adathordozó használatára feljogosított személy	Adathordozóhoz hozzáférés módja
asztali és, hordozható számítógépek merevlemezei	számítógép felelős megőrzője	felhasználó által kontrollált adatok írása, módosítása, törlése, a kinevezési okirat, szerződésnek, szabályzatoknak megfelelően
szerverek merevlemezei, a BSZRK informatikai rendszerein és megosztásain keresztül	informatikai felhasználók	felhasználó által kontrollált adatok írása, módosítása, törlése, a kinevezési okiratnak, szerződésnek, szabályzatoknak megfelelően
hordozható adathordozók	hordozható adathordozó felelős megőrzője	felhasználó által kontrollált adatok írása, módosítása, törlése, a kinevezési okiratnak, szerződésnek, szabályzatoknak megfelelően
számítógépek adathordozói	a BSZRK informatikai üzemeltetését támogató szakemberek, szervezetek	az üzemeltetéshez szükséges műveletek, a szerződéseknek, szabályzatoknak megfelelően
számítógépek adathordozói és hordozható adathordozók	ICS, IBF	adattartalom ellenőrzése
számítógépek adathordozói és hordozható adathordozók	ICS	adattartalom törlése, a szabályzatnak megfelelően

3.1.5.3 Adathordozók címkézése

A BSZRK EIR-einek adathordozóit címkével kell ellátni úgy, hogy abból egyértelműen kiderüljön melyik EIR adathordozója.

Az EIR adathordozóit csak abban az esetben lehetnek címkézés nélkül, amennyiben azok a BSZRK ICS által kontrollált területen belül maradnak.

3.1.5.4 Adathordozók tárolása

A BSZRK EIR-einek adathordozóit csak az arra kijelölt megfelelően ellenőrizhető és biztonságos helyen tárolja. Valamint gondoskodik az adathordozók védelméről mindaddig, amíg azokat a megfelelő eljárással meg nem semmisítették vagy törölték.

3.1.5.5 Adathordozók szállítása

A BSZRK adathordozóit csak az ICSV külön engedélyével lehet kivinni a szervezet által ellenőrzött területen kívülre. A szállítást megelőzően az adat hordozót be kell azonosítani és megfelelő jelzéssel kell ellátni, valamint meg kell győződni arról, hogy csak olyan adatok vannak rajta, amelyek kikerülhetnek a szervezetből. A kiszállítást minden esetben dokumentálni kell.

3.1.5.6 Adathordozók törlése

Az informatikai eszközök adathordozóit, illetve az önálló, hordozható adathordozókat újrahasznosítás, más felhasználó számára átadás, javításra átadás vagy selejtezés előtt át kell vizsgálni és a rajtuk levő adatokat (esetleges előzetes mentés után) visszaállíthatatlanul el kell távolítani. Ennek érdekében

- az adathordozókon tárolt adatokat törölni kell;
- a törlést az adattároló felelős megőrzőjének, használójának (elérhetetlensége esetén a munkahelyi felettesének) előzetesen írásban jóvá kell hagynia;
- garanciális eszközök esetén, ha az eszköz hibája miatt az adatok törlésére nincs mód, az ICSV dönt az eszköz cserére történő kiadhatóságáról vagy megsemmisítéséről.

Az adatok megfelelő módon történő eltávolításáért az adatgazda felelős. Az adatok eltávolítását az ICS végzi, az adatgazda és a felelős megőrző (elérhetetlensége esetén az ICSV vagy az IBF) jelenlétében.

Tárolt adat típusa	Törlési mechanizmus
nem nyilvános információ	egyszeres teljes felülírás
üzleti titok, személyes adatok	háromszoros teljes felülírás
egészségügyi adatok	nyolcszoros teljes felülírás

Az adatok eltávolítását, törlését annak körülményeivel, jellegzetességeivel jegyzőkönyvezni kell, a jegyzőkönyvet pedig a törlést végző személynek és a törlésen jelen lévő adatgazdának, valamint az adathordozó felelős megőrzőjének (elérhetetlensége esetén az ICSV-nek vagy az IBF-nek) alá kell írnia.

A kizárólag adatátadásra használt pendrive adattartalmának fent leírt módon való törlése abban az esetben helyettesíthető a fájl normál törlésével, ha a pendrive felelős megőrzője

- az adatátadás folyamatát személyesen figyelemmel tudja kísérni, és
- meggyőződik róla, hogy az adatátadásra használt pendrive csak a cserélendő fájl(oka)t tartalmazza,
- meggyőződik róla, hogy az adatátadásra használt pendrive-on más művelet nem kerül elvégzésre, csak a cserélendő fájl(ok) másolása,
- az adatcsere után az adatátadásra szolgáló pen drive-ot haladéktalanul eltávolítja, eltávolíttatja a számára idegen eszközből
- adatcsere után teljes kártékony kód elleni ellenőrzést végez a pendrive-on.

A csak romboló törlési technikával való adattörlésre alkalmas adathordozókat (CD, DVD stb.) adattörlési igény esetén fizikailag meg kell semmisíteni.

3.1.5.7 Adathordozók használata

A BSZRK csak az általa kiadott adathordozó használatát engedélyezi. Az adathordozót az a felhasználó használhatja, aki számára az adathordozó kiadásra került, illetve akinek a jogviszonyt megalapozó szerződése (kinevezési okirat, szerződés), és a BSZRK belső szabályzatai ezt engedélyezik; olyan mértékben és módon, ahogyan az a BSZRK által elvárt feladatai teljesítéséhez szükséges.

A BSZRK adathordozóit csak az adathordozó használója, felelős megőrzője használhatja, illetve adatcsere esetén az adatcserében részt vevő fél, de kizárólag az adatcsere idejére, az adathordozó felelős megőrzőjének felügyelete mellett.

Adatcserére használt adathordozón az adatcserében érintett adaton túl további adat nem tárolható, amelyről az adatcserét megelőzően az adathordozó használója, felelős megőrzője köteles meggyőződni.

Nem engedélyezett a BSZRK által tulajdonolt és/vagy kontrollált adathordozó informatikai eszközből való kiszerelése, megsemmisítése, vagy bármilyen módon a BSZRK kontrollja alóli kivonása, vagy a BSZRK adathordozó feletti kontrolljának csökkentése vagy módosítása, kivéve, ha erre az FI engedélyt ad.

Nem engedélyezett a BSZRK által tulajdonolt és/vagy kontrollált adathordozó átadása vagy megosztása olyan személlyel, szervezettel, amelyre a BSZRK nem adott engedélyt.

Nem engedélyezett a BSZRK által tulajdonolt és/vagy kontrollált adathordozóra olyan adat, információ másolása, amelyre a BSZRK nem adott engedélyt.

Nem engedélyezett a BSZRK által tulajdonolt és/vagy kontrollált adathordozóról olyan mentés készítése, amelyre a BSZRK nem adott engedélyt.

Az adathordozók használatát a BSZRK által megbízott foglalkoztatottjai vagy külső személy, BSZRK előzetes bejelentés nélkül ellenőrizheti.

Az adathordozók használatára vonatkozó elvárások megszegése szankcionálható, valamint feljelentéssel, kártérítéssel, kárenyhítéssel, sérelemdíj fizetésével járhat.

3.1.6 Fizikai és Környezeti védelem

3.1.6.1 Eljárásrend

Jelen fejezet alkalmazása során figyelemmel kell lenni a más jogszabályban meghatározott tűz-, és személyvédelmi, valamint a személyes adatok kezelésére vonatkozó rendelkezésekre, valamint arra, hogy e fejezet rendelkezései a BSZRK székhelyéül és telephelyéül szolgáló kórházi épületeknek csak a BSZRK által felügyelt, kontrollált területére vonatkoznak.

A BSZRK az ebben a fejezetben meghatározott módon kívánja definiálni, kezelni, dokumentálni és a BSZRK-n belül kihirdetni az EIR szempontjából érintett létesítményekre, helyiségekre érvényes fizikai védelmi eljárásrendet.

Az eljárásrendet rendszeresen, de legalább évente felül kell vizsgálni és frissíteni kell.

Az ebben a pontban leírtak végrehajtása, koordinálása az ICSV, ellenőrzése az IBF feladata

3.1.6.2 A fizikai belépési engedélyek

A BSZRK székhelyének, telephelyének helyt adó épületekbe a BSZRK Beléptetési rendre vonatkozó szabályzata szerint kell eljárni a következők figyelembevételével.

Belépési engedély nélkül a BSZRK által kontrollált területre belépni tilos.

Riasztókód és fizikai kulcs másnak átadása tilos.

A belépésre jogosult személyek listájáról el kell távolítani azokat, akik a belépésre már nem jogosultak.

Az IBF az ICSV és a MOV közösen rendszeresen, de legalább évente ellenőrzi a belépési jogosultságok negyedéves felülvizsgálatának megtörténtét, és ha szükségesnek ítéli, áttekinti, ellenőrzi a belépésre jogosult személyek listáját.

A fizikai kulcs elvesztését a BSZRK előírásai alapján kell kezelni és dokumentálni.

3.1.6.3 A fizikai belépés ellenőrzése

A BSZRK a fizikai belépés ellenőrzésével kapcsolatos alapvető elvárásokat, eljárásokat az alábbiaknak megfelelően határozza meg:

- A belépésre jogosultak számára a fizikai belépés kizárólag a BSZRK által meghatározott be-, és kilépési pontokon biztosított.
- Az engedély nélkül nem látogatható területekre bejutást nyújtó belépési pontokon a belépést fizikailag megakadályozó, gátló eszközöket kell felszerelni (sorompó, forgóvilla stb.), amelyek csak az engedélyezett belépéseket teszik lehetővé.
- A BSZRK önmaga vagy ezzel megbízott partnerei által naplózza a fizikai belépéseket.
- A BSZRK-nak ellenőrzés alatt kell tartania a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket, amelybe beletartozik a helyiségek videó megfigyelő rendszerrel való megfigyelése (amennyiben a BSZRK vagyonvédelmi vagy más okból szükségesnek tartja, a felvételek rögzítésével és előírásainak megfelelő megőrzésével, amelyet a BSZRK az általa alkalmazott elektronikus megfigyelő rendszer által rögzített képekkel és felvételekkel kapcsolatos adatkezelésről szóló szabályzata tartalmaz részletesen).
- A videomegfigyelő, illetve a felvételek rögzítését és visszanézését végző rendszer kezelését a BSZRK a személyes adatok védelmére vonatkozó, illetve további jogszabályoknak megfelelően köteles szabályozni és végezni. A szabályzás elkészítése az BSZRK DPO-nak a feladata, az előírások betartása pedig valamennyi érintett kötelessége.
- A létesítménybe meghívott, eseti belépésre jogosultakat a BSZRK számukra meghívót küldő, vagy a meghívó által megbízott foglalkoztatottja kíséri, és figyeli a meghívott tevékenységét.
- A rá bízott kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző, lehetővé tevő eszközt a BSZRK valamennyi foglalkoztatottja és partnere köteles megóvni és az elírásoknak megfelelően kezelni.
- A fizikai belépést ellenőrző, illetve lehetővé tevő eszközről nyilvántartást kell vezetni. A nyilvántartás vezetése az adott eszközt kiadó foglalkoztatott feladata.
- A fizikai belépést biztosító hozzáférési kódokat meghatározott rendszerességgel (de legalább évente), vagy haladéktalanul akkor kell megváltoztatni, ha a hozzáférési kód kompromittálódik.

- A fizikai belépést biztosító hozzáférési kulcsokat haladéktalanul le kell cserélni, ha a kulcs elvészik.
- Az egyéni belépési engedélyeket a belépési pontokon ellenőrizni kell. A BSZRK foglalkoztatottjainak figyelmét fel kell hívni a fizikai biztonsággal kapcsolatos rendellenességek, szokásos körülményektől eltérő körülmények, nem szokásos események jelentésére (és ezekre, valamint a jelentési kötelességre ki kell térni az információbiztonsági képzésben is). A jelentést az informatikai Help Desk számára kell elküldeni, akik az ICS belső előírásai szerint kezelik azokat.

3.1.6.4 Hozzáférés az adatátviteli eszközökhöz és csatornákhoz

A BSZRK adatátviteli eszközeit és a hozzájuk tartozó átviteli vezetékeket úgy kell kialakítani és elhelyezni, hogy azokhoz csak az erre feljogosított foglalkoztatottak férjenek hozzá.

Adatátviteli eszköz esetén ez biztosítható:

- zárt rack szekrényben történő elhelyezéssel,
- zárt közmű szekrényben történő elhelyezéssel

Átviteli vezetékek esetén:

- az elérhető aljzat fizikai leválasztásával,
- zárt kábelrendező használatával,
- védőcső, vagy kábeltálca használatával

3.1.6.5 A kimeneti eszközök hozzáférés-ellenőrzése

A BSZRK ellenőrzi az EIR kimeneti eszközeihez való fizikai hozzáférést annak érdekében, hogy jogosulatlan személyek ne férjenek hozzá az előállított kimenetekhez.

Ennek érdekében a kimeneti eszközök csak zárt, hozzáférés-ellenőrzött terekben helyezhetők el.

3.1.6.6 A fizikai hozzáférések felügyelete

A BSZRK az ICSV által

- ellenőrizni rendeli az EIR-eknek helyt adó helyiségekbe történt fizikai hozzáféréseket annak érdekében, hogy észlelje a fizikai biztonsági eseményt és reagáljon arra;
- rendszeresen, de legalább negyedévente 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 átvizsgálásokat.

A BSZRK behatolásjelző és megfigyelő rendszereket alkalmaz az EIR-eknek fizikailag helyet adó szerverszobák felügyeletére.

A BSZRK a felsorolt ellenőrzéseket a neki információtechnológiai szolgáltatást nyújtó partnereknél is jogosult indoklás nélkül ellenőrizni, az adott partner belső ellenőrét vagy a partner által erre kijelölt személyt a vizsgálatba bevonva. Az erre vonatkozó jogosultságot a partnerekkel kötött szerződésekben szerepeltetni kell, amely a IJ feladata; az ellenőrzésre pedig az IBF jogosult.

A jelen pontban leírt feladatok betartásának ellenőrzését az IBF végzi, legalább éves gyakorisággal.

3.1.6.7 Látogatói hozzáférési naplók

A BSZRK az EIR-einek helyt adó létesítményeibe lépő látogatók ellenőrzésével kapcsolatos alapvető elvárásokat az alábbiakban határozza meg:

- A BSZRK EIR-eknek helyt adó, általa felügyelt létesítményeibe (szerverszoba, informatikai raktár stb.) látogató csak kísérettel léphet be, tartózkodhat. A kísérőnek a látogatót meghívó, vagy általa kijelölt foglalkoztatottnak kell lennie.
- A látogatót a BSZRK erre kijelölt beléptetési pontjain kell fogadnia az őt kísérő foglalkoztatottnak, akinek a látogatás adatait nyilvántartásba kell vennie.
- Az EIR-eknek helyt adó létesítményekbe történt látogatói belépésekről szóló információkat egy évig dokumentált formában meg kell őrizni. A dokumentumnak legalább a következőket tartalmaznia kell:
    - a látogató nevét, szervezetét, beosztását,
    - a látogatót meghívó személyt és beosztását,
    - a látogatót kísérő személy nevét és beosztását,
    - a belépés és kilépés idejét
    - a kísérő fenti adatok megfelelőségét igazoló aláírását
- A nyilvántartás megoldható az elvárt adatok papíralapú vagy elektronikus nyilvántartásával, amely utóbbi történhet önálló alkalmazásban, vagy meglévő alkalmazás kiegészítésében, vagy más módon, ha a nyilvántartás vezetésének módja, körülményei egyébként megfelelnek ennek és a BSZRK további szabályzatainak, követelményeinek.
- A nyilvántartást egy évig meg kell őrizni, amely az ICSV feladata.
- A látogatói belépések nyilvántartásáért, a nyilvántartások kezeléséért, a nyilvántartás és beléptetés részletszabályainak kialakításáért az ICSV felelős.
- A látogatói be lépésekről készített információkat azonnal át kell vizsgálni, ha a rendelkezésre álló információk jogosulatlan belépésre utalnak - ennek felelőse az ICSV.

A jelen pontban leírt feladatok végrehajtásának ellenőrzését az IBF végzi, legalább éves gyakorisággal.

3.1.6.8 Áramellátó berendezések és kábelezés

A BSZRK EIR-einek áramellátását biztosító berendezéseket és kábelezést úgy kell kialakítani, hogy azokat ne érje sérülés vagy legyenek kitéve rongálásnak.

3.1.6.9 Vészkikapcsolás

A BSZRK az EIR-einek helyet adó szerverszobákban lehetőséget biztosít az áramellátás vészhelyzetben történő lekapcsolására.

Az ehhez szükséges kapcsolókat úgy kell elhelyezni, hogy azok zárt csak a megfelelő jogosultságokkal rendelkező személyek által hozzáférhető helyen legyenek elhelyezve és megközelítésük könnyű és biztonságos legyen.

Minden vészkikapcsolást dokumentálni kell és annak legalább a következő információkat tartalmaznia kell:

- a kikapcsolás ideje
- a kikapcsolás oka
- a kikapcsolást végző személy

3.1.6.10 Vészhelyzeti tápellátás

A BSZRK EIR-eit legalább akkora szünetmentes tápegységgel kell ellátni, hogy azok az elsődleges áramforrásuk kiesése esetén még biztonságos módon leállíthatóak legyenek.

A szünetmentes tápegységeket a gyártó által meghatározott módon karban kell tartani, meghatározott gyakorisággal tesztelni kell és ezeket a folyamatokat dokumentálni kell.

A feladat elvégzése az ICSV feladata, amit az IBF ellenőriz.

3.1.6.11 Vészvilágítás

A BSZRK a szerverszobában és az általa kontrollált irodai és egyéb tevékenységekre szolgáló területen automatikus vészvilágítási rendszer használatát írja elő, amely áramszünet esetén aktiválódik, és amely biztosítja a vészkijáratokat és a menekülési útvonalakat; egyben elrendeli ezen rendszer rendszeres karbantartását.

A pontban leírt elvárás teljesítéséért a BSZRK karbantartási feladatait ellátó külső szervezet felel.

3.1.6.12 Tűzvédelem

A tűzvédelemmel kapcsolatos általános előírásokat a BSZRK hatályos „Tűzvédelmi szabályzata" tartalmazza. Az ebben a szabályzatban leírt elvárások a Tűzvédelmi szabályzat követelményeit nem helyettesítik, hanem kiegészítik.

A BSZRK EIR-einek helyt adó létesítményeiben független áramellátással támogatott, az adatokat naplózó hőmérsékletmérő, valamint tüzet (hőmérséklet emelkedést, füstöt) észlelő, továbbá az informatikai eszközökhöz megfelelő tűzelfojtó berendezéseket kell alkalmazni, amelyeket rendszeresen (de legalább évente) a helyszínen karbantartani és tesztelni szükséges, az oltóponttal egyetemben.

Törekedni kell rá, hogy a BSZRK EIR-einek helyt adó létesítményeiben alkalmazott tűzelfojtó berendezések automatikus működésűek legyenek.

A BSZRK EIR-einek helyt adó létesítményeiben alkalmazott tűzelfojtó berendezések az EIR-eket, illetve az azok működését elősegítő informatikai infrastruktúra elemeket nem károsíthatják, sem működési elvük, sem elhelyezkedésük által.

A pontban leírt elvárás teljesítéséért a BSZRK tűzvédelmi felelőse felelős.

3.1.6.13 Környezeti védelmi intézkedések

A BSZRK elrendeli, hogy

- az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. adatközpont, szerver szoba, központi gépterem) az erőforrások biztonságos működéséhez szükséges szinten kell tartani a hőmérsékletet és páratartalmat

- az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. adatközpont, szerver szoba, központi gépterem) meg kell figyelni a hőmérséklet és páratartalom szintjét,
- a nem kívánatos tartományba eső hőmérsékletről és páratartalomról az ICS riasztást kell, hogy kapjon,
- a riasztást incidensként kell kezelni és ki kell rá dolgozni a megfelelő kezelési eljárásokat.

A pontban leírt elvárás teljesítéséért az ICSV felelős. Az elvárásnak megfelelést az IBF legalább évente ellenőrizni köteles.

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

A BSZRK a víz-, és más, csővezetéken szállított anyag okozta kár ellen az EIR-t az alábbiak szerint védi:

- az EIR-t védeni kell a csővezeték rongálódásból származó károkkal szemben,
- biztosítani kell, hogy a csővezetékek főelzáró szelepei hozzáférhetőek legyenek, és megfelelően működjenek, valamint a kulcsszemélyek (legalább az ICSV, valamint az ICS további, az ICSV által írásban kijelölt foglalkoztatottjai) számára elhelyezésük és használatuk ismert legyen;
- az informatikai erőforrásokat koncentráltan tartalmazó helyiségek tervezése (pl. adatközpont, szerver szoba, központi gépterem) során biztosítani kell, hogy az a víz-, és más hasonló kártól védett legyen, akár csővezetékek kiváltásával, áthelyezésével is.

A pontban leírt elvárás teljesítéséért az ICSV, illetve a BSZRK karbantartását végző külső szervezet felel. Az elvárásnak megfelelést az IBF legalább évente ellenőrizni köteles.

3.1.6.15 Be- és kiszállítás

A BSZRK által kontrollált területre csak az ICSV előzetes, írásos engedélyével és az ICS foglalkoztatottjainak jelenlétében szabad információs rendszerelemeket beszállítani, ott elhelyezni, vagy onnan elszállítani.

A beérkező információs rendszerelemet szállítólevélen át kell venni, majd az ICS elektronikus rendszerelem nyilvántartásába a rendszerelemet annak jellemzőivel együtt fel kell venni (nyilvántartásba kell venni), az ICS belső rendelkezéseinek megfelelő módon.

Az információs rendszerelemek mozgatását az ICS elektronikus rendszerelem nyilvántartásában kell dokumentálni, oly módon, hogy a rendszerelemek állapota és elérhetősége naprakész legyen.

A pontban leírt elvárás teljesítéséért az ICSV felelős. Az elvárásnak megfelelést az IBF legalább évente ellenőrizni köteles.

3.1.6.16 Munkavégzésre kijelölt alternatív helyszín

A BSZKR foglalkoztatottja számára az adott osztály vagy csoport vezetője jelölhet ki alternatív munkavégzési helyszínt a „Munkaszerződéstől - szokásos munkavégzés helyétől - eltérő foglalkoztatás szabályzata" szerint.

Amennyiben az alternatív munkavégzési helyszín a BSZRK által kontrolált területen kívül található a „3.2.1.12 Távoli hozzáférés" pont és a BSZRK „Távmunka végzés szabályzat" -a szerint kell eljárni.

Az alternatív munkavégzési helyszínen dolgozók ugyanúgy kötelesek jelenteni a BSZRK számára az általuk észlelt biztonsági eseményeket mintha a BSZRK területén lennénk.

3.1.7 Tervezés

3.1.7.1 Eljárásrend

A biztonságtervezési szabályzat és eljárásrend kidolgozása, dokumentálása és kiadatása az ICSV feladata, akit ebben az IBF támogat.

Az eljárásrendet rendszeresen, de legalább évente felül kell vizsgálni, aktualizálni kell. A felülvizsgálat és aktualizálás az ICSV feladata.

A tervezéssel kapcsolatos elvárások teljesülését az IBF feladata legalább évente ellenőrizni.

3.1.7.2 Rendszerbiztonsági terv

A BSZRK-nak, ha az EIR tervezése a hatáskörébe tartozik, az EIR-hez rendszerbiztonsági tervet kell készítenie, amely

- összhangban áll a BSZRK szervezeti felépítésével vagy szervezeti szintű architektúrájával;
- meghatározza az EIR hatókörét, alapfeladatait és biztosítandó szolgáltatásait;
- meghatározza azokat a személyeket, akik az EIR vonatkozásában felelősséget vagy szerepet töltenek be;
- meghatározza az EIR és az általa kezelt adatok jogszabály szerinti biztonsági osztályát;
- meghatározza és felsorolja az EIR-t érintő fenyegetéseket;
- meghatározza az EIR biztonsági osztályát;
- meghatározza az EIR működési körülményeit és más EIR-ekkel való kapcsolatait;
- a vonatkozó rendszerdokumentáció keretébe foglalja az EIR biztonsági követelményeit;
- meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedés bővítéseket, végrehajtja a jogszabály szerinti biztonsági feladatokat;
- meghatározza azokat az EIR-rel kapcsolatos biztonsági tevékenységeket, amelyekhez személyek és csoportok közötti koordináció szükséges;
- a tervet az ICSV végrehajtás előtt áttekinti és jóváhagyja;
- 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 EIR rendszerbiztonsági tervét;
- frissíti a rendszerbiztonsági tervet az EIR-ben vagy annak üzemeltetési környezetében történt változások és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén;
- gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

A rendszerbiztonsági terv készítése az adott rendszer tervezéséért felelős informatikus feladata, akit az ICSV ellenőriz. A rendszerbiztonsági tervek elkészítésének állapotát az IBF évente áttekinti.

3.1.7.3 Viselkedési szabályok

Az EIR-hez való hozzáférés engedélyezése előtt a hozzáférési jogosultságot igénylő személynek írásban nyilatkoznia kell, hogy az EIR használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, megértette; és azok betartását, az azoknak való megfelelést vállalja. A nyilatkozatot a foglalkoztatottak esetében a MOV, a szerződéses partnerek esetében az adott szerződésben a BSZRK oldaláról kijelölt kapcsolattartó feladata a hozzáférést igénylővel aláíratni, majd a nyilatkozatot a foglalkoztatottak esetében az érintett személy BSZRK-on belüli foglalkoztatotti jogviszonyának megszűnését, szerződéses partnerek esetében az adott szerződés lezárását követő 8 évig őrizni. A jogosultsági igényre vonatkozó döntés előtt a döntést meghozó személy köteles meggyőződni, hogy a jogosultságot igénylő a nyilatkozatot aláírta. A hozzáférés ezen nyilatkozat hiányában nem hagyható jóvá, illetve nem állítható be.

Az EIR hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységet és a betartandó viselkedési szabályokat legalább évente felül kell vizsgálni és frissíteni kell, amelynek koordinálása az IBF feladata.

Az EIR-ekel kapcsolatos elvárások változása esetén a hozzáféréssel rendelkezőkkel a változásokat meg kell ismertetni, különös tekintettel a velük szembeni elvárásokra, a rájuk vonatkozó szabályokra, felelősségükre, az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységre és a betartandó viselkedési szabályokra. Az IBSZ-en alapuló változásokat az IBF, a többi módosításról szóló tájékoztatás esetében az ICS feladata mindez.

A BSZRK-on kívüli irányban megvalósuló, ezen szabályzaton túlmutató információbiztonsági követelményeket az IBF-nek kell meghatároznia és koordinálnia, hogy azokat a BSZRK-val szerződéses kapcsolatra lépők a szerződéses kapcsolat aláírása előtt megismerjék, az elvárások megértéséről és betartásáról nyilatkozzanak (amely a szerződéses kapcsolat létrejöttének feltétele).

A BSZRK honlapjának oldalainak, felületeinek formai és tartalmi gondozása a közösségi médiáért felelős személy feladata, más szervezeti egység ezeket kizárólag a BSZRK FI-nek kifejezett, írásos kérése esetén módosíthatja, illetve rendelheti el a módosításukat.

A BSZRK közösségi médiában történő megjelenéseit az erre kijelölt szervezeti egység, személyek koordinálják. A foglalkoztatottak és szerződéses partnerek közösségi médiában való jelenléte a magánszférába tartozik, és ezt a BSZRK tiszteletben tartja, ugyanakkor a foglalkoztatottak és szerződéses partnerek nem léphetnek fel a BSZRK nevében a közösségi médiában, nem publikálhatnak, nem oszthatnak meg és semmilyen formában nem tehetnek közzé, vagy segíthetnek elérni a BSZRK-val kapcsolatos információkat, különösen védett szakmai/gazdasági/egészségügyi információkat, és nem hivatkozhatnak a BSZRK-ra, nem jeleníthetik meg a BSZRK-at annak értékeivel ellentétes módon.

Az BSZRK ezért

- tiltja és számon kéri
    - a BSZRK-al kapcsolatos információk Internet oldalakon és közösségi oldalakon, felületeken való közzétételét;
    - a BSZRK nevében vagy az BSZRK-hoz kapcsolhatóan végzett információterjesztést,

- az EIR és a szervezet vonatkozásában használt azonosítók és hitelesítési adatok használatát külső weboldalak esetén

amennyiben az nem a BSZRK által erre kinevezett szervezeti egységek, személyek által, vagy nem a BSZRK vezetése által kifejezetten erre felszólító döntés alapján történt (a felületekbe nem kizárólagosan beleértve a fórumokat, blogokat, chatalkalmazásokat, hirdetőtáblákat és más, információ megjelenítésre, megosztásra és tárolásra szolgáló BSZRK-on kívüli megoldásokat; a közlésbe és közzétételbe pedig beleértve valamennyi publikálást vagy elérhetővé tételt);

- tiltja és számon kéri
  - a BSZRK céljaival, szándékaival, érdekeivel ellentétes információ, tartalom terjesztését,
  - a BSZRK informatikai eszközeivel, illetve munkaidőben a munkavégzéshez nem kapcsolódó, az Interneten és közösségi oldalakon, felületeken megvalósuló tevékenységet, amelybe például (de nem kizárólagosan) beletartozik a kártékony kód letöltése/futtatása, a BSZRK erőforrásainak megosztásával végzett tevékenység (pl. kriptovaluta bányászata, erőforrás-megosztáson alapuló tevékenység végzése), erőszakos vagy jó erkölcsbe ütköző tartalmat kínáló oldalak látogatása; tartalom publikálása, megosztása vagy tovább osztása,
  - a BSZRK eszközeivel és/vagy munkaidőben a közösségi oldalak és magán postafiókok, tartalom- és/vagy információ cserélő megoldások használatát/elérését; és egyéb, a BSZRK szakmai céljaitól idegen tevékenységet.
  - a BSZRK informatikai eszközeivel, illetve munkaidőben a BSZRK céljaival és/vagy szándékaival ellentétes információ, tartalom terjesztését, értékelését, minősítését.

3.1.7.4 Információbiztonsági architektúra leírás

A BSZRK (ha a hatáskörébe tartozik, és ha más dokumentumban nem kerül meghatározásra, vagy azokból nem következik)

- elkészíti az EIR 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.

A BSZRK EIR-ének az információbiztonsági architektúra leírásának elkészítését az IBF koordinálja, a készítést az ICS támogatja, és az ICSV ellenőrzi az elkészült architektúra leírásokat.

Az információbiztonsági architektúra leírásnak

- összegeznie kell az EIR bizalmasságának, sértetlenségének és rendelkezésre állásának védelmét szolgáló filozófiát, követelményeket és megközelítést;
- meg kell fogalmaznia, hogy az információbiztonsági architektúra miként illeszkedik a BSZRK általános architektúrájába, és hogyan támogatja azt;
- le kell írnia a külső szolgáltatásokkal kapcsolatos információbiztonsági feltételezéseket és függőségeket

3.1.7.5 Biztonsági követelmények kiválasztása

A BSZRK az EIR-einek biztonsági alapkövetelményeit úgy választják ki, hogy azok megfeleljenek a törvények, végrehajtási rendeletek, irányelvek, szabályzatok, irányelvek, szabványok és iránymutatások által előírtaknak.

Továbbá a kiválasztás során figyelembe kell venni az adott EIR által tárolt, feldolgozott és továbbított adatok típusát, illetve a kockázatértékelések eredményét.

A kiválasztott biztonsági alapkövetelményeket az adott EIR rendszerbiztonsági tervében kell rögzíteni.

3.1.7.6 Biztonsági követelmények testre szabása

Amennyiben a BSZRK EIR-ének működési környezet és specifikus igényei szükségessé teszik a biztonsági alapkövetelményeket testre kell szabni.

Ez történhet:

- kiegészítő védelmi intézkedés bevezetésével
- egyedi védelmi intézkedés vagy biztonsági követelmény bevezetésével

Ezeket a testre szabott biztonsági követelményeket szintén az adott EIR rendszerbiztonsági tervében kell rögzíteni.

3.1.8 Személyi biztonság

3.1.8.1 Eljárásrend

A személybiztonsággal kapcsolatos eljárásoknak és elvárásoknak ki kell terjedniük a BSZRK teljes személyi állományára, valamint minden olyan természetes személyre, aki a BSZRK EIR-eivel kapcsolatba kerül, vagy kerülhet.

Azokban az esetekben, amikor az EIR-eivel tényleges vagy feltételezhető kapcsolatba kerülő személy nem a BSZRK foglalkoztatottja, 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).

3.1.8.2 Munkakörök biztonsági szempontú besorolása

A BSZRK-on belüli, nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat fel kell mérni, és valamennyi érintett BSZRK munkakört, vagy érintett BSZRK-hoz kapcsolódó feladatot biztonsági szempontból be kell sorolni a „Munkakörök biztonsági szempontú besorolása" külön álló dokumentum leírása alapján.

A besorolásokat a ICSV hajtja végre és küldi a FI-nek jóváhagyásra. A jóváhagyott besorolást a MO továbbítja az IBF és ICSV felé (ezen szabályzat előző bekezdésben említett függelékének frissítése érdekében).

A munkakörök és feladatok biztonság szempontú besorolását rendszeresen, legalább évente felül kell vizsgálni és frissíteni kell. A felülvizsgálatot és frissítést a besorolásért felelős személy koordinálja, végzi.

3.1.8.3 Személyek háttérellenőrzése

Az EIR-hez való hozzáférési jogosultság megadása előtt ellenőrizni kell, hogy az érintett személy munkaköre, illetve az érintett személy a biztonsági besorolásnak megfelelő feltételekkel rendelkezik-e.

A munkakörök megfelelő besorolását, illetve a munkakör ellátásához szükséges feltételek teljesülését folyamatosan ellenőrizni kell.

Az ezen pontban leírtakat a MO koordinálja.

3.1.8.4 Személyek munkaviszonyának megszűnése

A BSZRK foglalkoztatottjai esetében a jogviszony megszüntetésekor, illetve akkor, ha a további munkavégzéshez nem szükségesek:

- az érintett személy az általa használt, a BSZRK tulajdonát képező informatikai eszközöket az ICS-nak adja le, akik azokat átvételi elismervénnyel veszik vissza, és ezt igazolják az adott személy elszámoló lapján.
- a felhasználó e-mail címét, postafiókját és felhasználói azonosítóit az ICS szünteti meg és az az erre vonatkozó igazolást rávezeti az adott személy elszámoló lapjára.
- a leszerelő lapra felvezetett adatokról az ICS elektronikus levélben is köteles tájékoztatni a MO-t (a jogviszonyt megszüntető személy által fizikailag a MO-nak átadott, kitöltött leszerelő lap önmagában nem igazolja az eszközök visszavételét, jogosultságok visszavonását).
- a MOV tájékoztatja a munkaviszony megszüntetése alatt álló személyt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről.
- a megszűnő jogviszonyú személy EIR-rel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszonyt megszüntető foglalkoztatott közvetlen felettese köteles gondoskodni (amennyiben ez szükséges, illetve megoldható);
- az ICS a jogviszony megszűnésekor a megszűnt jogviszonyú személy esetleges EIR-t, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását a belső ügyrendjében meghatározott módon (a jogosultság megszüntetésén túl is) megelőzi (pl. a hozzáféréshez a továbbiakban nem szükséges eszközök érvényességének megszüntetésével, az érintett felhasználói azonosító(k) felfüggesztésével/zárolásával).
- a MO, illetve más jogviszony esetén a felhasználóval kapcsolatot tartó szervezeti egység vezetője a jogviszony megszűnéséről az általa meghatározott módon értesíti az általa szükségesnek tartott, megfelelő szerepköröket betöltő, feladatokat ellátó személyeket, a BSZRK-on belül, illetve a külső partnereknél.

Tartós (várhatóan 30 naptári napot meghaladó) távollét esetén (a keresőképtelenséget kivéve), a FI mérlegelése alapján, a folyamat a fent leírttal megegyezik, azzal a különbséggel, hogy

- a tartós távollét tényére és várható hosszára vonatkozó információt az ISZO köteles megosztani az ICS-val (a távollét pontos okát nem engedélyezett megosztani),
- az érintett jogosultságát vissza kell vonni/szüneteltetni kell,
- az általa használt eszközöket akkor kell visszavenne, ha a tartós távollét előre tervezhető volt,
- a tájékoztatást nem a munkaviszony megszüntetésére tekintettel kell adni, hanem a tartós távollétre hivatkozva (amelynek pontos okát nem engedélyezett a tájékoztatás során megosztani).

Ha a jogviszony megszűnésében, megváltozásában érintett személy, külső szervezet, partner informatikai rendszeréhez is jogosultsággal rendelkezik, ezeket a jogosultságokat a BSZRK-on belüli jogosultságokhoz hasonlóan vissza kell vonatni, amelyért az adott külső szervezettel, partnerrel kapcsolatot tartó személy a felelős. Ha ez a kapcsolattartó az érintett személy volt, akkor az új kapcsolattartónak kell intézkednie.

Megszűnt jogviszonyú személy nem rendelkezhet olyan aktív felhasználói azonosítóval, jogosultsággal, hozzáféréssel (sem a BSZRK-on belül, sem kívül), amelyet a személy a BSZRK-val fenntartott jogviszonya keretében, illetve emiatt kapott. A megfelelő deaktiválási lehetőségre már a felhasználói azonosító, jogosultság, hozzáférés igénylésekor fel kell készülni, az esetlegesen szükséges jogi és technológiai hátteret (pl. megfelelő szerződéses háttér, nyilatkozatok elkészítése) már az igénylés során ki kell alakítani, amely a felhasználói azonosítót, jogosultságot, hozzáférést igénylő feladata és felelőssége.

Tartós távollétről visszatérő személynek a korábban használt, felfüggesztett felhasználói azonosítóit kell visszaadni; annak az ismételt ellenőrzésével, hogy a felhasználó valamennyi korábbi jogosultsága visszavonásra került-e.

Megszüntetett jogviszonyú foglalkoztatott ismételt alkalmazásakor a foglalkoztatottnak a korábban használt, felfüggesztett informatikai felhasználói azonosítóit kell visszaadni, annak az ismételt ellenőrzésével, hogy a felhasználó valamennyi korábbi jogosultsága visszavonásra került-e.

A BSZRK-nak meg kell tartania a hozzáférés lehetőségét a kilépő foglalkoztatott által korábban használt, kezelt adatokhoz.

3.1.8.5 Az áthelyezések, átirányítások és kirendelések kezelése

Áthelyezés, átirányítás és kirendelés esetén személyi biztonsági szempontból „3.1.8.3 Személyek háttérellenőrzése" pontban írottaknak megfelelően kell eljárni.

Az áthelyezett, átirányított, kirendelt foglalkoztatott számára logikai és fizikai hozzáférést kell kérni, engedélyezni és beállítani az addig nem használt, de az áthelyezést, átirányítást, kirendelést követően használni szükséges elektronikus információs rendszerhez; egyben meg kell szüntetni a továbbiakban nem szükséges hozzáféréseket.

A felhasználók létrehozása, kezelése, jogosultság beállítása és karbantartása során meg kell előzni (vagy ha korábban kialakult, meg kell szüntetni) az összeférhetetlenséget a felhasználó

- ugyanazon időben, párhuzamosan betöltött munkakörei, szerepkörei, valamint használt azonosítói között, valamint a
- korábbi munkakörében, szerepkörében indított tranzakciói későbbi kezelése (jóváhagyása, ellenőrzése stb.) között.

Felhasználó saját magára vonatkozó, felhasználói azonosítót és jogosultságokat érintő döntéseket nem hozhat, kivéve a FI, aki személyi felelőssége miatt erre feljogosított.

Az esetleges összeférhetetlenség vizsgálata a felhasználói azonosítóra, illetve jogosultság igénylésre, karbantartásra vonatkozó igény kérelmezőjének és jóváhagyójának a feladata.

A hozzáférés igénylése, engedélyezése és beállítása megegyezik a „3.2.1.2 Fiókkezelés" pontban leírtakkal.

A jogviszony változásáról elektronikus levélben (vagy külső partnerek esetében a kapcsolódó szerződésekben meghatározott módon) értesíteni kell az érintettel korábban és a jövőben kapcsolatot tartó felhasználókat, személyeket.

Az áthelyezés, átirányítás és kirendelés kezelése során a BSZRK vonatkozó szabályzatában leírtakat be kell tartani.

3.1.8.6 Hozzáférési megállapodások

A BSZRK EIR-eiehez való hozzáférést szabályozza a „4.2 INFORMÁCIÓSBIZTONSÁGI HÁZIREND ÉS NYILATKOZAT (FOGLALKOZTATOTTAK ÉS PARTNEREK SZÁMÁRA" függelékben, amit a hozzáférés megadása elött el kell fogadtatni a hozzáférést igénylővel

A megállapodásban bekövetkezett változások esetén, de legalább kétévente újra el kell fogadtatni a hozzáférés feltételeit.

A hozzáférési megállapodást az IBF köteles legalább kétévente felülvizsgálni és az ICSV-vel koordináltan frissíteni.

3.1.8.7 Külső személyekhez kapcsolódó biztonsági követelmények

A BSZRK-nak a külső szervezettel kötött megállapodásban, szerződésben meg kell követelnie, hogy a külső szervezet határozza meg a BSZRK informatikai infrastruktúrájában számukra (munkavállalói, partnerei számára) a szerződés/megállapodás teljesítéséhez szükséges, információbiztonságot érintő szerep- és felelősségi köröket, és a kapcsolódó elvárásokat is.

A BSZRK-nak szerződéses kötelezettségként meg kell követelnie, hogy a szerződő fél feleljen meg a BSZRK által meghatározott személybiztonsági követelményeknek, és ezt dokumentáltan igazolja. Valamint, amennyiben a szerződéses félnek szüksége van hozzáférésre az BSZRK valamely EIR-éhez, ahhoz külön hozzáférést kell igényelni.

A BSZRK-nak a külső szervezettel kötött megállapodásban, szerződésben elő kell írnia, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik a BSZRK EIR-éhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor a változásról soron kívül (egy napon belül) küldjön értesítést a BSZRK-nak; a külső szervezettel kapcsolatot tartón keresztül. Az így beérkező értesítést haladéktalanul el kell juttatni a BSZRK MO-hoz, az ICS-nak és az IBF-nek, további intézkedésre (a jogosultságok haladéktalan visszavonása és a visszavonás ellenőrzése érdekében).

A BSZRK-nak folyamatosan ellenőriznie kell a szerződő partner által munkavégzésre, kapcsolattartásra kijelölt munkavállalójának, alvállalkozójának a személybiztonsági követelményeknek való megfelelését - ennek sikeressége érdekében a BSZRK-nak a szerződésben előzetesen elő kell írnia az ilyen ellenőrzések tűrését és támogatását.

Külső szervezettel nem engedélyezett olyan szerződést aláírni, amely nem felel meg az ebben a pontban meghatározott elvárásoknak.

Az ebben a pontban leírtak betartása, betartatása a MO feladata. A külső szervezettel kötött szerződésekben az elvárások szerepeltetése, valamint az elvárások érvényesítése, ellenőrzése a BSZRK oldaláról az adott szerződésben kijelölt kapcsolattartó feladata; az elvárások szerepeltetésének, érvényesítésének és ellenőrzésének az auditálása az IBF feladata.

3.1.8.8 Fegyelmi intézkedések

A BSZRK az általa meghatározott informatikai biztonsági szabályokat, illetve a kapcsolódó eljárásrendeket megsértő személyekkel szemben

- foglalkoztatott esetében munkajogi jogkövetkezményeket alkalmazhat;
- egyéb (megbízási vagy vállalkozási szerződésen alapuló kapcsolat) esetében érvényesíti a vonatkozó szerződésben meghatározott következményeket, valamint megvizsgálja az egyéb jogi lépések lehetőségét, majd szükség szerint megteszi azokat.

A jogviszony megszüntetésétől akkor lehet eltekinteni, ha az informatikai biztonsági szabályok, illetve a kapcsolódó eljárásrendek megsértése:

- nem eredményezett jogosulatlan hozzáférést,
- nem járt adatvesztéssel,
- nem járt adat nem tervezett változtatásával (létrehozással, módosítással, törléssel),
- nem járt a BSZRK szakmai/gazdasági/egészségügyi adatainak illetéktelenekkel való megismertetésével (az adatok nem kompromittálódtak),
- nem járt a BSZRK által kezelt vagy feldolgozott, természetes személyek személyes adatainak kompromittálódásával,
- nem eredményezte a BSZRK EIR-rének elérhetőségének és használhatóságának módosítását.

Az eset összes körülményét figyelembe véve és mérlegelve kizárólag a FI-nek van jogköre eltekinteni a jogviszony megszüntetés kezdeményezésétől, ha

- a szabályok megsértése miatt jogosulatlan hozzáférés vagy részletes/teljes adatvesztés történt,
- a felhasználói azonosításhoz használat szükséges információ (felhasználói név és jelszó) mással megosztásra került, függetlenül attól, hogy az illetéktelen használat megvalósult-e,
- a BSZRK EIR-réhez illetéktelen hozzáférést kíséreltek meg, vagy a meglévő jogosultság módosítását kísérelték meg, függetlenül attól, hogy a próbálkozás sikeres volt-e,
- a BSZRK EIR-ének illetéktelen módosítását kísérelték meg, függetlenül attól, hogy a próbálkozás sikeres volt-e,
- a BSZRK EIR-rében tárolt adatokhoz való illetéktelen hozzáférést kíséreltek meg, vagy az adatokat nem a BSZRK által megkövetelt módon kísérelték meg manipulálni (új adatot létrehozni, meglévő adatot módosítani vagy törölni, adatkapcsolatot létrehozni vagy azon változtatni, törölni), függetlenül attól, hogy a próbálkozás sikeres volt-e,
- a BSZRK EIR-ében tárolt adatokat illetéktelenen személlyel, szervezettel kísérelték meg megosztani, függetlenül attól, hogy a próbálkozás sikeres volt-e,
- a BSZRK EIR-ében tárolt adatoknak nem engedélyezett törlését kísérelték meg, függetlenül attól, hogy a próbálkozás sikeres volt-e,
- a BSZRK EIR-ének elérhetőségét, használhatóságát kísérelték meg módosítani, függetlenül attól, hogy a próbálkozás sikeres volt-e,

- a BSZRK informatikai, avagy kommunikációs eszközét illetéktelen számára használatra átadta, eladta, kölcsönadta, vagy ezeket megkísérelte, függetlenül attól, hogy a próbálkozás sikeres volt-e,
- a szabályzatban meghatározott, vagy a BE, illetve IBF által végezni kívánt ellenőrzések és/vagy az azokat végző személyek akadályozása vagy az akadályozás előkészítése történik, függetlenül attól, hogy az akadályozás sikeres-e.

A jogviszony megszüntetéséről, illetve az attól való eltekintésről a BSZRK FI dönt, saját kezdeményezése vagy az ICSV, vagy az IBF javaslata alapján.

3.1.8.9 Munkaköri leírások

A BSZRK munkaköri leírásainak tartalmaznia kell az ahhoz a munkakörhöz tartozó biztonsági szerepköröket és felelősségeket. Ez meghatározza, hogy az adott munkakörrel milyen biztonsági szabályzatok ismertethetőek meg, illetve milyen biztonsági képzéseket köteles elvégezni.

3.1.9 Ellátási Lánc kockázatkezelés

3.1.9.1 Eljárásrend

A BSZRK ellátási lánc kockázatkezelés folyamatát a jelen eljárásrendben foglaltak szerint kell kialakítani, az elszámoltathatóságot az itt leírtak alapján kell érvényesíteni.

Az eljárásrendet rendszeresen, de legalább évente felül kell vizsgálni, aktualizálni kell. A felülvizsgálat és aktualizálás az IBF feladata, akit ebben az ICS foglalkoztatottjai és az ICSV támogatnak.

Az ellátási lánc kockázatkezeléssel kapcsolatban írt elvárások teljesülését az ICSV legalább éves gyakorisággal ellenőrzi. Az ellenőrzések megtörténtét az IBF ellenőrzi.

3.1.9.2 Ellátási láncra vonatkozó kockázatmenedzsment szabályzat

A BSZRK az EIR-ei, rendszerelemei és rendszerszolgáltatásai tekintetében azok kutatás-fejlesztése, tervezése, gyártása, beszerzése, szállítása, integrációja, üzemeltetése és karbantartása, kivezetése, valamint a selejtezése során figyelmet fordít a felmerülő ellátási láncból eredő kockázatokra.

Ennek biztosításához a BSZRK ellátási lánc kockázatmenedzsment szabályzatot dolgoz ki (lásd „Ellátási lánc kockázatmenedzsment szabályzat" külön álló dokumentum), amit csak az erre feljogosított szerepkörök tagjaival ismertet meg.

3.1.9.3 Ellátási láncra vonatkozó követelmények és folyamatok

A BSZRK az EIR-ei, rendszerelemei és rendszerszolgáltatásai tekintetében azok kutatás-fejlesztése, tervezése során megállapítja az azok által magukba foglalt ellátási lánc kockázatokat, melyeket az adott EIR rendszerbiztonsági tervébe, vagy annak mellékletébe rögzít és az ezekre adott válaszlépések is ott kerülnek bővebb kifejtésre.

A feladat ellátása az adott EIR fejlesztésére, tervezésére felkért foglalkoztatott feladata, akit ebben a GI segít.

Az ellátási láncból eredő kockázatok nyomonkövetése az EIR-ek későbbi életciklus szakaszában az adott EIR-ért felelős személy feladata.

3.1.9.4 Ellátási lánc ellenőrzések és folyamatok – Alvállalkozók

A BSZRK megköveteli, hogy az EIR-eihez, rendszerelemeihez és rendszerszolgáltatásaihoz kapcsolódó szerződéses partnerei, az általuk igénybe vett alvállalkozóiktól is megköveteljék a BSZRK információbiztonsági követelményeinek alkalmazását a „4.2 INFORMÁCIÓSBIZTONSÁGI HÁZIREND ÉS NYILATKOZAT (FOGLALKOZTATOTTAK ÉS PARTNEREK SZÁMÁRA" függelékbe foglalt dokumentum elfogadásával.

3.1.9.5 Beszerzési stratégiák, eszközök és módszerek

A BSZRK EIR, rendszerelem vagy rendszerszolgáltatás beszerzése során kiemelt figyelmet fordít arra, hogy kivédje, azonosítsa és csökkentse az ellátási láncból eredő kockázatokat.

3.1.9.6 Beszállítók értékelése és felülvizsgálata

A BSZRK EIR-eihez, rendszerelemeihez és rendszerszolgáltatásaihoz kapcsolódó beszállítókról és szerződéses partnerekről legalább évente ellátási lánc kockázatfelmérést készít.

3.1.9.7 Értesítési megállapodások

A BSZRK szerződéseket és megállapodásokat köt az EIR, rendszereleme és rendszerszolgáltatás ellátási láncában szerepet játszó szervezetekkel.

3.1.9.8 Rendszerek vagy rendszerelemek vizsgálata

A BSZRK az adott EIR, rendszereleme és rendszerszolgáltatás beszerzését követően köteles ellenőrizést végezni, hogy felderítse az esetleges fizikai vagy logikai hamisítást.

3.1.9.9 Rendszerelem hitelessége

Amennyiben az előző pont szerint hamisítás gyanúja merül fel azt a vizsgálatot végzőnek jelenítenie kell az ICSV és az adott EIR-ért felelős személy számára.

A hamisítás gyanúját az ICSV vizsgálja a továbbiakban és az ő feladata az érintett beszállító és szükség esetén a hatóságok értesítése.

A BSZRK a hamisítás tényének könnyeb felismerése érdekében az ICS foglalkoztatottjai számára hamisítás elleni képzést biztosít, ami kitér a hamisított hardverek, szoftverek és firmware-ek felismerésének módszereire és technikáira.

A BSZRK konfigurációkezelési eljárás („3.2.4 Konfigurációkezelés" fejezete) kiterjed a javításra vagy újra üzembe helyezésre váló rendszerelemekre is.

3.1.9.10 Rendszerelem selejtezése, megsemmisítése

A BSZRK Hasznosítási és Selejtezési szabályzata szerint kell eljárni EIR rendszerelem és más informatikai berendezés és adattároló esetén. Az adattárolók esetében a [pont] figyelembevételével.

Papír alapú iratok esetében a BSZRK Iratkezelési szabályzata szerint kell eljárni.

3.2 Rendszer szintű elvárások

3.2.1 Hozzáférés-Felügyelet

3.2.1.1 Eljárásrend

Az eljárásrendet rendszeresen, de legalább évente felül kell vizsgálni, aktualizálni kell. A felülvizsgálat és aktualizálás az ICSV feladata, akit kérésére az IBF támogat. A felülvizsgálat ellenőrzése az IBF feladata.

A hozzáférések rendszeres ellenőrzése az ICSV feladata. Az egyes hozzáféréseket legalább éves gyakorisággal ellenőrizni szükséges. Az ellenőrzések megtörténtét az IBF legalább éves gyakorisággal ellenőrzi.

3.2.1.2 Fiókkezelés

A BSZRK az informatikai infrastruktúrájában az alábbi fióktípusokat határozza meg:

- Felhasználó (A szokásos ügymenet végrehajtásához szükséges, arra használt felhasználói fiók. A legtöbb foglalkoztatott ilyen fióktípussal rendelkezik. Szoftvertelepítésre nem jogosult, és a használt számítógép, operációs rendszer kiemelt jogosultságot igénylő beállításait sem tudja módosítani.)
- Kiemelt felhasználó (A szokásos ügymenet végrehajtásához szükséges, arra használt felhasználói fiók. Szoftvertelepítésre nem jogosult, és a használt számítógép, operációs rendszer kiemelt jogosultságot igénylő beállításait sem tudja módosítani. Sajátjukon kívül az általuk irányított munkafolyamatokban tevékenykedők aktivitását is látják, ellenőrizhetik, monitorozhatják.)
- Szervezeti egység vezetője (A szokásos ügymenet végrehajtásához szükséges, arra használt felhasználói fiók. Szoftvertelepítésre nem jogosult, és a használt számítógép, operációs rendszer kiemelt jogosultságot igénylő beállításait sem tudja módosítani. A szervezeti egységük fájlszerveren való adattárolását megszervezhetik, a szükséges könyvtárakat létrehozhatják, a könyvtárakhoz való hozzáféréseket és a könyvtárak tartalmát menedzselhetik. Sajátjukon kívül az irányításuk alá tartozó foglalkoztatottak tevékenységének eredményét is látják, ellenőrizhetik, monitorozhatják.)
- Adminisztrátor (A kiemelt jogosultságot igénylő, jellemzően informatikai szakértelmet követelő tevékenység elvégzéséhez. Csak az ICS néhány foglalkoztatottja, valamint a BSZRK informatikai támogatását végző külső támogató rendelkezik ilyen jogosultsággal. Szoftvertelepítést is végezhet, továbbá a használt számítógép, operációs rendszer kiemelt jogosultságot igénylő beállításait is tudja módosítani.)
- Auditor (Csak lekérdezést lehetővé tevő fióktípus. Új adatot felvenni, meglévő adatot módosítani vagy törölni nem tud.)
- Ideiglenes (meghatározott élettartam utána automatikusan törlődő adminisztrátori jogokkal rendelkező fiókok)
- Vészhelyzeti (meghatározott élettartam utána automatikusan letiltásra kerülő adminisztrátori jogokkal rendelkező fiókok)
- Rendszerfolyamatok (kimondottan rendszerfolyamatok számára létrehozott az adott folyamathoz korlátozott adminisztrátori jogokkal ellátott felhasználók, amiket valós személy nem használhat)

A fiókokat az adminisztrátorok, az adminisztrátori fiókokat az ICSV jogosult menedzselni.

A BSZRK szervezeti egységeinek vezetői kötelesek késedelem nélkül értesíteni az ICSV-t, ha a felhasználói fiókra a továbbiakban nincsen szükség.

Ha a hozzáférés alapjául szolgáló szerződés megszűnik, vagy felfüggesztésre kerül, a BSZRK-on kívüli felhasználó hozzáférését vissza kell vonni, amelyet az adott szerződést a BSZRK részéről kezelő foglalkoztatottnak kell kezdeményeznie az ICSV felé, írásban, oly módon, hogy a BSZRK-on kívüli felhasználó jogosultságai, hozzáférései a szerződés megszűnésével, felfüggesztésével egy időben kerüljenek megszüntetésre vagy felfüggesztésre - ennek végrehajtása az ICSV feladata.

A BSZRK-on belüli felhasználók kilépése, áthelyezése esetén a felhasználó jogosultságát, azonosítóját megfelelően meg kell szüntetni, illetve a jogosultságot módosítani kell. A kilépésről, áthelyezésről a MOV-nek kell írásban értesítenie az ICSV-t, aki a megszüntetésről, felfüggesztésről intézkedik.

A BSZRK EIR-eiben tapasztalt biztonsági esemény esetén az eseményhez köthető összes fiók jelentős kockázatú besorolásba kerül és az azonosítását követően legkésőbb egy órán belül le kell tiltani. A fiókkal kapcsolatos további teendőkről és annak esetleges visszaállításáról az ICSV dönt, akit ebben az IBF támogat.

A felhasználói fiókokat és azonosítókat az ICSV-nak legalább évente felül kell vizsgáltatnia, a beállított jogosultságokat meg kell erősíttetnie. A felülvizsgálat megtörténtét az IBF legalább évente ellenőrzi, amelynek során áttekinti a fiókkezelési követelményekkel való összhangot is.

A BSZRK EIR-ében felhasználói csoport, levelezőlista vagy új jogosultság (szerepkör) létrehozását kiemelt felhasználó, szervezeti egység vezető vagy adminisztrátor kezdeményezheti, a csoportot, jogosultságot (szerepkört) pedig

- az FI,
- az Igazgatók,
- az ICSV vagy
- az IBF

támogatásával lehetséges létrehozni.

A csoport tagságának módosulása esetén a csoport tagjai által használt jelszót meg kell változtatni és arról a csoport tagjait értesíteni kell (kivéve, ha a változás új csoporttag csatlakozása volt).

Felhasználó saját magára vonatkozó, felhasználói azonosítót és jogosultságokat érintő döntéseket nem hozhat, kivéve az FI, aki személyi felelőssége miatt erre feljogosított.

Az esetleges összeférhetetlenség vizsgálata a felhasználói azonosítóra, illetve jogosultság igénylésre, karbantartásra vonatkozó igény kérelmezőjének és jóváhagyójának a feladata.

Az állásajánlat elfogadását követően a BSZRK az „Infokommunikációs eszközök használatáról szóló szabályzat" -ban meghatározott módon biztosítja a leendő foglalkoztatott számára a felhasználói jogosultságot és a szükséges eszközöket (számítógép és tartozékai, mobiltelefon, SIM kártya).

A BSZRK EIR-eit úgy kell kialakítani, hogy azokban a fiókok létrehozását, engedélyezését, módosítását, letiltását és eltávolítását automatizált mechanizmusok végezzék, valamint az elvégzett műveletet naplózzák és az EIR fiókkezelőjét is értesíteniük kell.

Az automatizált mechanizmusoknak törölnie kell minden olyan fiókot, ami:

- lejárt
- nem kapcsolódik már felhasználóhoz vagy személyhez
- megszegi a szervezeti szabályokat
- 90 napja inaktív

Az automatizált mechanizmusok ezen felül képesnek kell lenniük a fiókok monitorozására és a megszokottól eltérő használat kimutatására.

A BSZRK EIR-eit és egyéb informatikai rendszereit úgy kell beállítani, hogy azok az inaktív felhasználókat automatikusan kijelentkeztessék. Ebből a szempontból inaktív felhasználónak tekinthető, aki:

- 1 órája nem végzett semmilyen műveletet
- megadott időpontban még mindig be van jelentkezve

3.2.1.3 Hozzáférési szabályok érvényesítése

A BSZRK EIR-ének lehetővé kell tennie a hozzáférések ellenőrzését, amelynek során legalább

- a hozzáférő felhasználó azonosítója,
- a felhasználó hozzáférési jogosultságai,
- a hozzáférés ideje,
- a hozzáférés során elvégezni szándékozott művelet,
- a művelet elvégzésének sikeressége és
- a hozzáférés során módosult adat előző és aktuális állapota

ellenőrizhető kell, hogy legyen.

A hozzáférések rendszeres legalább éves gyakoriságú ellenőrzése az ICSV feladata.

A hozzáférések rendszeres legalább éves gyakoriságú ellenőrzésének megtörténtéről az IBF köteles meggyőződni.

3.2.1.4 Információáramlási szabályok érvényesítése

A BSZRK EIR-einek információáramlási szabályairól az adott EIR Rendszerbiztonsági terve ír bővebben.

3.2.1.5 Felelősségek szétválasztása

A felhasználók létrehozása, kezelése, jogosultság beállítása és karbantartása során meg kell előzni (vagy ha korábban kialakult, meg kell szüntetni) az összeférhetetlenséget a felhasználó

- ugyanazon időben, párhuzamosan betöltött munkakörei, szerepkörei, külső elkötelezettségei és érdekeltségei, valamint használt azonosítói között, valamint a

- korábbi munkakörében, szerepkörében, érdekeltségében, vagy azonosítójával indított tranzakciói későbbi kezelése (jóváhagyása, ellenőrzése stb.) között.

3.2.1.6 Legkisebb jogosultság elve

A fióktípusokat úgy kell kialakítani, hogy az adott munkakör ellátásához szükséges minimális jogosultságokat biztosítsák.

A BSZRK EIR-einek biztonsági funkcióihoz és az ahhoz köthető biztonságkritikus információkhoz csak Adminisztrátor, Auditor és az azt közvetlen vagy közvetve kezelő Rendszerfolyamat fiókok számára biztosítható hozzáférés.

A BSZRK EIR-einek biztonsági funkcióihoz és az ahhoz köthető biztonságkritikus információkhoz hozzáférő személyek számára létre kell hozni olyan nem privilegizált fiókot, amivel nem fér hozzá ezekhez a funkciókhoz/információkhoz.

A privilegizált fiókok tulajdonosai kötelesek a nem privililegizált fiókjaikat használni, amennyiben az éppen aktuális feladatiak ellátásához nincs szükségük hozzáférésre az EIR biztonsági funkcióihoz és az ahhoz köthető biztonságkritikus információkhoz vagy bármilyen más privilegizált funkcióhoz.

A BSZRK EIR-einek privilegizált fiókjaihoz (például szuperfelhasználó, rendszer adminisztrátor) csak az ICSV-nek, illetve az általa kijelölt ICS foglalkoztatottaknak lehet hozzáférése.

A BSZRK EIR-einek naplózniuk kell bármilyen privilegizált funkció végrehajttatást, ezzel segítve a kompromittált vagy nem megfelelő jogosultságokkal ellátott fiókok azonosítását.

A nem privilegizált fiókok számára nem engedélyezettek a következő műveletek:

- biztonsági- és adatvédelmi megoldások letiltása, megkerülése vagy módosítása
- rendszerfiók létrehozása
- a rendszer sértetlenségének vizsgálata
- kriptográfiai kulcskezelési tevékenységek
- behatolásérzékelési és -megelőzési mechanizmusok letiltása, megkerülése vagy módosítása
- rosszindulatú kódfuttatás elleni védelmi mechanizmusok letiltása, megkerülése vagy módosítása

A BSZRK a kiadott jogosultságokról leltárat vezet, amit az ICSV évente felül vizsgál, annak érdekében, hogy azonosítsa és törölje vagy módosítsa azokat a jogosultságokat, amikre már nincs szükség. Ezt az IBF legalább évente ellenőrzi.

3.2.1.7 Sikertelen bejelentkezési kísérletek

A BSZRK informatikai infrastruktúrájában a következő fiókzárolási házirendet kell alkalmazni sikertelen bejelentkezési kísérletek esetén.

3 sikertelen belépési kísérletet követően 5 perces időtartamra zárolni kell a belépést. A sikertelen belépések számát a sikeres belépés nullázza.

3.2.1.8 A rendszerhasználat jelzése

A BSZRK informatikai infrastruktúrájába bejelentkező képernyőkön (beleértve az operációs rendszerbe belépést, a távoli kapcsolattal való kapcsolódást és az egyes szakmai informatikai

rendszerekbe, alkalmazásokba belépést) a BSZRK által meghatározott rendszer használatra vonatkozó figyelmeztető üzenetet vagy jelzést kell megjeleníteni, amely jelzi, hogy

- a felhasználó a BSZRK EIR-ét tervezi használni;
- a rendszerhasználatot a BSZRK figyelheti, rögzítheti, naplózhatja;
- a rendszer jogosulatlan használata tilos, és büntetőjogi vagy polgárjogi felelősségre vonással jár;
- a rendszer használatával a felhasználó elfogadja és tudomásul veszi a fentieket és a „4.2 INFORMÁCIÓSBIZTONSÁGI HÁZIREND ÉS NYILATKOZAT (FOGLALKOZTATOTTAK ÉS PARTNEREK SZÁMÁRA)" függelékben foglaltakat is.

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

A BSZRK által üzemeltetett, nyilvánosan elérhető EIR esetén a rendszernek

- ki kell jeleznie a rendszer használat feltételeit, mielőtt további hozzáférést biztosít;
- ha felügyelet, adatrögzítés vagy naplózás történik, ki kell jeleznie, hogy ezek megfelelnek az adatvédelmi szabályoknak;
- leírást kell biztosítania a rendszer engedélyezett felhasználásáról.

3.2.1.9 Eszköz zárolása

A BSZRK EIR-eit úgy kell beállítani, hogy azok a felhasználó kérésére vagy 30 perc inaktivitást követően zárolják a hozzáférést. Ez a rendszertől függően történhet operációs rendszer vagy alkalmazás szinten. Operációs rendszeri szint esetén a zárolás alatt képernyőkímélőt kell alkalmazni, hogy elrejtse a kijelzőn mutatott információkat.

A rendszernek ezt a zárolást mindaddig fenn kell tartania, amíg a felhasználó újra hitelesíti magát.

3.2.1.10 A munkaszakasz lezárása

A BSZRK EIR-eit úgy kell beállítani, hogy azok automatikus módon felhasználói kérésre vagy 30 perc inaktivitást követően lezárják az érintett munkaszakaszt. A lázárásnak úgy kell történnie, hogy az EIR hálózati kapcsolata nem szakítható meg közben, illetve megszakadjon minden a munkaszakaszhoz köthető felhasználói folyamat (ez alól kivételt képeznek azok a folyamatok, amiket direkt úgy hoztak létre, hogy ne álljanak le a munkaszakasz lezárását követően.).

3.2.1.11 Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

A BSZRK informatikai infrastruktúrájában, EIR-ében általában nem engedélyezett az azonosítás vagy hitelesítés nélküli tevékenység, kivéve

- a vendégek számára telepített Wí-Fi hálózat használata (ahol valamennyi felhasználó azonos jelszóval jelentkezik be), valamint
- a nyilvános honlap használata.
- a BSZRK belső intranete

A BSZRK az azonosítás vagy hitelesítés nélkül is végrehajtható felhasználói tevékenységeket az alábbiakban határozza meg:

3.2.1.12 Távoli hozzáférés

A BSZRK informatikai infrastruktúrájához, EIR-éhez történő távoli hozzáférés a BSZRK valamennyi foglalkoztatottja számára megengedett. A BSZRK-on kívüli felhasználók számára a távoli hozzáférésről a BSZRK és a külső szervezet közötti szerződésben kell rendelkezni.

A BSZRK levelező rendszeréhez való távoli hozzáférés (számítógépről, vagy mobiltelefonról) valamennyi BSZRK alkalmazásában álló levelező postafiókkal rendelkező felhasználó számára megengedett.

A távoli hozzáférésekre vonatkozó konfigurálási vagy a kapcsolódási követelményeket és a megvalósítási útmutatókat az ICS feladata elkészíteni és naprakészen tartani, valamint megosztani a hozzáférésre jogosultakkal.

A távoli hozzáféréseknek olyan csatornákon kell történnie, hogy azokon biztosítható legyen a hozzáférés biztonsága és sértetlensége. Ezért a BSZRK VPN-ek használatát követeli meg melyeknek a következő feltételeknek kell megfelelniük:

- két tényezős autentikáció
- TLS 1.2 vagy TLS 1.3 verzió
- A következő titkosítási csomagok valamelyikének használata:
    - TLS 1.2 esetén:
        - TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256
        - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
        - TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384
        - TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256
        - TLS_ECCPWD_WITH_AES_128_GCM_SHA256
        - TLS_ECCPWD_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384
        - TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256
        - TLS_ECDHE_PSK_WITH_AES_128_CCM_8_SHA256
        - TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256
        - TLS_ECCPWD_WITH_AES_128_CCM_SHA256
        - TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
        - TLS_ECDHE_ECDSA_WITH_AES_128_CCM
        - TLS_ECDHE_PSK_WITH_AES_128_CCM_8_SHA256
        - TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256
        - TLS_ECCPWD_WITH_AES_128_CCM_SHA256
        - TLS_ECCPWD_WITH_AES_256_CCM_SHA384
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256

        - TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
        - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
    - TLS 1.3 esetén a korábbiakon felül:
        - TLS_AES_256_GCM_SHA384
        - TLS_CHACHA20_POLY1305_SHA256
        - TLS_AES_128_GCM_SHA256
        - TLS_AES_128_CCM_8_SHA256
        - TLS_AES_128_CCM_SHA256
- tanúsítvány használata esetén, a tanúsítványnak:
    - legalább 2048 bit hosszúnak kell lennie
    - elfogadott CA-tól kell származnia
    - legfeljebb egy éves lejárattal rendelkezhetnek, melynek megújítását és kivonását automatizált mechanizmusoknak kell végezniük
- a hozzáférésnek a BSZRK által menedzselt hálózati hozzáférési ponton keresztül kell történnie

A távoli hozzáférés során elvárt viselkedési szabályok, rendszerhasználati követelmények megegyeznek az irodán belüli hozzáférés követelményeivel.

A BSZRK informatikai infrastruktúrájához, EIR-éhez történő távoli hozzáférés kizárólag olyan informatikai eszköztől megengedett, amely

- a BSZRK által elfogadott, jogszerűen alkalmazott és telepített, aktív, nem korlátozott üzemű vírusvédelmi, végpontvédelmi megoldással védett,
- a telepített védelmi megoldás rendszeresen (legalább napi gyakorisággal) frissül,
- a vírusvédelmi szignatúrák rendszeresen (legalább 4 óránként) frissítésre kerülnek,
- védelmi megoldása az operációs rendszerrel együtt betöltődő objektumokat minden indításkor átvizsgálja,
- védelmi megoldása a teljes eszközt legalább hetente egy alkalommal átvizsgálja,
- kizárólag a hozzáférésre jogosult által használt,
- úgy került elhelyezésre, hogy a képernyőn megjelenő információt csak a hozzáférésre jogosult tekinthesse meg.

Sikeres távoli hozzáférést követően a privilegizált jogosultságot igénylő műveletek és hozzáférések esetében úgy kell eljárni, hogy az adott foglalkoztatott helyi jogosultságai legyenek érvényesítve, megfelelő autentikációt követően.

A BSZRK informatikai infrastruktúrájához, EIR-éhez történő távoli hozzáférést automatizált mechanizmusokkal kell nyomon követni. A mechanizmusokat úgy kell kialakítani, hogy azok képesek legyenek a sikertelen hozzáférési kísérletek azonosítására és az arról való riasztások küldésre, valamint, ha biztonsági esemény vagy kompromitáció gyanúja merül fel a rendszernek képesnek kell lennie automatikusan korlátoznia a hozzáférést.

Az ERI-ekhez történő távoli hozzáférés egyedi feltételeit az adott EIR rendszerbiztonsági terve fejti ki.

3.2.1.13 Vezeték nélküli hozzáférés

A BSZRK által üzemeltetett vezetéknélküli hálózat

- neve nem utalhat a BSZRK-ra, név alapján nem lehet a BSZRK-hoz kapcsolható,

- jelszavát legalább évente cserélni szükséges és csak a használatra jogosultakkal szabad megosztani.

A BSZRK foglalkoztatottjai a BSZRK által a vendégek számára biztosított Wi-Fi hálózatot nem használhatják, csak hordozható számítógéppel. A vendég Wi-Fi hálózat nevét és hozzáférési kódját az ICS biztosítja az érintett foglalkoztatottak számára, olyan módon, hogy az csak a használatra jogosultak számára legyen ismert. A Wi-Fi hálózathoz kapcsolódni az adott hordozható számítógép felhasználói útmutatójában leírt módon lehetséges. A Wi-Fi hálózathoz való kapcsolódáshoz az ICS kérésre támogatást nyújt.

A vendég Wi-Fi hálózat jelszavát megkapó, a hálózatot hordozható számítógéppel használó foglalkoztatottakról az ICS nyilvántartás vezet.

A nyilvántartás alapján a vendég Wi-Fi hálózat havonta megváltozó jelszavát az ICS osztja meg a nyilvántartásban szereplő foglalkoztatottaknak (például az általuk használt zárt tárgyalóba telepített táblán).

3.2.1.14 Mobil eszközök hozzáférés-ellenőrzése

A BSZRK valamennyi foglalkoztatottja számára megengedett a BSZRK által nekik használatra adott mobiltelefonról a BSZRK levelező rendszeréhez való hozzáférés.

A mobiltelefonon keresztüli hozzáférésekre vonatkozó konfigurálási vagy a kapcsolódási követelményeket és a megvalósítási útmutatókat az ICS feladata elkészíteni és naprakészen tartani, valamint megosztani a hozzáférésre jogosultakkal.

A levelezőrendszer mobiltelefonon keresztüli elérése során elvárt viselkedési szabályok, rendszerhasználati követelmények megegyeznek a kórházon belüli hozzáférés követelményeivel.

Amennyiben az adott mobiltelefonon bármilyen szervezeti vagy a szervezet által kezelt adat található a készüléken teljes eszköztitkosítást vagy tárolóalapú titkosítás kell alkalmazni.

3.2.1.15 Külső elektronikus információs rendszerek használata

A BSZRK foglalkoztatottjai csak olyan külső EIR-eket használhatnak, aminek használatát a BSZRK külön engedélyezte az „Engedélyezett külső elektronikus információs rendszerek" külön álló dokumentumban. A külső EIR-ekre ugyanazoknak a biztonsági követelményeknek kell megfelelniük, mintha azokat a BSZRK üzemeltetné.

A BSZRK-nak meg kell győződni arról, hogy ezek az engedélyezett EIR-ek megfelelnek a megkövetelt biztonsági osztályuknak, vagy az üzemeltetetőikkel kötött szerződéseknek ki kell térniük a biztonsági követelményeknek való megfelelésre, vagy azt tanúsítvánnyal igazolják.

A külső EIR-ek biztonsági követelményeknek való megfelelésének és a tanúsítványok ellenőrzését az ICSV végzi, akit ebben a munkában az IBF támogat.

A biztonsági követelmények szerződésbe foglalásáért a IJ felel.

A BSZRK adathordozói nem használhatóak külső EIR-ekben.

Az egyes EIR-ek vonatkozásában a külső EIR-ekhez történő kapcsolatainak részleteit az adott EIR rendszerbiztonsági terve fejti ki bővebben.

3.2.1.16 Információmegosztás

A BSZRK által kezelt egészségügyi adatok megosztásáról a BSZRK Adatvédelmi szabályzata rendelkezik.

3.2.1.17 Nyilvánosan elérhető tartalom

A nyilvánosan elérhető, elektronikusan tárolt és elérhető tartalmakat a BSZRK honlapján kell közzétenni.

Döntést megelőzően a közzétenni szándékozott információt el kell juttatni a közösségi médiáért felelős személyhez, akinek át kell vizsgálnia azt annak érdekében, hogy a nyilvánosan közzétenni szándékozott információ véletlenül se tartalmazzon nem nyilvánosságnak szánt információt.

A BSZRK honlapján való információ közzétételéről a közösségi médiáért felelős személy döntenek.

A BSZRK honlapjára a közösségi médiáért felelős személy, valamint az erre írásban feljogosított foglalkoztatottak töltik fel a tartalmat (akiket a szervezeti egység vezetőjének kérésére az ICS foglalkoztatottjai támogatnak).

A nyilvánosan hozzáférhető EIR tartalmat a DPO-nak rendszeresen, de legalább fél évente át kell vizsgálnia és ellenőriznie kell, hogy található-e nem nyilvánosságnak szánt információ a közzétett információ között. Amennyiben ilyet azonosít, haladéktalanul intézkedik a nem nyilvánosságnak szánt információk eltávolításáról és tájékoztatja róla az IBF-et. Az átvizsgálás megtörténtét az IBF rendszeresen, de legalább évente ellenőrzi.

3.2.2 Naplózás és Elszámoltathatóság

3.2.2.1 Eljárásrend

A BSZRK informatikai infrastruktúrájában, EIR-elemeinek üzemeltetése kapcsán alkalmazott naplózást a jelen eljárásrendben foglaltak szerint kell kialakítani, az elszámoltathatóságot az itt leírtak alapján kell érvényesíteni.

Az eljárásrendet rendszeresen, de legalább évente felül kell vizsgálni, aktualizálni kell. A felülvizsgálat és aktualizálás az IBF feladata, akit ebben az ICS foglalkoztatottjai és az ICSV támogatnak.

A naplózási eljárásrendben írt elvárások teljesülését az ICSV legalább éves gyakorisággal ellenőrzi. Az ellenőrzések megtörténtét az IBF ellenőrzi.

3.2.2.2 Naplózható események

A BSZRK informatikai infrastruktúrájában, EIR-eiben legalább az alábbi eseményeket kell naplózni:

- a felhasználók adminisztrációs tevékenysége:
    - sikeres és sikertelen bejelentkezés;
    - kijelentkezés;
    - jelszómódosítás;
- a szakmai/gazdasági adatokat érintő módosítások az egyes rendszerekben az adat módosítás előtti állapotával;
- az adminisztrátorok adatbázisba történő

  - sikeres és sikertelen bejelentkezése;
  - kijelentkezése;
  - jelszómódosítása;
- az adminisztrátorok adatbázisban végrehajtott tevékenysége;
- a felhasználói jogosultságok módosítása;
- a szerepköröknek és a szerepkörök tartalmának módosítása;
- rendszeresemények, esetleges hibák;
- rendszerüzenetek;
- beállítási, konfigurációs módosítások.

A naplózás kialakításába be kell vonni a rendszer adminisztrátorát, adatgazdáját, szakmai felelősét és szállítóját is annak érdekében, hogy meghatározásra kerülhessenek azok a többletinformációk, amelyek a felhasználói tevékenységek nyomon követéséhez szükségesek.

A naplózási beállításokat az ICSV és az IBF évente felülvizsgálja abból a szempontból, hogy a tapasztalatok alapján a naplózott információ elegendő és megfelelő-e a biztonsági események kivizsgálásához.

3.2.2.3 Naplóbejegyzések tartalma

A BSZRK EIR-ének a naplóbejegyzésekben elegendő információt kell összegyűjtenie ahhoz, hogy ki lehessen mutatni, milyen események történtek, miből származtak ezek az események (mi indította, váltotta ki őket), és mi volt ezen események kimenetele. A naplóbejegyzéseknek ennek érdekében legalább a következőket kell tartalmazniuk:

- az érintett rendszerelem azonosítóját,
- az adatazonosítót (pl. fájl/rekord/mező/rendszerelem név),
- az esemény ismertetését/a funkcióazonosítót,
- a felhasználó azonosítóját,
- az esemény időpontját (századmásodperc pontossággal),
- az eseményt kezdeményező felhasználó által használt számítógép azonosítóját és IP címét,
- az esemény elemzéséhez szükséges adattartalmakat vagy az arra vonatkozó hivatkozásokat, illetve annak végrehajtási státuszát,
- az esemény sikerességét.

A naplóbejegyzések tartalma EIR és rendszerelem esetében további tartalommal bővíthető annak funkciójának függvényében. Erről az adott EIR rendszerbiztonsági terve ír bővebben.

A naplóbejegyzések tartalmát minden esetben úgy kell konfigurálni, hogy azok csak a szükséges információkat tartalmazzák.

3.2.2.4 Naplózás tárkapacitása

A naplók tárkapacitását a BSZRK informatikai infrastruktúrájának, EIR-einek szállítóinak a bevonásával kell kialakítani, lehetőleg az adott rendszerelem tervezése során, előzetes kapacitástervezési folyamat keretében, az érintett rendszerelem biztonsági osztályba sorolásából következő naplózási elvárások teljesítésére is tekintettel (biztosítva, hogy a naplóállományok az elvárt megőrzési időtartamon belül megőrzésre kerüljenek - részletesebben lásd a „ 3.2.2.10 A naplóbejegyzések megőrzése" pontban).

A napló tárkapacitás figyelését az informatikai infrastruktúra, és az EIR-ek felügyeleti tevékenységébe kell beépíteni.

A naplóállományok rendelkezésére álló tárterületet úgy kell biztosítani, hogy megfelelő méretű szabad tárterület álljon rendelkezésre a megnövekedett naplóállományok megőrzésére.

A biztonsági incidensekhez kapcsolódó, illetve azok kivizsgálásához szükséges, valamint bármely külső/belső audithoz elengedhetetlen naplóállományokat a vizsgálat/audit jegyzőkönyvének FI általi elfogadásáig meg kell őrizni és kérésre a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, illetve a vizsgálatokat végző további hatóság, szervezetrendelkezésére kell bocsátani.

A BSZRK központi naplózó rendszert üzemeltet, amiben aggregálja a különböző forrásokból származó naplóállományokat.

3.2.2.5 Naplózási hiba kezelése

A BSZRK EIR-ét, valamint ennek a naplózási funkcióját úgy kell kialakítani, hogy naplózási hiba esetén riasztást küldjön az ICSV és az adott rendszerelem üzemeltetését végző szervezet, személy számára.

A naplózási hiba kezelése kapcsán előzetesen meg kell határozni a lehetséges hibákat és azok tervezett kezelési módját (például a rendszer leállítását, a legrégebbi naplóbejegyzések felülírását, a naplózási folyamat leállítását - az adott rendszerelem esetében egyedileg meghatározott módon, amiről az adott EIR rendszerbiztonsági terve ír bővebben).

3.2.2.6 Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

A BSZRK informatikai infrastruktúrájának és EIR-einek a naplóállományait

- az általános napi üzemeltetési feladatok során az üzemeltetést végzőnek,
- esetenként (de legalább negyedévente az ICSV-nek)

át kell vizsgálnia, és elemeznie kell annak érdekében, hogy a nem megfelelő vagy szokatlan működésre utaló jelek azonosításra kerüljenek. Az átvizsgálás, elemzés megtörténtét az IBF feladata ellenőrizni.

A hibabejegyzéseket az érintett rendszer(elem) üzemeltetését végző ICS foglalkoztatott feladata kivizsgálni és kezelni, illetve az ICSV-t és az IBF-et tájékoztatni, a „3.2.10.2 Hibajavítás" fejezetben leírtak alapján.

A naplóban levő biztonsági eseményeket az érintett rendszer(elem) üzemeltetését végző ICS foglalkoztatott feladata kivizsgálni és kezelni, illetve az ICSV-t és az IBF-et tájékoztatni. A szokatlan működésre és biztonsági eseményre utaló jeleket a „3.1.3 Biztonsági események kezelése" fejezetben leírtak alapján kell kezelni.

A BSZRK központi naplózó rendszerének képesnek kell lennie a naplóbejegyzések automatikus feldolgozására és azokból jelentés készítésére.

3.2.2.7 Naplóbejegyzések csökkentése és jelentéskészítés

A naplóbejegyzések könnyebb értelmezhetősége érdekében a BSZRK olyan automatizált mechanizmusokat alkalmaz, melyek segítségével jelentések készíthetőek a naplóbejegyzésekből, úgy,

hogy azok tartalma és időbelisége érintetlen marad. A mechanizmusnak lehetővé kell tennie a naplóbejegyzések keresését, rendezésesét/rendszerezését és feldolgozását.

3.2.2.8 Időbélyegek

A BSZRK informatikai környezetének és EIR-einek legalább a pénzügyi kötelezettséget jelentő műveletekhez kapcsolódó naplóbejegyzéseit időbélyeggel kell ellátni, melyhez a rendszerórát kell alapul venni. Az időbélyegeket legalább század-másodperc pontossággal kell rögzíteni.

A BSZRK informatikai környezetét és EIR-eit úgy kell kialakítani, hogy az egyes rendszerórákat hálózati időszinkron protokoll segítségével szinkronizálja a domain kontrollerhez, azt pedig a Microsoft időszerveréhez (ezáltal az egyezményes koordinált világidőhöz), 0-24 óra formátumban.

Az időszinkronizációt öt percenként kell elvégezni. Az engedélyezett időeltérés 0,25 másodperc.

3.2.2.9 Naplóinformációk védelme

A BSZRK informatikai infrastruktúráját, ERI-eit és az ezek eseményeit naplózó megoldásokat úgy kell kialakítani, hogy az EIR megvédje a naplóinformációt és a naplót kezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

A védelem keretében a naplóinformációhoz való felhasználói hozzáférést korlátozni kell, úgy, hogy ahhoz csak adminisztrátor férhet hozzá olvasási jogosultsággal a rögzített naplóinformációhoz. A naplóbejegyzések módosítása és törlése privilegizált műveletnek minősül, így arra csak bizonyos szerepkörök jogosultak. Ezeket a szerepköröket az adott EIR rendszerbiztonsági terve fejti ki.

A naplóbejegyzésekkel kapcsolatos jogosulatlan hozzáférést, módosítást és törlésről a rendszernek riasztást kell küldenie az adott rendszer üzemeltetője számára.

3.2.2.10 A naplóbejegyzések megőrzése

A BSZRK informatikai infrastruktúrájában, EIR-eiben képződött naplóinformációit rendszeresen menteni kell a BSZRK szokásos mentési rendszere segítségével („3.2.5.8 Az elektronikus információs rendszer mentései" pont szerint). A napló tárkapacitással összhangban a mentéseket úgy kell kialakítani, hogy naplóbejegyzések ne vesszenek el.

A munkaállomások és hordozható eszközök naplóinformációit hetente legalább egyszer (de lehetőleg naponta) központi, csak az adminisztrátorok számára hozzáférhető tárhelyre kell menteni.

A naplóbejegyzéseket legalább félévig meg kell őrizni, a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

3.2.2.11 Naplóbejegyzések létrehozása

A BSZRK informatikai infrastruktúráját, EIR-eit fel kell készíteni a naplózással kapcsolatos alábbi követelmények teljesítésére:

- biztosítania kell a naplóbejegyzések előállítási lehetőségét a „3.2.2.2 Naplózható események" pontban meghatározott naplózható eseményekre, a „3.2.2.3 Naplóbejegyzések tartalma" pont alapján;

- lehetővé kell tennie az üzemeltetésért felelős személyeknek és az ICSV, valamint az IBF számára, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az EIR egyes elemei esetében;
- naplóbejegyzéseket kell tudnia megőriznie a „3.2.2.10 A naplóbejegyzések megőrzése" pontban és megvédenie a „3.2.2.9 Naplóinformációk védelme" pontban meghatározottak szerint.

3.2.3 Értékelés, Engedélyezés és Monitorozás

3.2.3.1 Eljárásrend

Az eljárásrendet rendszeresen, de legalább évente felül kell vizsgálni, aktualizálni kell. A felülvizsgálat és aktualizálás az IBF feladata.

Az ebben a fejezetben meghatározott, biztonságelemzéssel és a biztonságelemzési eljárásrenddel, biztonsági értékeléssel kapcsolatos feladatokat az IBF koordinálja, illetve esetenként végzi, valamint számon kéri a feladatoknak a BSZRK foglalkoztatottjainak vagy támogatást végző külső partnerek általi elvégzését.

Az ebben a fejezetben meghatározott elvárások teljesülésének, feladatok végrehajtásának az ellenőrzése az FI feladata, amelyet legalább éves gyakorisággal el kell végeznie.

3.2.3.2 Biztonsági értékelések

Az ICSV-nak és az IBF-nek közösen el kell készíteniük a BSZRK EIR-einek Biztonságértékelési tervét, melynek tartalmaznia kell az adott EIR-rel kapcsolatosan:

- bizonyítékkal alátámasztott biztonsági intézkedéseit és eljárását
- az értékelendő biztonsági intézkedéseket
- védelmi intézkedések hatékonyságának megállapításához használt értékelési eljárásokat
- az értékelés környezetét
- értékelést végző csoportokat és azok feladatait

A terv jóváhagyását és ellenőrzését az FI vagy kijelölt képviselője végzi a terv végrehajtását megelőzően.

A Biztonságértékelési terv meghatározza, hogy az egyes védelmi intézkedések értékelését, illetve a hozzájuk kapcsolódó kontrollok kiértékelését milyen gyakorisággal kell elvégezni.

A Biztonságértékelési terv a „4.3 KOCKKÁZATMENEDZSMENT KERETRENDSZER" függelék része.

Az így kapott eredményekből összefoglaló jelentést kell készíteni, amit meg kell ismertetni az EIR üzemeltetésével kapcsolatos szerepkörök tagjaival, valamint az FI-val. Az azonosított hiányosságok kezelésére intézkedési tervet kell kidolgozni.

A BSZRK a 2024. évi LXIX. törvény 16. § (1) bekezdése szerint kiberbiztonsági auditra kötelezett szervezet. Ezáltal a kiberbiztonsági követelményeknek való megfelelést független külső auditor bevonásával végzett kiberbiztonsági audittal is igazolnia kell.

A független auditor szervezettel való kapcsolatfelvétel és kapcsolattartás a IJ feladata és az audithoz szükséges anyagok összeállításáért és az auditorokkal való közreműködés az IBF és az ICSV feladata.

A BSZRK-nak a kiberbiztonsági audit kétévente vagy a kiberbiztonsági hatóság által elrendelt esetben kell végrehajtania.

3.2.3.3 Információcsere

A BSZRK EIR-ei és más rendszerek közötti információcserét úgy kell kialaktani, hogy olyan rendszereknél, amiknek azonos az engedélyező személye, az adott EIR Rendszerbiztonsági tervében dokumentálva legyenek az információcseréhez használt interfész jellemzői, biztonsági követelményei, védelmi intézkedései, felelősségi körei, valamint a megosztott információk hatásának szintjei, az adott EIR rendszerbiztonsági tervében.

Különböző engedélyező személyek és szervezetek esetén az információcsere feltételeit nem az EIR rendszerbiztonsági tervében, hanem külön biztonsági megállapodásban kell rögzíteni.

A biztonsági megállapodások kialakításakor kiemelt figyelmet kell fordítani arra, hogy az eltérő biztonsági osztályba tartozó és különböző védelmi intézkedésekkel ellátott rendszerek közötti információcsere megemelkedett kockázathoz vezethet.

A megállapodásokat az IBF éves rendszerességgel felülvizsgálja és szükség esetén frissíti.

3.2.3.4 Az intézkedési terv és mérföldkövei

A BSZRK védelmi intézkedések értékelései, felülvizsgálatai, folyamatos felügyeleti tevékenységei vagy a kiberbiztonsági audit által feltárt hiányosságok és gyengeségek csökkentésére vagy megszűntésére Intézkedési tervet (4.3 KOCKKÁZATMENEDZSMENT KERETRENDSZER függelék szerint) dolgoz ki. Az Intézkedési terv kivitelezését elősegítő mérföldköveket kell meghatározni, amik segítségével nyomon követhető a terv kivitelezettségének állapota.

Az Intézkedési tervel kapcsolatos tervezett és megvalósított védelmi intézkedéseket dokumentálni kell, az adott dokumentumban meghatározott felelős feladata, akit ebben az IBF támogat.

3.2.3.5 Engedélyezés

A BSZRK EIR-eihez engedélyezésért felelős személyt kell kijelölni, akinek a feladata az EIR üzembehelyezését megelőzően:

- a más rendszerekből áthozott (átörökített) biztonsági követelmények elfogadása,
- a rendszer engedélyeztetése a FI-val.

Az EIR-ek engedélyezésért felelős személye az adott EIR rendszerbiztonsági tervében vannak kijelölve.

Az engedélyezési folyamatot dokumentálni kell és azt az IBF feladata legalább éves szinten felülvizsgálni.

3.2.3.6 Folyamatos felügyelet

A BSZRK az EIR-eihez folyamatos felügyeleti stratégiát dolgoz ki (lásd Folyamatos Felügyeleti Stratégia külön álló dokumentum), aminek legalább a következőket tartalmaznia kell:

- az adott rendszer biztonsági intézkedéseinek hatékonyságát mutató metrikákat
- a szervezet kockázattűrési szintjét
- azokat az eseteket, amikben szükség van független értékelők bevonására
- a szervezet által a védelmi intézkedésekről összegyűjtött információk kiértékeléséből származó eredményeket
- a szervezet által a kockázatkezelési intézkedésekről összegyűjtött információk kiértékeléséből származó eredményeket
- védelmi intézkedések értékelése és elemzése alapján meghatározott válaszintézkedéseket
- kockázatkezelési intézkedések értékelése és elemzése alapján meghatározott válaszintézkedéseket
- a válaszintézkedések aktuális állapotát és mérföldköveit

A stratégia állapotáról az IBF éves szinten jelentést készít a FI számára.

3.2.3.7 Belső rendszerkapcsolatok

A belső rendszerkapcsolatokat az adott EIR-ek Rendszerbiztonsági tervei fejtik ki bővebben.

3.2.4 Konfigurációkezelés

3.2.4.1 Eljárásrend

A BSZRK-nak a konfigurációkezeléssel kapcsolatos elvárásokat, eljárásrendet rendszeresen, de legalább évente felül kell vizsgálni, aktualizálni kell. A felülvizsgálat és az aktualizálás az ICSV feladata, akit kérésre az IBF támogat.

Jelen pontban meghatározott feladatokat az ICSV feladata elvégezni, illetve az elvégzést koordinálni, továbbá (koordinálás esetén) az adott feladatok elvégzését számon kéri a BSZRK foglalkoztatottjaitól vagy támogatást végző külső partnereitől.

Az ebben a fejezetben meghatározott elvárások teljesülésének, feladatok végrehajtásának az ellenőrzése az IBF feladata, amelyet legalább éves gyakorisággal el kell végeznie.

3.2.4.2 Alapkonfiguráció

A BSZRK az EIR-eihez alapkonfigurációt fejleszt ki, dokumentálja és karbantartja azt, valamint leltárba foglalja a rendszer lényeges elemeit.

A BSZRK EIR-eihez készített alapkonfiguráció dokumentált leírását, telepítőkészleteit biztonságos helyen kell tárolni, ahol csak a telepítést végző foglalkoztatottak és/vagy külső támogató, valamint az ICSV és az IBF fér hozzá. A telepítőkészletek kapcsán a "3.2.4.10 A szoftverhasználat korlátozásai" pontban leírt további védelmi intézkedéseket is alkalmazni kell.

A dokumentációnak az alapkonfigurációnak minimálisan a következő elemeire kell kiterjednie:

- hardverelemek;
- szoftverek;
- telepítőkészletek és telepítési útmutató;
- szükséges szoftverkomponensek alapkonfigurációi.

Az informatikai alapinfrastruktúra szoftveres elemeit és a telepítéshez szükséges telepítőkészletek tartalmát felül kell vizsgálni a következő esetekben:

- rendszerelem telepítése vagy frissítésekor,
- ha azt a rendszerben bekövetkezett változások vagy biztonsági események indokolják,
- legalább évente.

A felülvizsgálat és a módosítások átvezetése az ICSV feladata, felelőssége. A felülvizsgálatot az IBF-nek ellenőriznie kell.

Az alapkonfiguráció változása esetén legalább kettő korábbi verziót meg kell tartani, amíg az új alapkonfiguráció nincs ismét változtatva, de legalább fél évig.

Az alapkonfigurációnak ki kell terjednie a szerverekre és felhasználók által használt számítógépekre, valamint az operációs rendszerre és általános irodai alkalmazásokra, amelyeket (szükség és az ICSV döntése esetén) az egyes szervezeti egységek által használt egyedi elvárásokkal ki kell egészíteni.

A BSZRK központi leltározó informatikai rendszerének az alapkonfigurációkat is tartalmaznia kell.

3.2.4.3 A konfigurációváltozások felügyelete (változáskezelés)

A BSZRK informatikai infrastruktúrájában, EIR-elemei esetében a következő tevékenységek tartoznak a változáskezelés hatálya alá:

- olyan fejlesztések, verzióváltások, amelyek a jogosultsági rendszert vagy az adott információs rendszer lényegi részét vagy naplózási megoldását, felhasználó azonosítási vagy jogosultság beállítási módját érintik,
- a rendszerelemek cseréje közül a
    - mentőrendszer vagy komponensének cseréje,
    - szerveroldali hardver cseréje más típusra,
    - szerveroldali szoftver cseréje másik szoftverre,
    - aktív hálózati elem cseréje más gyártó eszközére vagy ugyanazon gyártó más gyártmányú eszközére,
    - szerver operációs rendszerének és a kliensek tömeges operációs rendszer cseréje,
    - a szakmai rendszerek működésének jelentős módosítása,
    - a gyártó által kiadott frissítések telepítése,

A rosszindulatú szoftverek elleni védelmet biztosító rendszer és a levélszemét szűrő leíró állományainak cseréje nem tartozik a változáskezelési folyamat hatálya alá.

A változáskezeléssel kapcsolatosan az alábbi előírásokat kell figyelembe venni:

- Bármely funkciót megváltoztató művelethez (beleértve a verzióváltást és egyéb, jelentős beavatkozást igénylő hangolást, beállítást) az ICSV és az adatgazda előzetes, írásos engedélye szükséges.
- Az egyes információs rendszerek, rendszerelemek esetében az azok üzemeltetését végző szervezet vagy szakember feladata a változtatás kezdeményezése, de változtatást kezdeményezhet az ICSV és az IBF is.
- A változtatási igényt (amely tartalmazza a tervezett változtatást, annak indokát, a módosítás szállító/gyártó általi alátámasztottságát, a tervezett módosítás lépéseit, valamint

a módosítást követő állapot leírását) írásban el kell juttatni az ICSV számára, aki a kapott információ alapján dönt a változtatás elfogadásáról és arról, szükséges-a biztonsági hatásvizsgálat. Amennyiben igen, azt az ICS feladata elvégezni, amelyet az IBF ellenőriz.

- Nem igényel biztonsági hatásvizsgálatot olyan módosítás, amely nem tartozik a változáskezelés hatálya alá.
- Amennyiben a biztonsági hatásvizsgálat nem szükséges, vagy a hatásvizsgálat azt az eredményt adja, hogy a tervezett módosításnak nincs nagy kockázata, vagy a kockázatot a BSZRK vállalja, az ICSV feladata dönteni róla, hogy a tervezett változtatás tesztelésre kerülhet-e.
- A módosítást az üzemi rendszerekben való alkalmazás előtt tesztkörnyezetben ki kell próbálni. A tesztelést az érintett EIR (elem) üzemeltetést végzőnek kell végeznie, szükség esetén az ICS, illetve az IBF bevonásával.
- Az előzetes információ és a teszteredmények alapján az ICSV feladata dönteni, végrehajtható-e a tervezett módosítás az üzemi környezetben. Pozitív döntés esetén a változtatást a rendszer üzemeltetőjének kell elvégeznie, a változással érintett adatok, rendszerek teljes mentését követően. A változtatást csak indokolt esetben szabad munkaidőben elvégezni.
- Amennyiben a változtatáshoz az információs rendszer leállítása szükséges, arról az ICSV a felhasználókat lehetőleg 5 munkanappal a tervezett leállítást megelőzően tájékoztatni köteles.
- A változtatással kapcsolatos valamennyi dokumentációt (beleértve a változáskezelési folyamatban készített döntéselőkészítő anyagokat és a döntések dokumentációját) az ICSV, illetve az általa megbízottak feladata nyilvántartásba venni és visszakereshető formában tárolni legalább egy évig a változást követően.

A konfiguráció, illetve az EIR megváltoztatása előtt az új verziót az üzemi környezettel minél nagyobb mértékben megegyező tesztkörnyezetben tesztelni kell.

A tesztkörnyezetben alkalmazott rendszerek verziójának, naplózási és biztonsági beállításainak meg kell egyezniük az üzemi (vagy a változáskövetéssel megcélzott új üzemi környezettel), továbbá a tesztkörnyezetben kötelező alkalmazni mindazon védelmi és naplózási megoldásokat, engedélyeket és korlátozásokat, amelyek az üzemi (vagy a változáskövetéssel megcélzott új üzemi) környezetben alkalmazottak.

A tesztkörnyezetben létrehozott esetleges azonosítók, többletjogosultságok az üzemi környezetbe nem másolhatóak át, kivéve, ha a tesztelés ezek használatára, használatba vételi lehetőségének előzetes ellenőrzésére szolgált.

A tesztelés során olyan teszteseteket kell végrehajtani, és olyan tesztadatokat kell használni, hogy a módosításnak lehetőleg minél több hatása ellenőrizhető legyen. A tesztesetek összeállítása és a tesztadatok meghatározása, előállítása a tesztelést végző feladata.

A tesztelés körülményeit (beleértve a tesztkörnyezet és az üzemi környezet közötti eltéréseket), végrehajtását, végrehajtóit, a teszteseteket és a tesztadatokat, valamint a tesztelés eredményét megfelelő módon dokumentálni és értékelni szükséges.

A megfelelő dokumentálásba beleértendő, hogy

- a tesztelést a leírás alapján egy megfelelő szaktudással rendelkező, tesztelésben részt nem vett szakember változatlan kezdeti feltételekkel, módon és eredménnyel meg tudja ismételni,
- a megismételt tesztelés az eredetivel megegyező eredményt produkáljon,
- a tesztelés valamennyi reálisan előfordulható lehetséges esetet figyelembe vegyen,
- a tesztelés eredménye alapján a tervezett változtatásoknak az üzemi környezetre gyakorolt hatása kellő bizonyossággal megítélhető legyen.

A megfelelő értékelésbe beleértendő, hogy

- a tesztelés körülményei, végrehajtása, a tesztesetek és a tesztadatok, valamint a dokumentálás is értékelésre került (minőségi és mennyiségi értékelés),
- valamennyi módosítás teljes mértékben, hatásaival áttekintésre, tesztelésre, dokumentálásra és értékelésre került,
- a tesztelés valamennyi eredménye annak súlyának megfelelően figyelembe lett véve,
- a tesztelt módosításnak az üzemi környezetre gyakorolt valamennyi várható hatása értékelésre került.

A tesztelés előkészítése, elvégzése, dokumentálása és előzetes értékelése a tesztelést végző feladata.

A tesztelés végső értékelését az ICSV végzi és az IBF ellenőrzi.

A változáskezelési előírások betartását és a változáskezelési folyamatot az IBF-nek rendszeresen, de legalább évente ellenőriznie kell.

3.2.4.4 Biztonsági hatásvizsgálatok

A BSZRK-nak az EIR-ben tervezett változtatásoknak az információbiztonságra való hatását meg kell vizsgálnia és értékelnie kell, még a változtatások megvalósítására vonatkozó döntést megelőzően.

Az értékelést az ICS végzi, amelyet kérésére az IBF támogat. Az értékelés eredményét az ICSV köteles megosztani a változást kezdeményezővel, a tesztelést végzőkkel és az IBF-fel.

A változást követően ellenőrizni kell, hogy a meghatározott védelmi intézkedések helyesen és hatékonyan lettek bevezetve. Ez ellenőrzést dokumentálni kell és legalább a következőket tartalmaznia kell:

- az ellenőrzés időpontja
- az ellenőrzött védelmi intézkedés állapota
- az ellenőrzés eredménye
- az esetleges azonosított problémák és hiányosságok
- az azonosított problémákra és hiányosságokra adott válaszlépések

A változást követő ellenőrzést az ICS végzi, amelyet kérésére az IBF támogat. Az ellenőrzés eredményét az ICSV köteles megosztani a változást kezdeményezővel, a tesztelést végzőkkel és az IBF-fel.

3.2.4.5 A változtatásokra vonatkozó hozzáférés korlátozások

A BSZRK EIR-ein csak az arra kijelölt szerepkörök és meghatározott külső szervezetek számára engedélyezi az EIR-ben való változtatást.

Amennyiben a változtatást végző nem rendelkezik az adott EIR-hez a változtatáshoz szükséges privilegizált funkciókhoz és adatokhoz való hozzáférést biztosító fiókkal, az ICSV külön engedélyével átmeneti privilegizált fiókot kell neki létrehozni, amit a változtatása után haladéktalanul törölni kell a „3.2.1.3 Hozzáférési szabályok érvényesítése" pont szerint.

Amennyiben a változtatáshoz fizikai jelenlét is szükséges és a változtatást végző foglalkoztatott normál esetben nem jogosult az EIR-t vagy annak rendszerelemét tartalmazó helyiségbe való belépésre, azt az ICSV soron kívül, megfelelően dokumentált módon, átmenetileg engedélyezheti. Az ilyen feladatokat az ICS belépésre jogosult foglalkoztatottjának felügyelete mellett kell elvégezni.

3.2.4.6 Konfigurációs beállítások

A BSZRK informatikai infrastruktúrája, EIR-ei kapcsán az ICSV koordinálásával meg kell határozni a működési követelményeket, valamint az ehhez tartozó konfigurációs beállítást, amelyet kötelezően alkalmazandó konfigurációként elő kell írni.

Az így meghatározott konfiguráció elemeit az ICS tartja nyilván és tájékoztatja arról a BSZRK-on belül az érintetteket, valamint szintén az ICS ellenőrzi, hogy valóban a kívánt konfiguráció kerüljön alkalmazásra (telepítésre, karbantartáskor frissítésre).

Az egyes informatikai rendszerelemeknek, illetve informatikai infrastruktúrának

- az informatikai üzemeltetést érintő konfigurációs beállításait az EIR valamennyi elemében az adott elemet üzemeltető szervezet szakemberének,
- a szakmai üzemeltetést érintő konfigurációs beállításokat az EIR valamennyi elemében az adott elem legfőbb szakmai felhasználójának

feladata elvégezni.

Amennyiben a meghatározott elemek konfigurációs beállításaiban eltérés szükséges, az erre vonatkozó írásos igényt az ICSV számára kell eljuttatni, aki dönt az eltérés alkalmazhatóságáról. A döntés eredményéről az ICSV-nek írásban értesíteni kell a kérelmezőt és a kérelemben érintett rendszerelem üzemeltetőjét. A kérelmet és a döntést, az értesítésekkel együtt az ICSV-nek, illetve az általa megbízottnak nyilvántartásba kell vennie. A nyilvántartást kereshető módon kell kialakítani.

A konfigurációs beállítások változtatásait az IBF rendszeresen, de legalább évente ellenőrzi.

3.2.4.7 Legszűkebb funkcionalitás

Az alapkonfigurációt úgy kell kialakítani, hogy a követelményeknek még megfelelő, de biztonsági szempontból a lehető leginkább korlátozott funkcionalitást (legszűkebb funkcionalitást, a "szükséges minimum" elv alapján) kell alkalmazni.

A BSZRK informatikai infrastruktúráját, úgy kell konfigurálni, hogy csak azok a szolgáltatások, portok, protokollok legyenek engedélyezve, melyek a rendszer biztonságos működéséhez, a szolgáltatások megfelelő igénybevételéhez szükségesek; minden további, funkciót, portot, protokollt, szolgáltatást és szoftvert tiltani szükséges.

A beállításokat az ICSV évente felül vizsgálja és a szükségtelennek vagy nem biztonságosnak ítélt, funkciókat, portokat, protokollokat, szolgáltatásokat és szoftvereket kikapcsolja vagy eltávolítja.

A BSZRK által engedélyezett szoftvereket és azok futtatásának feltételeit az „Engedélyezett szoftverek" külön álló táblázat és adott EIR vonatkozásában azok Rendszerbiztonsági terveinek mellékletei részletezik. A melléklet által nem tartalmazott szoftverek általános érvényűen tiltottak. A tiltott vagy nem megfelelően futatott szoftverek tiltásának érvényesítését, a BSZRK a szoftverek telepítésének adott jogosult szerepkörhöz kötésével és a hordozható programok fútatásának tiltásával érvényesítni.

Az engedélyezett szoftverek listáját az ICSV-nek rendszeresen frissítenie kell, ha új szoftver kerül bevezetésre az EIR-be.

A beállítások és a tiltások megfelelő érvényesülését az IBF feladata rendszeresen, de legalább éves gyakorisággal ellenőrizni.

3.2.4.8 Rendszerelem leltár

A BSZRK által használt EIR elemeiről (a teljes informatikai infrastruktúráról) leltárt kell vezetni.

A leltárban fel kell tüntetni valamennyi hardver- és szoftverelemet, valamint azok dokumentációját. A nyilvántartásnak olyan részletességűnek kell lennie, hogy a rendszerelemek és jellemzőik, valamint azok állapota egyértelműen azonosítható legyen. Ennek érdekében nyilván kell tartani legalább a hardver- vagy szoftverelem

- elnevezését,
- verzióját,
- gyártási számát/sorozatszámát (ha értelmezhető),
- gyártóját,
- szállítóját,
- szállítás idejét,
- állapotát,
- telepített frissítéseit (ha értelmezhető),
- a rendelkezésre álló számosságát,
- a felhasználás állapotát,
- telepítési/felhasználási/tárolási helyét,
- felelős megőrzőjét,
- legutolsó ellenőrzési/láthatósági idejét,

A leltárt úgy kell kialakítani, hogy belőle az általában szokásos jelentések, riportok elkészíthetők legyenek.

A leltárt a rendszerelemeket érintő változásokkor frissíteni, évente egy alkalommal pedig felül kell vizsgálni.

A leltár elkészítése, naprakészen tartása és felülvizsgálata az ICSV feladata.

3.2.4.9 Konfigurációkezelési terv

A BSZRK az EIR-einek a rendszerfejlesztési életciklusának fejlesztési és beszerzési szakaszban Konfigurációkezelési tervet kell kidolgozni, amit az adott EIR Rendszerbiztonsági tervében vagy annak mellékletében kell rögzíteni.

A terv leírja, hogy az adott EIR vonatkozásában, hogyan lehet változtatásokat végrehajtani a változáskezelési folyamatokon keresztül, frissíteni a konfigurációs beállításokat és az alapkonfigurációkat, fenntartani az elemleltárakat, ellenőrizni a fejlesztési, tesztelési és működési környezeteket, valamint kidolgozni, kiadni és frissíteni a kulcsdokumentumokat.

A tervnek meg kell határozni, hogy az EIR mely konfigurációs elemei esnek a konfigurációkezelés hatálya alá és annak változása esetén a tervet frissíteni kell.

A tervnek meg kell határoznia, azokat a személyeket, akik felelősek a rendszerekhez javasolt változások felülvizsgálatáért és jóváhagyásáért, valamint azokat a személyeket, akik biztonsági vizsgálatot végeznek az EIR-ekben javasolt változásokkal kapcsolatban mielőtt azokat ténylegesen végrehajtanák.

A tervet az adott EIR fejlesztője és engedélyezője közösen dolgozzák ki és frissítik. A kész tervet az ICSV hagyja jóvá és az IBF ellenőrzi.

A tervet a BSZRK védi a jogosulatlan módosításoktól és csak azokkal a személyekkel és szerepkörökkel ismerteti meg azt, akiknek az EIR-en végzett munkájához az szükséges.

3.2.4.10 A szoftverhasználat korlátozásai

A BSZRK informatikai infrastruktúrájában kizárólag az ICSV által engedélyezett (lásd „Engedélyezett szoftverek" külön álló táblázat), jogtiszta szoftver használható, amelynek használatára vonatkozó licenccel vagy más engedéllyel a BSZRK rendelkezik.

A rendelkezésre álló és a felhasznált licencek számát naprakészen az ICS-nak nyilván kell tartania.

A Szabadon használható vagy nyílt forráskódú szoftverek használatbavételét az ICSV engedélyezi. Ezeket a szoftvereket használatba vétel előtt biztonságos körülmények között tesztelni kell.

A másolatok, megosztások, telepített szoftverpéldányok ellenőrzése érdekében a telepítőkészleteket és az aktiváló kulcsokat egymástól elkülönítetten, elzártan, vagy korlátozott hozzáférésű tárterületen kell tárolni. A telepítőkészletekhez és az aktiváló kulcsokhoz az ICSV, illetve az általa kijelölt ICS foglalkoztatottak férhetnek hozzá.

3.2.4.11 Felhasználó által telepített szoftver

A BSZRK informatikai infrastruktúráját használó felhasználók jogosultságát úgy kell beállítani, hogy szoftvertelepítési jogosultsággal csak az ezzel megbízott személyek és szerepkörök rendelkezzenek.

Az telepítésre nem feljogosított felhasználó szoftvert a BSZRK informatikai infrastruktúrájába nem telepíthet, és ott telepítést nem igénylő, a BSZRK által hivatalosan nem használt, és/vagy számára nem engedélyezett szoftvert sem futtathat.

A felhasználók beállított szoftvertelepítési korlátozását rendszeresen, de legalább évente egy alkalommal felül kell vizsgálni, és meg kell győződni a korlátozások fennállásáról. A felülvizsgálat és annak dokumentálása, az esetleges eltérések kezelése az ICSV feladata.

A felülvizsgálat megtörténtét és megfelelőségét az IBF ellenőrzi, legalább éves rendszerességgel.

3.2.4.12 Információ helyének azonosítása és dokumentálása

A BSZRK azonosítja és dokumentálja, hogy az EIR-eiben/rendszerelemben, milyen információk kerülnek tárolásra és feldolgozásra, és azokhoz milyen felhasználói csoportoknak van hozzáférése.

Az EIR-ben vagy rendszerelemben bekövetkezett az információk tárolását és feldolgozását érintő változásokat szintén dokumentálni kell.

Az azonosítás és dokumentálás az ICSV feladata, akit ebben az IBF segít.

3.2.5 Készenléti tervezés

3.2.5.1 Eljárásrend

A BSZRK készenléti tervezése során a jelen eljárásrendben foglaltak szerint kell eljárni.

A készenléti tervezése eljárásrend célja, hogy biztosítsa a BSZRK informatikai infrastruktúrájának, EIR-einek elvárt szintű rendelkezésre állását, folyamatos működését, valamint minimalizálja a nem várt események bekövetkezési valószínűségét, illetve csökkentse a nem várt esemény bekövetkeztekor keletkező károk hatásait, és elősegítse az informatikai infrastruktúra és EIR-ek üzemszerű működésének minél rövidebb időn belüli visszaállítását.

Az eljárásrendet rendszeresen, de legalább évente felül kell vizsgálni, aktualizálni kell. A felülvizsgálat és aktualizálás az ICSV feladata, aki a tervezéshez kérheti az IBF támogatását.

3.2.5.2 Üzletmenet-folytonossági terv

A BSZRK-nak el kell készítenie, dokumentálnia, valamint ki kell hirdetnie az EIR-ekre vonatkozó üzletmenet-folytonossági tervet (továbbiakban: informatikai üzletmenetfolytonossági terv, vagy IT BCP), oly módon, hogy az csak a BSZRK-on belül, a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyek és szervezetii egységek számára legyen hozzáférhető, jogosulatlanok számára nem.

Az informatikai üzletmenet-folytonossági tervnek összhangban kell lennie a BSZRK más területi folytonosságára készített tervvel (amelynek elkészítése a BSZRK megfelelő szakmai területeinek feladata).

Az elkészült informatikai üzletmenet-folytonossági tervet rendszeresen, de legalább évente felül kell vizsgálni, aktualizálni kell; az EIR vagy a működtetési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémákból levont tanulságok alapján.

Az informatikai üzletmenet-folytonossági terveket az adott EIR vonatkozásában azok Rendszerbiztonsági terve vagy annak melléklete tartalmazza.

Az IT BCP-t frissíteni kell továbbá:

- új információs rendszer(elem) beszerzése, üzembe állítása esetében
- meglévő információs rendszer(elem) módosítását követően (különösen, ha a módosítás a telepítést, üzembe állítást és üzemeltetéshez szükséges paraméterek módosításával járt együtt),
- az operációs rendszer változása esetén,
- ha változások következnek be:

- a BSZRK felépítésben,
- a kapcsolattartókban és kapcsolattartáshoz szükséges adatokban (nevekben, beosztásokban, címekben, telefonszámokban),
- az informatikai stratégiában,
- az informatikai biztonsági stratégiában,
- a helyszínekben, segédprogramokban és erőforrásokban,
- a jogszabályi háttérben,
- az EIR-ek működését támogató partnerekben,
- az EIR-ek használatára vonatkozó folyamatokban
- az üzletmenet-folytonossági terv bármely peremfeltételében.

Az IT BCP változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket tájékoztatni kell.

A folyamatos működés tervezésére vonatkozó tevékenységeket össze kell hangolni a biztonsági események kezelésével.

Az IT BCP tervezése során

- meg kell határozni a terv életbe léptetésének feltételeit, azt is beleértve, hogyan kell a helyzetet értékelni és kiket kell bevonni az értékelésbe);
- össze kell foglalni a vészhelyzet esetén követendő eljárásokat, különös tekintettel a működést és/vagy az emberi életet veszélyeztető incidens bekövetkezte esetén elvégzendő teendőket (beleértve a nyilvánosság kezelésének módját, a hatóságokkal (rendőrséggel, tűzoltósággal, önkormányzattal stb.) történő hatékony kapcsolatfelvétel módját és menetét;
- meg kell határozni az üzletmenet folytonossági terv egyes feladatainak végrehajtásáért felelős személyeket
- meg kell határozni a szolgáltatás, működés újraindításának lépéseit;
- elő kell írni az üzletmenet folytonossági terv tesztelésének módját és gyakoriságát, beleértve az üzletmenet-folytonossági terv karbantartásának módját és menetét;
- ki kell térni az érintettek oktatására és tudatosságának növelésére.

Az IT BCP-ben

- meg kell határozni a BSZRK informatikai alapfeladatait (a biztosítandó szolgáltatásokat) és alapfunkcióit, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket, összhangban a BSZRK többi alapfeladatával;
- definiálni kell, hogyan lehet fenntartani a BSZRK által előzetesen meghatározott alapszolgáltatásokat akkor is, ha az EIR összeomlik, kompromittálódik, vagy meghibásodik;
- rendelkezni kell a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről;
- jelölni kell a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket;
- ki kell dolgozni a végleges, teljes EIR helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

A működés folytonossági tervben meg kell továbbá határozni

- az alapvető tevékenység folytatásának (szükségüzem) lehetőségeit;
- az automatizált folyamatok kézi póteljárásait;

- az infokommunikációs erőforrások dinamikus átcsoportosításának, tartalék egységek beiktatásának a lehetőségét, vagy egy külső szervezet eszközeinek igénybevételére épülő tartalék megoldást, illetve a beüzemelés lépéseit;
- mely ERI-ek élveznek prioritást korlátozott vészhelyzeti működés esetén;
- a katasztrófa elhárítás előfeltételeként elvégzendő mentések rendszerét.

Az ebben a pontban leírtak végrehajtását az ICSV feladata koordinálni, aki a tervezéshez kérheti az IBF támogatását.

3.2.5.3 A folyamatos működésre felkészítő képzés

A BSZRK-nak az EIR folyamatos működésére felkészítő képzést kell tartania a felhasználók számára, azok szerepköreinek és felelősségeinek megfelelően.

A képzést a felhasználó számára az új szerepkörbe vagy felelősségbe kerülésüket követő egy hónapon belül meg kell tartani.

A képzést rendszeresen (legalább évente) meg kell ismételni, a képzésen elhangzottakat fel kell eleveníteni.

A képzést meg kell ismételni akkor is, ha az üzletmenet-folytonossági terv jelentősen módosult.

A képzés mellett javasolt az EIR folyamatos működésével kapcsolatos leginkább szükséges tudnivalókat írásban, felhasználó centrikusan összefoglalnia és elérhetővé tennie a felhasználók számára az adott EIR Rendszerbiztonsági tervének részeként vagy mellékleteként, például a BSZRK belső hálózatán, tárhelyén (az Intraneten).

Az ebben a pontban leírtak végrehajtását az ICSV feladata koordinálni.

3.2.5.4 Üzletmenet-folytonossági terv tesztelése

A BSZRK IT BCP tervét rendszeresen, de legalább évente tesztelni kell. A teszteléshez gyakorlatok és szimulációk is használhatóak, amik keretében egy fiktív üzletmenetre hatással lévő esemény megoldási módját kell megvizsgálni az IT BCP tervet követve.

A tesztelés eredményeit ki kell értékelni, hogy azonosíthatók legyenek a terv esetleges gyengeségei és meg kell határozni az azokra adott válaszintézkedéseket. Ezek az intézkedések járhatnak a IT BCP vagy a folyamatos működésre felkészítő képzés módosításával.

Az IT BCP terv tesztelését egyeztetni kell a BSZRK más folytonosági terveiért felelős személyekkel.

3.2.5.5 Biztonsági tárolási helyszín

A BSZRK az EIR rendszereinek helyet adó elsődleges szerver szobához hasonló kialakítással egy másodlagos szerver szobát alakít ki a kórház területén lévő másik épületben. Biztonsági szempontból a másodlagos helyszínnek ugyanazoknak a követelményeknek kell megfelelnie, mint az elsődlegesnek.

A másodlagos helyszínnek szűkség esetén képesnek kell lennie átvenni az elsődleges helyszín adattárolásban betöltött szerepét.

3.2.5.6 Alternatív feldolgozási helyszín

A BSZRK másodlagos szerver szobája alternatív feldolgozási helyszín szerepét is be kell töltenie és az ott lévő informatikai rendszereknek képeseknek kell lenniük az elsődleges EIR-ek funkcióinak ellátására az adott pótlandó EIR-től függő meghatározott időn belül.

Több EIR kiesése esetén a BSZK által biztosított szolgáltatásokat, az érintett EIR-ek Rendszerbiztonsági tervében lévő IT BCP szerinti prioritási sorrendben és meghatározott időn belül, kell elindítani az alternatív feldolgozási helyszínen.

3.2.5.7 Telekommunikációs szolgáltatások

A BSZRK-nak úgy kell szerződést kötnie a telekommunikációs szolgáltatókkal, hogy az általuk biztosított szolgáltatások szolgáltatásprioritása, rendelkezésre állása és hibaelhárítási ideje megfeleljen a BSZK által biztosított szolgáltatások számára meghatározott céloknak.

A BSZRK elsődleges infokommunikációs vonalán felül egy másodlagos vonalat is fenn kell tartani, ami a lehetőségekhez mérten a lehető legkevesebb az elsődleges vonallal közös hibalehetőségi ponttal rendelkezhet.

A szolgáltatókkal kötött szerződésekben foglalt vállalásokat a BSZRK-nak mérnie kell és az annak való nem megfelelés esetén válaszlépéseket kell tenni.

3.2.5.8 Az elektronikus információs rendszer mentései

A BSZRK EIR-ében tárolt adatokról, a rendszerekről, valamint azok üzemeltetési környezetéről (beleértve a beállításokat és dokumentációt) meghatározott gyakorisággal mentést kell készíteni.

A mentésnek alkalmasnak kell lennie arra, hogy a BSZRK EIR-ei és azok működési környezete, beállításai belőlük helyreállíthatóak legyenek a BSZRK eredeti informatikai infrastruktúráján, vagy egy annak megfeleltethető informatikai környezetben. A BSZRK részletes mentési tervét az adott EIR Rendszerbiztonsági tervében vagy annak mellékletében kell rögzíteni.

A mentésnek tartalmaznia kell az EIR-ben tárolt felhasználói és rendszerszintű adatokat, valamint az egyes EIR-ekhez tartozó különböző dokumentációkat.

A mentést úgy kell megtervezni és ütemezni, hogy a mentés az EIR-ek normál üzletvitelét ne zavarja; továbbá összhangban legyen a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.

Amennyiben az adott EIR-re más eljárást a BSZRK vagy jogszabály, hatóság más elvárást nem fogalmazott meg, a mentéseket az alábbi gyakorisággal, módon kell elvégezni:

- a változásokat legalább félévente el kell menteni (inkrementális mentés),
- a teljes adatállományt, üzemeltetési környezetet, dokumentációt, beállításokat hetente kell menteni,
- az egyes mentéseket legalább egy évig tárolni szükséges.

A BSZRK szakmai területeinek (az egyes területek vezetőinek) meg kell határozniuk azokat a kiemelt adatköröket és ezek speciális állapotokat, amelyek változatlan formában való megőrzése későbbi ellenőrzés vagy bármi más okból szükséges (pl. éves számviteli zárás állapota adott támogatási konstrukció esetében); egyben definiálva a megőrzendő adatkör és állapot elvárt megőrzési idejét is.

A mentések sikerességét ellenőrizni szükséges. A sikertelen mentés okát fel kell deríteni, a mentést gátló tényezőket kezelni kell, a mentést pedig meg kell ismételni.

A mentéseket két példányban kell készíteni. A példányokat egymástól földrajzilag elkülönített helyszínen a „3.2.5.5 Biztonsági tárolási helyszín" pont szerint kell tárolni olyan módon, hogy az eredeti infrastruktúra és rendszer, vagy az egyik mentési példány bármilyen sérülése, megsemmisülése ne legyen befolyással a másik mentési példányra.

A mentett információ bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen biztosítani kell.

A mentéseket a bennük tárolt információktól függően kriptográfiai módszerekkel titkosítani kell. A szükséges titkosítás erősségét és a tesztelési gyakoriságát a DPO határozza meg.

Az ebben a pontban leírtak végrehajtását az ICSV feladata koordinálni. A feladatok végrehajtását az IBF-nek rendszeresen, de legalább évente ellenőriznie kell.

3.2.5.9 Az elektronikus információs rendszer helyreállítása és újraindítása

A BSZRK-nak (közvetlenül vagy megbízottja útján) gondoskodnia kell az EIR utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.

Az EIR helyreállítási módját, menetét, lépéseit, a szükséges erőforrásokat, azok elvárt közreműködését, a helyreállítás időszükségletét és korlátait megfelelő részletességű leírásban össze kell foglalni az adott EIR Rendszerbiztonsági tervében vagy annak mellékletében, a leírás megfelelőségét pedig legalább éves gyakorisággal végzett teszteléssel ellenőrizni szükséges.

A BSZRK tranzakció alapú EIR-ei esetében a helyreállítást/újraindítást úgy kell elvégezni, hogy a tranzakciók is helyreálljanak.

Az ebben a pontban leírtak végrehajtását az ICSV feladata koordinálni. A feladatok végrehajtását az IBF-nek rendszeresen, de legalább évente ellenőriznie kell.

3.2.6 Azonosítás és Hitelesítés

3.2.6.1 Eljárásrend

Az eljárásrendet rendszeresen, de legalább évente felül kell vizsgálni, aktualizálni kell. A felülvizsgálat és aktualizálás az ICSV feladata.

Az azonosítással és hitelesítéssel kapcsolatos elvárások teljesülését az IBF legalább éves gyakorisággal, mintavétellel ellenőrzi.

3.2.6.2 Azonosítás és hitelesítés

A BSZRK EIR-einek egyedileg azonosítani és hitelesíteni kell a BSZRK felhasználóit, és a felhasználók által végzett tevékenységet, ennek érdekében a BSZRK informatikai infrastruktúrájához, EIR-eihez hozzáférők számára egyedi, személyhez rendelt felhasználói azonosítókat kell képezni.

A felhasználói azonosító igénylését, jóváhagyását, képzését, beállítását az „Infokommunikációs eszközök használatáról szóló szabályzat" elvárásai alapján kell végezni.

A humán felhasználók felhasználói azonosítóját a felhasználó vezetéknevéből és keresztnevéből kell képezni. Ettől abban az esetben lehet eltérni, ha ez egy másik már létező felhasználóval azonos felhasználónevet eredményezne.

Adott felhasználói azonosítót csak az használhat, aki számára az létre lett hozva/ki lett adva, más számára ez tiltott. Adott felhasználói több személy általi használata nem engedélyezett.

A technikai felhasználókat humán felhasználó nem használhatja, ennek érdekében a technikai felhasználók jelszavait jelszómegosztással kell kezelni.

A nevesítetlen felhasználókat személyhez kell rendelni, vagy meg kell szüntetni.

A BSZRK informatikai infrastruktúrájában használt eszközöket, levelezőcsoportokat stb. egyedi azonosítóval kell ellátni.

A jelszószéfben tárolt jelszavak mentéséről gondoskodni szükséges.

A BSZRK EIR-einek többtényezős hitelesítést kell alkalmazniuk a különleges jogosultsághoz kötött (úgynevezett privilegizált) felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez, illetve jelentős biztonsági besorolású EIR esetében minden felhasználó esetén.

A BSZRK EIR-einek hitelesítési folyamatait úgy kell kialakítani, hogy azok ellenálóak legyenek a viszajátszásos támadások ellen.

3.2.6.3 Eszközök azonosítása és hitelesítése

A BSZRK jelentős biztonsági besorolású EIR-eihez kacsolódó eszközeit a 802.1X szabványnak megfelelően azonosítja és hitelesíti mielőtt azok hozzáférhetnének az EIR-ekhez hozzáférést biztosító hálózathoz.

3.2.6.4 Azonosító kezelés

A BSZRK informatikai infrastruktúrájában használt azonosítóknak egyedinek kell lenniük.

A külső partnerek, támogatók, felhasználói azonosítójának tartalmaznia kell az arra vonatkozó jelzést, hogy a felhasználó nem a BSZRK által foglalkoztatott, hanem külső partner. A felhasználói azonosító BSZRK által olvasható leírásában pedig szerepelnie kell az adott felhasználót delegáló külső szervezet megnevezésének.

Az azonosítás során megkülönbözetett felhasználóknak, felhasználói csoportoknak, szerepköröknek, eszközöknek a meghatározása az ICSV feladata.

Az azonosítók ismételt felhasználása tilos.

Az azonosítókat rendszeresen felül kell vizsgálni, és negyedéves inaktivitást követően (ellenkező érvényű vezetői kérés hiányában) le kell tiltani. A felülvizsgálat és letiltás az ICS feladata, a felülvizsgálat és a letiltások megtörténtét az ICSV legalább havonta, az IBF évente ellenőrzi.

3.2.6.5 A hitelesítésre szolgáló eszközök kezelése

A BSZRK a hitelesítésre szolgáló eszközei kapcsán

- 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 típusára 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.

A BSZRK

- a jelszóra a következő elvárásokat érvényesíti:
  - kis- és nagybetűk megkülönböztetése és elvárása;
  - a karakterek számának meghatározása (az alábbiak szerint);
    - a kisbetűk, nagybetűk, számok és speciális karakterek megkülönböztetése és elvárása, és
    - minimálisan 8 (adminisztrátori jelszó esetén: 16, nem személy által használt jelszó esetén: 24) karakter jelszóhosszúság elvárása;
- 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, amely szerint
  - felhasználói és adminisztrátori jelszó 1 évig érvényes,
  - nem személy által használt jelszó korlátozás nélkül érvényes,
- 12 új jelszóig megtiltja a jelszavak ismételt felhasználását, és
- a rendszerbe első lépést lehetővé tevő ideiglenes jelszó lecserélésére kötelezi a felhasználót (kivéve a nem személy által használatos jelszavaknál).
- kell, hogy a felhasználó által megadott jelszavak szerepelnek-e a gyakran használt, könnyen kitalálható vagy kompromittált jelszavak listáján

A BSZRK informatikai infrastruktúrájában

- az azonosítóhoz tartozó jelszót az ICS hozza létre oly módon, hogy kezdeti jelszót állít be az azonosítóhoz;
- az azonosítóhoz tartozó kezdeti jelszót az ICS átadja az érintett felhasználónak, amelyet az az első bejelentkezéskor kötelezően megváltoztat VAGY az érintett felhasználó jelenlétében az ICS foglalkoztatottja belép az eredeti jelszóval, amelyet a felhasználó az ICS foglalkoztatottja jelenlétében (de nem a szeme láttára) megváltoztat;

- a felhasználó a jelszavát köteles titokban tartani;
- a felhasználó felelőssége, ha jelszavának megismerésével a nevében visszaélést követnek el;
- a felhasználói jelszót TILOS leírni (a kezdeti, felhasználónak átadott, kötelezően megváltoztatandó jelszó kivételével);
- a felhasználói jelszót TILOS bármely alkalmazással, megoldással megjegyeztetni (pl. a böngészőben eltárolni), kivéve az erre szolgáló, az NKTK által jóváhagyott jelszószéf megoldást;
- ha bármilyen jel arra mutat, hogy a jelszót illetéktelenek megismerték (a jelszó kompromittálódott), azonnal meg kell azt változtatni és értesíteni kell az ICSV-t és az IBF-et, az esetet pedig incidensként kell kezelni;
- nem tehető a felhasználói azonosító és jelszó egy automatikus bejelentkezési folyamat részévé, pl. nem szabad makróba illeszteni, vagy funkció billentyűhöz kapcsolni;
- alkalmazott felhasználói azonosító biztonsága függ a jelszó hosszától és komplexitásától, ezért a jelszavak megadásánál az alábbi elvárásokat kell betartani:
    - a jelszó ne alapuljon olyan tényen, információn, amely alapján azt más személy kitalálhatja (nevek, telefonszámok, születési dátumok, irodában előforduló márkanevek, projektazonosítók, rövidítések stb. kerülendőek);
    - a jelszó ne legyen a gépnévre vagy a felhasználói névre utaló;
    - a jelszó ne legyen sorozat (az 1234abCD, Qwertzui, 1Qay2Wsx stb. kerülendő).

A fenti szabályokat a BSZRK informatikai infrastruktúrájában lehetőleg ki kell kényszeríteni (ha technikailag lehetséges, az informatikai infrastruktúrában a jelszavakra vonatkozó elvárások között be kell állítani).

A BSZRK informatikai infrastruktúrájában alkalmazott jelszó idegen kézbe kerülése, a jelszó kompromittálódása, illetve a jelszószabályok be nem tartása biztonsági incidensnek minősül, ezért ezekben az esetekben ennek megfelelően kell eljárni.

A BSZRK elektronikus információs rendszerében nyilvános kulcsú infrastruktúra alapú hitelesítés esetén

- ellenőrizni kell a tanúsítványokat egy elfogadott megbízható pontig tartó tanúsítványlánc felépítésével és ellenőrzésével, beleértve a tanúsítvány állapot információ ellenőrzését is;
- ki kell kényszeríteni a megfelelő magánkulcshoz való jogosult hozzáférést;
- össze kell kapcsolni a hitelesített azonosságot az egyéni vagy csoport fiókkal;
- meg kell valósítani a visszavonási adatok helyi tárolását a tanúsítványlánc felépítésének és ellenőrzésének támogatására arra az esetre, amikor a visszavonási információk a hálózaton keresztül nem elérhetők.

A BSZRK az adott EIR-hez hozzáférést biztosító hitelesítési eszköz az EIR biztonsági osztályától függően védelemmel látja el.

3.2.6.6 Hitelesítési információk visszajelzésének elrejtése

A BSZRK EIR-ében alkalmazott hitelesítésre szolgáló eszköz hibás azonosító, vagy jelszó megadása esetén csak olyan hibaüzenetet adhat vissza, melyből nem szerezhető további információ sem az azonosítóról, sem a jelszó összetételéről, illetve a birtokláson alapuló eszköz jellegéről, állapotáról.

3.2.6.7 Hitelesítés kriptográfiai modul esetén

A BSZRK EIR-ének egy adott kriptográfiai modulhoz való hitelesítése során olyan mechanizmusokat kell használnia, amelyek megfelelnek az adott hitelesítési szolgáltató által az adott kriptográfiai modulhoz rendelkezésre bocsájtott hitelesítési útmutatónak.

3.2.6.8 Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

A BSZRK-on kívüli felhasználók EIR-hez történő hozzáférése során a BSZRK-on belüli felhasználók kapcsán leírtaknak megfelelően kell eljárni, azzal a különbséggel, hogy a BSZRK-on kívüli személy részére csak akkor hozható létre felhasználói azonosító, ha

- a személy vagy a munkáltatója és a BSZRK között érvényes szerződés vagy megbízás van, amely rendelkezik az azonosítók és hitelesítő eszközök használatáról, továbbá
- a BSZRK-on kívüli személy előzetesen aláírta a BSZRK által készített titoktartási nyilatkozatot és
- dokumentált formában megismerte a BSZRK vonatkozó információbiztonsági előírásait.

3.2.6.9 Újrahitelesítés

A BSZRK EIR-eit úgy kell beállítani, hogy azok a „3.2.1.9 Eszköz zárolása" ponton felül a következő esetekben kérjenek újra hitelesítést a felhasználóktól:

- az adott szerepkörben vagy a szerepkör által elért funkciókban bekövetkező változás
- a hitelesítő adatokat vagy eszközöket érintő változás
- az EIR biztonsági osztályának változása

3.2.6.10 Személyazonosság igazolása

Az EIR-hez hozzáférést adó azonosítókat egyedi személyek számára kell kiállítani, akiknek személyazonosságáról az MO a megfelelő jogszabályokban meghatározott személyazonosságot igazoló bizonyítékok ellenőrzésével már meggyőződött.

Az azonosítás során keletkező dokumentumok és rögzített adatok védelme és megőrzése az MO feladata.

Az azonosításhoz használt személyazonosságot igazoló bizonyítékot a hozzáférést biztosító fiók regisztrációja során az IO számára külön be kell mutatnia a regisztrálónak és a regisztrációt végzőnek ellenőriznie kell.

A BSZRK-n kívüli külsős támogató szervezet felhasználóinak regisztrálása során fizikai vagy elektronikus cím megerősítése is szükséges.

3.2.7 Kockázatkezelés

3.2.7.1 Eljárásrend

A BSZRK az informatikai kockázatelemzési és kockázatkezelési eljárásrendet a következőknek megfelelően határozza meg, dokumentálja, illetve hirdeti ki.

A kockázatelemzési és kockázatkezelési eljárásrendet rendszeresen, de legalább évente felül kell vizsgálni és aktualizálni kell, ami az IBF feladata.

A kockázatelemzési eljárásrendnek ki kell terjednie

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

3.2.7.2 Biztonsági osztályba sorolás

A BSZRK-nak a jogszabályban meghatározott szempontok alapján meg kell vizsgálnia a „3.1.1.5 Az elektronikus információs rendszerek nyilvántartása" pontban leírt követelmények alapján nyilvántartásba vett EIR-eit, és meg kell határoznia, hogy azok melyik biztonsági osztályba sorolandók.

A besorolást az IBF-nek jóvá kell hagyatnia az FI-vel. A jóváhagyott besorolást az IBF-nek rögzítenie kell az adott EIR rendszerbiztonsági tervében a besorolást alátámasztó indokokkal együtt.

A BSSRK EIR-einek biztonsági osztályba sorolását az EIR-eket érintő jelentős változások után ismételten el kell végezni.

Jelentős változásnak számít az EIR-nek vagy környezetének a BSZRK által korábban nem támogatott alapvető feladatait érintő érdemi funkcionális bővülése (pl. a rendszer a BSZRK olyan alapfeladatait támogatja érdemben, amelyet korábban nem, vagy ellenkezőleg: megszűnik adott alapfeladat támogatása),

- a felhasználók azonosítási módja érdemben változik,
- a felhasználók jogosultság-kezelése érdemben változik,
- a naplózási módja érdemben változik,
- a zártságát, integritását biztosító megoldások érdemben változnak,
- az elérhetőségét biztosító megoldások érdemben változnak,
- az üzemeltetési körülményei érdemben változnak (beleértve, ha jelentős új fenyegetések vagy sebezhetőségek jelentek meg).

A jelentős változásról az IBF-et a változás tervezése során megfelelően, dokumentáltan tájékoztatni szükséges, amely az ICSV feladata.

A BSZRK EIR-einek biztonsági osztályba sorolása jelentős változását eredményező változásra kizárólag az ICSV előzetes, írásos engedélye alapján kerülhet sor.

A EIR jelentős változását eredményező megrendelést külső vállalkozónak kizárólag az ICSV előzetes, írásos engedélyével szabad kiadni; ennek hiányában végzett megrendelés érvénytelen.

A BSZRK EIR-einek osztályba sorolási eredményét az „3.1.1.4 Az intézkedési terv és mérföldkövei" pontban leírt tevékenységek végrehajtásakor fel kell használni.

3.2.7.3 Kockázatelemzés

A BSZRK-nak rendszeresen, de legalább évente biztonsági kockázatelemzéseket kell végeznie, amelynek keretében a korábbi kockázatelemzések eredményeit is felül kell vizsgálni. A kockázatelemzés elkészítését az IBF koordinálja, a tevékenységet az ICSV kiemelten támogatja.

A kockázatelemzést a szabályzat „4.3 KOCKKÁZATMENEDZSMENT KERETRENDSZE" függelék alapján kell elvégezni.

A kockázatelemzést a tervezett rendszerességtől eltérően, egyedileg is el kell végezni (illetve a legutóbbi kockázatelemzést frissíteni kell), ha jelentős változás áll be az EIR-ben vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését), továbbá olyan körülmények esetén, amelyek befolyásolják az EIR biztonsági állapotát.

A kockázatelemzésnek ki kell térnie az ellátási láncból eredő kockázatokra is.

A kockázatelemzések eredményét kockázatelemzési jelentésben dokumentálni kell és az IBF-nek meg kell ismertetnie az FI-vel és az ICSV-vel, valamint a BSZRK érintett EIR-einek üzemeltetőivel, fejlesztőivel.

A kockázatelemzési jelentésben dokumentált kockázatok kezelésére a jelentésben megadott felelősöknek megfelelő intézkedéseket kell kidolgozniuk, majd azok végrehajtásáról gondoskodniuk. Az intézkedési terv kidolgozását és megvalósítását a BSZRK érintett EIR-einek üzemeltetőinek és fejlesztőinek aktívan támogatniuk kell.

A kockázatelemzési eredmények kezelése során a BSZRK Kockázatmenedzsment stratégiája alapján kell eljárni, kiemelten biztosítva az eredmények illetéktelen hozzáféréstől védett tárolását, kezelését, azok jogosulatlanok általi elérésének, megismerésének megakadályozását.

3.2.7.4 Sérülékenységek ellenőrzése

A BSZRK sérülékenység ellenőrzést végez legalább negyedévente vagy abban az esetben, ha az EIR-en vagy annak rendszerelemén futó szoftverek esetén sérülékenységet azonosítanak, vagy jelentenek.

Az azonosított hibákat és hiányosságokat a kockázatkezelési eljárásrend szerint kell kijavítani az adott sebezhetőséghez rendelt CVSS (Common Vulnerability Scoring System) értéke vagy ha rendelkezésre áll az adott gyártó/fejlesztő ajánlása alapján meghatározott időn belül.

CVSS érték	Súlyosság	Válaszidő
9-10	Kritikus	legfeljebb 15 nap
7-8.9	Magas	legfeljebb 30 nap
4-6.9	Közepes	legfeljebb 90 nap
0.1-3.9	Alacsony	legfeljebb 180 nap

Amennyiben az érintett sérülékenység a rendszerelem vagy szoftver kiterjedt használata miatt a meghatározott válaszidőn belül nem javítható; a kockázat csökkentése érdekében további intézkedéseket kell bevezetni.

3.2.7.5 Sérülékenységmenedzsment

A BSZRK EIR-ei és rendszerelemeiről a központi monitorozó rendszeren keresztül automatikus mechanizmusok segítségével átfogó sérülékenység ellenőrzéseket kell végezni a „3.2.7.4 Sérülékenységek ellenőrzése" pontban meghatározott esetekben.

Az eljárásnak meg kell mutatniuk a különböző platformokon feltárt szoftverhibákat és helytelen konfigurációkat, valamit azok esetleges hatásait és az azokhoz rendelt szemmértékeket. Az eljárásnak

ki kell térnie az EIR-ről vagy rendszerelemről, annak kompromitálása nélkül, elérhető információk vizsgálatára is.

Az ehhez használt programok adatbázisát automatikusan kell frissíteni a változáskezelési eljáráson hatályán kívül.

Az eljárás megfelelő kivitelezését elősegítendő az egyes EIR-ek és rendszerelemekhez ellenőrző listákat és tesztelési eljárásokat kell kidolgozni.

Az eljárás elvégzéséhez a BSZRK privilegizált elérést biztosít a tesztelést végző számára.

A feltárt hibákat a „3.2.7.4 Sérülékenységek ellenőrzése" pontban és a „3.2.7.6 Kockázatokra adott válasz" pontban leírtak szerint kell kijavítani, amiben az automatikus mechanizmusok is segítséget biztosítanak.

A felfedezett sérülékenységeket a BSZRK-n belül a tesztelés végzőnek meg kell osztani az ICSV-vel, az IBF-fel, valamint az egyes EIR-ek felelős személyeivel.

A BSZRK csatornát hoz létre, melyen keresztül fogadja az EIR-ek és rendszerelemek sérülékenységeiről szóló jelentéseket.

A sérülékenységmenedzsmentről kivitelezési módjáról a BSZRK „Sérülékenységmenedzsment" külön álló dokumentuma ir bővebben.

3.2.7.6 Kockázatokra adott válasz

A kockázatelemzés, a sérülékenység ellenőrzés és a sérülékenységmenedzsment eredményeként feltárt kockázatokat a BSZRK-nak kezelnie kell a következő módokon:

- a kockázat csökkentésével
- a kockázat elfogadásával
- a kockázat megosztásával
- a kockázat áthárításával
- új biztonsági követelmény bevezetésével
- meglévő biztonsági intézkedés kibővítésével/megerősítésével

Ha a válaszintézkedés nem azonnal (vagy rövid időn belül) megvalósítható a BSZRK-nak intézkedési tervet kell kidolgoznia a „3.1.1.4 Az intézkedési terv és mérföldkövei" pontban foglaltaknak megfelelően.

A kockázatokra adott válaszintézkedéseket az FI, hagyja jóvá és annak kivitelezése és dokumentálása az ICSV feladata.

3.2.7.7 Rendszerelemek kritikusságának elemzése

A BSZRK EIR-einek életciklusában a tervezési fázisban, valamint a már működő rendszerek fejlesztése, módosítása vagy frissítése esetén meg kell vizsgálni az érintett rendszerelemek vagy rendszerszolgáltatások kritikusságát.

A vizsgálat eredménye alapján meghatározható, hogy mely rendszerelemek és funkciók kiesése jelent komoly problémát az EIR működésében. Az így azonosított kockázatokat a 3.2.7.6 Kockázatokra adott válasz pont szerint kell kezelni.

3.2.8 Rendszer- és szolgáltatásbeszerzés

3.2.8.1 Eljárásrend

A BSZRK által megfogalmazott, dokumentált és a BSZRK-on belül kihirdetett általános beszerzési eljárásrendnek a BSZRK EIR-ére is vonatkoznia kell.

A BSZRK EIR-ével, illetve az ehhez kapcsolódó szolgáltatásoknak és az információs rendszer biztonsági eszközeinek beszerzésére vonatkozó szabályokat, és a szabályok betartásának ellenőrzésének módját, menetét jelen szabályzat tartalmazza.

A jelen szabályzatban definiált elvárások teljesülését az ICSV feladata koordinálni (hacsak ez a szabályzat egyes pontokban másként nem rendeli).

3.2.8.2 Erőforrások rendelkezésre állása

A BSZRK az informatikai és a kapcsolódó emberi erőforrás igények felmérését az egyes beszerzési eljárásokhoz kapcsolódóan egyedileg végzi és ennek keretében meg kel határozni az adott EIR vagy rendszerelem információbiztonsági követelményeit. Az erőforrásigények felmérését és a követelmények meghatározását az ICSV koordinálja.

Az EIR-ek biztonsági költségeit külön költségvetési tételként kell kezelni a beszerzés során.

3.2.8.3 A rendszer fejlesztési életciklusa

A BSZRK a rendszerek fejlesztési életciklusa kapcsán elrendeli, hogy

- a BSZRK-ban alkalmazott EIR-ek teljes életútján, azok minden (alábbiakban meghatározott) életciklus-szakaszában figyelemmel kell kísérni az EIR-ek informatikai biztonsági helyzetét és meg kell tenni a megfelelő intézkedéseket, hogy az EIR-rel kapcsolatban támasztott információbiztonsági elvárások teljesüljenek;
- a fejlesztési életciklus egészére meg kell határozni és dokumentálni szükséges az információbiztonsági szerepköröket és felelősségeket.

A beszállítók, szolgáltatók, illetve az EIR-ek, rendszerelemek kiválasztásánál a szakmai/gazdasági szempontokon túl figyelembe kell venni, hogy az egyes lehetőségek (eszközök, rendszerek, szolgáltatások stb.)

- milyen információbiztonsági előnyöket/veszélyeket jelentenek a BSZRK számára,
- milyen védelmi lehetőségeket biztosítanak a szándékos támadások és a gondatlanság okozta események kivédésére, felderítésére, bizonyítására,
- milyen lehetőségeket biztosítanak az esetleges szándékos támadás vagy gondatlanság okozta események kivédésére, felderítésére, bizonyítására,
- milyen erőforrásokat igényelnek a BSZRK-tól és külső partnereitől a védelem kívánt szintjének fenntartása, üzemeltetése érdekében.

A fejlesztési/beszerzési fázisban az ajánlatok értékelésekor figyelemmel kell lenni továbbá arra, hogy

- milyen informatikai infrastruktúra elemekhez, EIR-hez vagy rendszerelemhez és milyen módon, mértékben szándékoznak az ajánlattevők hozzáférni,
- az ajánlattevők milyen információbiztonsági eljárásokat, megoldásokat alkalmaznak,

- az ajánlattevők milyen alvállalkozó(ka)t kívánnak bevonni, a szolgáltató kíván-e alvállalkozót bevonni.

A szállítói és szolgáltatói szerződéseket megfogalmazásánál a szerződésben meg kell határozni az ezen szabályzatban definiált elvárásokon túl

- a fejlesztés, karbantartás szakmai/gazdasági, informatikai és információbiztonsági követelményeit és sikerkritériumokat,
- a kapcsolattartók megnevezését,
- a kapcsolattartás módját,
- a BSZRK rendszereihez való hozzáférés szabályait,
- a fejlesztés során betartandó biztonsági követelményeket,
- a tesztelés, tesztadatok, tesztesetek alapvető jellemzőit,
- a hibabejelentés és a hibajavítási feladatok elfogadásának, teljesítésének módját,
- a verziók átadás-átvételének formáját és módját,
- az utánkövetés jellemzőit,
- az átadott EIR(elem) tulajdon- és használati jogával kapcsolatos elvárásokat,
- garanciális és teljesítési követelményeket, továbbá
- azon intézkedéseket, amelyek az információbiztonsági incidensek megelőzését, megakadályozását, hatásának csökkentését szolgálják.

Az EIR(elem) átvételét megelőzően a BSZRK kötelezi a fejlesztőjét, hogy a meghatározott védelmi intézkedésekhez biztosítson tervezési és megvalósítási információkat, amiknek tartalmazniuk kell:

- a biztonsági szempontból releváns külső rendszerinterfészeket,
- a magas szintű rendszertervet,
- az alacsony szintű rendszertervet,
- a forráskódot vagy a hardversémákat,

valamint határozza meg az EIR(elem) használatára tervezett funkciókat, portokat, protokollokat és szolgáltatásokat.

Az EIR(elem) átvételekor ellenőrizni kell, hogy azokat a rendszer(elem)eket, funkciókat, megoldásokat, információbiztonsági megoldásokat kapta-e a BSZRK, amelyek a specifikációban és a megrendelésben szerepeltek.

Az átvenni tervezett EIR(elem)et átvétel előtt ki kell próbálni, az üzembe/használatba vétel előtt pedig jóvá kell hagyni annak érdekében, hogy az valamennyi vonatkozó információbiztonsági irányelvnek és követelménynek megfeleljen. Az elvárttól eltérő teljesítésről jegyzőkönyvet kell felvenni. Hiba esetén a garanciát érvényesíteni kell. A próbát, tesztelést, értékelést és szükség esetén az eset rendezését az ICSV koordinálásával, a szállító képviselője és (ha információbiztonsági funkcionalitású rendszer(elem) a fejlesztés tárgya, akkor) az IBF bevonásával kell elvégezni.

Kizárólag olyan informatikai, telekommunikációs megoldás, szolgáltatás, EIR(elem) szerezhető be (függetlenül annak későbbi használójától, funkciójától és üzemeltetési módjától, körülményeitől), amely megfelel a BSZRK szabályzataiban, valamint a vonatkozó jogszabályokban, jogforrásokban megfogalmazott követelményeknek. Az elvárásoknak való megfelelésről a szállítót először

nyilatkoztatni kell, illetve kétség esetén a követelményeknek megfelelést elbírálását az ICS végzi, információbiztonsági funkcionalitású rendszer(elem) esetén az IBF bevonásával.

A BSZRK-nak a szerződéses kötelezettségek keretében a szerződéses partnereitől a szerződéses kapcsolat kezdetekor, a szerződés aláírásával egyidőben meg kell követelnie, hogy a szerződéses partner nyilatkozzon arról, hogy a szolgáltatási szerződés alapján a BSZRK által igénybe venni/kifejlesztetni szándékozott EIR, szolgáltatás megfelel a BSZRK által elvárt elektronikus információbiztonsági követelményeknek (a „4.1 IGÉNYBE VETT SZOLGÁLTATÁSOK, MEGVÁSÁROLT, VALAMINT KIFEJLESZTETT RENDSZEREK KAPCSÁN ELVÁRT ELEKTRONIKUS INFORMÁCIÓ-BIZTONSÁGI KÖVETELMÉNYEK BETARTÁSÁNAK VÁLLALÁSA" szerződési tervezet alapján készített szerződés aláírásával);.

A partnerektől elvárás a BSZRK értékrendjének vállalása, valamint az informatikai biztonsággal kapcsolatos alapvető elvárások betartásának vállalása, ezért a szerződéses kapcsolat kezdetén, a szerződés aláírásával egyidejűleg nyilatkoztatni kell őket a „4.2 INFORMÁCIÓSBIZTONSÁGI HÁZIREND ÉS NYILATKOZAT (FOGLALKOZTATOTTAK ÉS PARTNEREK SZÁMÁRA)" függelék dokumentumban részletezett alapelvek, elvárások elfogadásáról, betartásáról. A szerződés ezen nyilatkozat aláírásának elmaradása vagy megtagadása esetén nem léptethető életbe.

3.2.8.4 Beszerzések

A BSZRK informatikai beszerzései kapcsán a BSZRK beszerzési és közbeszerzési szabályzata alapján kell eljárni, az egyedi követelményeket ezen szabályzat elvárásaival (lásd 3.2.8.3 A rendszer fejlesztési életciklusa pont) kiegészítve szükséges alkalmazni.

3.2.8.5 Az elektronikus információs rendszerre vonatkozó dokumentáció

A BSZRK számára fejlesztett, illetve a BSZRK által beszerzett EIR-eknek, rendszerelemeknek, szolgáltatásoknak a megfelelő minőségű és biztonságú üzemeltetés és kontroll érdekében megfelelő dokumentációval kell rendelkezniük. Ennek biztosítása érdekében a BSZRK-nak

- ha hatókörébe tartozik, meg kell követelnie és birtokába kell vennie az EIR-re, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amelynek tartalmaznia kell
    - a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését kiemelten beleértve a rendszer
        - felhasználói adminisztrációjának és
        - jogosultsági rendszerének leírását és használatának bemutatását,
        - mentését és a mentésekből visszaállítás, valamint
        - a naplózás és a naplózott információ értelmezésének leírását, továbbá
        - az adatkapcsolatoknak és az adatkapcsolatok megfelelő működése érdekében szükséges beállításoknak a leírását.
    - a biztonsági funkciók hatékony alkalmazását és fenntartását,
    - a rendszer funkcionális tesztelését,
    - a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket, valamint azok javításáról szóló intézkedési tervét leíró dokumentumokat;

- meg kell követelnie és birtokába kell vennie az EIR-re, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amely tartalmazza
    - a felhasználó által elérhető funkciók részletes használati leírását, olyan módon, hogy annak alapján a funkció segítség nélkül, hibamentesen végrehajtható legyen,
    - 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;
- gondoskodni kell róla, hogy amennyiben a fentebb említett dokumentumok nem léteznek vagy nem állnak rendelkezésre, azokat a BSZRK a rendszer üzembe helyezése előtt pótolja,
- gondoskodni kell róla, hogy az információs rendszerre vonatkozó (különösen az adminisztrátori és fejlesztői) dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható (ebből a szempontból jogosulatlannak számít mindenki, akinek a dokumentációban foglaltak nem szükségesek a feladatai elvégzéséhez);
- gondoskodni kell a dokumentációknak a BSZRK által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismeréséről.

3.2.8.6 Biztonságtervezési elvek

A BSZRK a következő biztonságtervezési elveket használja az EIR tervezési, fejlesztési és megvalósítási fázisában:

- mélységi védelem kialakítása,
- biztonsági jógyakorlatok alkalmazása,
- biztonsági architektúra és követelmények létrehozása a tervezés és fejlesztés alapjául,
- a biztonsági követelmények beépítése az EIR fejlesztési életciklusába,
- fizikai és logikai biztonsági határok meghatározása,
- fenyegetésmodellezés készítése a használati esetek, fenyegetést jelentő szereplők, támadási vektorok és minták, tervezési minták és a kockázat csökkentéséhez szükséges kiegészítő védelmi intézkedések azonosításához.

3.2.8.7 Külső elektronikus információs rendszerek szolgáltatásai

A BSZRK-nak a külső EIR szolgáltatásaira vonatkozó szerződéses kötelezettségei keretében a partnereitől a szerződéses kapcsolat kezdetekor, a szerződés aláírásával egyidőben meg kell követelnie, hogy a szerződéses partner nyilatkozzon róla, hogy a szolgáltatási szerződés alapján a BSZRK által igénybe venni/kifejlesztetni szándékozott EIR, szolgáltatás megfelel a BSZRK által elvárt elektronikus információbiztonsági követelményeknek (az „ 4.1 IGÉNYBE VETT SZOLGÁLTATÁSOK, MEGVÁSÁROLT, VALAMINT KIFEJLESZTETT RENDSZEREK KAPCSÁN ELVÁRT ELEKTRONIKUS INFORMÁCIÓ-BIZTONSÁGI KÖVETELMÉNYEK BETARTÁSÁNAK VÁLLALÁSA" szerződési tervezet alapján készített szerződés aláírásával).

A partnerektől elvárás a BSZRK értékrendjének vállalása, valamint az informatikai biztonsággal kapcsolatos alapvető elvárások betartásának vállalása, ezért a szerződéses kapcsolat kezdetén, a szerződés aláírásával egyidejűleg nyilatkoztatni kell őket a „4.2 INFORMÁCIÓSBIZTONSÁGI

HÁZIREND ÉS NYILATKOZAT (FOGLALKOZTATOTTAK ÉS PARTNEREK SZÁMÁRA)" függelék dokumentumban részletezett alapelvek, elvárások elfogadásáról, betartásáról. A szerződés ezen nyilatkozat aláírásának elmaradása vagy megtagadása esetén nem léptethető életbe.

A BSZRK által elvárt védelmi intézkedések meglétét és megfelelőségét a BSZRK-nak rendszeresen, de legalább évente, és legalább

- a szolgáltató szervezet tanúsítványainak ellenőrzésével, vagy
- a szolgáltató szervezet nyilatkoztatásával vagy
- véletlen mintavétellel

ellenőriznie kell, az ellenőrzés eredményét pedig dokumentálnia szükséges.

Ha a BSZRK külső partnertől informatikai vagy információbiztonsági szolgáltatást tervez igénybe venni, a külső partnernek az EIR „fejlesztés vagy beszerzés" életciklus-szakaszban az ajánlatadás során meg kell határoznia a szolgáltatások igénybevételéhez a BSZRK-tól vagy a BSZRK másik szolgáltatójától elvárt, szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat.

Az ebben a pontban említett követelményeket az IBF és az ICSV közösen határozza meg.

A követelmények betartását az IBF az ICSV támogatásával ellenőrzi.

3.2.8.8 Fejlesztői változáskövetés

A BSZRK előírja, hogy az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztője az EIR-ek teljes életciklusa során – ideértve azok tervezését, fejlesztését, bevezetését, üzemeltetését, valamint kivonását – alkalmazzon konfigurációkezelési folyamatokat.

A fejlesztő köteles:

- a szervezet által meghatározott konfigurációs elemek változtatásait dokumentálni, kezelni és ellenőrizni, valamint biztosítani ezek sértetlenségét a fejlesztési és üzemeltetési folyamatok során;
- kizárólag olyan változtatásokat végrehajtani az EIR-en, rendszerelemen vagy rendszerszolgáltatáson, amelyeket a BSZRK az erre kijelölt eljárásrend szerint előzetesen jóváhagyott;
- a jóváhagyott változtatásokat megfelelően dokumentálni, és azok lehetséges információbiztonsági hatásait értékelni és rögzíteni;
- a rendszer, rendszerelem vagy szolgáltatás biztonsági hibáit naprakészen nyilvántartani, a hibák kijavításáról gondoskodni, valamint az ezekkel kapcsolatos észrevételeket, incidenseket haladéktalanul jelenteni a BSZRK által kijelölt kapcsolattartó(k) részére;
- a változáskövetés során alkalmazott dokumentációkat a jogosulatlan hozzáférés ellen védeni, és kizárólag a BSZRK által kijelölt személyek részére elérhetővé tenni.

A változáskövetés keretében a fejlesztőnek biztosítania kell, hogy minden módosítás visszakövethető legyen, és ne veszélyeztesse az EIR működésének, integritásának és biztonságának fenntartását.

3.2.8.9 Fejlesztői biztonsági tesztelés

A BSZRK előírja, hogy az EIR, rendszereleme vagy rendszerszolgáltatása fejlesztője az alábbi biztonságtervezési és tesztelési követelményeknek feleljen meg.

A fejlesztő:

- köteles biztonságértékelési tervet készíteni, amelyben részletezi az EIR-rel kapcsolatos információbiztonsági kockázatok kezelésének módját, valamint az ezekhez kapcsolódó védelmi intézkedéseket. A tervet a fejlesztési folyamat során végre kell hajtani, és a végrehajtás eredményeit dokumentálni szükséges,
- a rendszerfejlesztéshez illeszkedő módon, köteles egység-, integrációs-, rendszer- és regressziós tesztelést végezni,
- a tesztelések eredményeit a BSZRK által meghatározott eljárásrend szerint kiértékeli,
- a biztonságértékelési terv végrehajtásáról, valamint a végrehajtott biztonsági tesztek eredményeiről részletes dokumentációt készít,
    - a dokumentációnak tartalmaznia kell a tesztelés során feltárt hibákat, sérülékenységeket és hiányosságokat, azok súlyossági besorolását, valamint a kijavításukra vonatkozó intézkedések leírását,
- köteles bevezetni és fenntartani egy dokumentált, nyomon követhető hibajavítási folyamatot, amely biztosítja, hogy minden azonosított hiba kezelése megfelelő prioritással történjen, és annak javítása ellenőrizhető módon megvalósul,
- feladata a tesztelés és értékelés során azonosított információbiztonsági hibák és hiányosságok kijavítása, valamint a javítások utóellenőrzésének és dokumentálásának biztosítása.

3.2.8.10 Fejlesztési folyamat, szabványok és eszközök

A BSZRK előírja, hogy az EIR, rendszereleme vagy rendszerszolgáltatása fejlesztője dokumentált fejlesztési folyamatot alkalmazzon, amely során:

- kiemelten kezeli a BSZRK által meghatározott biztonsági követelményeket,
- meghatározza a fejlesztés során használt szabványokat és eszközöket,
- dokumentálja a fejlesztés során használt speciális eszköz konfigurációkat és opciókat,
- a fejlesztési szakaszban az adott EIR biztonsági osztályát figyelembe véve, kritikussági elemzést végez, a BSZRK által meghatározott mérföldkő vagy döntési pont elérése után,
- nyilvántartja a változásokat,
- biztosítja, hogy a változások nyilvántartásához illetéktelenek ne férjenek hozzá,
- legalább éves gyakorisággal áttekinti a biztonsági követelményeknek való megfelelést,

3.2.8.11 Támogatással nem rendelkező rendszerelemek

Amennyiben a BSZRK EIR-einek rendszerelemeihez vagy rendszerszolgáltatásaihoz nem elérhető támogatás a fejlesztőtől, szállítótól vagy gyártótól, köteles lecserélni a rendszerelemet vagy rendszerszolgáltatást.

A lecseréléstől akkor lehet eltekinteni, ha a rendszerelem vagy rendszerszolgáltatás létfontosságú üzlet vagy ügymeneti funkciót lát el, vagy a biztonsági követelményeknek megfelelő cseréjéhez nem áll rendelkezésre elég idő.

A BSZRK köteles ezekhez a támogatással nem rendelkező rendszerelemekhez vagy rendszerszolgáltatásokhoz alternatív támogatást biztosítani, amivel a támogatás elvesztése miatti megnövekedett kockázat csökkenthető. Ennek biztosítására külső szolgáltató is bevonható.

Az alternatív támogatott rendszerelemek vagy rendszerszolgáltatások cseréjéhez vagy támogatásának folytatásához intézkedési tervet kell kidolgozni.

3.2.9 Rendszer- és kommunikációvédelem

3.2.9.1 Eljárásrend

Az eljárásrendet rendszeresen, de legalább évente felül kell vizsgálni, aktualizálni kell. A felülvizsgálat és aktualizálás az IBF feladata, akit ebben a tevékenységben az ICSV támogat.

A rendszer- és kommunikáció védelmének megfelelőségét az ICSV feladata rendszeresen ellenőrizni. Az ellenőrzések megtörténtét és megfelelőségét az IBF legalább éves gyakorisággal ellenőrzi.

3.2.9.2 Rendszer és felhasználói funkciók szétválasztása

A BSZRK EIR-eit úgy kell beállítani, hogy a rendszer üzemeltetési (privilegizált) funkcióihoz, csak meghatározott szerepkör felhasználói férjenek hozzá.

3.2.9.3 Információk az osztott használatú rendszererőforrásokban

A BSZRK EIR-eit úgy kell beállítani, hogy azok meggátolják a megosztott erőforrásokon keresztül történő jogosulatlan vagy véletlen információátvitelt.

3.2.9.4 Szolgáltatásmegtagadással járó támadások elleni védelem

A BSZRK informatikai infrastruktúráját és EIR-eit összekötő hálózatot, úgy kell kialakítani, hogy a szolgáltatásmegtagadással járó támadások mérsékléséhez elegendő kapacitással és redundanciával rendelkezzen.

A BSZRK szolgáltatásmegtagadással járó támadások kivédésére alkalmas hálózati eszközeit úgy kell beállítani, hogy azok használják ezen funkcióikat.

3.2.9.5 A határok védelme

A BSZRK informatikai infrastruktúrájának, valamint EIR-einek határvédelmét tűzfalakkal kell biztosítani oly módon, hogy az informatikai infrastruktúrája és az EIR-ek ne legyenek jogosulatlanul elérhetőek a BSZRK-on kívülről, az Internet irányából, illetve róluk csak a tűzfalakon keresztül legyen elérhető az Internet vagy más külső hálózat.

A BSZRK EIR-eit úgy kell kialakítani, hogy azok lehetőség szerint a legkevesebb külső hálózati kapcsolattal rendelkezzenek és az érintett szolgáltatásaik csak a tűzfalon keresztül megfelelő forgalomirányítási szabályokkal ellátott módon legyenek elérhetőek.

A BSZRK EIR-einek meg kell akadályozniuk a szabályoknak nem megfelelő megosztott csatornahasználatot végző távoli eszközök kapcsolódását.

A BSZRK belső informatikai hálózatát szegmentálni, több részre kell osztani oly módon, hogy

- a szerverek,
- az irodaikörnyezet
- a mentésre szolgáló rendszerelemek,
- a naplóállományok központi gyűjtését és elemzését biztosító rendszerelemek,
- a tesztelésre szolgáló informatikai környezet és rendszerelemek

egymástól elkülönített hálózati szegmensen legyenek, amely szegmensek közötti kommunikáció belső tűzfalakon keresztül, védett, szabályozott módon történjen.

A vendég Wi-Fi szolgáltatását annak Internet kijáratával együtt a BSZRK belső informatikai hálózatától elkülönített, de tűzfalakkal szintén védett hálózaton kell üzemeltetni.

A BSZRK tűzfalainak interfészein védeni kell az átvitt adatok bizalmasságát és sértetlenségét. Továbbá a tűzfalaknak blokkolniuk kell minden nem engedélyezett adatfolyamot és közzé kell tenniük azokat az információkat, amelyek segítségével a távoli hálózatok észlelhetik a nem engedélyezett vezérlőadat-forgalmat.

A külső és belső tűzfalakat úgy kell konfigurálni, hogy csak a minimálisan szükséges portok, protokollok és szolgáltatások legyenek engedélyezve, valamint minden külön nem engedélyezett forgalom elutasításra kerüljön.

A BSZRK belső hálózatáról kifelé irányuló kommunikációt hitelesített proxykiszolgálónk keresztül irányítja.

A BSZRK-nak dokumentálnia kell minden kivételt a forgalomáramlási szabályok alól a dokumentációnak minimum a következőket kell tartalmaznia:

- a kivételt alátámasztó működési cél vagy üzleti igény
- a kivétel pontos meghatározása (port, protokoll, szolgáltatás stb.)
- az igényelt kivétel időtartama

A kivételeket szükségességét az ICSV évente ellenőrzi és a fölöslegessé vált kivételeket törli. Ezt az IBF évente felülvizsgálja.

A tűzfalak felügyeletét folyamatosan biztosítani kell.

3.2.9.6 Az adatátvitel bizalmassága és sértetlensége

A BSZRK informatikai infrastruktúráján, valamint EIR-ein áthaladó adatok bizalmasságát és sértetlenségét biztosítani kell. Ezt fizikai módszerekkel a „3.1.6.4 Hozzáférés az adatátviteli eszközökhöz és csatornákhoz" pont szerint logikai módon pedig az „3.2.6.3 Eszközök azonosítása és hitelesítése" pont szerint kell elvégezni.

A BSZRK továbbá az adatok átviteléhez kriptográfiai védelmet biztosít, aminek feltételeiről és szabályairól a „3.2.1.12 Távoli hozzáférés" pont ír bővebben.

3.2.9.7 A hálózati kapcsolat megszakítása

A BSZRK EIR-eit úgy kell beállítani, hogy azok a munkaszakasz lezárásakor vagy tűzfalban meghatározott inaktivitást követően bontsák a hálózati kapcsolatot.

3.2.9.8 Kriptográfiai kulcs előállítása és kezelése

A BSZRK informatikai infrastruktúrájában, EIR-eiben alkalmazott kriptográfiához szükséges kriptográfiai kulcsokat, tanúsítványokat a BSZRK-nak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatótól kell vásárolnia vagy a BSZRK-n belüli használatra a BSZRK is generálhat tanúsítványokat.

Az ICS által igényelt/generált kulcsok szétosztását az ICS végzi. A szétosztást dokumentálni és jegyzőkönyvezni kell. A jegyzőkönyvet a kulcsok szétosztását végző személynek, az érintettnek és az ICSV-nek ellen kell jegyeznie.

A kulcsok, tanúsítványok tárolása során az alábbi alapelveknek megfelelően kell eljárni:

- a személyi aláíró, a személyi titkosító és az üzleti authentikációs tanúsítványt (vagy tokent) és a hozzá tartozó jelszót az érintett személy feladata megfelelően tárolni és kezelni,
- a softtokent az azt használó személy feladata megfelelően tárolni és kezelni,
- az SSL tanúsítványokat az ICS közös területén kell tárolni, más által nem hozzáférhetően, de valamennyi hozzáférést naplózva,
- minden további típusú tanúsítványt és a használatához szükséges jelszót, kódot, azonosítót stb. az adott személy tanúsítványt használó személy feladata megfelelően tárolni és kezelni.

A BSZRK által generált tanúsítványokat csak olyan helyzetben, környezetben szabad használni, ahol a felhasználó/informatikai rendszer(elem) azonosítására a belső tanúsítványon túl más megoldás is használatban van és a belső tanúsítvány mellett az is szükséges a BSZRK adataihoz való hozzáféréshez.

Személy által kezelt tanúsítvány/token csak olyan zárt helyen tárolható, amely kizárólag az adott személy által hozzáférhető, az illetéktelen hozzáférés pedig csak javítás nélkül helyre nem állítható roncsolással lehetséges.

Tanúsítványt nem szabad átadni, megosztani illetéktelen személlyel. (Illetéktelennek számít minden olyan személy, aki a tanúsítvány jogszerű használatára nincsen meghatalmazva, feljogosítva.) A tanúsítvány illetéktelennek átadása, megosztása információbiztonsági incidens, amelyet a BSZRK kivizsgál és szankcionálhat, a „3.1.8.8 Fegyelmi intézkedések" pontban leírtaknak megfelelően.

A NISZ által kibocsátott, elvesztett vagy ellopott, kompromittálódott tanúsítvány esetén az érintettnek kell közvetlenül felvennie a kapcsolatot a NISZ-szel az erre szolgáló telefonszámon; illetve jelentenie kell az elvesztést, ellopást, kompromittálódást az ICS felé, akik incidensként nyilvántartásba veszik a történteket.

A szükségtelen tanúsítványt dokumentáltan és helyre nem állítható módon meg kell semmisíteni. A megsemmisítésről készített jegyzőkönyvet az ICS megsemmisítést végző foglalkoztatottja mellett legalább egy másik ICS foglalkoztatottnak is ellen kell jegyeznie.

A BSZRK saját kiállítású kulcsainak előállításáról a BSZRK „Kriptográfiai kulcs elállítási szabályzata" ír bővebben.

A jegyzőkönyvekből valamennyi aláíró számára egy-egy eredeti aláírásokkal ellátott példányt kell biztosítani. A jegyzőkönyveket az azt kapó személynek 8 évig meg kell őriznie.

3.2.9.9 Kriptográfiai védelem

A BSZRK informatikai infrastruktúrája, EIR-e működtetése során csak olyan kriptográfiai megoldás alkalmazható, mely megfelel a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény előírásainak, illetve az elektronikus aláírást felügyelő hatóság ajánlásainak és állásfoglalásainak.

3.2.9.10 Együttműködésen alapuló informatikai eszközök

A BSZRK informatikai infrastruktúrájában, EIR-ei kapcsán az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválása nem engedélyezett, és a távoli aktiválást az EIR-ek beállításai meg kell, hogy akadályozzák.

3.2.9.11 Nyilvános kulcsú infrastruktúra tanúsítványok

Nyilvános kulcsok előállítása esetén figyelembe kell venni a „3.2.9.8 Kriptográfiai kulcs előállítása és kezelése" pontban foglaltakat.

A BSZRK tanúsítvány tárolóiba csak jóváhagyott és hitelesített tanúsítványok vehetőek fel.

3.2.9.12 Mobilkód korlátozása

A BSZRK az „Engedélyezett szoftverek" külön álló táblázatban felsorolt kivételekkel, tiltja bármilyen mobilkód futtatását.

3.2.9.13 Biztonságos név/cím feloldási szolgáltatás (hiteles forrás)

A BSZRK EIR-ének a név/cím feloldási kérésekre a hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozó kiegészítő adatokat is biztosítania kell.

A BSZRK EIR-ének ellenőriznie kell, hogy a név/cím feloldási kérésre a válasz attól a forrástól érkezik-e, amelyhez a feloldási kérést a BSZRK elküldte. Ennek biztosításához a rendszernek eredethitelesítést és adatsértetlenség ellenőrzést kell kérnie és végrehajtania.

3.2.9.14 Architektúra és tartalékok név/cím feloldás

A BSZRK név/cím feloldási szolgáltatást nyújtó EIR-ének hibatűrőnek, redundánsnak kell lennie, és meg kell valósítania a belső/külső szerepkör szétválasztást.

3.2.9.15 Munkaszakasz hitelessége

A BSZRK EIR-einek védelmi megoldásait úgy kell beállítani, hogy azok ne csak a csomagok szintjén, hanem a munkaszakasz szintjén is védelmet biztosítsanak a közbeékelődéses támadások (man-in-the-middle), a munkaszakasz-eltérítések (session hijacking), és a hamis információk munkaszakasz történő beszúrása ellen.

3.2.9.16 Tárolt (at rest) adatok védelme

A BSZRK EIR-ének védenie kell a BSZRK által meghatározott maradvány és archivált információk bizalmasságát, sértetlenségét. Ennek biztosítása érdekében az információkat tároló rendszerelem vagy adattárolón kriptográfiai eljárásokkal titkosíteni kell az adatokat.

A BSZRK ennek keretében védeni rendeli az átmeneti fájlokat és a kimeneti információ véglegest megelőző állapotait, komponenseit.

3.2.9.17 A folyamatok elkülönítése

A BSZRK EIR-einek elkülönített végrehajtási tartományt kell fenntartaniuk minden végrehajtó folyamat számára. Ez magába foglalja a rendszerek által használt címtartományok elkülönítését is.

3.2.10 Rendszer- és információsértetlenség

3.2.10.1 Eljárásrend

A fejezetben leírtakat adott EIR tekintetében akkor kell alkalmazni, ha az adott EIR-t a BSZRK üzemelteti.

Amennyiben a BSZRK adott EIR-ét külső szervezet üzemelteti, az ebben a fejezetben leírtakat a rendszerüzemeltetést végző külső szervezet és a BSZRK közötti szerződésben szerződéses kötelemként kell érvényesíteni oly módon, hogy az e fejezetben leírt elvárásoknak való megfelelést a külső szervezet biztosítsa.

A BSZRK informatikai infrastruktúrájának, informatikai rendszerelemeinek és a bennük tárolt adatok, információ védelme, a rendszerek és az információ sértetlensége érdekében a jelen eljárásrendben foglaltak szerint kell eljárni.

Az eljárásrendet rendszeresen, de legalább évente felül kell vizsgálni, aktualizálni kell. A felülvizsgálat és aktualizálás az IBF feladata.

A hozzáférések ellenőrzésével kapcsolatos elvárások teljesülését az IBF legalább éves gyakorisággal ellenőrzi.

3.2.10.2 Hibajavítás

A BSZRK informatikai infrastruktúrájában, EIR-eiben keletkező hibákat megfelelően, azok súlyosságához mérten kell kezelni. A hibákat az esetleges külső támogatók bevonásával, megfelelő tesztelési és jóváhagyási folyamatoknak megfelelően kell javítani, alapvetően a változáskezelési eljárásrendnek megfelelően (részletesebben lásd: „3.2.4.3 A konfigurációváltozások felügyelete (változáskezelés)" pont), a változáskezelés és hibajavítás közötti természetes különbségekre tekintettel.

A hibajavítás nem eredményezhet súlyosabb hibát, mint az elhárítani tervezett hiba, valamint a hibajavítás adminisztrációjának mértéke enyhíthető, amennyiben a hiba csekély súlyú.

A hibajavítást az ICSV tudtával és előzetes írásos hozzájárulásával kell végezni. Amennyiben a hiba javításának megkezdéséig az írásos hozzájárulás nem adható meg, a hibajavítás szóbeli engedély alapján is el lehet kezdeni, de a szóbeli hozzájárulást később (legfeljebb 72 órán belül) írásban is meg kell erősíteni.

A felmerült hibákról és javítási engedélyekről az ICS nyilvántartást vezet, amely tartalmazza legalább a hiba leírását és azonosításának idejét, körülményeit.

Amennyiben a javításhoz külső támogató bevonása is szükséges azt csak olyan külső támogató végezhet, amely/aki érvényes szerződéssel vagy megbízással rendelkezik; adathordozóval is kapcsolatos javítás esetén pedig aláírta a BSZRK által készített titoktartási nyilatkozatot és dokumentált formában megismerte a BSZRK vonatkozó információbiztonsági előírásait.

A javítást végző külső támogatókról nyilvántartást kell vezetni, melynek minimálisan a következőket kell tartalmaznia:

- szervezet megnevezése,

- szerződésszám,
- szerződés időtartama,
- szerződéses kapcsolattartó neve, elérhetősége,
- javítást végzők neve, elérhetősége,
- szerződés tárgya, hatálya (mely rendszerelemre terjed ki).

Külső támogató helyszíni vagy távoli munkavégzése esetén az ICSV feladata kijelölni azt a foglalkoztatott szakembert (javításfelügyelőt), akinek folyamatos felügyeletet kell biztosítania a javítás során és őt előre tájékoztatni a javítás várható jellegzetességeiről, valamint a javítást végző személyekről.

A külső támogatóval kötött szerződésbe kell foglalni, hogy a javításfelügyelő jogosult kérni a helyszíni javítást végző személy személyazonosságának igazolását, illetve, hogy a helyszíni javítást végző személynek kötelessége a felszólításra a szükséges iratokat bemutatni.

A helyszíni javítási tevékenységet az ICSV vagy az általa kijelölt javításfelügyelő előzetes jóváhagyásával szabad elkezdeni.

A javítást a javításfelügyelőnek folyamatosan felügyelni kell, függetlenül attól, hogy azt a helyszínen vagy távolról végzik.

Amennyiben a javításhoz szükséges az EIR vagy a rendszerelemek kiszállítása a BSZRK által kontrollált területről, a kiszállítást előzetesen, írásban engedélyezni szükséges a „3.1.6.15 Be- és kiszállítás" pont szerint. Az engedélyt az ICSV adhatja meg.

Az EIR vagy a rendszerelemek kiszállítása előtt azokról valamennyi adatot és információt - ellenőrzött, sikeres mentést követően - visszaállíthatatlan módon törölni kell.

Az elszállított rendszer, rendszerelem külső javítási helyszínen végzett javítását a javításfelügyelőnek nem szükséges a helyszínen ellenőriznie.

Az elvégzett javítás után az eszköz/rendszerelem és a javítás jellegétől függő funkcionális és biztonsági teszteket kell végezni, melynek eredményét rögzíteni kell a javítási dokumentációban. Sikertelen teszt esetén az eszköz/rendszerelem nem helyezhető újra éles üzembe. Az eseményt jelezni kell az ICSV felé, aki dönt a további intézkedésekről.

A javításokat megfelelően dokumentálni kell, legalább az alábbiakat rögzítve:

- az érintett rendszerelem, eszköz megnevezése és azonosítója,
- az eredeti hiba leírása,
- a javítás során elvégzett tevékenység,
- a javítás engedélyezője,
- a javítás elvégzője,
- a javítás dátuma,
- leállási idő (ha volt ilyen),
- javítást követő tesztelés eredménye,
- javító neve, beosztása és aláírása
- javítást felügyelő neve, beosztása és aláírása
- tesztelő, átvevő neve, beosztása és aláírása

A hibajavítással kapcsolatos szoftverfrissítéseket a BSZRK üzemi rendszerébe, környezetébe telepítés előtt tesztelni kell annak érdekében, hogy a szoftverfrissítésnek a BSZRK feladatellátásának hatékonyságára gyakorolt hatása, valamint a további lehetséges következmények azonosíthatóak legyenek. A szoftverfrissítés üzemi környezetben való alkalmazhatóságáról a tesztelés eredménye alapján kell döntést hozni, a javítást végző szervezet javaslata alapján, az ICSV által.

A biztonsági szoftverfrissítéseket a frissítés kiadását követő egy hónapon belül, a kritikus szoftverfrissítéseket 14 napon belül telepíteni, telepíteni szükséges. A funkcionális javítást, bővítést tartalmazó szoftverfrissítések telepítéséről az ICSV dönt, az adott rendszert, rendszerelemet üzemeltető ICS foglalkoztatottjának javaslata alapján.

A szoftver- és firmware-frissítések rendelkezésre állását a BSZRK automatizált módszerekkel is vizsgálja legalább féléves rendszerességgel.

A javítás tapasztalatai alapján, amennyiben szükséges,

- az alapkonfigurációt vagy az egyedi konfigurációkat, valamint
- a karbantartási eljárásrendet, karbantartási folyamatot, illetve a karbantartási tervet frissíteni szükséges annak érdekében, hogy a hiba a későbbiekben ne forduljon elő. A frissítésre az az adott rendszert, rendszerelemet üzemeltető ICS foglalkoztatottnak kell javaslatot tennie, illetve azt az ICSV és az IBF is kezdeményezheti.

Az azonosított hiba nem megoldható vagy sikertelen javítása esetén a hibában érintett rendszerelem támogatását végző külső szervezet javaslata alapján az adott rendszert, rendszerelemet üzemeltető ICS foglalkoztatott, az ICSV és a BSZRK hiba miatt érintett/akadályozott szakmai területeinek vezetői kidolgozzák a szükséges további lépéseket (amennyiben több módon is lehetséges a helyzetet kezelni, több lehetőséget is kidolgoznak) és javaslatot tesznek a továbblépésre. A lehetséges/szükséges további lépésekről és a javaslatról az ICSV tájékoztatja a FI-t, aki dönt a további lépésekről.

3.2.10.3 Kártékony kódok elleni védelem

A BSZRK-nak meg kell őriznie az informatikai infrastruktúrájának és az EIR-einek, valamint a bennük tárolt adatoknak, információnak a bizalmasságát, sértetlenségét és rendelkezésre állását a kártékony kódok támadásaival és a kéretlen üzenetekkel szemben is.

A BSZRK-nak az informatikai infrastruktúráját és EIR-eit azok belépési és kilépési pontjain védenie kell a kártékony kódok ellen, az alábbiaknak megfelelően:

- Munkaállomások és szerverek esetében központilag felügyelt kártékony kód elleni megoldásokat kell alkalmazni.
- Kártékony kód elleni megoldás nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem üzemeltethető.
- A BSZRK számítógépein úgy kell a kártékony kód elleni védelmi alkalmazást konfigurálni, hogy memóriában rezidensként fusson, valamint hetente egyszer ütemezett, teljes körű ellenőrzést futtasson le.
- A memóriában rezidens modul ellenőrzésének minden írási és olvasási műveletre ki kell terjednie.
- Folyamatok, könyvtárak és állományok kizárása a kártékony kód elleni védekezés alól csak a legkorlátozottabb módon, az adott rendszert, rendszerelemet üzemeltető ICS foglalkoztatott

javaslatára, az ICSV előzetes, írásos jóváhagyását követően, előzetesen tesztelt módon, az informatikai rendszer dokumentációjában rögzített módon történhet. A kizárásról az IBF-et előzetesen írásban, megfelelően tájékoztatni szükséges.

- A külső forrásokból származó fájlok valós idejű ellenőrzését a végpontokon, illetve a hálózati belépési vagy kilépési pontokon el kell végezni minden esetben, amikor a fájlokat letöltik, megnyitják, vagy elindítják.
- Kártékony kód általi fertőzés esetén a védelmi szoftver elsődleges akcióként próbálja meg tisztítani, ha az sikertelen, akkor tegye karanténba a fertőzött állományt.
- Egyéb infokommunikációs eszközök tekintetében a gyártói ajánlások és a lehetőségek figyelembevételével törekedni kell a kártékony kódok elleni védekezésre (például a mobiltelefonok esetében).
- A kártékony kód elleni alkalmazások adatbázisát rendszeresen, a szállító által meghatározott ütemezéssel, vagy automatikusan frissíteni kell, legalább napi gyakorisággal.
- A kártékony kód elleni alkalmazáshoz tartozó szoftverfrissítések kezelése a változáskezelés és konfigurációkezelés hatálya alá esik, ezért ebben az esetben a „3.2.4 Konfigurációkezelés" fejezetben leírtak alkalmazása kötelező.
- A hordozható számítógépek esetében az üzemeltető felhasználónak gondoskodnia kell a kártékony kód elleni alkalmazás adatbázisának automatikus frissítéséről, közvetlenül a hordozható számítógép bekapcsolása után.
- Cserélhető adathordozók használatba vétele előtt automatikus kártékony kód ellenőrzést kell végezni.
- A felhasználókat meg kell ismertetni a kártékony kód felmerülésének esetében követendő előírásokkal.
- A kártékony kód felfedezésekor teendő intézkedéseket és a jelentési rendszert a „3.1.3 Biztonsági események kezelése" fejezet tartalmazza azzal a kiegészítéssel, hogy a kártékony kódirtó rendszert úgy kell konfigurálni, hogy riasztás esetén automatikusan elektronikus levélben értesítse a BSZRK informatikai támogatását végző szervezet képviselőit és az ICSV-t, valamint el nem távolítható fertőzés esetén az IBF-et is.
- A kártékony kód észlelésével és elhárításukkal kapcsolatban tett intézkedéseket dokumentálni kell.
- A téves riasztásokat elemezni szükséges és a tanulságokat megfelelően alkalmazni kell annak érdekében, hogy a téves riasztások száma és hatása csökkenthető legyen.

3.2.10.4 Az EIR monitorozása

A BSZRK informatikai infrastruktúrájának, EIR-einek üzemeltetésébe beleértendő a működés felügyelete, a mentések elvégzése, illetve hiba esetén az eszközök javítását végzők bevonása.

A BSZRK informatikai infrastruktúrájának, EIR-einek felügyelete az informatikai hálózat, szerverek, munkaállomások és hordozható számítógépek, alapszoftverek és alkalmazások, valamint a mobiltelefonok működésének folyamatos figyelemmel kísérését kívánja meg.

A figyelemmel kísérés keretében a BSZRK-nak

- felügyeleti eszközöket kell alkalmaznia a meghatározott alapvető információk gyűjtésére, és a rendszer ad hoc területeire a potenciálisan fontos, speciális típusú tranzakcióknak a nyomon követésére;

- védeni kell a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;
- meg kell tenni minden olyan ésszerű és elvárható intézkedést, amellyel észlelni lehet a kibertámadásokat a meghatározott figyelési céloknak megfelelően;
- fel kell tárni a jogosulatlan lokális, hálózati és távoli kapcsolatokat, azonosítani kell az EIR jogosulatlan használatát;
- erősíteni kell az EIR felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelet észlel;
- módosítani szükséges az EIR felügyeleti tevékenység szintjét, amennyiben változik a szervezeti műveletekkel, az eszközökkel, az egyénekkel, a külső szervezetekkel kapcsolatos kockázati szintje;
- elemezni kell a monitorozás során észlelt eseményeket és rendelleneségeket;
- a monitorozást automatizált eszközökkel és mechanizmusokkal kell támogatni, hogy az eseményekről a lehető leghamarabb értesüljön a BSZRK;
- az automatizált eszközök és mechanizmusok segítségével rendszeresen figyelni kell a bejövő és kimenő kommunikációs forgalmat az olyan mintázatok felismerése érdekében, melyek szokatlan, jogosulatlan tevékenységre utalnak a hálózaton;
- jogi állásfoglalást szükséges kérni az EIR felügyeleti tevékenységeiről;
- meghatározott gyakorisággal biztosítani kell az EIR felügyeleti információkat az ICSV és az IBF, valamint a BSZRK informatikai infrastruktúráját, illetve EIR-eit üzemeltetők felé, továbbá (az ICSV és az IBF bevonásával, közvetítésével) rendszeresen az FI által kijelölt foglalkozatott részére;
- az EIR-nek riasztást kell küldenie az ICSV és az IBF, valamint a BSZRK informatikai infrastruktúráját, illetve EIR-eit üzemeltetők felé, amennyiben az EIR meghatározott indikátorok alapján kompromittálódás jeleit mutatja

3.2.10.5 Biztonsági riasztások és tájékoztatások

A BSZRK-nak

- folyamatosan figyelnie kell a Kormányzati Eseménykezelő Központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;
- folyamatosan figyelemmel kell kísérni a NEIH-től érkező értesítéseket;
- folyamatosan figyelemmel kell kísérni a NKI-től érkező értesítéseket
- szükség esetén belső biztonsági riasztást és figyelmeztetést kell kiadnia;
- a belső biztonsági riasztást és figyelmeztetést el kell juttatnia az illetékes személyekhez;
- ki kell alakítania és működtetnie a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, és kapcsolatot kell tartani az érintett, külön jogszabályban meghatározott szervekkel;
- megfelelő ellenintézkedéseket és válaszlépéseket kell tennie.

3.2.10.6 Szoftver- és információsértetlenség

A BSZRK informatikai infrastruktúrájának, EIR-einek felügyelete során sértetlenségellenőrző eszközöket kell alkalmazni, hogy kimutathatóak legyenek a szoftver, firmware és információkban bekövetkezett jogosulatlan változtatások. A jogosulatlan változtatások biztonsági eseménynek

minősülnek és annak megfelelően kell eljárni velük kapcsolatban, valamint a sértetlenségellenőrzést az általános szervezeti monitorozó rendszerbe kell integrálni.

A BSZRK EIR-ei esetében a sértetlenségellenőrzést kell végezni a következő esetekben:

- az EIR(elem) indítása, újraindítása vagy leállítása,
- új hardver, szoftver vagy firmware telepítése,
- a már telepített új hardver, szoftver vagy firmware kapcsán a BSZRK tudtára jutott új fenyegetés esetén.

3.2.10.7 Kéretlen üzenetek elleni védelem

A BSZRK a levelező rendszerének részeként levélszemét és káros kód ellenni védelmi rendszert üzemeltet. Ennek a rendszernek a frissítése a „3.2.4 Konfigurációkezelés" pont hatálya alá esik, viszont adatbázisait automatikus frissítésekkel folyamatosan naprakészen kell tartani.

3.2.10.8 Bemeneti információ ellenőrzés

A BSZRK EIR-eitnek bemeneti információs mezőit úgy kell beállítani/kialakítani, hogy azok ellenőrizzék a bevitt információk meghatározott kritériumoknak való megfelelését.

3.2.10.9 Hibakezelés

A BSZRK EIR-eit úgy kell beállítani, hogy azok hibaüzenetei ne tartalmazzanak kihasználható információkat és a hibaüzenetek csak a meghatározott szerepkörök tagjai számára jelenjenek meg.

3.2.10.10 Információ kezelése és megőrzése

A kimeneti információk (pl.: nyomtatás, rendszerekből kinyerhető riportok, adatexportok) kezelésével és szétosztásával kapcsolatban a következők az előírások:

- gondoskodni kell a kimeneti információ tartalmi ellenőrzéséről,
- gondoskodni kell róla, hogy a kimeneti információhoz történő fizikai és logikai hozzáférés csak az arra feljogosított személyekre korlátozódjon,
- gondoskodni kell róla, hogy a jogosult személyek időben megkapják az elkészült kimeneti információkat,
- biztosítani kell, hogy a megsemmisítési eljárások során a kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.

A kimeneti információ fenti követelményeinek kialakítására javaslattétel az adott kimeneti információt előállító szervezeti egység vezetőjének feladata. A javaslatot tevő, az ICSV-vel és az IBF-fel közösen javaslatot tesz az FI-nek, aki dönt a bevezetendő, alkalmazandó folyamatról és kontroll intézkedésekről.

A folyamat véglegesítése, szabályozása és a kontroll intézkedések kidolgozása, bevezetése a javaslatot tevő, valamint az ICSV és az IBF feladata, akik saját hatáskörben kötelesek intézkedni az általuk elvégezni jogosult feladatokról és a további feladatok végrehajtását pedig kötelesek megfelelően koordinálni.

3.2.10.11 Memóriavédelem

A BSZRK EIR-eit és rendszerelemeit úgy kell beállítani, hogy lehetőség szerint hardver szintű Adatvégrehajtás-megelőzés (Data Execution Prevention (DEP)) használjanak a memóriájukban futó programok védelmére. Amennyibe erre nincs lehetőség a védelem szoftveres DEP és Véletlenszerű címtár elhelyezés (Address Space Layout Randomization (ASLR)) technológiákkal is megoldható.

4. FÜGGELÉKEK

4.1 IGÉNYBE VETT SZOLGÁLTATÁSOK, MEGVÁSÁROLT, VALAMINT KIFEJLESZTETT RENDSZEREK KAPCSÁN ELVÁRT ELEKTRONIKUS INFORMÁCIÓ-BIZTONSÁGI KÖVETELMÉNYEK BETARTÁSÁNAK VÁLLALÁSA

Alulírott, mint a .... [Szállító] törvényes képviseletére jogosult személy tudomásul veszem, hogy az ebben a dokumentumban felsorolt követelményeket az általam képviselt szervezetnek a Rendszer fejlesztése/bevezetése/alkalmazása/használatba vétele kapcsán ÉÉÉÉ.HH.NN-n keltezett, az BSZRK és a .... [Szállító] között aláírt, ... számú szerződés kapcsán leszállítani vállalt Rendszernek teljesítenie kell:

a) Az igénybe venni szándékozott szolgáltatásnak, beszerzendő vagy kifejlesztendő infrastrukturális elemnek, rendszerelemnek, alkalmazásnak, szoftvernek, szoftverkomponensnek, szolgáltatásnak, a közöttük lévő és külső rendszerkapcsolatoknak (továbbiakban együtt: Rendszer) együttesen alkalmasnak kell lenniük a BSZRK által elvárt biztonsági osztályhoz tartozó, a 2024. évi LXIX. törvényben meghatározott funkcionális és biztonsági követelmények teljesítésére.
b) A nem a BSZRK számára egyedileg fejlesztett Rendszer esetében a fejlesztési dokumentációval kapcsolatos elvárások teljesítése alól egyedileg felmentés adható, amelyet az ICSV és az IBF együttesen, a beszerzési eljárás kezdete előtt, írásban, dokumentált formában tud megtenni.
c) A Rendszer beszerzése vagy fejlesztés akkor kezdhető el, ha a BSZRK-nak a Rendszert a későbbiekben használó szervezeti egységei (továbbiakban: Szakmai Terület) írásban, részletesen meghatározták a számukra szükséges funkcionális és további követelményeket (továbbiakban: Szakmai Követelmények).
d) A Rendszer beszerzése, fejlesztése során a Szakmai Követelményektől eltérni kizárólag akkor lehetséges, ha az azt meghatározó szervezeti egység(ek) írásban, dokumentáltan kijelentik, hogy az adott követelmény a továbbiakban nem, vagy más módon elvárt részükről, és egyben átadják a módosított, teljes, részletes Szakmai Követelményeket.
e) A Rendszernek a Szakmai Követelményekben meghatározottak mellett teljesítenie kell a biztonsági elvásárokat (továbbiakban: Biztonsági Követelmények) is, beleértve az a) pontban említett jogszabályi, és a BSZRK (ICSV, IBF, DPO stb.) által támasztott kiegészítő biztonsági és adatvédelmi követelményeket (továbbiakban: Adatvédelmi Követelmények) is.
f) A Rendszerrel kapcsolatos elvárások teljesülésének igazolására meg kell követelni a Rendszer szállítójának, értékesítőjének, fejlesztőjének (továbbiakban: Szállító) írásos, dokumentált, hiteles nyilatkozatát, amelynek valamennyi elvárt követelményre és azok teljesülésére kiterjedőnek kell lennie. Az esetlegesen nem teljesített követelményeket a Szállítónak tételesen fel kell sorolnia; a részteljesüléseket a Szállítónak tételesen fel kell sorolnia, a teljesült és nem teljesült elvárásrészletekkel egyetemben. A Szállító nyilatkozatát a Szakmai Követelmények kapcsán a Szakmai Területnek, a Biztonsági Követelmények kapcsán az ICSV-nek és az IBF-nek, az Adatvédelmi Követelmények esetében a DPO-nak meg kell vizsgálnia (tesztelnie kell) és a nyilatkozatot írásban, dokumentáltan jóvá kell hagynia.

g) A Rendszer fejlesztői dokumentációjának áttekinthető formában kell készülnie és meg kell felelnie a 2024. évi LXIX. törvény elvárásainak, különös tekintettel a Rendszer felépítésének, működtetésének az ellenőrzéséhez szükséges rendszerleírások, modellek, az adatok szintaktikai szabályainak, és az adatok tárolási szerkezetének rendelkezésre állásának tekintetében (például funkcionális specifikáció, use-case-ek, rendszerterv, adatmodell, objektum-modell, adatbázis specifikáció). A működtetés ellenőrzéséhez szükséges rendszerleírás vagy modell gyanánt nem fogadható el szoftverrel generált olyan dokumentáció, amelyben nem szerepel érdemi és releváns információ a dokumentált adatszerkezet, objektum, funkció, modul, program, egyéb rendszerkomponens szerepéről és működéséről. A Rendszer, és annak elemeinek dokumentáltsága olyan legyen, hogy a BSZRK azt a Szállító nélkül is képes legyen szakszerűen felhasználni, biztonságosan üzemeltetni, tárgyi eszköz szállítása esetén pedig pótolni.

h) A Szállító a szoftver átadásával egyidejűleg köteles átadni az adatok szintaktikai szabályait és az adatok tárolási szerkezetét is tartalmazó részletes adatbázis specifikációt. A Szállító a fejlesztést a Biztonsági Követelmények implementálását elősegítő módon, BSZRK projektkeretek között, megfelelő szerepkörök, felhatalmazások kialakításával, a felelősségek elkülönítésével és alkalmas személyek kijelölésével, ellenőrzötten és dokumentáltan végzi.

i) A Szállító gondoskodik róla, hogy a BSZRK ICSV-je és IBF-e már a fejlesztés tervezésétől kezdődően, annak teljes életciklusába folyamatosan bevonásra kerüljön. A legfontosabb fejlesztési szakaszok lezárása a Szakmai Terület képviselőjének, valamint az ICSV és az IBF személyes jelenlétében történhet, miután ők dokumentált módon meggyőződhettek az adott fejlesztési fázis követelményeinek teljesítéséről, és számukra megnyugtató, dokumentált, írásos választ kaptak a korábban és ott elhangzott észrevételeikre.

j) A tervezési szakaszban a Szállítónak dokumentáltan azonosítania kell a fejlesztési folyamatból és a fejlesztendő/bevezetendő Rendszer funkcionális működéséből és architektúrájából, külső és belső rendszerkapcsolataiból származó kockázatokat (például threat modelling, vagy más, azzal egyenértékű módszertan segítségével), intézkedéseket kell tennie azok elfogadható értékűre történő csökkentésére. A folyamat során Szállító kiemelten köteles azonosítani a szoftver biztonságát érintő use case-eket, támadási vektorokat, támadási mintákat és a kivédésükhöz szükséges kompenzációs kontrollokat.

k) A j) pontban foglalt fenyegetettségi vizsgálatot a Szállító köteles minden további lényeges mérföldkő elérésekor vagy jelentősebb rendszerváltozások esetén elvégezni és dokumentálni. Jelentősebb változásnak értékelendő (továbbiak mellett kiemelten) az új interfész implementálása, futtatókörnyezetben bekövetkező változások, szoftver funkcióinak bővülés, biztonsági funkciók működésének módosulása (kiemelten a felhasználó azonosítás, jogosultságadás és naplózás területen végzett módosítás).

l) A Szállító (szükség szerint a BSZRK képviselőjének bevonásával) köteles a fejlesztés megkezdése, hardver összeállítása, szolgáltatás megkezdése előtt azonosítani a BSZRK tevékenységéből, valamint a leszállítandó Rendszer funkciójából, rendszerkapcsolataiból és működési körülményeiből származó, a Rendszer funkcióira, képességeire ható összes vonatkozó jogszabályi rendelkezést, és köteles intézkedéseket tenni a jogszabályi megfelelőség biztosítására.

m) A Szállító a Rendszer fejlesztéséhez köteles zárt, ellenőrzött informatikai környezetet létrehozni. A környezetben csak nyilvántartott, engedélyezett, (kihasználható) ismert

sérülékenységet nem tartalmazó rendszerelemek használhatók (operációs rendszer, futtatókörnyezet, Integrált fejlesztői környezet (IDE), IDE plugin stb.).

n) A fejlesztés során a fejlesztőeszközöknek, fordítóprogramoknak, futtató környezetnek, és egyéb használt szoftverkomponenseknek az elérhető legfrissebb verzióit kell használni. A használt szoftverek verziója a fejlesztési életciklus során folyamatosan naprakészen kell tartani.

o) A Szállító köteles elkülöníteni saját informatikai környezetét, valamint a BSZRK üzemi tevékenységre szolgáló informatikai környezetét a fejlesztésre és tesztelésre használt környezetekről.

p) A Szállító köteles megfelelő változáskövetési és változáskezelési eljárásokat, módszereket használni annak érdekében, hogy a Rendszer egyes verziói és azok funkcionális, biztonsági tartalma, a fejlesztés, tesztelés és az átadás fázisa egyértelműen azonosítható legyen.

q) A Szállító köteles a forráskódot és a hozzá tartozó fejlesztői dokumentációt olyan verziókövető- rendszerben tárolni, amely biztosítja, hogy nyomon követhető legyen, ki és mikor módosította a forráskódot vagy a konfigurációs fájlokat, valamint biztosítja a dokumentáció központi, ellenőrzött tárolását. Minden szöveges formátumú és Szállító által létrehozott (nem generált) fájlban a verziókövető rendszerrel megegyezően tárolni kell, meg kell jeleníteni a fájl pontos azonosítására szolgáló verziószámot. A verziókövető-rendszer valamennyi humán és technikai felhasználójának egyedi, saját használatú, más által nem igénybe vehető felhasználói azonosítójának kell lennie, és a Szállítónak biztosítania kell, hogy a verziókövető rendszer csak ennek a segítségével legyen használható.

r) Szállító köteles olyan technológiát és programozási nyelvet használni, amely elterjedt és támogatott, valamint amelyeket a munkavállalói és alvállalkozói megfelelően ismernek és kellő tapasztalatot szereztek a használatukban. A Szállítónak igazoltan biztosítania kell, hogy fejlesztői környezetében minden fejlesztő azonosítsa, elsajátítsa és alkalmazza az adott környezetre jellemző, biztonságos kódolási szabályokat, iparági ajánlásokat. A BSZRK jogosult a szükséges ismeret és tapasztalat meglétére vonatkozó nevesített, ellenőrizhető (kapcsolattartási információkat tartalmazó) referenciákat kérni a Szállítótól - amennyiben ezek megosztását a Szállító megtagadja, vagy nem megfelelő, esetlegesen téves, hibás referenciát, adatokat ad meg, vele az együttműködés nem folytatható, a szakmai és üzleti kapcsolatot meg kell szakítani.

s) Törekedni kell rá, hogy a fejlesztés során alkalmazott fejlesztési technológia, programozási nyelv, eljárások, algoritmusok stb. megfeleljenek a vonatkozó iparági ajánlásoknak (FIPS, NIST), beleértve a megfelelő, elfogadott és validált titkosítási eljárások alkalmazását, amelyek kiválasztásánál a fejlesztés indulásakor érvényes Biztonsági Követelmények mellett figyelembe kell venni a Rendszer tervezett élettartamát annak érdekében, hogy az elvárható titkosítási védelem a Rendszer teljes élettartama alatt biztosított legyen.

t) A fejlesztéshez nem választható szűk körben használt, speciális nyelv, vizsgálni és kerülni kell a potenciálisan veszélyes függvények használatát.

u) A Szállító köteles átlátható, tagolt, egységes kódolási konvenciókat alkalmazó, jól olvasható, könnyen értelmezhető, magyarázatokkal megfelelő részletességgel ellátott forráskódot készíteni.

v) A Szállító köteles figyelembe venni és alkalmazni a biztonságos kódolással kapcsolatos érvényes ajánlásokat és módszereket (OWASP, SANS, SAFECode).

w) A Szállító köteles a Rendszer fejlesztése, előállítása, összeállítása, beállítása során kiemelten gondoskodni az alábbi elvárások teljesüléséről:
   a. a Rendszer valamennyi felhasználójának egyedileg azonosíthatónak kell lennie,
   b. a Rendszer lényegi funkciói csak azonosított felhasználó számára legyenek elérhetőek (azaz általános leírás, közérdekű tartalom azonosítatlan felhasználó számára is közzétehető),
   c. a Rendszer egyes funkcióit, a benne tárolt, vagy általa kezelt adatokat a szükséges minimális („need to know") adathozzáférés és a feladat ellátásához szükséges minimális („need to do") műveletvégzési lehetőség elv alapján szabad a felhasználóknak elérniük, kezelniük,
   d. a Rendszer egyes funkcióihoz, adatokhoz a felhasználók jogosultságát csak egyedi engedélyezést és beállítást követően szabad hozzárendelni - a Rendszernek alkalmasnak kell lennie ennek megvalósítására,
   e. kerülni kell a Rendszer egyes funkcióihoz, adataihoz való egyedi hozzáférések adását: a Rendszer funkcióit szerepkörökbe kell tudni rendezni, a felhasználók jogosultságait pedig az általuk használható szerepkörökhöz rendeléssel kell megvalósítani,
   f. a felhasználók létrehozásának és karbantartásának, valamint a jogosultságaik karbantartásának (beleértve a funkciók szerepkörhöz, valamint a szerepkörök felhasználókhoz rendelését) felhasználói felületről, fejlesztői vagy informatikai üzemeltetői segítség nélkül megvalósíthatónak kell lennie,
   g. a Rendszerben végzett valamennyi felhasználói és rendszerműveletet, eseményt és ezek kísérletét, hibát, hibaüzenetet megfelelően naplózni szükséges; a naplóbejegyzésekben tárolva minimálisan:
      i. az érintett rendszerelem azonosítóját,
      ii. az adatazonosítót (pl. fájl/rekord/mező/rendszerelem név),
      iii. az esemény ismertetését/a funkcióazonosítót,
      iv. a felhasználó azonosítóját,
      v. az esemény időpontját (századmásodperc pontossággal),
      vi. az eseményt kezdeményező felhasználó által használt számítógép azonosítóját és IP címét,
      vii. az esemény elemzéséhez szükséges adattartalmakat vagy az arra vonatkozó hivatkozásokat, illetve annak végrehajtási státuszát,
   h. a Rendszernek megfelelően védenie kell a naplóállományokat a nemkívánatos hozzáféréstől, módosítástól, törléstől, kiegészítéstől,
   i. a jelszavakat nem szabad tárolni (naplóállományban sem), ellenben kizárólag biztonságos jelszókódolási eljárásokat szabad használni és csak az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hasító értéket szabad tárolni, valamint „sózni" kell a jelszavakat,
   j. a jelszóházirendnek felhasználói felületről (fejlesztői vagy informatikai üzemeltetői támogatás nélkül) módosíthatónak kell lennie,
   k. a Rendszerben alkalmazott házirendnek alkalmasnak kell lennie legalább az alábbi paraméterek beállítására:
      i. különböző típusú felhasználókhoz különböző jelszóházirendek használatára és ezen belül a felhasználótípusok meghatározására, valamint az egyes felhasználóknak a megfelelő típusokba sorolására,

ii. kisbetűk, nagybetűk, számok és speciális karakterek megkülönböztetése és elvárása, és
iii. a minimális és maximális karakterek számának meghatározása 0-255 karakter tartományban,
iv. kezdeti jelszó kötelező megváltoztatásának előírási lehetőségére vagy annak mellőzésére,
v. új jelszó megadásakor az előzőhöz képest adott számú karakter módosításának elvárására (a jelszó hosszához viszonyítva),
vi. az ismételt jelszófelhasználás lehetőségének megadására (a teljes tiltástól az ismételt felhasználás engedélyezéséig terjedő tartományban, a két azonos jelszó használata között szükséges más jelszavak száma szerint (nullától a végtelenig terjedő tartományban), illetve a két azonos jelszó használata között minimálisan eltelni szükséges idő megadhatóságával),
vii. a minimális és maximális jelszóélettartam megadására (0 perctől a korlátlan élettartamig terjedő tartományban),
viii. nem alkalmazható jelszavak (tiltott szavak) szótáralapú listájának importálására,
ix. a felhasználónév jelszóban használhatóságának beállítására (a felhasználónévben előforduló egymást követő karakterek számának jelszóban előfordulási számának meghatározásával, a kettőtől a végtelenig terjedő tartományban),

l. a Rendszernek nem szabad megjelenítenie a jelszót, a jelszó helyett helykitöltő „status bar" - t kell jeleznie annak érdekében, hogy az alkalmazott jelszó karaktereinek száma se legyen kiolvasható,
m. a jelszó mezőből annak tartalma nem szabad, hogy kimásolható legyen, és oda nem szabad engedni a beillesztést,
n. a Rendszernek illeszkednie kell a BSZRK-nál üzemelő és bevezetni tervezett további biztonsági és jogosultságkezelési architektúrába, különös tekintettel az alkalmazott authentikációs eljárásra, az AD alkalmazására (a BSZRK foglalkoztatottjai esetében), a jelszómenedzsment rendszerrel való együttműködésre, a logmenedzsment és incidenskezelési követelményekre - ennek keretében a Biztonsági Követelményekben meg kell határozni, hogy a single sign-on (egyszeri azonosítás) alkalmazható-e az adott Rendszer esetében,
o. az alkalmazott interfészeknek biztonságosnak kell lenniük, a továbbított és fogadott adatok ellenőrzését központilag kell végezni, az esetleges adattovábbítási hibákat a Rendszernek jeleznie kell, és megfelelő eljárásokat bevezetve gátolni kell az adatok ismételt feldolgozását,
p. meg kell akadályoznia a többszörözött adatfogadást az interfészek használatakor, valamint adattovábbítás során (más rendszerekkel való funkcionális kapcsolatok, továbbá felhasználói interfészek esetén egyaránt),
q. valamennyi adat input lehetősége esetében meg kell határozni, milyen típusú adat fogadható el, és a más típusú adat érvényesítését meg kell akadályozni, amelynek során az adat vizsgálatát a Rendszer központi komponensében (szerveroldalon) kell elvégezni; kliensoldali input validáció alkalmazása tilos,

r. meg kell akadályozni a nem adat típusú inputok alkalmazását (pl. az sql injection jellegű támadásakat),
s. a Rendszer, mind backup, mind nagy rendelkezésre állást biztosító funkcióiban támogassa a BSZRK érintett Rendszere kapcsán elvárt RTO/RPO követelmények kielégítését,
t. a Rendszer megfelelően biztosítsa az informatikai biztonsággal kapcsolatos technológiai továbblépés lehetőségeit, ideértve a szolgáltatásfolytonosság követelményeit is,
u. az azonosított fenyegetettség elleni védelmet be kell építeni a Rendszerbe, a fejlesztés minél korábbi fázisában,
v. a Szállítónak el kell készíteni és a BSZRK-nak át kell adnia a Rendszerre vonatkozó adminisztrátori dokumentációt, amelynek tartalmaznia kell
    i. a Rendszer, rendszerelem vagy szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését kiemelten beleértve a Rendszer
        1. felhasználói adminisztrációjának és
        2. jogosultsági rendszerének leírását és használatának bemutatását,
        3. mentését és a mentésekből visszaállítást, valamint
        4. a naplózás és a naplózott információ értelmezésének leírását, továbbá
        5. az adatkapcsolatoknak és az adatkapcsolatok megfelelő működése érdekében szükséges beállításoknak a leírását,
    ii. a biztonsági funkciók hatékony alkalmazásához és fenntartásához szükséges információt,
    iii. a Rendszer funkcionális tesztelési leírását,
    iv. a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket, valamint azok javításáról szóló intézkedési tervet leíró dokumentumokat,
w. a Szállítónak el kell készíteni és a BSZRK-nak át kell adnia a Rendszerre vonatkozó felhasználói dokumentációt, amely tartalmazza
    i. a felhasználó által elérhető funkciók részletes használati leírását olyan módon, hogy annak alapján a funkció segítség nélkül, hibamentesen végrehajtható legyen,
    ii. a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját,
    iii. a Rendszer biztonságos használatának módszereit,
    iv. a felhasználó kötelezettségeit a Rendszer biztonságának a fenntartásához.

x) A Rendszer alapbeállításait úgy kell megválasztani, hogy már közvetlenül a Rendszer telepítése, használatba vétele után is biztosítsák a biztonságos, elvárt működést.
y) A Rendszer és paraméterei éles üzembe állítását megelőző, tervezett, dokumentált, elvárható gondosságú teszteléséről a Szállítónak kell gondoskodnia, beleértve a funkcionális és a nem funkcionális tesztek elvégzéséről, közöttük az informatikai biztonsági teszteket is.
z) A tesztelés vagy fejlesztés során a Szállító feladata arról gondoskodni, hogy csak olyan adat legyen felhasználva, amely megfosztásra került azoktól a jellemzőktől, amelyek miatt az adat bizalmasnak minősül. Így különösen elvárás az ügyféladat, a pénzügyi és az egészségügyi adat felismerhetetlenné tétele minden olyan környezetben, amely az éles környezettől elkülönített (így tesztelési vagy fejlesztési) céllal működik.

aa) Tesztelési, illetve hibakeresési eljárás során éles adat csak akkor kezelhető a Rendszer tesztkörnyezetében, ha a tesztkörnyezetre vonatkozó kontrollok megegyeznek vagy szigorúbbak az éles rendszerekre vonatkozó kontrolloknál és az élesítési vagy hibakeresési teszt környezet egyedileg, teljes körűen dokumentált eljárásban, a BSZRK által jóváhagyott módon, meghatározott időintervallumra és felhasználói körre kerül kialakításra, a tesztkörnyezethez kizárólag az éles üzemi környezet felhasználói férnek hozzá az éles üzemi környezetben beállított jogosultságaikkal megegyezően, valamint a tesztelési eljárást követően a teszt környezetből az éles adatok azonnal törlésre kerülnek.

bb) A BSZRK megbízásából elvégzett informatikai biztonsági teszteknek ki kell terjednie legalább a forráskód készítőtől független, automatikus eszközökkel végzett (manuálisan validált), vagy manuális kódfelülvizsgálatára. A tesztek során meg kell erősíteni továbbá a funkcionális specifikációban rögzített biztonsági követelmények teljesítését, megvalósításának módját.

cc) A publikusan elérhető, illetve használható Rendszer esetében szakértő személy vagy BSZRK bevonásával el kell végezni a Rendszer sérülékenységvizsgálatát és a feltárt sérülékenységeket megfelelően dokumentálni és kezelni szükséges; majd a sérülékenység vizsgálatot ismételten el kell végezni annak érdekében, hogy a BSZRK bizonyosságot szerezzen

i. a feltárt sérülékenységek megfelelő módon és határidőre végzett kezeléséről,
ii. arról, hogy a korábban azonosított sérülékenységek kezelése nem generált újabb sérülékenységet.

dd) A Szállító a fejlesztési folyamat végén köteles átadni a BSZRK részére az ebben a dokumentumban meghatározott dokumentációkat, továbbá a Rendszer (dokumentált, teljeskörűen fordítható vagy fordítás nélkül futtatható állapotú, egyértelműen azonosított és aktuális) forráskód állományát és hozzájárulását kell adnia, hogy azok felett a BSZRK a továbbiakban jogszerűen és teljeskörűen rendelkezhessen - ezek hiányában a teljesítési igazolás nem adható ki és a kapcsolódó számlát a BSZRK nem fogadhatja be, nem egyenlítheti ki.

ee) A Szerződés bármilyen okból történő megszűnése esetén a Szállító a tőle független technológia segítségével is feldolgozható formátumban átadja az általa közvetlenül vagy közvetve kezelt, feldolgozott vagy keletkeztetett, jogilag a BSZRK-hoz tartozó (pl. általa birtokolt, felelősen kezelni átvett, előállított stb. adatokat), és egyben visszaállíthatatlanul törli a saját (Szállító által kontrollált) infrastruktúrában tárolt hasonló adatokat; valamint ezekről nyilatkozik a BSZRK számára, egyben nyilatkozva arról is, hogy valamennyi általa átvett, illetve szerződésteljesítés során megismert adatot visszaállíthatatlan módon törölt, illetve ha ez nem így van, arról is nyilatkoznia kell, mely adatoknál és milyen okból nem teljesült ez az elvárás. A megmaradó adatállományok tekintetében a Szállító vállalja, hogy a BSZRK utasításai szerint jár el.

ff) A BSZRK a szerződés teljes időtartama alatt annak tárgyában tájékoztatást kérhet, továbbá a fejlesztési folyamatot helyszíni ellenőrzés keretében jogosult vizsgálni. A BSZRK joga, hogy az ellenőrzések eredményének függvényében olyan korrektív intézkedéseket kezdeményezzen, amellyel a jelen szerződésben megfogalmazott védelmi feladatok teljesíthetők. A szükséges intézkedések végrehajtása a Szállító számára kötelező.

gg) A Szállító a szerződéssel érintett tevékenységben résztvevő foglalkoztatottjait rendszeresen tájékoztatja a szerződésben foglalt, végrehajtandó kötelezettségeikről, feladataikról. A tájékoztatás megtörténtét a BSZRK kezdeményezésére köteles igazolni.

hh) A Szállító részéről alvállalkozó igénybevétele a szerződés teljesítése során nem tiltott, azonban ennek tényéről és a bevonni kívánt alvállalkozókról a BSZRK-t előzetesen írásban értesíteni kell szerződéskötés előtt, hozzájárulását kérve. Amely alvállalkozó alkalmazásához a BSZRK nem járul hozzá, azt a Szállító nem alkalmazhatja. A Szállító valamennyi alvállalkozója és erőforrást nyújtó szervezete teljesítéséért úgy felel, mintha maga teljesített volna. Alvállalkozó tekintetében jelen dokumentum előírásaink betartása minden esetben kötelező.

ii) Amennyiben a Szállító a tevékenysége során a BSZRK-on kívül más szervezet számára is nyújt szolgáltatást, úgy köteles megfelelő műszaki és személyi feltételek mellett biztosítani a különböző megbízói Rendszereinek és adatállományainak elkülönítését az adatok illetéktelenek általi hozzáférésének, megismerésének megakadályozása, az adatkezelés biztonsági szempontú ellenőrzése céljából, továbbá azt, hogy a különböző szervezetek által kezelt adatok jogosulatlan összekapcsolására ne kerüljön sor.

jj) A Szállító fenntartja a jogot az elkészült Rendszer saját hatáskörben végzett biztonsági vizsgálatára. Amennyiben a BSZRK által elvégzett biztonsági vizsgálat a Rendszer biztonságát súlyosan és közvetlenül sértő kockázatot tár fel, a Rendszer átvételét megtagadhatja mindaddig, amíg a Szállító a feltárt kockázat(ok) igazolt javításáról nem gondoskodott.

A dokumentumban említett BSZRK-specifikus követelmények jelentése:

- ICSV: Informatikai osztályvezető
- DPO: Adatvédelmi tisztviselő
- IBF: elektronikus információbiztonsági felelős

A leírtakat tudomásul vettem, betartásukért az általam képviselt szervezet nevében felelősséget vállalok, egyben kijelentem, hogy ezen nyilatkozat tételére és a nevem alá írt szervezet (amelyre ebben a dokumentumban Szállítóként hivatkoztunk) képviseletére jogosult vagyok

A nyilatkozatot a Rendszer fejlesztése/bevezetése/alkalmazása/használatba vétele kapcsán ÉÉÉÉ.HH.NN-n keltezett, az BSZRK és a ..... [Szállító] között aláírt, ... számú szerződés kapcsán tettem, egyben tudomásul vettem, hogy hivatkozott szerződés ezen nyilatkozat aláírása nélkül vagy a nyilatkozatban foglaltak be nem tartása (illetve be nem tartás esetén a vállalt kötelezettségek az BSZRK-val megegyezett módon és határidőre történő helyreállításának hiányában) az BSZRK kérheti a hivatkozott szerződés érvénytelenítését vagy megsemmisítését - ebben az esetben a ..... [Szállító] kártérítésre, kárenyhítésre, költségtérítésre nem tarthat igényt.

....., ÉÉÉÉ.HH.NN.

.....

X Y [név és beosztás], a

.... [Szállító] képviseletében teljes joggal eljárva

Tanúsítom, hogy X Y fenti nyilatkozatot tiszta tudattal, döntéshozatalra képes állapotban, minden kényszer nélkül, saját kezűleg, jelenlétemben írta alá.

....

XY [név], XY [név],

Név: ..... Név:.....

Lakcím: ..... Lakcím:.....

4.2 INFORMÁCIÓSBIZTONSÁGI HÁZIREND ÉS NYILATKOZAT (FOGLALKOZTATOTTAK ÉS PARTNEREK SZÁMÁRA)

A BSZRK elkötelezett a foglalkoztatottjai fejlődése, a munka és magánélet közötti megfelelő egyensúly biztosítása, a jogszerű és tisztességes foglalkoztatás, a munkajogi alapelvek tiszteletben tartása mellett, és ugyanezt várjuk el szakmai partnereinktől és a külső érintettektől is.

A BSZRK elkötelezett a kölcsönös bizalmon alapuló munkakörnyezet megteremtésében, ahol mindenkit, aki a BSZRK-nak dolgozik, megbecsülnek és mindenki emberi méltóságát tiszteletben tartják.

A BSZRK és a vele kapcsolatba kerülő belső és külső érintettek között bizalmi kapcsolat van, ennek megfelelően elvárt, hogy valamennyi foglalkoztatott és szerződött partner adja meg a megfelelő tiszteletet egymásnak.

A BSZRK felelős a vagyonát képező tárgyi eszközök, egészségügyi adatok, üzleti titkok, szellemi tulajdon megfelelő kezeléséért, védelméért és biztosítja a megfelelő adatbiztonságot a papíralapon és elektronikusan tárolt információ vonatkozásában egyaránt.

A BSZRK jelentős értéket képviselő tárgyi és immateriális vagyonnal, pénzügyi és nem pénzügyi forrásokkal és eszközökkel rendelkezik, amelynek a szakmai/gazdasági célok elérése érdekében történő jogszerű, megfelelő és ésszerű, engedélyezett módú és mértékű használata, kezelése, védelme valamennyi foglalkoztatott és partner kötelessége és felelőssége.

A BSZRK vagyonának és erőforrásainak helytelen, vagy gondatlan kezelése sérti az állampolgárok érdekét és rontja az ügyfelek számára nyújtott szolgáltatás színvonalát, ezért kerülendő. A foglalkoztatottak és a partnerek munkaerejének, a szervezeti és köztulajdonban álló eszközöknek, berendezéseknek és egyéb javaknak, közpénzből megrendelt szolgáltatásoknak, továbbá a szervezeti, költségvetési, valamint egyéb közösségi célú pénzügyi forrásoknak hasznos, hatékony és gazdaságos kezelésére és felhasználásra különös gondot szükséges fordítani, különösen, ha azok felhasználásában jelentős döntési szabadsággal rendelkezik a foglalkoztatott és a partner.

Különös gondot szükséges fordítani arra is, hogy az irodai eszközöket, berendezéseket (írószer, papír, fénymásoló, nyomtató, számítógép, telefon stb.) magáncélra ne használják a foglalkoztatottak és a partnerek. Az otthoni munkavégzést is szolgáló, magánhasználatot is lehetővé tevő eszközök (mobiltelefon, laptop, táblagép stb.) használatában is gondosan és takarékosan kell eljárni.

Az információk, adatok és tudás kritikus fontosságú vagyonelemek a BSZRK és partnerei számára.

A BSZRK kizárólag jogszerű módon gyűjt adatokat, valamint nyilvánosan hozzáférhető információforrásokat használ a szakmai/gazdasági, felhasználói, beszállítói és technológiai tendenciák

és magatartásminták, illetve többek között jogszabálytervezetek, egyéb szabályozói intézkedések és kommunikációs kampányok értékelése során.

A BSZRK elkötelezett foglalkoztatottjai és partnerei, illetve valamennyi ember magánélethez való jogának tiszteletben tartása és személyes adataik bizalmas kezelése mellett.

A BSZRK megelőző biztonsági intézkedéseket tesz az adatbázisokban tárolt személyes adatok védelmére, hogy elkerülje a megsemmisülés, adatvesztés és a jogosulatlan hozzáférés kockázatát.

A BSZRK kizárólag a hatékony működéséhez szükséges személyes adatokat gyűjt, tárol és kezel a jogszabályoknak megfelelően.

A BSZRK elvárja, hogy foglalkoztatottjai és partnerei

- ismerjék meg a személyes adatok védelmére vonatkozó törvényi és jogszabályi előírásokat;
- ismerjék meg és alkalmazzák a BSZRK megoldásait az üzleti és egészségügyi titok és információk védelme érdekében;
- megfelelő körültekintéssel járjanak el mind a külső, mind a belső kommunikáció tekintetében;
- tartsák be a titoktartási és az egyéb vonatkozó szabályzatokat;
- korlátozzák a védett információkhoz való hozzáférést a szükséges minimumra (a „szükséges és elégséges" elvnek megfelelően);
- kizárólag olyan személyes adatokat gyűjtsenek és kezeljenek, melyek munkájuk elvégzéséhez, feladatuk ellátásához szükségesek és megfelelőek; és ezeket az adatokat kizárólag a meghatározott eljárások alkalmazásával gyűjtsék és kezeljék, a jogosulatlan hozzáférés elleni védelmet biztosító módon tárolják;
- korlátozzák a személyes adatokhoz történő hozzáférést az erre jogosult személyek körére;
- a személyes adatokat bizalmas információként kezeljék;
- használjanak figyelmeztető jelzést a bizalmas információ jelölése és védelme érdekében;
- kizárólag tisztességes és törvényes célra használják a megfelelő jogosultság birtokában hozzáférhető személyes adatokat;
- gondoskodjanak róla, hogy bizalmas információhoz hozzáférő foglalkoztatottjai és partnerei rendelkezzenek aláírt titoktartási nyilatkozattal.

A BSZRK foglalkoztatottjai és partnerei felelősek a BSZRK-on belül, vagy a BSZRK-val fennálló kapcsolat során létrehozott, érkezett, módosított, átadott, megosztott, tárolt vagy használt adatok bizalmas jellegének, sértetlenségének és hozzáférhetőségének védelméért ezek tényleges helyétől és megjelenési formájától függetlenül (elektronikus, papíralapú, egyéb formátum stb.).

A BSZRK tiszteli mások munkáját, és odafigyel rá, hogy ne sértse meg mások szellemi tulajdonhoz fűződő jogait, és ugyanezt várja el saját szellemi tulajdona vonatkozásában másoktól is. A számítógépes hardverek, szoftverek, a BSZRK digitális rendszerein tárolt információk, valamint a foglalkozatottak otthoni vagy egyéb, nem a BSZRK tulajdonban lévő digitális rendszerein tárolt, a BSZRK-val kapcsolatos információk szervezeti tulajdonnak minősülnek és ennek megfelelően szükséges kezelni őket.

A BSZRK foglalkoztatottjai és partnerei hivatali célú levelezésük során kizárólag a BSZRK által jóváhagyott levelezőrendszert és kapcsolati adatokat (e-mail cím stb.) használhatják.

A BSZRK szellemi tulajdonának védelme megköveteli, illetve lehetővé teszi, hogy a BSZRK megakadályozza, hogy azt bárki engedély nélkül használja, valamint díjat számítson fel ezek használati jogáért.

A BSZRK foglalkoztatottjainak és partnereinek minden tőlük telhetőt meg kell tenni a tudomásukra jutott adatok biztonságának és - a közérdekű adatok és a közérdekből nyilvános adatok kivételével - bizalmasságának megőrzése érdekében. Más számára adatok csak a vonatkozó jogszabályok és munkahelyi előírások betartásával adhatók át.

Nem szabad betekinteni bizalmas adatokba kivéve, ha erre a foglalkoztatottnak és partnernek joga és feladatainak ellátásához szüksége van, és tartózkodni kell az adatoknak az adatkezelés céljával ellentétes felhasználásától.

Sem a munkahelyen, sem azon kívül nem terjeszthetők olyan információk, amelyekről okkal feltételezhetők, hogy azok tévesek vagy pontatlanok. Nem tartható vissza közérdekű vagy közérdekből nyilvános információ.

A munka során szerzett bizalmas vagy mások számára hozzá nem férhető információk nem használhatók fel a foglalkoztatottak és partnerek saját anyagi vagy más haszonszerzésük céljára.

A BSZRK elkötelezett a kiberbiztonsági kultúra kialakítása, fenntartása, fejlesztése mellett, amelyet teljes tevékenysége során, annak minden résztvevője esetében ösztönöz. A BSZRK elkötelezett az elektronikusan tárolt adatok bizalmas kezelése, sértetlenségének és hozzáférhetőségének megőrzése iránt saját informatikai megoldások és belső szabályozó eszközök alkalmazásával az adatok teljes életciklusa, azok tárolása, feldolgozása és továbbítása során. Ennek megfelelően:

- valamennyi, a BSZRK informatikai infrastruktúrájának kezelése, használata és működése által érintett felhasználó köteles rendszeresen részt venni az információbiztonsági tudatosság elmélyítését szolgáló képzésen,
- kizárólag hitelesített és megfelelő jogosultságokkal rendelkező felhasználók kaphatnak hozzáférést az információs infrastruktúrához a "szükséges mérték" elvének érvényesítése mellett.

A nem munkavégzéssel kapcsolatos internethasználat annyiban megengedett, ha nem veszélyezteti a rendszer és a hálózat biztonságát, teljesítményét vagy stabilitását, és nem akadályozza a munkaköri feladatok ellátását, de a BSZRK informatikai vagy telekommunikációs eszközeire végzett adatletöltés, vagy magánjellegű adatoknak a BSZRK eszközein tárolása ekkor sem engedélyezett.

A megfelelő biztonság érdekében (a magánélet tiszteletben tartására vonatkozó és az adatvédelmi jogszabályok által biztosított kereteken belül) a BSZRK fenntartja a jogot, hogy a karbantartási-, gazdasági-, és jogszabályi követelmények teljesítése érdekében hozzáférjen az eszközökhöz és a rajtuk tárolt adatokhoz.

A BSZRK elvárja, hogy foglalkoztatottjai, partnerei

- ismerjék meg és alkalmazzák a BSZRK informatikai- és információbiztonsági elveit és szabályzatait, megoldásait;
- a folyamatok lehető legkorábbi szakaszában azonosítsák, kezeljék és javítsák az elektronikusan tárolt adatok hibáit és hiányosságait;

- haladéktalanul jelezzék az információs infrastruktúrát vagy annak bármely elemét, vagy a BSZRK tulajdonát képező, vagy általa kezelt elektronikusan tárolt adatokat érintő káreseményeket, helytelen használatot és egyéb problémákat.

A BSZRK törekszik rá, hogy kommunikációja mindig pontos és megfelelő, félreérthetetlen legyen.

A foglalkoztatottaknak és partnereknek szem előtt kell tartaniuk nem csupán azt, hogy a tőlük származó kommunikációt a BSZRK egészére vonatkozóan értelmezik, de az jogvita során fel is használható.

A BSZRK elvárja, hogy foglalkoztatottjai és partnerei

- szóbeli és írásbeli kommunikációban a legszigorúbb magatartási szabályokat kövessék;
- valós, naprakész, megfelelő, pontos, érthető, tényszerű és helytálló információkat nyújtsanak a kommunikációjuk során, kerüljék a félrevezető megfogalmazásokat;
- minden szakmai/gazdasági tevékenységgel kapcsolatos információt bizalmasan kezeljenek, ha annak nyilvánosságra hozatala még nem engedélyezett;
- ne feledkezzenek meg róla, hogy saját megnyilvánulásaik nem feltétlenül azonosak a BSZRK álláspontjával, és még látszatát sem kelthetik annak, hogy a BSZRK nevében nyilvánulnak meg, a BSZRK álláspontját közlik.

A BSZRK nyílt, átlátható és kiegyensúlyozott kétirányú kommunikációt folytat a külső érintettekkel.

A BSZRK célja, hogy minden releváns médián keresztül teljes, átfogó és megbízható információk kerüljenek közzétételre tevékenységeiről és törekvéseiről és ehhez pozitív és kiemelkedően magas színvonalú szakmai kapcsolatokat szándékozik kialakítani a médiával.

A BSZRK nevében a média, valamint a külső érintettek felé irányuló kommunikáció nyilvános közleménynek minősül, amely körültekintést, a jogi és a médiával kapcsolatos terület alapos ismeretét igényli, és ezért csak a megfelelő jóváhagyások birtokában, az arra feljogosítottak számára engedélyezett.

A BSZRK nem tűri és nem tolerálja a nyilvánosság félrevezetését.

A BSZRK foglalkoztatottjainak gondoskodniuk kell róla, hogy a BSZRK működésére vonatkozó tartalmú, nyilvános közleménynek minősülő külső, például szakmai fórumokon tartandó előadással kapcsolatban rendelkezzenek a megfelelő vezetői jóváhagyással.

A BSZRK közösségi médiában történő megjelenéseit az erre kijelölt szervezeti egység, személyek koordinálják. A foglalkoztatottak, partnerek közösségi médiában való jelenléte a magánszférába tartozik, és ezt a BSZRK tiszteletben tartja, ugyanakkor a foglalkoztatottak, partnerek nem léphetnek fel a BSZRK nevében a közösségi médiában, nem publikálhatnak, nem oszthatnak meg és semmilyen formában nem tehetnek közzé vállalati információkat, különösen védett szakmai/gazdasági információkat, és nem hivatkozhatnak a BSZRK-ra, nem jeleníthetik meg a BSZRK-t annak értékeivel ellentétes módon.

Az „Informatikai biztonsági házirend és nyilatkozat" dokumentumban leírtakat megértettem, tudomásul vettem, betartásukat a munkakörömben elvárt módon vállalom.

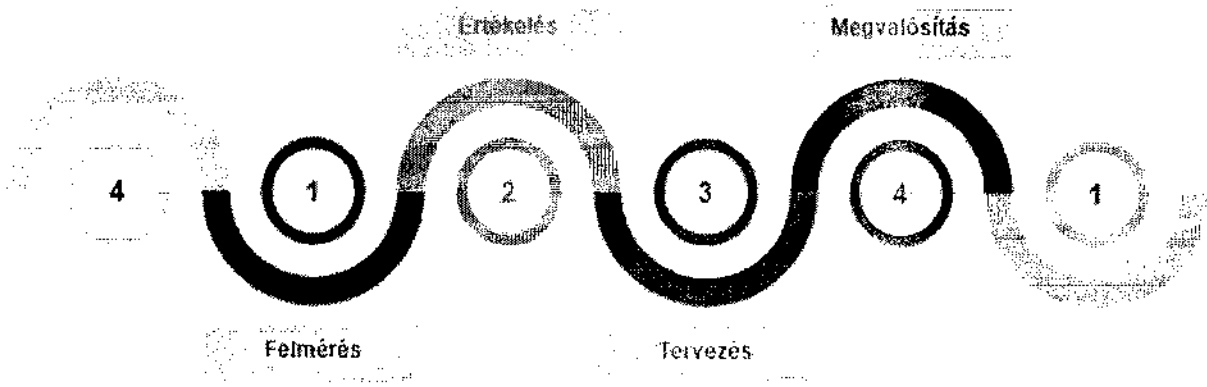
Fenti nyilatkozatot tiszta tudattal, döntéshozatalra képes állapotban, minden kényszer nélkül tettem, amelyet saját kezű aláírásommal megerősítek.

....., ÉÉÉÉ.HH.NN.

X Y [név és beosztás],

[munkáltató megnevezése

4.3 KOCKKÁZATMENEDZSMENT KERETRENDSZER



A függelékhez kizárólag a következő személyek számára engedélyezett a hozzáférés:

- Főigazgató,
- Általános Főigazgató-helyettes,
- Humánpolitikai igazgató,
- Jogi igazgató,
- Informatikai osztályvezető,
- Elektronikus információbiztonsági felelős,
- Belső ellenőr,

M4.3.1. Az informatikai kockázatfelmérés és értékelés alapelvei

Az informatikai kockázatfelmérés és értékelés (a továbbiakban együttesen: **kockázatelemzés)** tervezése során az alábbi elveket kell követni:

- A kockázatfelmérés tervezését lehetőleg tevékenységekre, folyamatokra és az azokban rejlő kockázatokra kell alapozni. Amennyiben létezik korábbi informatikai kockázatelemzés, annak eredményeit a tervezésben fel kell használni.
- A kockázatfelmérés során elsősorban a BSZRK számára legfontosabb tevékenységekre és az azokat támogató informatikai rendszerelemekre kell fókuszálni, az ilyen tevékenységeket és rendszerelemeket akár a többi rendszerelemnél gyakrabban felmérve, értékelve.
- A kockázatfelmérésnek és értékelésnek rendszeresnek kell lennie, azaz a korábbi évek informatikai kockázatfelmérésein szerzett tapasztalatok alapján az informatikai kockázatfelmérési, értékelési tervet célszerű évente felülvizsgálni, átgondolni, és amennyiben szükséges, akár korábban már vizsgált tevékenységeket, rendszerelemeket ismételten vizsgálni szükséges.

- A tervezésnek rugalmasnak kell lennie, azaz a BSZRK működése során felmerült akut vagy bármi okból a FI által kiemeltnek minősített területek kockázatait soron kívül felmérni és értékelni szükséges, az eredetileg tervezett tevékenységeket megfelelően áttervezve.
- A kockázatfelmérés és értékelés tervezésének a BSZRK-ra ható változásokhoz igazodnia kell, azaz, ha bármely tevékenység, rendszerelem kevesebb vagy ellenkezőleg: megnövekedett kockázatnak van kitéve, az ellenőrzések gyakoriságát, tartalmát, mélységét, az alkalmazott mintavételt stb. megfelelően át kell gondolni és az ellenőrzési tervet ennek megfelelően módosítani szükséges.

Az informatikai kockázatfelmérés és értékelés tervezése során alkalmazott alapelveket a FI-val egyeztetni, jóváhagyatni szükséges.

M4.3.2. Az informatikai kockázatfelmérés és értékelés tervezése, előkészítése

Az informatikai kockázatfelmérés és értékelés tervezése, valamint a tevékenység során

- elemezni kell a külső és belső kontrollkörnyezetet annak érdekében, hogy azonosításra kerüljenek az informatikai kockázatfelmérésre és értékelésre vonatkozó elvárások, különösen
  - a hazai, Európai Unió-n belüli és egyéb nemzetközijogszabályi elvárások,
  - a hazai, Európai Unió-n belüli és egyéb nemzetközi szabványelvárások,
  - a BSZRK stratégiája, célkitűzései, rövid- és hosszú távú feladatai,
  - a BSZRK működési környezete,
  - az egészségügyi környezet elvárásai,
  - a Főigazgató elvárásai.
- azonosítani kell a lényegi folyamatokat és folyamatgazdákat (az adott folyamat irányításáért, működtetéséért felelős személy),
- azonosítani kell a releváns informatikai rendszerelemeket és szerepüket a BSZRK informatikai támogatásában.

Az informatikai kockázatfelmérés és értékelés tervezése során az IBF feladata, hogy valamennyi általa ismert lényegi körülményre tekintettel levő kockázatfelmérés és értékelés készüljön.

M4.3.3. Informatikai kockázatfelmérési és értékelési ciklus

A BSZRK legalább 2 évente a BSZRK valamennyi lényegi tevékenységét és informatikai rendszerelemét fel kell mérni (a továbbiakban erre az időszakra „ciklus" néven fogunk hivatkozni); azonosítani kell a lehetséges kockázataikat és értékelni kell azokat, valamint intézkedéseket kell kidolgozni a megfelelő kezelésükre (amely kockázat esetében ez szükséges); továbbá az ezen alapelvektől való eltérést indokolni szükséges.

Amennyiben a meghatározott ciklus alatt nem lehetséges a BSZRK valamennyi lényegi tevékenységét, rendszerelemét felmérni és értékelni, döntést kell hozni róla, hogy

- kockázatértékelés alapján egyes tevékenységek, rendszerelemek felmérésére, értékelésére a ciklus hosszánál nagyobb időközönként kerül sor (pl. azért, mert nem volt változás a tevékenységben, rendszerelemekben és környezetükben),
- a ciklus meghosszabbításra kerül (pl. az elvárt 2 év helyett 3 vagy 4 évente kerülnek felmérésre és értékelésre bizonyos tevékenységek és/vagy informatikai rendszerelemek) – amennyiben erre a jogszabályi környezet lehetőséget nyújt,

- a BSZRK pótlólagos erőforrást von be a szükséges kockázatfelmérésbe és értékelésbe, intézkedési terv készítésbe.

A döntést az IBF-nek és az ICSV-nek kell előkészíteni és a FI elé terjeszteni, aki meghozza a szükséges döntést.

M4.3.4. Informatikai kockázatfelmérés és értékelés típusai

A 2024. évi LXIX. törvény (továbbiakban: Kibertan tv.) egyik oldalról előírja a rendszeres kockázatelemzés elvégzését, és meghatározza a kockázatelemzés alapelveit, azonban a részletekben nem köti meg az érintett BSZRK kezét.

A BSZRK többféle célú és módszerű informatikai kockázatfelmérést és értékelést végezhet; ezekből néhány példa:

- az Kibertan tv. által meghatározott követelmények alapján meghatározott nemmegfelelések miatti sérülékenységek értékelése, elemzése (nem compliance jellegű felmérés és értékelés, a sérülékenységek miatt bekövetkező következmények valószínűségeit is figyelembe veszi),
- az ISO27001 információbiztonsági szabványnak megfelelő kockázatfelmérés és értékelés,
- egyedi kockázatértékelések (pl. a FI által meghatározott területek vagy az IBF, esetleg a belső ellenőr által végzett vizsgálatokon azonosított nem-megfelelőségek kockázatfelmérése és értékelése).

M4.3.4.A Az elektronikus információs rendszerek biztonsági osztályából eredő elvárásoknak megfelelés értékelése

A BSZRK a megfelelés szintjének minél könnyebb követhetősége érdekében a Rendeletben előírt kockázatelemzés mellett megfelelőségi vizsgálatot is végez, amely számszerűsíti, hogy a Rendeletben meghatározott biztonsági intézkedések esetében,

- az adott időszakban mely biztonsági osztálynak kell megfelelnie,
- az elvárt biztonsági osztály elvárásai közül melyeknek felelt meg és melyeknek nem,
- a magasabb (adott időszakban nem kötelezően elérendő) biztonsági osztály elvárásaiból melyeknek felelt meg a BSZRK (az elvártnál korábban).

A vizsgálat a megfelelőségi kockázatot méri, azaz nem valószínűségalapú.

Az elemzés során az NKI által kibocsátott Osztályba sorolás és védelmi intézkedés (OVI) táblázatokat kell használni és az azok alapján azonosított nemmegfelelőségeket kell megfelelően értékelni.

Az ilyen elemzést az IBF feladata elvégezni.

M4.3.4.B Az elektronikus információs rendszerek biztonsági osztálya miatti kockázatelemzés

A BSZRK a megfelelés szintjének minél könnyebb követhetősége és értékelése érdekében olyan vizsgálatot is végeztethet, amely értékeli, hogy a Rendelet elvárásainak nem-megfelelés miatti sérülékenység milyen valószínűséggel vezethet káreseményhez, és az milyen mértékű lehet; a lehetséges kockázatot pedig ezek alapján számítja ki.

Az ilyen módon végzett kockázatértékelés

- építhet az „M4.4.A Az elektronikus információs rendszerek biztonsági osztályából eredő elvárásoknak megfelelés értékelése " pontban említett megfelelési (compliance) értékelésre, és
- megfelel a Rendeletben elvárt kritériumoknak, azaz ilyen módon végzett kockázatértékelés mellett további kockázatértékelést végezni nem szükséges.

Az ilyen elemzést az IBF feladata elvégezni.

M4.3.4.C ISO27001 információbiztonsági szabványnak megfelelő kockázatelemzés

Az ISO27001 szabványnak megfelelő kockázatelemzések az egyes sérülékenységek bekövetkezési valószínűségén és a sérülékenység kihasználása esetén bekövetkező lehetséges kár nagyságán alapulnak; a kockázat mértéke ezekre tekintettel kerül meghatározásra.

Az ilyen elemzést az IBF feladata elvégezni.

M4.3.4.D Egyéb kockázatértékelések

Az ilyen kockázatelemzések az egyes sérülékenységek bekövetkezési valószínűségén és a sérülékenység kihasználása esetén bekövetkező lehetséges kár nagyságán alapulnak; a kockázat mértéke ezekre tekintettel kerül meghatározásra.

Az ilyen elemzést az IBF és esetlegesen az FI által kijelölt külső szakértő feladata elvégezni.

M4.3.5. Adminisztratív felkészülés

Az egyes kockázatértékelések előtt

- egyeztetni szükséges a tervezett kockázatértékelés módszerét, időzítését és területét a FI-val és ha az FI egyetért vele, az érintett terület vezetőjével,
- meg kell határozni a szükséges közreműködőket és a tőlük elvárt közreműködés módját, időszükségletét,
- el kell kérni és tanulmányozni szükséges a kapcsolódó belső szabályozásokat,
- el kell kérni és tanulmányozni a kapcsolódó egyéb dokumentációt (munkaköri leírások, nyilvántartások, folyamatleírások, naplók stb. - ezeket az adott ellenőrzés alapján meghatározva)
- tanulmányozni szükséges a kapcsolódó hazai és nemzetközi jogszabályok aktuális tartalmát,
- tanulmányozni szükséges a kapcsolódó hazai és nemzetközi szabványok aktuális tartalmát,
- el kell kérni és tanulmányozni a korábbi informatikai kockázatértékelések és külső/belső ellenőri megállapításokat, valamint a kapcsolódó intézkedési terveket, továbbá azok megvalósítási állapotát,
- meg kell határozni a kockázatértékeléshez szükséges összegyűjtendő adatokat és azok időtávját, mennyiségét.

M4.3.6. Az értékelt szervezeti egység képviselőjének értesítése

Az egyes informatikai kockázatértékelés előtt értesíteni kell a kockázatfelmérés tényéről és amennyiben szükséges, a tartalmáról a kockázatértékelésbe bevont szervezeti egység vezetőjét, képviselőjét; és ha érintett, akkor az adott külső közreműködő, szolgáltató képviselőjét is.

Az előzetes értesítés elhagyható, amennyiben a Főigazgató (az IBF javaslatára vagy anélkül) ezt szükségesnek tartja. Az előzetes bejelentés elhagyása általában akkor indokolt, ha

- feltételezhető, hogy az előzetes értesítés és a kockázatértékelés közötti időszakban az érintett szervezeti egység képviselői módosítanák vagy törölnék a felmérni szándékozott területről rendelkezésre álló adatokat, vagy
- a kockázatértékelésben érintett szervezeti egység, külső közreműködő, szolgáltató szabálytalanság vagy csalás gyanújában érintett, vagy
- az értékelendő tevékenységért felelős szervezeti egység, külső közreműködő, szolgáltató vezetői várhatóan meghiúsítanák az eredményes kockázatértékelést.

M4.3.7. A kockázatértékelés módszereinek meghatározása

Az informatikai kockázatértékelés során törekedni kell az egyszerű, áttekinthető módszerek alkalmazására, amely jellemzően

- előzetes adatgyűjtésen,
- személyes interjúkon,
- adatok elemzésén, értékelésén,
- belőlük következtetések levonásán,
- az értékelésnek az érintett területtel való egyeztetésén és
- a kockázatértékelés véglegesítésén

alapul.

A kockázatértékelési módszert és technikát, valamint ezek összességét az adott kockázatértékelés célkitűzéseinek, tárgyának, típusának, továbbá a rendelkezésre álló erőforrásoknak megfelelően kell meghatározni.

M4.3.8. Kiemelt kockázat észlelése esetén követendő eljárás

Amennyiben a kockázatétékelés során kiemelt besorolású kockázatra derül fény, a kockázatértékelést végzőnek

- haladéktalanul kezdeményeznie kell a tevékenységért felelős személynél a megfelelő kockázatkezelési intézkedés megkezdését,
- késedelem nélkül tájékoztatnia kell az érintett szervezeti egység vezetőjét és az FI-t (azaz ilyen esetben nem szükséges és nem szabad megvárni az intézkedéssel a kockázatértékelés véglegesítését).

M4.3.9. Az informatikai kockázatértékelés menete és tartalma

Az informatikai kockázatértékelés menete és tartalma során az alábbi struktúrát célszerű követni:

Tapasztalt állapot felmérése

Pontosan fel kell mérni a tapasztalt állapotot, meg kell határozni az észlelt nem-megfeleléseket, jobbítandó területeket, valamint az azonosított pozitívumokat (pl. meglévő kontrollintézkedéseket), annak érdekében, hogy valóban prudens, lehetőleg teljes kép alapján készülhessen az értékelés.

Bizonyítékok megnevezése

A tapasztalt állapotról gyűjtött információt megfelelő mértékben dokumentálni szükséges és ezeket a dokumentált információ-példányokat pontosan megnevezve a kockázatértékeléshez szükséges csatolni annak érdekében, hogy egyértelmű legyen, milyen információ alapján készült a tapasztalt állapot (és később az értékelés stb.) leírása.

Amennyiben a felmért terület részéről egyetértés van a tapasztalt állapot megítélésében, a bizonyítékgyűjtési tevékenység korlátozható, a kockázatértékelés során felhasznált erőforrások ésszerű szinten tartása érdekében.

Megállapítás megfogalmazása

A tapasztalt állapot alapján meg kell határozni az egyes nem-megfeleléseket, jobbítandó területeket, olyan elemi egységenként, hogy a kezelésük egyértelmű és egyszerű legyen (azaz az összetett nemmegfeleléseket lehetőleg elemi egységekre kell bontani, szükség esetén jelölve a közöttük levő kapcsolatot).

A minél kisebb önálló egységként megfogalmazott megállapítás előnye, hogy a kezelésére általában nem komplex, több lépéses, több felelős tevékenység szükséges, így a kapcsolódó intézkedési terv egyszerű, áttekinthető lehet.

A kis önálló egységként definiált megállapítások további előnye, hogy a kapcsolódó intézkedési terv megvalósításának esetleges késése nem egy soklépéses feladat számos lépését hátráltatja, csak egy áttekinthetően kezelhető feladatot érint, így a késés kiváltó okának azonosítása és kezelése is egyszerűbb, ráadásul nincsen hatással további nem-megfelelések kapcsán meghatározott megállapításokra és azok kezelésére. (Nem lesznek komplex, áttekinthetetlen, végeláthatatlan lépésekből álló feladatok, amelyek végrehajtása beláthatatlan ideig elhúzódhat, természetesen mindig jól megmagyarázható és elfogadható okokból - a késések tényén nem változtatva.)

Egy példa a megállapításra:

- A BSZRK épületeit nem védi villámhárító (példa, valójában védi).

Lehetséges következmény

Az egyes megállapításokban leírt nem-megfelelés okozta következményt olyan részletességgel kell leírni, hogy a nem szakmai olvasó is megfelelő mélységben megértse, miért probléma a BSZRK számára a nem-megfelelés.

Példa: a hiányzó villámhárító (mint nem-megfelelés) lehetséges következménye, hogy

- a BSZRK épületeit villámcsapás érheti,
- ha a BSZRK egyik épületét villámcsapás éri, az
    - tüzet okozhat,
    - károsíthatja az elektromos készülékeket, informatikai eszközöket,
    - adatvesztéshez vezethet stb.

A lehetséges következményhez kapcsolódóan meg kell határozni a lehetséges következmény mértékét (a lehetséges kár nagyságát). A könnyebb besorolhatóság és áttekinthetőség érdekében a lehetséges következmény mértékét ötfokozatú skálán határozzuk meg, amelynek részletei az „M4.II.I. Nemmegfelelések lehetséges következményének "pontban kerülnek bemutatásra.

Lehetséges következmény bekövetkezési valószínűsége

Az azonosított nem-megfelelés nem feltétlenül okoz azonnali következménykárt a BSZRK számára.

Példa: a hiányzó villámhárító (mint nem-megfelelés) nem jelenti automatikusan, hogy

- a BSZRK épületét feltétlenül villámcsapás éri, illetve
- ha a BSZRK épületét villámcsapás éri, ez azonnal vagy néhány napon belül be fog következni,
- a BSZRK épületét esetlegesen érő villámcsapás feltétlenül tüzet fog okozni vagy valamennyi elektromos készülék teljes és helyreállíthatatlan tönkremeneteléhez vezet, illetőleg a BSZRK valamennyi adatát visszaállíthatatlanul megsemmisíti.

A lehetséges következmény bekövetkezési valószínűségét a szakmai legjobb gyakorlat alapján kell meghatározni. - ahol „történelmi adatok" állnak rendelkezésre, ott azokat megfelelően figyelembe véve.

A valószínűségek meghatározása során tudomásul kell venni (az értékelőnek és az értékelést olvasónak egyaránt), hogy nemcsak a valószínűség okoz bizonytalanságot a lehetséges következmény bekövetkezése során, hanem a valószínűségnek magának is van bizonytalansága, hibahatára.

Példa: ha a BSZRK épületeinek környékén az elmúlt három év során minden nyáron volt vihar és villámcsapás, az nem jelenti automatikusan azt, hogy

- a BSZRK épületei körül ebben az évben is lesz nyári vihar,
- a nyári vihar során erős villámlás lesz tapasztalható,
- a villámok a földben fognak kisülni (villámcsapás fog bekövetkezni).

A lehetséges következmény bekövetkezési valószínűségét megfelelőségi (compliance) vizsgálatnál nem kell meghatározni, mivel

- az azonosított nem-megfelelés valószínűsége 100%,
- a bizonyított megfelelés valószínűsége szintén 100%.

A könnyebb besorolhatóság ás áttekinthetőség érdekében a lehetséges következmény bekövetkezési valószínűségét ötfokozatú skálán határozzuk meg, amelynek részletei az „M4.II.2. Lehetséges következmény bekövetkezési valószínűségének osztályozása" pontban kerülnek bemutatásra.

Kockázati besorolás

Az egyes nem-megfelelőségek kockázatát

- a lehetséges következmény és
- a lehetséges következmény bekövetkezési valószínűsége

alapján határozzuk meg, az „M4.II.3. Azonosított kockázatok meghatározása" pontnak megfelelően.

Adott nem-megfelelésnek több lehetséges következménye is lehet - ilyenkor az egyes lehetséges következményekhez más-más bekövetkezési valószínűségek tartozhatnak, és ezért a különböző lehetséges következményeket külön tételként kell nyilvántartani, kezelni.

Példa: A villámcsapás következménye lehet:

- tűz,
- elektromos eszközök, informatikai berendezések károsodása,
- adatvesztés stb.

Elvárt intézkedés

Az egyes nem-megfelelés, fejlesztendő terület kezelésére meg kell határozni az elvárt intézkedéseket, olyan részletességgel, hogy az érintett terület, felelős egyértelműen tudja értelmezni a tőle elvárt tevékenységet.

Egy megállapításhoz (nem-megfeleléshez) több javaslat is kapcsolódhat és hasonlóan: több megállapítás (nem-megfelelés) is kezelhető egy javaslattal.

Példa: A villámcsapás következménye lehet:

- tűz,
- elektromos eszközök, informatikai berendezések károsodása,
- adatvesztés stb.

Az elvárt intézkedés lehet átfogó:

- a BSZRK épületeinek megvédése a villámcsapás következményeitől,

de az egyes következmények önállóan is kezelhetők:

- tűz: automatikus tűzoltó rendszer,
- elektromos eszközök, informatikai berendezések károsodása: túlfeszültségvédelem,
- adatvesztés: adatok másolatának tárolása távoli másodlagos helyszínen, illetve off-line, tűzbiztos Faraday-kalitkában.

A javaslatokban lehetőleg kerülni kell a konkrét szállító, megoldás megnevezését (azokat a felelős fogja azonosítani, értékelni, kiválasztani), helyette a szükséges megoldás jellemzőit kell kellő részletességgel meghatározni.

Az elvárt intézkedést a szükséges intézkedések végrehajtásáért felelős személyek és a vonatkozó határidők megjelölésével kell elkészíteni.

Az elvárt intézkedést és a hozzá kapcsolódó határidőt úgy kell meghatározni, hogy az számonkérhető legyen. Ha az elvárt intézkedés várható végrehajtási ideje egy éven túl mutat, akkor részfeladatokat, illetve részhatáridőket kell meghatározni, ahol ez értelmezhető.

Az elvárt intézkedés végrehajtásáért felelős személyt beosztásának megnevezésével kell meghatározni (szervezetii egység nem lehet felelős). Ha az adott beosztás bármilyen okból megszűnik, annak „jogutóda" a felelős. Ha az adott beosztás „jogutód" nélkül megszűnik, az eredeti felelős beosztás közvetlen felettese lesz a felelős és így tovább.

Javasolt időtáv

A javasolt intézkedések időtávját az " M4.3.11.4. Elvárt intézkedés osztályozása a megvalósítás javasolt időtávja alapján" pontban leírtak szerint kell meghatározni.

Ráfordításigény

A javasolt intézkedés ráfordításigényét az " M4.3.11.5. Elvárt intézkedés osztályozása a megvalósítás várható ráfordításigénye alapján" pontban leírtak szerint kell meghatározni.

Törekedni kell a minél kisebb külső és belső ráfordítást igénylő megoldások javaslására, továbbá a minél kisebb adminisztrációs feladatot jelentő megoldások ajánlására (azaz például a beruházást, beszerzést igénylő megoldások helyett a beruházás, beszerzési procedúra nélkül megvalósítható megoldásokat javasolt előnyben részesíteni).

Törekedni kell továbbá arra, hogy a javasolt intézkedéseknek ne csak a megvalósítása, hanem a fenntartása is ráfordítás, valamint erőforráshatékony legyen.

M4.3.10. Kockázatértékelés során alkalmazott osztályozások

M4.3.10.1. Nem-megfelelések lehetséges következményének osztályozása

A kockázatértékelés során azonosított nem-megfelelőség (gyakorlat, hiányosság stb.) értékelésekor a nem-megfelelőség miatti lehetséges következményt az alábbi osztályozás alapján rangsoroljuk:

Lehetséges következmény	Lehetséges következmény jelentése
Csekély	A megállapításban említett állapot, gyakorlat, hiányosság hatásaként legfeljebb jelentéktelen káresemény következhet be
Alacsony	A megállapításban említett állapot, gyakorlat, hiányosság hatásaként csekély káresemény következhet be.
Közepes	A megállapításban említett állapot, gyakorlat, hiányosság hatásaként közepes káresemény következhet be.
Magas	A megállapításban említett állapot, gyakorlat, hiányosság hatásaként nagy káresemény következhet be.
Kiemelt	A megállapításban említett állapot, gyakorlat, hiányosság hatásaként kiemelkedően nagy káresemény következhet be.

Csekély besorolású a megállapításban említett állapot, gyakorlat, hiányosság, ha a lehetséges hatásaként

- nem várható közvetlen vagy közvetett anyagi kár,
- nincs külső bizalomvesztés, a probléma kisebb, a BSZRK-on belül marad, és BSZRK-on belül meg is oldható,
- az érintett EIR nem kezel jogszabályok által védett (pl.: személyes) adatot,
- a hiányosság nem jelent közvetlen veszélyt szakmai célra használt EIR-re, illetve abban tárolt adatra.

Alacsony besorolású a megállapításban említett állapot, gyakorlat, hiányosság, ha a lehetséges hatásaként

- a közvetlen és közvetett anyagi kár a BSZRK költségvetéséhez, szellemi és anyagi erőforrásaihoz képest alacsony,
- az esetlegesen lehetséges társadalmi-politikai hatás a BSZRK-on belül kezelhető,

- az üzlet-, vagy ügymenet szempontjából csekély értékű, és/vagy csak belső (BSZRK-ra vonatkozó) szabályzattal védett adat vagy EIR elérése, rendelkezése állása, bizalmassága sérülhet,
- téves belső következtetés levonásához vezethet a BSZRK által használt EIR jellemzőiről.

Közepes besorolású a megállapításban említett állapot, gyakorlat, hiányosság, ha a lehetséges hatásaként

- a közvetlen és közvetett anyagi kár a BSZRK költségvetéséhez, szellemi és anyagi erőforrásaihoz képest erősen érzékelhető (a közvetlen és közvetett anyagi kár eléri vagy meghaladja a BSZRK költségvetésének 5%-át),
- bizalomvesztés állhat elő a BSZRK-on belül vagy a BSZRK-val kapcsolatban, esetlegesen BSZRK szabályzatában foglalt kötelezettségek sérülhetnek,
- az üzlet-, vagy ügymenet szempontjából közepes értékű, vagy a BSZRK szempontjából érzékeny folyamatokat kezelő EIR, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat elérése, rendelkezésre állása sérülhet,
- téves külső következtetés levonásához vezethet a BSZRK által használt EIR jellemzőiről.

Magas besorolású a megállapításban említett állapot, gyakorlat, hiányosság, ha a lehetséges hatásaként

- a közvetlen és közvetett anyagi kár a BSZRK költségvetéséhez, szellemi és anyagi erőforrásaihoz képest jelentős (a közvetlen és közvetett anyagi kár eléri vagy meghaladja a BSZRK költségvetésének 10%-át),
- személyi sérülések esélye megnőhet (ideértve például a káresemény miatti szolgáltatás kimaradását, illetve a rendszer irányítatlansága miatti veszélyeket),
- az üzlet-, vagy ügymenet szempontjából nagy értékű, üzleti titkot, vagy a BSZRK szempontjából különösen érzékeny folyamatokat kezelő EIR, vagy információt képező adat elérése, rendelkezése állása, bizalmassága tömegesen, vagy jelentősen sérülhet,
- a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, illetve bekövetkezhet a bizalomvesztés a BSZRK-on belül vagy az BSZRK-val kapcsolatosan,
- jelentősen téves külső következtetés levonásához vezethet a BSZRK által használt EIR jellemzőiről.

Kiemelt besorolású a megállapításban említett állapot, gyakorlat, hiányosság, ha a lehetséges hatásaként

- különösen nagy értékű üzleti titok, a BSZRK szempontjából kiemelten érzékeny információt képező adat sérülhet,
- a közvetlen és közvetett anyagi kár eléri vagy meghaladja a BSZRK költségvetésének 15%-át,
- a BSZRK iránti társadalmi, politikai bizalom sérülhet,
- alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;
- az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított,
- a BSZRK adatvagyona helyreállíthatatlanul megsérülhet,

- emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be.

Az adott kategóriába soroláshoz nem feltétlenül szükséges az adott kategória minden feltételét teljesítenie az intézkedésnek; a leginkább jellemző kategória került megadásra.

A megadott követelmények a BSZRK sajátosságaira tekintettel kerültek meghatározásra, más szervezet, társaság, informatikai környezet esetében az egyes kategóriákhoz eltérő követelmények lehetségesek.

M4.3.11.2. Lehetséges következmény bekövetkezési valószínűségének osztályozása

A kockázatértékelés során azonosított nem-megfelelőség értékelésekor (a kockázati szint megállapításakor) az alábbi osztályozás alapján rangsoroljuk a nem-megfelelőség okozta lehetséges következmény előfordulási valószínűségét:

Előfordulás valószínűsége	Előfordulás valószínűségének jelentés
Elenyésző	A megállapításban említett állapot, gyakorlat, hiányosság hatásaként előforduló lehetséges következmény (káresemény) várhatóan hároméves túl, vagy hároméves gyakoriságnál ritkábban következhet be (eddigi tapasztalataink alapján).
Alacsony	A megállapításban említett állapot, gyakorlat, hiányosság hatásaként előforduló lehetséges következmény (káresemény) várhatóan három éven belül, vagy hároméves gyakorisággal következhet be (eddigi tapasztalataink alapján).
Közepes	A megállapításban említett állapot, gyakorlat, hiányosság hatásaként előforduló lehetséges következmény (káresemény) várhatóan éven belül, vagy éves gyakorisággal következhet be (eddigi tapasztalataink alapján).
Magas	A megállapításban említett állapot, gyakorlat, hiányosság hatásaként előforduló lehetséges következmény (káresemény) várhatóan féléven belül, vagy féléves gyakorisággal következhet be (eddigi tapasztalataink alapján).
Szinte bizonyos	A megállapításban említett állapot, gyakorlat, hiányosság hatásaként előforduló lehetséges következmény (káresemény) várhatóan negyedéven belül, vagy negyedéves gyakorisággal következhet be (eddigi tapasztalataink alapján).

M4.3.11.3. Azonosított kockázatok meghatározása

A kockázatértékelés során azonosított nem-megfelelések miatti lehetséges következmények, valamint ezek előfordulási valószínűsége alapján az alábbi módon rangsoroljuk a nem-megfelelőség okozta kockázatokat:

Előfordulás valószínűség / Lehetséges hatás	Elenyésző	Alacsony	Közepes	Magas	Szinte bizonyos
Csekély	Marginális	Marginális	Alacsony	Alacsony	Közepes
Alacsony	Alacsony	Alacsony	Közepes	Közepes	Közepes
Közepes	Alacsony	Közepes	Közepes	Magas	Magas
Magas	Közepes	Közepes	Magas	Magas	Végzetes
Kiemelt	Közepes	Magas	Végzetes	Végzetes	Végzetes

M4.3.11.4. Elvárt intézkedés osztályozása a megvalósítás javasolt időtávja alapján

A végrehajtani ajánlott intézkedéseket a megvalósításuk időigénye, időszükséglete alapján az alábbi kategóriákba soroltuk:

Javasolt időtáv	Javasolt időtáv jelentése
Hosszú távon megvalósítani javasolt	3-5 éven belül (illetve jelentősebb egyéb módosítás esetén azzal együttesen) megvalósítani javasolt.
Közepes időtávon megvalósítani javasolt	1-2 éven belül megvalósítani javasolt.
Rövid távon megvalósítani javasolt	Az adott éven belül megvalósítani javasolt.
Hamarosan megvalósítani javasolt	Más feladatok fontosságát is átgondolva, rövid időn (preferáltan negyedéven) belül megvalósítani javasolt.
Haladéktalanul megvalósítani javasolt	Más feladatok fontosságát is átgondolva, a lehető: legrövidebb időn (preferáltan néhány napon) belül megvalósítani javasolt.

M4.3.11.5. Elvárt intézkedés osztályozása a megvalósítás várható ráfordításigénye alapján

Javaslatainkat, a végrehajtani ajánlott intézkedéseket a megvalósítás várható ráfordításigénye alapján az alábbi kategóriákba soroltuk:

Ráfordításigény	Ráfordításigény magyarázata
Elenyésző	A megvalósítás várható időigénye legfeljebb 4 munkaóra. A megvalósítás jellemzően belső erőforrás /foglalkoztatott közreműködését igényli, külső támogatás bevonása várhatóan nem szükséges vagy minimális. Anyagi ráfordítás várhatóan nem szükséges, vagy minimális (legfeljebb 1.000,- EUR).
Alacsony	A megvalósítás időigénye várhatóan 3 munkanapnál kevesebb. A megvalósítás jellemzően belső erőforrás / foglalkoztatott közreműködését igényli, külső támogatás bevonása valószínűleg nem szükséges vagy

	legfeljebb kismértékű (néhány munkaóra, egy-két munkanap). Anyagi ráfordítás várhatóan nem szükséges, vagy kismértékű (1.000,-5.000,- EUR).
Közepes	A megvalósítás időigénye várhatóan 4-15 munkanap. A megvalósítás jellemzően belső erőforrás / foglalkoztatott közreműködését igényli, külső támogatás bevonása valószínűleg 10 munkanap alatti. A várható anyagi ráfordítás (CAPEX) közepes mértékű (5.001-25.000,- EUR).
Magas	A megvalósítás időigénye várhatóan 16-60 munkanap. A megvalósítás belső erőforrás / foglalkoztatott közreműködése mellett külső szakmai támogatást is igényel, várhatóan 11-30 munkanap között. A várható anyagi ráfordítás (CAPEX) 25.000,- EUR feletti.
Kiemelt	A megvalósítás időigénye várhatóan 60 munkanap feletti és/vagy Főigazgató által jóváhagyott projektet igényel. A megvalósítás a belső erőforrás / foglalkoztatott mellett erős külső szakmai támogatást., és esetlegesen több szervezet együttműködését is igényli. A várható anyagi ráfordítás (CAPEX) jelentős.

Az adott kategóriába soroláshoz nem feltétlenül szükséges az adott kategória minden feltételét teljesítenie az intézkedésnek; a leginkább jellemző kategória került megadásra.

A megadott számértékek (idő- és anyagi ráfordítások) a BSZRK sajátosságaira tekintettel kerültek meghatározásra, más szervezet, társaság, informatikai környezet esetében az egyes jellemzőkhöz megadott számértékek más nagyságot vehetnek fel.

M4.3.12. Elvárt intézkedés tervezése (intézkedési terv)

Amennyiben az intézkedések megvalósítása hosszabb időt vesz igénybe a következő minta alapján Intézkedési tervet kell leírni:

Intézkedési terv (minta)

A tervet készítette: .....

A tervet jóváhagyta: .....

A terv végrehajtásának felelőse: .....

Az azonosított kezelni kívánt kockázat rövid összefoglalása: .....

.....

.....

A kijelölt válaszintézkedés rövid leírása: .....

.....

.....

A tervel kapcsolatos mérföldkövek:

Mérföldkő	Felelős	Határidő

A tervhez kapcsolódó egyéb dokumentumok: .....

.....

M4.3.13 Elvárt intézkedések megvalósítása

Az elvárt intézkedés megvalósításáért felelős személyt az intézkedés végrehajtásában a BSZRK valamennyi foglalkoztatottja és partnerének támogatnia kell, munkakörük és szerződésük mértékéig.

Az elvárt intézkedéseket az ICSV nyilvántartja.

Az egyes elvárt intézkedések végrehajtásáért felelős személy a határidő lejáratát megelőzően legfeljebb egy alkalommal írásban, megfelelő indoklással, az ICSV-vel és az IBF-fel végzett egyeztetést követően a FI-től határidő, illetve feladat módosítást kérhet. A kérelem elfogadásáról vagy elutasításáról a Főigazgató az ICSV és az IBF véleményének kikérését követően dönt, és erről tájékoztatja a felelős személyt és a BSZRK érintett egységének vezetőjét is.

A határidő, illetve feladat módosítására vonatkozó kérelem elbírálásának jogát a FI átruházhatja az ICSV-re vagy az IBF-re. Az így meghatalmazott személy köteles a FI-nek rendszeresen (de legalább félévente) beszámolni a feladat- és határidő módosítási kérelmekről, valamint azok elfogadásáról vagy elutasításáról.

Az egyes elvárt intézkedések megvalósítását az ICSV rendszeresen, de legalább félévente ellenőrzi. A határidőre meg nem valósított elvárt intézkedés végrehajtására az ICSV felszólítja az elvárt intézkedés felelősét, egyidőben a késedelemről értesíti a felelős közvetlen felettesét és az IBF-et.

Az IBF az elvárt intézkedések végrehajtásának megfelelő ellenőrzéséről rendszeresen, de legalább évente mintavétellel meggyőződik, és ha nem megfelelő ellenőrzést azonosít, azt jelzi az ICSV felé.

A felelős az elvárt intézkedés lezárását az elvégzett feladatok megfelelő, írásos, dokumentált igazolásával (bizonyításával) köteles haladéktalanul jelenteni az ICSV felé.

A sikeresen teljesítettnek jelentett elvárt intézkedéseket az ICSV ellenőrzi és miután meggyőződött a feladat megfelelő teljesítéséről, az adott elvárt intézkedést lezártként tartja nyilván; az elvégzett feladatok írásos, dokumentált bizonyítékait pedig az elvárt intézkedésekkel együtt nyilvántartásba veszi. Ha a teljesítettnek jelentett elvárt intézkedés végrehajtása nem megfelelő, az ICSV jelzi ezt az elvárt intézkedés felelősének, aki a feladatot köteles megfelelő minőségben folytatni.

Az IBF a lezárt intézkedéseket és azok megfelelő dokumentáltságát rendszeresen, de legalább évente mintavétellel áttekinti, és ha nem megfelelőséget azonosít, azt jelzi az ICSV felé.

Az IBF az elvárt intézkedések kezelése kapcsán gyűjtött tapasztalatairól rendszeresen, de legalább évente köteles beszámolni a FI számára.

4.4 BIZTONSÁGI ESEMÉNYKEZELÉSI TERV

A BSZRK biztonsági eseménynek (incidensnek) számít minden olyan történés, cselekvés, vagy ezek elmaradása, amely a BSZRK informatikai vagy telekommunikációs infrastruktúrájának, felhasználóinak, illetve az ebben tárolt adatoknak a bizalmasságát, sértetlenségét vagy rendelkezésre állását a BSZRK által nem kívánt módon befolyásolja.

Biztonsági eseményre példa:

- jogosulatlan hozzáférést eredményezhet, például:
  - jelszó felírása, felírt jelszó elvesztése,
  - jelszó megosztása mással,
  - jelszó beírása olyan módon, hogy azt más is láthatja,
  - más felhasználó hozzáférési azonosítójának, jelszavának használata vagy ennek elősegítése, illetve a használat korlátozásának befolyásolása,
  - azonosító kártya, tanúsítvány elhagyása vagy másnak átadása,
  - beléptetőkártya másnak átadása,
  - informatikai vagy telekommunikációs eszköz másnak átadása, használatra átengedése,
  - informatikai megoldáshoz hozzáférés engedése vagy ennek elősegítése,
  - beléptetőkártyával további személyek be- vagy kilépésének engedélyezése vagy lehetővé tétele stb.
- adatvesztést eredményezhet, például:
  - adat munkafolyamat céljától eltérő módosítása vagy törlése,
  - adatmentés mellőzése,
  - biztonsági másolat készítésének mellőzése, vagy a biztonsági másolat nem megfelelő kezelése,
  - informatikai vagy telekommunikációs eszköz másnak átadása, használatra átengedése,
  - adathordozó megsértése, elhagyása vagy másnak átengedése,
  - nemkívánatos szoftver telepítése a BSZRK informatikai infrastruktúrájában, vagy ilyen szoftver futtatásának, futásának elősegítése vagy a futtatást gátló megoldás működésének befolyásolása, akadályozása stb.
- adat nem tervezett változtatását (létrehozását, módosítását, törlését) eredményezheti, például:
  - adat munkafolyamat céljától eltérő rögzítése, módosítása vagy törlése,
  - adatmentés mellőzése,
  - informatikai vagy telekommunikációs eszköz másnak átadása, használatra átengedése,
  - jelszó megosztása mással,
  - informatikai vagy telekommunikációs eszköz másnak átadása, használatra átengedése,
  - adathordozó megsértése, elhagyása vagy másnak átengedése stb.
- a BSZRK szakmai/gazdasági/egészségügyi adatainak illetéktelenekkel való megismertetése vagy ennek elősegítése, illetve az illetéktelenek általi megismerés korlátainak befolyásolása (az adatok nem kompromittálása vagy ennek elősegítése),
  - adatok megosztása azok megismerésére nem jogosultakkal,
  - adatok olyan módon való kezelése, hogy azokat illetéktelenek is megismerhetik,

- adatok engedély nélküli lemásolása,
- titkosított adatról titkosítatlan másolat készítése,
- hozzáférési, módosítási, továbbítási vagy más típusú védelmének eltávolítása vagy annak megkísérlése,
- képernyőn vagy nyomtatásban megjelenített adat lefényképezése, lemásolása,
- nyomtatott információnak a BSZRK által elvárttól eltérő tárolása, szállítása stb.

- a BSZRK által kezelt vagy feldolgozott, természetes személyek személyes adatainak kompromittálása, például:
  - munkafolyamathoz nem kapcsolódó személyes adatok megismerésére törekvés vagy az adatok megismerése,
  - munkafolyamathoz kapcsolódó személyes adatok munkafolyamaton túlmutató, vagy attól eltérő felhasználása, megosztása, vagy ezeknek megkísérlése, illetve a megismerés, megosztás támogatása,
  - személyes adatok olyan módon való kezelése, hogy azokat illetéktelenek is megismerhessék,
  - személyes adat jogosultjával a munkafolyamathoz nem kapcsolódó kommunikáció vagy annak megkísérlése, illetve ennek elősegítése, támogatása stb.
- a BSZRK EIR-ének elérhetőségének és használhatóságának módosítása, például:
  - az informatikai vagy telekommunikációs rendszer munkafolyamatoktól eltérő felhasználása, különösen, ha ez a rendszer túlterheléséhez vagy rosszindulatú szoftverrel való megfertőzéséhez vezet, vagy azt elősegíti,
  - az informatikai vagy telekommunikációs rendszer használatáról szóló, vagy ahhoz szükséges információ BSZRK által nem támogatott elérhetővé tétele, megosztása, módosítása, törlése,
  - az informatikai vagy telekommunikációs rendszer munkafolyamatoktól eltérő felhasználása, különösen, ha ez a rendszer túlterheléséhez vagy rosszindulatú szoftverrel való megfertőzéséhez vezet, vagy azt elősegíti,
  - az informatikai vagy telekommunikációs rendszer működési környezetének, vagy a rendszer komponenseinek engedély nélküli módosítása, befolyásolása, vagy ezek elősegítése stb.

A biztonsági eseményeket az azt észlelő személynek haladéktalanul jelentenie kell az ICS felé bármilyen elérhetőségén (e-mailben, telefonon vagy személyesen).

A biztonsági esemény jelentésének késleltetése vagy elmulasztása munkajogi jogkövetkezményeket vonhat maga után.

A biztonsági esemény kezelése során figyelembe kell venni a „Cselekvési terv informatikai katasztrófaesemény bekövetkezése esetén" és az „Infokommunikációs eszközök használatáról szóló szabályzat" dokumentumban leírtakat, egyébként pedig ezen szabályzat, és különösen az ebben a függelékben leírtak szerint kell eljárni.

Az ICS a biztonsági eseményekről értesülhet az általa üzemeltetett informatikai, telekommunikációs infrastruktúra jelzéseiből, valamint a szolgáltatók által üzemeltetett jelzőrendszer üzenetei alapján is.

Az ilyen jelzéseket a személyes bejelentésekkel megegyező prioritással és módon kell kezelni.

A biztonsági eseményt (incidenst) vagy annak gyanúját az ICS-nak haladéktalanul nyilvántartásba kell vennie, majd ki kell vizsgálnia, amelynek során a bejelentést kapó ICS foglalkoztatottnak haladéktalanul értesítenie kell az ICSV-t és a valószínűsíthetően érintett rendszerelem működtetéséért felelős felelősöket, külső szervezetet (amennyiben külső szolgáltató is érintett), ezt követően össze kell gyűjteniük a bejelentés vizsgálatához, értékeléséhez szükséges információt, adatokat.

A bejelentett biztonsági eseményt (incidenst) vagy annak gyanúját az összegyűjtött információ alapján osztályozni szükséges. Az osztályozás alapja a biztonsági esemény (incidens) hatására várhatóan bekövetkező következmény mértéke, amelyet az „M4.3.10.1. Nem-megfelelések lehetséges következményének osztályozása" pont alapján kell elvégezni. Az osztályozást az ICSV feladata elvégezni.

Amennyiben a biztonsági esemény (incidens) lehetséges következménye

- közepes vagy magasabb besorolású, haladéktalanul értesíteni kell az eseményről az ICS-t, a FI-t és az IBF-et.
- személyes adat kompromittálódása, akkor haladéktalanul értesíteni kell az eseményről a DPO-t és az IBF-et; további személyek értesítéséről a DPO és az ICSV dönt, illetve erre az IBF tehet javaslatot.

Az értesítéseket az ICSV-nek kell elvégeznie.

A biztonsági esemény további kezelésébe az ICS-n túl be kell vonni mindazokat, akik az esemény kezelésében, a lehetséges következmények csökkentésében szerepet játszhatnak.

Törekedni kell rá, hogy a lehetséges következmények minél alacsonyabb szintűek legyenek és minél rövidebb idő alatt vissza lehessen térni a szokásos munkamenetre.

A biztonsági esemény kezelése akkor tekinthető lezártnak, amikor a szokásos munkamenethez visszatérés maradéktalanul megtörtént.

Az ICSV-nek mérnie és rögzítenie kell (nyilvántartásba kell venni)

- a biztonsági esemény bejelentőjét,
- a bejelentés idejét,
- a bejelentő által elmondottakat,
- az érintett rendszerelemeket,
- a lehetséges következményt,
- a biztonsági esemény besorolását (osztályát),
- a megoldásba bevontakat,
- a biztonsági esemény kezelése során tett intézkedéseket (azok kezdeményezőjével, kezdési és befejezési idejével, valamint az adott intézkedésbe bevontak körével és az intézkedés végrehajtása során tapasztalt lényeges körülményekkel, tapasztalatokkal együtt,
- a biztonsági esemény kiváltó okát,
- a biztonsági esemény lezárási idejével,

a biztonsági esemény által okozott tényleges kárral együtt.

Az ICSV-nek elemeznie kell és javaslatot kell tennie arra vonatkozóan, hogyan lehetne megelőzni vagy megfelelőbben kezelni a több alkalommal előforduló hasonló biztonsági eseményeket, a hasonló kiváltó okra visszavezethető biztonsági eseményeket, valamint hogyan lehetne tanulni a közepes és magasabb besorolású biztonsági eseményekből, annak érdekében, hogy a később előforduló hasonló események kezelése magasabb színvonalú lehessen.

A biztonsági eseményekről az ICSV-nek évente összefoglaló tájékoztatást kell adnia a FI, az integritás tanácsadó és az IBF számára. A tájékoztatásban az adott év során előforduló biztonsági eseményeket

- össze kell hasonlítani a megelőző évek biztonsági eseményeivel,
- meg kell határozni a jellemző trendeket és értékelni kell azokat; valamint
- meg kell határozni azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására.

A biztonsági eseménykezelés hatékonyságának növelése érdekében

- ajánlott elektronikus nyilvántartás vezetni a biztonsági eseményekről,
- ajánlott korai jelzőrendszert bevezetni a biztonsági események minél korábbi kezelésére,
- ajánlott képzéseket tartani a foglalkoztatottak számára a biztonsági események felismerésére és megfelelő kezelésére.

A biztonsági eseménykezelés hatékonyságának növelésére az IBF is javaslatot tehet.

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
NEMZETI KIBERVÉDELMI INTÉZET
HATÓSÁGI FŐOSZTÁLY
1022 Budapest, Törökvész út 32-34.
✉: 1399 Budapest, 62. Pf.: 710/37
@: hatosag@nki.gov.hu☎: +36-1-206-9320
Hivatali kapu: NBSZ (KRID: 427386978)

Bajai Szent Rókus Kórház

Tárgy: információbiztonsági szabályzat hatósági nyilvántartásba vétele

Hiv. sz.:

H A T Á R O Z A T

A Bajai Szent Rókus Kórház (székhely: 6500 Baja, Rókus utca 10. – a továbbiakban: Ügyfél) információbiztonsági szabályzatát (a továbbiakban: Szabályzat) a hatósági nyilvántartásba

b e j e g y z e m .

Döntésem ellen fellebbezésnek nincs helye, az a közlés napján véglegessé válik. Döntésemmel szemben önálló jogorvoslatként közigazgatási per indítható. A keresetlevelet e döntés közlésétől számított 30 napon belül, a Nemzetbiztonsági Szakszolgálatnál (a továbbiakban: Hatóság) kell előterjeszteni. A közigazgatási per lefolytatására a Szegedi Törvényszék jogosult.

I n d o k o l á s

Az Ügyfél 2025.06.30. napján, hivatali kapun benyújtott kérelemmel a 2025.06.30. napján hatályba lépett Szabályzat hatósági nyilvántartásba vételét kezdeményezte. A kérelemhez csatolta 5. verziószámú Szabályzatát.

Tekintettel arra, hogy a kérelem és mellékletei a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.), valamint a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet (Kiberbiztonsági vhr.) előírásainak megfeleltek, a rendelkező részben foglaltak szerint döntöttem.

A fellebbezés lehetőségét az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban: Ákr.) 116. § (1) bekezdése és a (4) bekezdés a) pontja zárja ki. A véglegessé válásra az Ákr. 82. §-ának (1) bekezdése irányadó. A közigazgatási per indításának lehetőségét az Ákr. 114. § (1) bekezdése, benyújtásának helyét és határidejét a közigazgatási perrendtartásról szóló 2017. évi I. törvény (a továbbiakban: Kp.) 39. § (1) bekezdése, az elbírálására jogosult szervet a Kp. 13. § (1) bekezdés c) pontja és a bíróságok elnevezéséről székhelyéről és illetékességi területének meghatározásáról szóló 2010. évi CLXXXIV. törvény 4. melléklete határozza meg.

A Hatóság hatáskörét és illetékességét a Kiberbiztonsági tv. 23.§ (1) bekezdés a) pontja, illetve a Kiberbiztonsági vhr. 16.§ (1) bekezdése állapítja meg.

Budapest, *elektronikus dátumbélyegző szerint*

dr. Kiss Csaba
nemzetbiztonsági főtanácsos
főigazgató nevében és megbízásából:

Erdélyi Attila
osztályvezető

Készült: egy elektronikus példányban
Melléklet:
Kapja: Bajai Szent Rókus Kórház
Készítette/Gépelte: Karikás Csaba
Tel.: (1) 206-9320
Irattári jelzés:
Azonosító:

ZÁRADÉK

A dokumentum elektronikus aláírással hitelesített

30710-2/1335-3/2025.Tük.