EMBERI ERŐFORRÁS
TÁMOGATÁSKEZELŐ

Az Emberi Erőforrás Támogatáskezelő Informatikai biztonsági szabályzata

készítette:

.....
Sipos János
információbiztonsági felelős

jóváhagyta:

.....
Monszpart Zsolt
főigazgató

Iktatószám: EMET/4708-1/2022
Hatályos: 2022. május 5.

TARTALOMJEGYZÉK

1. ÁLTALÁNOS RENDELKEZÉSEK

1.1. A SZABÁLYZAT CÉLJA

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

A Támogatáskezelő döntése alapján az Támogatáskezelőnek az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII.15.) BM rendeletben meghatározott 3. szintnek megfelelő védelmi osztály követelményeit kell teljesítenie, és ezzel összhangban a Támogatáskezelő elektronikus információs rendszereinek a 3. biztonsági osztály elvárásait kell teljesíteniük; ezért ez a szabályzat az ezeknek megfelelő területeket tartalmazza, elvárásokat fogalmazza meg.

1.2. A SZABÁLYZAT HATÁLYA

1.2.1. SZERVEZETI-SZEMÉLYI HATÁLY

1.2.1.1. Szervezeti hatály

A szabályzat szervezeti hatálya a Támogatáskezelő valamennyi szervezeti egységére kiterjed.

1.2.1.2. Személyi hatály

A szabályzat személyi hatálya a Támogatáskezelővel jogviszonyban álló természetes és jogi személyekre terjed ki; különösen azokra, akik kapcsolatba kerülnek, vagy kapcsolatba szándékoznak kerülni a Támogatáskezelő informatikai architektúrájával, elektronikus információs rendszereivel (használják, fejlesztik, telepítik, üzemeltetik, javítják stb. azokat), így:

- közalkalmazotti jogviszony alapján foglalkoztatottakra,
- a Támogatáskezelővel szerződéses kapcsolatban álló természetes és jogi személyekre,
- más szervezetek képviseletében a Támogatáskezelő által kontrollált területen tartózkodó, illetve a Támogatáskezelő informatikai rendszereihez hozzáférő személyekre (például az ellenőrző hatóságok képviselői).

A szabályzatban megadott szervezeti egységek és szerepkörök rövidítése a következő:

- Főigazgató: továbbiakban: FI
- Általános Főigazgató-helyettes: továbbiakban: ÁFIH
- Főigazgatói Kabinet: továbbiakban: FK,
- Főigazgatói Kabinetvezető: továbbiakban: FKV,
- Gazdasági igazgatóság: továbbiakban: GI,
- Gazdasági igazgató: továbbiakban: GII,
- Jogi és Compliance igazgatóság: továbbiakban: JCI,
- Jogi igazgató: továbbiakban: JI,
- Stratégiai és humánpolitikai igazgatóság: továbbiakban: SHI,
- Stratégiai és humánpolitikai igazgató: továbbiakban: SHII,
- Humánpolitikai osztály: továbbiakban: HO,
- Humánpolitikai osztályvezető: továbbiakban: HOV,
- Operatív igazgatóság: OI,
- Operatív igazgató: OII,
- Informatikai osztály: továbbiakban: IO,

- Informatikai osztályvezető: továbbiakban: IOV,
- Elektronikus információbiztonsági felelős: továbbiakban: IBF
- Belső ellenőrzés: továbbiakban: BE
- Belső ellenőr: továbbiakban: BEE,
- Adatvédelmi tisztviselő: továbbiakban: DPO,
- Üzemeltetési Osztály: ÜO
- Üzemeltetési osztályvezető: ÜOV
- Illetményszámfejtési Osztály: ISZO

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

1.2.2. TÁRGYI HATÁLY

A szabályzat tárgyi hatálya kiterjed a Támogatáskezelő informatikai architektúrájára, elektronikus információs rendszereire, beleértve az azokat alkotó

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

valamint a Támogatáskezelő informatikai architektúrájában, elektronikus információs rendszereiben kezelt adatokkal összefüggésben használt bármilyen adatrögzítésre, tárolásra, feldolgozásra vagy továbbításra képes elektronikus információs rendszerre 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.

1.2.3. TERÜLETI HATÁLY

A szabályzat területi hatálya kiterjed a Támogatáskezelő székhelyére, telephelyére valamint valamennyi földrajzi lokációra, ahol a Támogatáskezelő informatikai architektúrája, elektronikus információs rendszerei használatra kerülnek.

1.2.4. 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 negyed éven belül az adott rendszerért, rendszerelemért, beállításért, folyamatért felelős informatikusnak fel kell mérnie és a nem megfelelésről tájékoztatnia kell az IOV-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) a Főigazgató 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 Támogatáskezelő, vagy a Támogatáskezelő informatikai architektúrájának, elektronikus információs rendszereinek 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, ÁFIH, FKV, JI, IOV és az IBF kezdeményezheti.

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

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

1.4. HATÁSKÖRI ÉS ILLETÉKESSÉGI SZABÁLYOK

A szabályzat belső használatú dokumentum: a Támogatáskezelő közalkalmazottjai, illetve egyéb érintettek (a Támogatáskezelővel szerződéses kapcsolatban álló természetes és jogi személyek, más Szervezetek képviseletében a Támogatáskezelő által kontrollált területen tartózkodó személyek) megismerhetik és kezelhetik, de illetékteleneknek nem adhatják tovább és tartalmát illetéktelenekkel nem oszthatják meg.

A Támogatáskezelő valamennyi közalkalmazottja és szerződött partnere köteles végrehajtani a számára kötelező feladatokat, és kerülni a szabályzatban számára nem engedélyezettként jelzett tevékenységeket.

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

1.5. KAPCSOLÓDÓ DOKUMENTUMOK

1.5.1. JOGSZABÁLYOK

- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)
- A közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény
- A köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény
- A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
- A Munka Törvénykönyvéről szóló 2012. évi I. törvény
- A Polgári Törvénykönyvről szóló 2013. évi V. törvény
- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.)
- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet (a továbbiakban. BM rendelet)
- Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény

1.5.2. SZABVÁNYOK, AJÁNLÁSOK

- MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények

2. INFORMÁCIÓBIZTONSÁGI ALAPFOGALMAK

A szabályzatban használt fogalmak, szakkifejezések értelmezése az *1.5.1. Jogszabályok pontban* felsorolt jogforrások alapján az alábbi:

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 adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől feltéve, hogy a technikai feladatot az adatokon végzik;

adatfeldolgozó: az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi;

adatgazda: annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik;

adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése;

adatkezelő: az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajttatja;

adminisztratív védelem: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás;

auditálás: előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;

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;

biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;

biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége;

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

biztonsági szint: a Támogatáskezelő felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

biztonsági szintbe sorolás: a Támogatáskezelő felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese;

A szabályzat alkalmazásában egy elektronikus információs rendszernek kell tekinteni adott adatgazda által, adott cél érdekében az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttesét.

elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

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

észlelés: a biztonsági esemény bekövetkezésének felismerése;

felhasználó: egy adott elektronikus információs rendszert igénybe vevők köre;

fenyegetés: olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;

fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;

folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;

információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti;

IRC: Internet Relay Chat, valós idejű kommunikációt lehetővé tevő hálózati protokoll, nagy számosságú résztvevő számára ideális kommunikációs mód (pl. csatornák, szobák létrehozásával, ahová bárki meghívás és engedély nélkül beléphet, ott kommunikálhat);

IT DRP: informatikai DRP (Disaster Decovery Plan), informatikai katasztrófa utáni helyreállítási terv;

jelszószéf: a jelszószéf a jelszavakat biztonságos adatbázisban tárolja, amelyhez csak egy központi kulcs, az úgynevezett mesterjelszó segítségével lehet hozzáférni – a felhasználónak elegendő ezt az egyetlen jelszót megtanulnia – a széfben tárolt jelszavakat pedig nem szükséges megjegyezni, a jelszószéf tárolja ezeket, valamint beilleszti a kívánt jelszómezőbe a felhasználó helyett;

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

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

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

kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;

korai figyelmeztetés: valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;

kritikus adat: személyes adat, különleges adat vagy valamely jogszabállyal védett adat;

logikai védelem: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;

megelőzés: a fenyegetés hatása bekövetkezésének elkerülése;

reagálás: a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;

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

rendszerterv: az adott rendszerelem hardver-szoftver környezetének leírását, valamint a rendszerelem jelentősebb jellegzetességeit, sajátosságait, kapcsolatait, funkcióit, függőségeit, limitációit tartalmazza;

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

sérülékenység: az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;

sérülékenység-vizsgálat: az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;

SLA: Service Level Agreement, szolgáltatási szint megállapodás, a szolgáltatási szint megfelelőségére vonatkozó leírás, amelyben a megrendelő és a szolgáltató a szerződés megkötésekor megállapodik, és amelyben kitérnek (legalább) arra, hogy a szolgáltatónak mit kell teljesítenie, a teljesítést a megrendelő milyen minőségi kritériumok mentén fogadja el, hogyan fogja a megrendelő ezeket a minőségi kritériumokat mérni, ezen mért minőségi mutatókkal arányosan mekkora számlát fog a szolgáltatótól elfogadni (azaz kölcsönösen meghatározzák a jó teljesítés feltételeit);

softtoken: kétfaktoros azonosításhoz használt olyan információ, amely birtokláson alapuló faktorként kezelhető (a felhasználónál levő mobiltelefonra küldött SMS, a felhasználó számítógépére telepített szoftveres azonosító stb.), de nem szükséges hozzá speciális, csak tokenként használható hardveres eszköz;

SSL: Secure Sockets Layer, a kommunikációnak egy weboldal vagy szoftver és a felhasználók böngészője, kliensprogramja közötti titkosítását végző technológia, amely azon alapul, hogy a weboldalt vagy

szoftvert egy egyedi, biztonságos tanúsítvánnyal azonosítja (hitelesíti), a kommunikációt pedig ennek a tanúsítványnak a felhasználásával titkosítja;

s*úlyos biztonsági esemény:* olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy a Támogatáskezelővel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;

számítógépes eseménykezelő központ: az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik [(európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team), hazai környezetben: NEIH (Nemzeti Elektronikus Információbiztonsági Hatóság)] ;

Szervezet: az adatkezelést végző, illetve az adatfeldolgozást végző vagy végeztető jogi személy vagy egyéni vállalkozó, valamint az üzemeltető;

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

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

védelmi feladatok: megelőzés és korai figyelmeztetés,

VPN: Virtual Private Networks, virtuális magánhálózat, a nyilvános távközlési infrastruktúrán keresztül folytatott biztonságos összeköttetési megoldás.

3. INFORMÁCIÓBIZTONSÁGI ELVÁRÁSOK

3.1. ADMINISZTRATÍV VÉDELMI ELVÁRÁSOK

3.1.1. SZERVEZETI SZINTŰ ALAPFELADATOK

3.1.1.1. Informatikai biztonsági szabályzat

3.1.1.1.1. Informatikai biztonsági szabályzatra vonatkozó alapkövetelmények

A Támogatáskezelő informatikai biztonsági szabályzatát ki kell hirdetni és elérhetővé kell tenni a szabályzat „*1.2.2.2. Személyi hatály*" fejezetében meghatározott személyek számára.

A szabályzatot és a benne előírt dokumentumokat, nyilvántartásokat a Támogatáskezelő 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, mellékletekhez (átfogóan: tartalomhoz) az alábbi személyek férhetnek hozzá:

- Főigazgató,
- Általános Főigazgató-helyettes,
- Főigazgatói kabinetvezető,
- Informatikai osztályvezető ,
- Stratégiai és humánpolitikai igazgató,
- jogi igazgató,
- Operatív igazgató,
- Elektronikus információbiztonsági felelős,
- Védelmi referens,

- Belső ellenőr (ellenőrzés tárgyához kötötten),
- Integritás tanácsadó
- 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 Támogatáskezelőnek ki kell neveznie, meg kell bíznia a Támogatáskezelő elektronikus információs rendszer biztonságáért felelős személyt (információbiztonsági felelőst, vagy IBF-et), aki ellátja az Ibtv. 13. §-ában, valamint az ebben a szabályzatban meghatározott feladatokat.

3.1.1.3. Az intézkedési terv és mérföldkövei

3.1.1.3.1. Az intézkedési tervre vonatkozó alapkövetelmények

A Támogatáskezelőnek a BM rendelet 1. és 2. melléklete, valamint az érvényes OVI táblázatok alapján fel kell mérnie és a nem publikus „1.A. sz. melléklet – Elektronikus információs rendszerek biztonsági osztálya" és „1.B. sz. melléklet – Támogatáskezelő biztonsági szintje" dokumentumokban rögzítenie kell az elektronikus információs rendszereinek biztonsági osztályát és a Támogatáskezelő biztonsági szintjét. A felmérést az IBF koordinálja, akit ebben a tevékenységben az IOV támogat.

Amennyiben a felmérés a célként megadott biztonsági osztályra, illetve biztonsági szintre 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 nem publikus *„2. sz. melléklet – Intézkedési terv"* dokumentumban). Az intézkedési terv készítése az IOV 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 Támogatáskezelő kockázatkezelési stratégiája és a kockázatokra adott válasz tevékenységek prioritása alapján). A felülvizsgálatot az IBF koordinálja, akit ebben a tevékenységben az IOV támogat.

Az ebben a pontban meghatározott feladatok végrehajtásáról az IBF rendszeresen, de legalább évente köteles beszámolni a Támogatáskezelő Főigazgatójának.

3.1.1.4. Az elektronikus információs rendszerek nyilvántartása

3.1.1.4.1. Az elektronikus információs rendszerek nyilvántartására vonatkozó alapkövetelmények

A Támogatáskezelő elektronikus információs rendszereiről nyilvántartást kell vezetni (a nem publikus „3. sz. melléklet – Rendszernyilvántartás" és/vagy az Excel táblázatban meghatározott *„EMET_applications_YYYYMMDD.xlsx"* struktúra alapján) és a nyilvántartást rendszeresen (de legalább negyedévente) aktualizálni szükséges.

A nyilvántartás vezetése és aktualizálása az IOV feladata.

3.1.1.4.2. A nyilvántartás tartalma

A nyilvántartásnak minden rendszerre nézve tartalmaznia kell:

- annak alapfeladatait;
- a rendszerek által biztosítandó szolgáltatásokat;
- az érintett rendszerekhez tartozó licenc számot (ha azok a Támogatáskezelő 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.

A nyilvántartáshoz szükséges adatokat a *„3. sz. melléklet – Rendszernyilvántartás”* dokumentumnak megfelelő struktúrában kell nyilvántartani (bővebb adatkör nyilvántartása – pl. az Excel táblázatban meghatározott *„EMET_applications_YYYYMMDD.xlsx”* struktúrában - lehetséges).

3.1.1.5. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás

A Támogatáskezelő elektronikus információbiztonságát érintő változtatásokat előzetesen engedélyeztetni kell.

Az elektronikus információbiztonsággal kapcsolatos engedélyezésnek ki kell terjednie valamennyi, a Támogatáskezelő hatókörébe tartozó

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

Az engedélyeztetést a változtatást kezdeményezőnek kell indítania. Az engedélyeztetés menetét, részleteit ezen szabályzat *„3.3.6.3.1. A konfigurációváltozások felügyelete (változáskezelés*)” pontja tartalmazza.

3.1.2. KOCKÁZATELEMZÉS

3.1.2.1. Kockázatelemzési és kockázatkezelési eljárásrend

3.1.2.1.1. Kockázatelemzési és kockázatkezelési eljárásrend alapkövetelményei

A Támogatáskezelő 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.

3.1.2.1.2. Az eljárásrend kiterjedése

A kockázatelemzési eljárásrendnek ki kell terjednie

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

3.1.2.2. Biztonsági osztályba sorolás

3.1.2.2.1. Biztonsági osztályba sorolás alapkövetelményei

A Támogatáskezelőnek a jogszabályban meghatározott szempontok alapján meg kell vizsgálnia a „*3.1.1.4. Az elektronikus információs rendszerek nyilvántartása*” pontban leírt követelmények alapján nyilvántartásba vett elektronikus információs rendszereit, és meg kell határoznia, hogy azok melyik biztonsági osztályba sorolandók (lásd a *„3.1.1.3.1. Az intézkedési tervre vonatkozó alapkövetelmények”* pontban leírtakat).

A besorolást az IBF-nek jóvá kell hagytatnia az FI-val . A jóváhagyott besorolást az IBF-nek rögzítenie kell az Információbiztonsági szabályzatban, annak *„1.A. sz. melléklet – Elektronikus információs rendszerek biztonsági osztálya”* (nem publikus) mellékletében.

3.1.2.2.2. Biztonsági osztályba sorolásra vonatkozó elvárások

A Támogatáskezelő elektronikus információs rendszereinek biztonsági osztályba sorolását az elektronikus információs rendszereket érintő jelentős változások után ismételten el kell végezni.

Jelentős változásnak számít az elektronikus információs rendszernek vagy környezetének

- a Támogatáskezelő által korábban nem támogatott alapvető feladatait érintő érdemi funkcionális bővülése (pl. a rendszer a Támogatáskezelő 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 IOV feladata.

Támogatáskezelő elektronikus információs rendszereinek biztonsági osztályba sorolása jelentős változását eredményező változásra kizárólag az IOV előzetes, írásos engedélye alapján kerülhet sor.

Az elektronikus információs rendszer jelentős változását eredményező megrendelést külső vállalkozónak kizárólag az IOV előzetes, írásos engedélyével szabad kiadni; ennek hiányában végzett megrendelés érvénytelen.

A Támogatáskezelő elektronikus információs rendszereinek osztályba sorolási eredményét az *„3.1.1.3. Az intézkedési terv és mérföldkövei”* fejezetben leírt tevékenységek végrehajtásakor fel kell használni.

3.1.2.3. Kockázatelemzés

3.1.2.3.1. Kockázatelemzésre vonatkozó alapkövetelmények

A Támogatáskezelőnek 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 IOV kiemelten támogatja.

4. sz. *melléklet – Informatikai kockázatfelmérési és kockázatkezelési eljárásrend"* alapján kell végezni.

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

A kockázatelemzések eredményét kockázatelemzési jelentésben dokumentálni kell és az IBF-nek meg kell ismertetnie az FI-val és az IOV-vel, valamint a Támogatáskezelő érintett elektronikus információs rendszereinek 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 Támogatáskezelő érintett elektronikus információs rendszereinek üzemeltetőinek és fejlesztőinek aktívan támogatniuk kell.

A kockázatelemzési eredmények kezelése során a *„3.1.1.1.1. Informatikai biztonsági szabályzatra vonatkozó alapkövetelmények"* fejezetben leírtaknak megfelelően kell eljárni, kiemelten biztosítva az eredmények illetéktelen hozzáféréstől védett tárolását, kezelését, azok jogosulatlanok általi elérésének, megismerésének megakadályozását.

3.1.3. ELEKTRONIKUS INFORMÁCIÓS RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS

3.1.3.1. Beszerzési eljárásrend

3.1.3.1.1. Beszerzési eljárásrendre vonatkozó alapkövetelmények

A Támogatáskezelő által megfogalmazott, dokumentált és a Támogatáskezelőn belül kihirdetett általános beszerzési eljárásrendnek („*Emberi Erőforrás Támogatáskezelő Berszerzési és közbeszerzési szabályzata")* a Támogatáskezelő elektronikus információs rendszerére is vonatkoznia kell.

A Támogatáskezelő elektronikus információs rendszerével, 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 IOV feladata koordinálni (hacsak ez a szabályzat egyes pontokban másként nem rendeli).

3.1.3.2. Erőforrás igény felmérés

A Támogatáskezelő az informatikai és a kapcsolódó emberi erőforrás igények felmérését az egyes beszerzési eljárásokhoz kapcsolódóan egyedileg végzi. Az erőforrásigények felmérését az IOV koordinálja.

3.1.3.3. Beszerzések

A Támogatáskezelő informatikai beszerzései kapcsán „*Emberi Erőforrás Támogatáskezelő Beszerzési és közbeszerzési szabályzata""* alapján kell eljárni, az egyedi követelményeket ezen szabályzat elvárásaival kiegészítve szükséges alkalmazni.

3.1.3.4. Az elektronikus információs rendszerre vonatkozó dokumentáció

3.1.3.4.1. Dokumentációs alapkövetelmények

A Támogatáskezelő számára fejlesztett, illetve a Támogatáskezelő által beszerzett elektronikus információs rendszereknek, rendszerelemeknek, szolgáltatásoknak a megfelelő minőségű és biztonságú üzemeltetés és kontroll érdekében megfelelő dokumentációval kell rendelkezniük. Ennek biztosítása érdekében a Támogatáskezelőnek

- ha hatókörébe tartozik, meg kell követelnie és birtokába kell vennie az elektronikus információs rendszerre, 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 elektronikus információs rendszerre, 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 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 Támogatáskezelő által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismeréséről.

3.1.3.5. Külső elektronikus információs rendszerek szolgáltatásai

3.1.3.5.1. Külső elektronikus információs rendszerek szolgáltatásaira vonatkozó alapkövetelmények

A Támogatáskezelőnek a külső elektronikus információs rendszerek 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 Támogatáskezelő által igénybe venni/kifejlesztetni szándékozott elektronikus információs rendszer, szolgáltatás megfelel a Támogatáskezelő által elvárt elektronikus információbiztonsági követelményeknek (az *„5. sz. melléklet – Igénybe vett szolgáltatások, megvásárolt, valamint kifejlesztett rendszerek kapcsán elvárt elektronikus információ-biztonsági követelmények betartásának* vállalása*”* aláírásával).

A partnerekről elvárás a Támogatáskezelő értékrendjének vállalása, valamint az informatikai biztonsággal kapcsolatos alapvető elvárások betartásának vállalása, ezért a szerződéses kapcsolat kezdetén, a szerződés aláírásával egyidejűleg nyilatkoztatni kell őket ezen (*„6. sz. melléklet – Információbiztonsági házirend és nyilatkozat”* dokumentumban részletezett) alapelvek, elvárások

elfogadásáról, betartásáról. A szerződés ezen nyilatkozat aláírásának elmaradása vagy megtagadása esetén nem léptethető életbe.

A Támogatáskezelő által elvárt védelmi intézkedések meglétét és megfelelőségét a Támogatáskezelőnek 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.

A Támogatáskezelőnek meg kell határoznia és dokumentálnia kell a külső elektronikus információs rendszerek szolgáltatásainak igénybe vételével kapcsolatban a Támogatáskezelő munkavállalóinak a feladatait és kötelezettségeit (*„6. sz. melléklet – Információbiztonsági házirend és nyilatkozat”*), amelyeknek megfelelést a Támogatáskezelőnek rendszeresen, de legalább évente, és legalább véletlen mintavétellel ellenőriznie kell, az ellenőrzés eredményét pedig dokumentálnia szükséges.

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

A követelmények betartását az IBF az IOV támogatásával ellenőrzi.

3.1.3.6. Folyamatos és rendszeres ellenőrzés

3.1.3.6.1. Folyamatos és rendszeres ellenőrzés alapkövetelményei

A Támogatáskezelőnek az eseti ellenőrzések mellett folyamatba épített rendszeres és folyamatos ellenőrzéseket is végeznie kell.

A tervezett ellenőrzések kapcsán előre meg kell határozni és kihirdetni (a *„7. sz. melléklet – Tervezett ellenőrzések rendje”* dokumentumnak megfelelően):

- az ellenőrizendő területeket;
- az ellenőrzések, valamint az ellenőrzéseket támogató értékelések gyakoriságát;
- az ellenőrzés végzésének módját;
- az ellenőrzött jellegzetességeket, tevékenységeket, állapotokat - kiemelten a Támogatáskezelő biztonságát befolyásoló jellemzők felmérésére;
- az ellenőrzött jellegzetesség, tevékenység, állapot megfelelő (elfogadható) és nem megfelelő értékeit (ahol lehetséges, számszerűen, mérőszámmal és mértékegységgel; ahol máshogyan nem lehetséges: szabatos leírással);
- a Támogatáskezelő elvárt reagálását a nem megfelelésekre;
- a nem megfelelések létrejöttében, fennmaradásában felelősökkel szemben érvényesítendő szankciókra.

A folyamatos ellenőrzés során gyűjtött adatokat és az azokból készített elemzéseket rendszeresen, de legalább évente be kell mutatni az FI és az ellenőrzött személyek, területek, szervezeti egységek számára (utóbbiaknak a számukra tanulságokat bemutató részletességgel és mértékben).

Az ebben a pontban leírtak végrehajtását a „*3.3.5. Tesztelés, képzés és felügyelet*” fejezetben leírtakkal összhangban kell végezni.

Az ebben a pontban leírtak végrehajtását az IBF-nek kell koordinálnia.

3.1.4. ÜZLETMENET- (ÜGYMENET-) FOLYTONOSSÁG TERVEZÉSE

3.1.4.1. Üzletmenet-folytonosságra vonatkozó eljárásrend

3.1.4.1.1. Üzletmenet-folytonosságra vonatkozó eljárásrend alapkövetelményei

A Támogatáskezelő üzletmenet- (ügymenet) folytonosság tervezése során a jelen eljárásrendben foglaltak szerint kell eljárni.

Az üzletmenet-folytonossági eljárásrend célja, hogy biztosítsa a Támogatáskezelő informatikai infrastruktúrájának, elektronikus információs rendszereinek 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 elektronikus információs rendszerek üzemszerű működésének minél rövidebb időn belüli visszaállítását.

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

3.1.4.2. Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

3.1.4.2.1. Az üzletmenet-folytonossággal kapcsolatos elvárások

A Támogatáskezelőnek el kell készítenie, dokumentálnia, valamint ki kell hirdetnie az elektronikus információs rendszerekre vonatkozó üzletmenet-folytonossági tervet (továbbiakban: informatikai üzletmenet-folytonossági terv, vagy IT BCP), oly módon, hogy az csak a Támogatáskezelőn 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 Támogatáskezelő szakmai/gazdaságitevékenységének folytonosságára készített tervvel (amelynek elkészítése a Támogatáskezelő megfelelő szakmai területeinek feladata).

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

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 Támogatáskezelő 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 elektronikus információs rendszerek működését támogató partnerekben,
    - az elektronikus információs rendszerek 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 Támogatáskezelő informatikai alapfeladatait (a biztosítandó szolgáltatásokat) és alapfunkcióit, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket (a Támogatáskezelő informatikai tevékenység (szolgáltatás) katalógusa alapján – amely a „8.2. sz. melléklet – Informatikai tevékenység (szolgáltatás) katalógus" oldalain részletezett), összhangban a Támogatáskezelő szakmai területei által meghatározott tevékenység katalógussal – amely a *„8.1. sz. melléklet – Tevékenység (szolgáltatás) katalógus"* oldalakon felsorolt);
- definiálni kell, hogyan lehet fenntartani a Támogatáskezelő által előzetesen meghatározott alapszolgáltatásokat akkor is, ha az elektronikus információs rendszer 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 elektronikus információs rendszer 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 elektronikus információs rendszerek élveznek prioritást korlátozott vészhelyzeti működés esetén;
- a katasztrófa elhárítás előfeltételeként elvégzendő mentések rendszerét.

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

3.1.4.3. A folyamatos működésre felkészítő képzés

A Támogatáskezelőnek az elektronikus információs rendszer 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 elektronikus információs rendszer folyamatos működésével kapcsolatos leginkább szükséges tudnivalókat írásban, felhasználó centrikusan összefoglalnia és elérhetővé tennie a felhasználók számára (a *„9. sz. melléklet – Informatikai rendszerek folyamatos működésével kapcsolatos legfontosabb tudnivalók szerkezete”* tartalmával összhangban), például a Támogatáskezelő belső hálózatán, tárhelyén (az Intranet-en).

Az ebben a pontban leírtak végrehajtását az IOV feladata koordinálni.

3.1.4.4. Az elektronikus információs rendszer mentései

3.1.4.4.1. Mentésekkel kapcsolatos elvárások

A Támogatáskezelő elektronikus információs rendszerében 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 Támogatáskezelő elektronikus információs rendszerei és azok működési környezete, beállításai belőlük helyreállíthatóak legyenek a Támogatáskezelő eredeti informatikai infrastruktúráján, vagy egy annak megfeleltethető informatikai környezetben.

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

Amennyiben az adott elektronikus információs rendszerre más eljárást a Támogatáskezelő 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 Támogatáskezelő 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 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 mentésnek alkalmasnak kell lennie arra, hogy a Támogatáskezelő elektronikus információs rendszerei és azok működési környezete, beállításai belőlük helyreállíthatóak legyenek a Támogatáskezelő eredeti informatikai infrastruktúráján, vagy egy annak megfeleltethető informatikai környezetben. (A Támogatáskezelő részletes mentési tervét a *„10. sz. melléklet – Mentési terv”*, nem publikus melléklet alapján kell elkészíteni. A mentési tervet az IO mentések készítéséért felelős munkavállalójának kell elkészítenie.)

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

3.1.4.5. Az elektronikus információs rendszer helyreállítása és újraindítása

3.1.4.5.1. Helyreállítással és újraindítással kapcsolatos elvárások

A Támogatáskezelőnek (közvetlenül vagy megbízottja útján) gondoskodnia kell az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.

Az elektronikus információs rendszer helyreállítási módját, menetét, lépéseit, a szükséges erőforrásokat, azok elvárt közreműködését, a helyreállítás időszükségletét és korlátait megfelelő részletességű leírásban össze kell foglalni (IT DRP), a leírás megfelelőségét pedig legalább éves gyakorisággal végzett teszteléssel ellenőrizni szükséges.

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

3.1.5. A BIZTONSÁGI ESEMÉNYEK KEZELÉSE

3.1.5.1. A biztonsági események kezelésével kapcsolatos elvárások

Ezen szabályzat és a Támogatáskezelő szempontjából biztonsági eseménynek számít valamennyi olyan tett, cselekedet vagy történés, vagy azok elmaradása, amely a Támogatáskezelő elektronikus információs rendszereinek az elvárt rendelkezésre állását, integritását vagy bizalmasságát kedvezőtlenül befolyásolja.

A Támogatáskezelő elektronikus információs rendszereit 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,
- elektronikus információs rendszerelem (hardver) sérülése, megsemmisülése,
- elektronikus információs rendszerben tárolt adat nem kívánt létrehozása/módosítása/törlése
- a szabályzatoknak vagy irányelveknek való nem megfelelés;
- a fizikai 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

A biztonsági események kezelésére megfelelő mértékben fel kell készülni. A racionálisan előre tervezhető lépéseket az IOV koordinálásával előzetesen meg kell határozni (részletesebben lásd a *„3.1.5.5. Biztonsági eseménykezelési terv”* fejezetben).

Az események kezelésekor a lehető leghamarabb mérséklő intézkedésnek kell születnie.

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

Az eseményt az azt észlelőnek haladéktalanul jelezni kell az IOV 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 IOV feladata az esemény kivizsgálásának és dokumentálásának koordinálása. Az IOV 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 Támogatáskezelő informatikai infrastruktúrájának és a benne kezelt adatoknak a zártságát, integritását és rendelkezésre állását.

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

Az IOV feladata ezenkívül a biztonsági események kezelési eljárásait összehangolni az üzletmenet-folytonossági tervhez (IT BCP) 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 fejezetben leírtakat rendszeresen, de legalább évente a megadott felelős(ök)nek felül kell vizsgálni és frissíteni kell.

Az eseménykezelési tervvel kapcsolatban ebben és a kapcsolódó további pontokban előírtakat az eseménykezelési tervben kell pontosan meghatározni (felelősök, időtartamok, folyamatok stb.).

3.1.5.2. A biztonsági események figyelése

A Támogatáskezelő elektronikus információs rendszereit 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.

3.1.5.3. A biztonsági események jelentése

3.1.5.3.1. A biztonsági események jelentésével kapcsolatos elvárások

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 elektronikus információs rendszerek biztonságának felügyeletét ellátó szerveknek (amennyiben az esemény jelentési kötelezettséggel jár).

3.1.5.4. Segítségnyújtás a biztonsági események kezeléséhez

3.1.5.4.1. Tanácsadás és támogatás

Az elektronikus információs rendszer felhasználóinak a biztonsági események kezeléséhez és jelentéséhez az IO munkavállalói támogatást nyújtanak.

3.1.5.5. Biztonsági eseménykezelési terv

3.1.5.5.1. Biztonsági eseménykezelési tervvel kapcsolatos elvárások

A Támogatáskezelő a közalkalmazottjai és partnerei számára a biztonsági események kezelési módjaira iránymutatást adó biztonsági eseménykezelési terve a *„11. sz. melléklet – Biztonsági eseménykezelési terv”* mellékletben található. A tervet az IOV dolgozza ki, az IBF pedig legalább éves rendszerességgel ellenőrzi azt.

A biztonsági eseménykezelési terv ismertetni a biztonsági eseménykezelési lehetőségek struktúráját és Támogatáskezelőét, valamint bemutatja, hogy a biztonsági eseménykezelési lehetőségek hogyan illeszkednek a Támogatáskezelő 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 „*3.3.5. Tesztelés, képzés és felügyelet*” fejezetben 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 elektronikus információs rendszer és a Támogatáskezelő 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.

3.1.5.6. Képzés a biztonsági események kezelésére

3.1.5.6.1. A biztonsági események kezelésével kapcsolatos elvárások

A Támogatáskezelőnek 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, meghatározott időtartamon belül, vagy amikor ezt az elektronikus információs rendszer változásai megkívánják, vagy évente kell megtartani.

3.1.6. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY – BIZTONSÁG

3.1.6.1. Személybiztonsági eljárásrend

A személybiztonsággal kapcsolatos eljárásoknak és elvárásoknak ki kell terjedniük a Támogatáskezelő teljes személyi állományára, valamint minden olyan természetes személyre, aki a Támogatáskezelő elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet.

Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges vagy feltételezhető kapcsolatba kerülő személy nem a Támogatáskezelő közalkalmazottja, a jelen fejezet szerinti elvárásokat a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).

3.1.6.2. Munkakörök, feladatok biztonsági szempontú besorolása

3.1.6.2.1. Munkakörök, feladatok biztonsági szempontú besorolásával kapcsolatos elvárások

A Támogatáskezelőn belüli, nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat fel kell mérni, és valamennyi érintett Támogatáskezelői munkakört, vagy érintett Támogatáskezelőhez kapcsolódó feladatot biztonsági szempontból be kell sorolni a *„12. sz. melléklet – Munkakörök biztonsági szempontú besorolása"* (nem publikus melléklet) leírása alapján. A besorolások során a „42/2021. (IX. 28.) EMMI rendelet az emberi erőforrások minisztere feladat- és hatáskörét érintően a nemzetbiztonsági ellenőrzés alá eső személyek meghatározásáról" jogszabály útmutatása alapján kell eljárni.

A besorolásokat a Stratégiai és humánpolitikai igazgató hajtja végre és küldi a FI-nak jóváhagyásra. A jóváhagyott besorolást a HOV továbbítja az IBF és IOV felé (ezen szabályzat előző bekezdésben említett mellékletének 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.

3.1.6.3 A személyek ellenőrzése

3.1.6.3.1. Személyek ellenőrzésével kapcsolatos elvárások

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

A nemzetbiztonsági ellenőrzés alá tartozó munkaköröket betöltő vagy ilyen feladatokat ellátó személyek tekintetében kezdeményezni kell a nemzetbiztonsági szolgálatokról szóló törvényben meghatározott nemzetbiztonsági ellenőrzést.

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

Az ezen pontban leírtakat a Stratégiai és humánpolitikai igazgató koordinálja.

3.1.6.4 Eljárás a jogviszony létesítése, módosítása és megszűnése esetén

3.1.6.4.1. Jogviszonylétesítésével, megszűnésével és megváltozásával kapcsolatos elvárások

A közalkalmazotti jogviszony kezdetén elvárás a Támogatáskezelő értékrendjének vállalása, valamint az informatikai biztonsággal kapcsolatos alapvető elvárások betartásának vállalása, ezért a jogviszony kezdetén, a kinevezés aláírásával egyidejűleg nyilatkoztatni kell az új belépőket ezen (*„6. sz. melléklet – Információbiztonsági házirend és nyilatkozat"* dokumentumban részletezett) alapelvek, elvárások elfogadásáról, betartásáról. A közalkalmazotti jogviszonyezen nyilatkozat aláírásának elmaradása vagy megtagadása esetén jogviszony nem létesíthető.

Alapelv, hogy minden felhasználó kizárólag a számára mindenképpen szükséges és a feladatai ellátásához elégséges jogosultsággal rendelkezzen, amelynek biztosítása a közalkalmazotti jogviszony esetében az érintett felhasználó közvetlen felettesének, megbízási és vállalkozási szerződéses (partneri) jogviszony esetében a szerződésben kijelölt kapcsolattartó feladata és felelőssége.

Közalkalmazott közalkalmazotti jogviszonyának létesítése esetén az alábbi eljárásrendet kell alkalmazni, informatikai biztonsági szempontból:

- A jogviszony létesítését a HO írásban, a kinevezési okirat érvényessé válását követően haladéktalanul jelzi az IO felé, a Bitrix „Munkavállaló felvételi űrlap" megfelelő kitöltésével és IO-nak küldésével.
- Az új felhasználó informatikai jogosultságait az érintett felhasználó közvetlen felettese igényli a Bitrix „Jogosultságkezelés" űrlap megfelelő kitöltésével és IO-nak küldésével. Az űrlapon fel kell tüntetni az érintett személy munkaügyi azonosítóját is (amely a humánpolitikai rendszer által

generált felhasználói kód), amelyet az IO a felhasználói azonosító létrehozása során köteles rögzíteni valamennyi alkalmazásban (az informatikai felhasználó egyértelmű azonosíthatósága érdekében).

- Amennyiben a jogviszony nem közalkalmazotti jogviszony, hanem más jogviszony, a jelzést a felhasználóval kapcsolatban lévő szervezeti egységnek kell megtennie az IO felé, egyebekben a korábban leírttal megegyező módon.
- A felhasználó e-mail címét, postafiókját a HO igényli a NISZ-től; a létrehozásukra vonatkozó értesítést viszont az IO kapja a NISZ-től, majd állítja be a felhasználónak kiadandó eszközön a felhasználói fiókot és az e-mail elérhetőséget.
- A változásra vonatkozó dokumentált jelzés alapján az IO belső ügyrendjében meghatározott módon a jelzésben meghatározott időpontban létrehozza az érintett felhasználó elektronikus információs rendszerbeli jogosultságait (illetve az IO intézkedik a meghatározott időpontban történő létrehozásáról), beleértve a távoli és a mobiltelefonon keresztül történő hozzáférési lehetőségeket is.
- Az érintett személy egyéni hitelesítő eszközeit az IO belső ügyrendjében meghatározott módon átvételi elismervénnyel adja ki (jogviszony létesítésekor).
- Az érintett személy által használandó, a Támogatáskezelő tulajdonát képező informatikai eszközöket (beleértve a telefont) az IO, a belépőkártyát a HO, a többi eszközt az ÜO adja át az érintettnek, aki azokat átvételi elismervénnyel veszi át.
- A HOV (illetve nem közalkalmazotti jogviszony, hanem más jogviszony esetén a felhasználóval kapcsolatban lévő szervezeti egység vezetője) tájékoztatja a jogviszonyt létesítő személyt a reá vonatkozó, jogi úton is kikényszeríthető kötelezettségekről.

Közalkalmazott közalkalmazotti jogviszonyának módosítása, megszűnése esetén az alábbi eljárásrendet kell alkalmazni, informatikai biztonsági szempontból:

- A jogviszony várható, illetve tényleges változását a HO köteles írásban, a szükséges okiratok érvényessé válását, vagy a jogviszony megszüntetésére vonatkozó döntésnek az érintettel történt közlését követően haladéktalanul jelezni az IO felé, az informatikai Help Desk számára küldött üzenetben. Az üzenetben meg kell adni az
    - az érintett személy személyes adatait és munkaügyi azonosítóját (amely a humánpolitikai rendszer által generált felhasználói kód),
    - a változás tartalmát (jogviszony megszüntetése, tartós távollét stb.),
    - a változásban érintett időszak kezdetét (ha ismert, a várható végdátumát is),
    - a változásnak a felhasználó által kezelt informatikai eszközökkel és jogosultságokkal várhatóan kapcsolatos, beavatkozást igénylő további részleteit.
- Amennyiben a jogviszony nem közalkalmazotti jogviszony, hanem más jogviszony volt, a jelzést a felhasználóval kapcsolatot tartó szervezeti egységnek kell megtennie az IO felé, egyebekben a korábban leírttal megegyező módon.
- A változásra vonatkozó dokumentált jelzés alapján az IO belső ügyrendjében meghatározott módon a jelzésben meghatározott időpontban felfüggeszti/visszavonja az érintett felhasználó elektronikus információs rendszerbeli jogosultságait (illetve az IO intézkedik a meghatározott időpontban történő megszüntetésről), beleértve a távoli és a mobiltelefonon keresztül történő hozzáférési lehetőségeket is.
- Az érintett személy egyéni hitelesítő eszközeit az IO belső ügyrendjében meghatározott módon átvételi elismervénnyel visszaveszi (jogviszony megszüntetésekor, illetve akkor, ha azok nem szükségesek a további munkavégzéshez), és ezt igazolja az adott személy leszerelő lapján.
- Jogviszony megszüntetésekor, illetve akkor, ha a további munkavégzéshez nem szükségesek, az érintett személy az általa használt, a Támogatáskezelő tulajdonát képező informatikai eszközöket (beleértve a telefont) az IO-nak adja le, a belépőkártyát a HO-nak, a többi eszközt az

ÜO-nak, akik azokat átvételi elismervénnyel veszik vissza, és ezt igazolják az adott személy leszerelő lapján.

- Jogviszony megszüntetésekor, illetve akkor, ha a további munkavégzéshez nem szükséges, a felhasználó e-mail címének és postafiókjának megszüntetését a HO igényli a NISZ-től, és hasonlóan a HO kéri az e-mail címre irányuló üzenetek átirányítását (ha ez szükséges). A kérés teljesítését igazoló levelet az IO kapja és az erre vonatkozó igazolást rávezeti az adott személy leszerelő lapjára.
- A leszerelő lapra felvezetett adatokról az IO elektronikus levélben is köteles tájékoztatni a HO-t (a jogviszonyt megszüntető személy által fizikailag a HO-nak átadott, kitöltött leszerelő lap önmagában nem igazolja az eszközök visszavételét, jogosultságok visszavonását).
- A HOV (illetve nem közalkalmazotti jogviszony, hanem más jogviszony esetén a felhasználóval kapcsolatot tartó szervezeti egység vezetője) tájékoztatja a jogviszonyt megszüntető személyt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről. Kilépő közalkalmazott esetében a tájékoztatás írásban is megtörténik, a leszerelőlap átadásával egyidőben a HO által neki átadott nyomtatványon.
- A megszűnő jogviszonyú személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszonyt megszüntető közalkalmazott közvetlen felettese köteles gondoskodni (amennyiben ez szükséges, illetve megoldható);
- Az IO a jogviszony megszűnésekor a megszűnt jogviszonyú személy esetleges elektronikus információs rendszert, 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 HO, 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 Támogatáskezelőn 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 IO-val (a távollét pontos okát nem engedélyezett megosztani),
- az érintett jogosultságát vissza kell vonni / szüneteltetni kell,
- az általa használt eszközöket akkor kell visszavenni, 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 Támogatáskezelőn 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 Támogatáskezelőn belül, sem kívül), amelyet a személy a Támogatáskezelővel 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 közalkalmazott ismételt alkalmazásakor a közalkalmazottnak a korábban használt, felfüggesztett informatikai felhasználói azonosítóit kell visszaadni, annak az ismételt ellenőrzésével, hogy a felhasználó valamennyi korábbi jogosultsága visszavonásra került-e.

A Támogatáskezelőnek meg kell tartania a hozzáférés lehetőségét a kilépő közalkalmazott által korábban használt, kezelt adatokhoz.

3.1.6.5 Az áthelyezések, átirányítások és kirendelések kezelése

3.1.6.5.1. Áthelyezések, átirányítások és kirendelések kezelésével kapcsolatos elvárások

Áthelyezés, átirányítás és kirendelés esetén személyi biztonsági szempontból *„3.1.6.3 A személyek ellenőrzése”* pontban írottaknak megfelelően kell eljárni.

Az áthelyezett, átirányított, kirendelt közalkalmazott 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 *„3.3.10.2.1. Felhasználói fiókok kezelésének alapvető elvárásai”* 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 Támogatáskezelő vonatkozó szabályzatában leírtakat be kell tartani.

3.1.6.6. A Támogatáskezelővel szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények

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

A Támogatáskezelőnek szerződéses kötelezettségként meg kell követelnie, hogy a szerződő fél feleljen meg a Támogatáskezelő által meghatározott személybiztonsági követelményeknek, és ezt dokumentáltan igazolja.

A Támogatáskezelőnek a külső szervezettel kötött megállapodásban, szerződésben elő kell írnia, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik a Támogatáskezelő elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor a változásról soron kívül (egy napon belül) küldjön értesítést a Támogatáskezelőnek; a külső szervezettel kapcsolatot tartón keresztül. Az így beérkező értesítést haladéktalanul el kell juttatni a Támogatáskezelő HOV-hez, az IO-nak (informatikai Help Desk-nek) és az IBF-nek, további intézkedésre (a jogosultságok haladéktalan visszavonása és a visszavonás ellenőrzése érdekében).

A Támogatáskezelőnek folyamatosan ellenőriznie kell a szerződő partner által munkavégzésre, kapcsolattartásra kijelölt munkavállalójának, alvállalkozójának a személybiztonsági követelményeknek való megfelelését – ennek sikeressége érdekében a Támogatáskezelőnek 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 HOV feladata. A külső szervezettel kötött szerződésekben az elvárások szerepeltetése, valamint az elvárások érvényesítése, ellenőrzése a Támogatáskezelő oldaláról az adott szerződésben kijelölt kapcsolattartó feladata; az elvárások szerepeltetésének, érvényesítésének és ellenőrzésének az auditálása az IBF feladata.

3.1.6.7. Munkajogi intézkedések

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

- közalkalmazott esetében munkajogi jogkövetkezmményeket 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 Támogatáskezelő szakmai/gazdasági adatainak illetéktelenekkel való megismertetésével (az adatok nem kompromittálódtak),
- nem járt a Támogatáskezelő által kezelt vagy feldolgozott, természetes személyek személyes adatainak kompromittálódásával,
- nem eredményezte a Támogatáskezelő elektronikus információs rendszerének elérhetőségének és használhatóságának módosítását.

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

- a szabályok megsértése miatt jogosulatlan hozzáférés vagy részletes/teljes adatvesztés történt,
- a felhasználói azonosító vagy beléptetőkártya más számára került átadásra, vagy a használathoz szükséges információ (felhasználói név és jelszó) mással megosztásra került, függetlenül attól, hogy az illetéktelen használat megvalósult-e,

- felhasználói azonosító vagy beléptetőkártya jogosulatlanul került felhasználásra (pl. adott személy más felhasználóhoz tartozó azonosítót próbált használni), függetlenül attól, hogy a próbálkozás sikeres volt-e,
- a Támogatáskezelő elektronikus információs rendszeréhez illetéktelen hozzáférést kíséreltek meg, vagy a meglévő jogosultság módosítását kísérelték meg, függetlenül attól, hogy a próbálkozás sikeres volt-e,
- a Támogatáskezelő elektronikus információs rendszerének illetéktelen módosítását kísérelték meg, függetlenül attól, hogy a próbálkozás sikeres volt-e,
- a Támogatáskezelő elektronikus információs rendszerében tárolt adatokhoz való illetéktelen hozzáférést kíséreltek meg, vagy az adatokat nem a Támogatáskezelő 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 Támogatáskezelő elektronikus információs rendszerében tárolt adatokat illetéktelenen személlyel, szervezettel kísérelték meg megosztani, függetlenül attól, hogy a próbálkozás sikeres volt-e,
- a Támogatáskezelő elektronikus információs rendszerében tárolt adatoknak nem engedélyezett törlését kísérelték meg, függetlenül attól, hogy a próbálkozás sikeres volt-e,
- a Támogatáskezelő elektronikus információs rendszerének elérhetőségét, használhatóságát kísérelték meg módosítani, függetlenül attól, hogy a próbálkozás sikeres volt-e,
- a Támogatáskezelő 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 Támogatáskezelő belső ellenőre, IBF-e által végezni kívánt ellenőrzések és/vagy az azokat végző személyek akadályozása vagy az akadályozás előkészítése történik, függetlenül attól, hogy az akadályozás sikeres-e.

A fenti felsorolásban az „elektronikus információs rendszer" alatt a Támogatáskezelő normál működése során használt elektronikus információs rendszer (lásd a *„2. Információbiztonsági alapfogalmak"* fejezetet) és annak valamennyi eleme, valamint mentése és dokumentációja értendő.

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

3.1.6.8. Belső egyeztetés

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

A tervezés és egyeztetés keretében az IOV az elektronikus információs rendszerrel kapcsolatos tervezésekbe, tevékenységekbe azok minél korábbi fázisába bevonásra kerül, és minden, ilyen rendszereket érintő döntés esetén (különösen szerződéskötéssel vagy megrendeléssel járó művelet előtt) kötelezően ki kell kérni a véleményét.

Az elektronikus információs rendszerekkel kapcsolatos döntések, szerződések, megrendelések és módosítások esetében az IOV és IBF vétójoggal rendelkeznek, amelynek érvényesítéséről kötelesek haladéktalanul beszámolni a Támogatáskezelő FI-nak, aki a vétójoggal megakadályozott tevékenység további sorsáról kizárólagosan jogosult döntést hozni.

3.1.6.9. Viselkedési szabályok az Interneten

A Támogatáskezelő honlapjának oldalainak, felületeinek formai és tartalmi gondozása az FK feladata, más szervezeti egység ezeket kizárólag a Támogatáskezelő FI-nak kifejezett, írásos kérése esetén módosíthatja, illetve rendelheti el a módosításukat.

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

A Támogatáskezelő ezért

- tiltja és számon kéri
    - a Támogatáskezelővel kapcsolatos információk Internet oldalakon és közösségi oldalakon, felületeken való közzétételét;
    - a Támogatáskezelő nevében vagy a Támogatáskezelőhöz kapcsolhatóan végzett információterjesztést,

  amennyiben az nem a Támogatáskezelő által erre kinevezett szervezeti egységek, személyek által, vagy nem a Támogatáskezelő 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 Támogatáskezelőn kívüli megoldásokat; a közlésbe és közzétételbe pedig beleértve valamennyi publikálást vagy elérhetővé tételt);
- tiltja és számon kéri
    - a Támogatáskezelő céljaival, szándékaival, érdekeivel ellentétes információ, tartalom terjesztését,
    - a Támogatáskezelő 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 Támogatáskezelő 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 Támogatáskezelő eszközeivel és/vagy munkaidőben a közösségi oldalak és magán postafiókok, tartalom- és/vagy információ cserélő megoldások használatát/elérését; és egyéb, a Támogatáskezelő szakmai céljaitól idegen tevékenységet.
    - a Támogatáskezelő informatikai eszközeivel, illetve munkaidőben a Támogatáskezelő céljaival és/vagy szándékaival ellentétes információ, tartalom terjesztését, értékelését, minősítését.

3.1.6.10. Etikus információ- és eszközhasználat, etikus kommunikáció

A Támogatáskezelő közalkalmazottjainak és szerződött 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.

A Támogatáskezelő által használt számítógépes hardverek, szoftverek és a Támogatáskezelő digitális rendszerein tárolt információ a Támogatáskezelő vagyonának részei és ennek megfelelően szükséges kezelni őket.

A Támogatáskezelő információs vagyona vagy annak része kizárólag a Támogatáskezelő által felügyelt, kontrollált eszközökön tárolható, kezelhető; a Támogatáskezelő által előírt módon, mértékben és ideig, a Szervezet által meghatározott személyek és szervezeti egységek által. Az ettől eltérő

információtárolást, kezelést annak tudomásul vétele után haladéktalanul jelenteni kell az informatikai Help Desk felé, amely a bejelentésről tájékoztatni köteles az IOV-t és az IBF-t.

Nem szabad betekinteni bizalmas adatokba, kivéve, ha erre a munkatársnak 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 feltételezhető, hogy azok tévesek vagy pontatlanok.

A munka során szerzett bizalmas vagy mások számára hozzá nem férhető információk nem használhatók fel a saját anyagi, vagy más haszonszerzés céljára.

Az elektronikus kommunikáció során be kell tartani a „Netikett" *(„13. sz. melléklet – Netikett: A számítógépes kommunikáció illemszabályai, különös tekintettel az internetre")* előírásait.

Minden kommunikáció során szem előtt kell tartani nem csupán azt, hogy a kommunikációt a Támogatáskezelő egészére vonatkozóan értelmezik vagy értelmezhetik, azt is, hogy a kommunikáció esetleges jogvita során fel is használható.

3.1.7. INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG ÉS KÉPZÉS

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

A Támogatáskezelőnek kapcsolatot kell kialakítania és fenntartania az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és e célt szolgáló ágazati szervezetekkel,

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

érdekében.

A kapcsolattartást az IBF végzi. Amennyiben szükséges a Támogatáskezelő további közalkalmazottjának vagy partnerének bevonása a kapcsolattartásba, az IBF feladata az érintett értesítése és bekapcsolása a kommunikációba.

Amennyiben a kapcsolattartás a Támogatáskezelő Hivatali Kapujának segítségével történik, a Hivatali Kapu használatára kijelölt szervezeti egység, személy köteles támogatóan együttműködni az IBF-fel.

3.1.7.2. Képzési eljárásrend

A Támogatáskezelőnek meg kell fogalmaznia, dokumentálnia és ki kell hirdetni a Támogatáskezelőn belül a képzési eljárásrendet, majd ezt legalább éves gyakorisággal felül kell vizsgálja és frissíteni kell.

A feladatot a HOV-nek kell végeznie.

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

3.1.7.3. Biztonság tudatosság képzés

A Támogatáskezelőnek 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.

3.1.7.4. Munkakör, vagy feladat alapú biztonsági képzés.

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

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

3.1.7.5. A biztonsági képzésre vonatkozó dokumentációk

A Támogatáskezelőnek dokumentálnia kell a biztonságtudatosságra vonatkozó alap-, és munkakör 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 munkavállaló kilépését követő év végéig, vagy külső érintettnél a kapcsolódó szerződés megszűnésétől számított 8 évig.

A megőrzés közalkalmazott esetében a HOV, külső érintett esetében a JCI, illetve az OI feladata.

3.2. FIZIKAI VÉDELMI INTÉZKEDÉSEK

3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM

3.2.1.1. Fizikai védelemmel kapcsolatos alapelvárás

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 Támogatáskezelő székhelyéül és telephelyéül szolgáló irodaháznak csak a Támogatáskezelő által felügyelt, kontrollált területére vonatkoznak.

3.2.1.2. Fizikai védelmi eljárásrend

A Támogatáskezelő az ebben a fejezetben meghatározott módon kívánja definiálni, kezelni, dokumentálni és a Támogatáskezelőn belül kihirdetni az elektronikus információs rendszerek 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 IOV, ellenőrzése az IBF feladata.

3.2.1.3. Fizikai belépési engedélyek.

A Támogatáskezelő a fizikai belépési engedélyeket az alábbiaknak megfelelően rendeli el kezelni:

A Támogatáskezelő székhelyének, telephelyének helyt adó irodaépületbe és a Támogatáskezelő irodai területére való

- rendszeres belépéshez szükséges belépőkártyát közalkalmazott számára a Támogatáskezelő HOV, szerződéses partner részére az ÜO; a parkolási jogosultságot, kulcsot, riasztókódot stb. az ÜO,
- egyedi belépéshez szükséges okmányt, belépőkártyát, parkolási jogosultságot stb. a Támogatáskezelőnek az érintett számára meghívót küldő, vagy őt fogadó közalkalmazottja

intézi a Támogatáskezelő erre vonatkozó előírásai, folyamatai alapján (amennyiben máshogyan nem lehetséges, az informatikai Help Desk, riasztókód és fizikai kulcs esetében az ÜO segítségével), ezért a felsoroltakra vonatkozó igényeket neki(k) kell eljuttatni.

A fizikai belépési engedély kizárólag azon területre vonatkozhat, amelynek látogatása az érintett számára szükséges és engedélyezett. A területi korlátozás érvényesíthetősége érdekében a Támogatáskezelő által kontrollált területet zónákra kell osztani és a belépést csak a szükséges zónákra engedélyezni. A zónákra osztás megvalósítása és a zónák meghatározása az ÜOV feladata.

A kiadott okmány, belépőkártya stb. belépni szándékozónak eljuttatását az azt intéző közalkalmazott köteles elvégezni, vagy személyesen átadva, vagy az érintett számára zárt borítékban, névre szólóan a belépési hely élőerős védelmét biztosító személynél letétbe helyezve.

A rendszeres használatra alkalmas kiadott okmány, belépőkártya, rendszeres (legalább negyedévente egyszeri) felülvizsgálatáról, valamint a nem szükséges okmány, belépőkártya visszavonásáról a Támogatáskezelő HOV köteles gondoskodni.

Törekedni kell rá, hogy a beléptetőkártya a belépésre jogosult neve mellett annak fényképét is tartalmazza, az ellenőrizhetőség megkönnyítése érdekében.

Törekedni kell rá, hogy a közalkalmazottak és a más okból belépésre jogosultak beléptetőkártyája más színű legyen, az ellenőrizhetőség megkönnyítése érdekében.

A fizikai belépés szabályozására szolgáló kulcsoknak szokásos módszerekkel másolhatatlannak kell lenniük.

Belépési engedély nélkül a Támogatáskezelő által kontrollált területre belépni tilos.

A beléptetőkártyát a belépésre jogosult köteles a Támogatáskezelő területén tartózkodás teljes időtartama alatt jól látható, ellenőrzést megkönnyítő módon viselni, és kérésre ellenőrzésre alkalmas módon bemutatni az IO, a biztonsági szolgálat vagy az IBF számára.

A munkavégzést követően leadandó fizikai kulcsokat a Vagyonvédelmi szabályzat részét képező „A kulcskezelés rendje” (XIII. fejezet) előírásainak megfelelően kell kezelni, kiemelten figyelve rá, hogy a kulcsokat átvenni és a kulcsszekrénybe tenni, valamint a kulcsokat a kulcsszekrényből kivenni és a jogosultnak átadni kizárólag a kulcsszekrény fizikai őrzésével (is) megbízott őrszemélyzet feladata. A kulcsok leadása és felvétele során az „önkiszolgálás” tilos.

Beléptetőkártya, riasztókód, fizikai kulcs másnak átadása tilos.

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

A belépési jogosultságot igazoló dokumentum visszavonása, érvénytelenítése, törlése, megsemmisítése iránt a közalkalmazottak esetében a HOV köteles intézkedni. A külső személyek jellemzően vendégkártyával érkeznek a Támogatáskezelő által felügyelt területre, a nekik kiadott belépőkártya egyszeri belépésre jogosít, és távozáskor le kell adni. A vendégkártya a belépőkapu kártyaelnyelő nyílásába helyezéssel automatikusan érvénytelenítésre kerül..

A belépőkártya, „otthon felejtése” esetén az érintett a gyalogos belépésre lehetőséget adó ponton egyszeri belépésre lehetőséget adó vendégkártyát igényelhet, kaphat. A beléptetőkártya hat egymás követő napi „otthonfelejtése” után a beléptetőkártyát elveszettnek kell tekinteni és ennek megfelelően kezelni.

A belépőkártya elvesztését az érintettnek jelentenie kell az IOV-nek, az IBF-nek és a HOV-nek, parkolókártya elvesztését az érintettnek jelentenie kell az IOV-nek, az IBF-nek és az ÜO-nak.

A beléptetőkártya elvesztéséről jegyzőkönyvet kell felvenni, amely tartalmazza a kártya és a birtokosa adatait, valamint a kártya elvesztésének körülményeit.

Az elveszett beléptetőkártya letiltásáról és pótlásáról a HOV intézkedik.

Az elveszett beléptetőkártya díját - annak teljes pótlási költsége alapján- a HO illetve az ÜO vezetőjének kell meghatároznia. A pótlási költség megfizetéséről vagy az ettől való eltekintésről a FI jogosult döntést hozni.

Az IBF az IOV és a HOV 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 Támogatáskezelő előírásai alapján kell kezelni és dokumentálni.

3.2.1.4. A fizikai belépés ellenőrzése

3.2.1.4.1. A fizikai belépés ellenőrzésével kapcsolatos alapvető elvárások

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

- A belépésre jogosultak számára a fizikai belépés kizárólag a Támogatáskezelő által meghatározott be-, és kilépési pontokon biztosított.
- A belépési pontokon a belépést fizikailag megakadályozó, gátló eszközöket kell felszerelni (sorompó, forgóvilla stb.), amelyek csak az engedélyezett belépéseket teszik lehetővé.
- A Támogatáskezelő önmaga vagy ezzel megbízott partnerei által naplózza a fizikai belépéseket.
- A Támogatáskezelőnek ellenőrzés alatt kell tartania a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket, amelybe beletartozik a helyiségek videó megfigyelő rendszerrel való megfigyelése (amennyiben a Támogatáskezelő vagyonvédelmi vagy más okból szükségesnek tartja, a felvételek rögzítésével és előírásainak megfelelő megőrzésével (amelyet *„Az Emberi Erőforrás Támogatáskezelő által alkalmazott elektronikus megfigyelő rendszer által rögzített képekkel és felvételekkel kapcsolatos adatkezelésről”* szóló szabályzat tartalmaz részletesen)).
- Az érvénytelen beléptetőkártya, parkolókártya használatára, valamint az érintett számára nem engedélyezett területre történő belépési kísérletre a beléptetőrendszernek fel kell hívni a belépési ponton szolgálatot teljesítő élőerős biztonsági szolgálat képviselőjének figyelmét, illetve riasztást kell küldeni a meghatározott személyeknek (alapbeállításban az ÜO és az IO kijelölt közalkalmazottjainak). Az érvénytelen belépési kísérletet az élőerős őrzést végző személynek az ilyen esetekre vonatkozó eljárásrendje alapján kell kezelnie.
- A videomegfigyelő, illetve a felvételek rögzítését és visszanézését végző rendszer kezelését a Támogatáskezelő a személyes adatok védelmére vonatkozó, illetve további jogszabályoknak megfelelően köteles szabályozni és végezni. A szabályzás elkészítése a Támogatáskezelő DPO-nak a feladata, az előírások betartása pedig valamennyi érintett kötelessége.
- A Támogatáskezelő által kontrollált területre kizárólag sikeres beléptetést követően szabad lépni; mással együtt végzett belépés, „besurranás”, piggy backing, a belépést korlátozó szerkezet megkerülése vagy hatástalanítása tilos.
- A létesítménybe meghívott, eseti belépésre jogosultakat a Támogatáskezelő számukra meghívót küldő, vagy a meghívó által megbízott közalkalmazottja kíséri, és figyeli a meghívott tevékenységét.
- A rá bízott beléptetőkártyákat, parkolókártyákat, kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző, lehetővé tevő eszközt a Támogatáskezelő valamennyi közalkalmazottja 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 közalkalmazott feladata.
- A fizikai belépést biztosító hozzáférési kódokat és kulcsokat meghatározott rendszerességgel (de legalább negyedévente), vagy haladéktalanul akkor kell megváltoztatni, ha a kulcs elvész, a hozzáférési kód kompromittálódik, vagy az adott személy elveszti a belépési jogosultságát.
- Az egyéni belépési engedélyeket a belépési pontokon ellenőrizni kell.

A Támogatáskezelő közalkalmazottjainak 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 IO belső előírásai szerint kezelik azokat (pl. eljuttatva az ÜO számára).

3.2.1.5. A fizikai hozzáférések felügyelete

3.2.1.5.1. A fizikai hozzáférések felügyeletével kapcsolatos alapvető elvárások

A Támogatáskezelő az ÜOV által

- ellenőrizni rendeli az elektronikus információs rendszereknek helyt adó létesítményekbe 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 Támogatáskezelő 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 JCI feladata; az ellenőrzésre pedig az IBF jogosult.

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

3.2.1.6. A látogatók ellenőrzése

3.2.1.6.1. A látogatók ellenőrzésével kapcsolatos alapvető elvárások

A Támogatáskezelő az elektronikus információs rendszereinek helyt adó létesítményeibe lépő látogatók ellenőrzésével kapcsolatos alapvető elvárásokat az alábbiakban határozza meg:

- A Támogatáskezelő elektronikus információs rendszereknek helyt adó, általa felügyelt létesítményeibe (szerverszoba, informatikai raktár stb.) látogató csak kísérettel léphet be, tartózkodhat. A kísérőnek a látogatót meghívó, vagy általa kijelölt közalkalmazottnak kell lennie.
- A látogatót a Támogatáskezelő erre kijelölt beléptetési pontjain kell fogadnia az őt kísérő közalkalmazottnak, akinek a látogatás adatait nyilvántartásba kell vennie.
- Az elektronikus információs rendszereknek helyt adó létesítményekbe történt látogatói belépésekről szóló információkat egy évig meg kell őrizni, ennek keretében a *„14. sz. melléklet – Látogatók nyilvántartása”* dokumentumnak megfelelően nyilván kell tartani
    - 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 Támogatáskezelő további szabályzatainak, követelményeinek.
- A nyilvántartást egy évig meg kell őrizni, amely az IOV feladata.
- A látogatói belépések nyilvántartásáért, a nyilvántartások kezeléséért, a nyilvántartás és beléptetés részletszabályainak kialakításáért az IOV felelős.
- A látogatói belépésekről készített információkat azonnal át kell vizsgálni, ha a rendelkezésre álló információk jogosulatlan belépésre utalnak – ennek felelőse az IOV.

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

3.2.1.7. Vészvilágítás

A Támogatáskezelő 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 az ÜO felelős.

3.2.1.8. Tűzvédelem

3.2.1.8.1. Tűzvédelem alapvető elvárásai

A tűzvédelemmel kapcsolatos általános előírásokat az Emberi Erőforrás Támogatáskezelő *Tűzvédelmi szabályzata"* belső utasítása tartalmazza. Az ebben a szabályzatban leírt elvárások a Tűzvédelmi szabályzat követelményeit nem helyettesítik, hanem kiegészítik.

A Támogatáskezelő elektronikus információs rendszereinek 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 Támogatáskezelő elektronikus információs rendszereinek helyt adó létesítményeiben alkalmazott tűzelfojtó berendezések automatikus működésűek legyenek.

A Támogatáskezelő elektronikus információs rendszereinek helyt adó létesítményeiben alkalmazott tűzelfojtó berendezések az elektronikus információs rendszereket, illetve az azok működését elősegítő informatikai infrastruktúra elemeket nem károsíthatják, sem működési elvük, sem elhelyezkedésük által.

A pontban leírt elvárás teljesítéséért a Támogatáskezelő tűzvédelmi felelőse felelős.

3.2.1.9. Hőmérséklet és páratartalom ellenőrzés

A Támogatáskezelő 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 IO riasztást kell, hogy kapjon,
- a riasztást incidensként kell kezelni és ki kell rá dolgozni a megfelelő kezelési eljárásokat.

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

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

3.2.1.10.1. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem alapvető elvárásai

A Támogatáskezelő a víz-, és más, csővezetéken szállított anyag okozta kár ellen az elektronikus információs rendszert az alábbiak szerint védi:

- az elektronikus információs rendszert 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 IOV, az Üzemeltetési osztályvezető valamint az IO további, az IOV által írásban kijelölt közalkalmazottja) 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 IOV, illetve az Üzemeltetési Osztályvezető felelős. Az elvárásnak megfelelést az IBF legalább évente ellenőrizni köteles.

3.2.1.11. Be- és kiszállítás

A Támogatáskezelő által kontrollált területre csak az IOV előzetes, írásos engedélyével és az IO közalkalmazottjának jelenlétében szabad információs rendszerelemeket beszállítani, ott elhelyezni, vagy onnan elszállítani.

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

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

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

3.2.1.12. Karbantartók

3.2.1.12.1. Karbantartókkal kapcsolatos alapelvárások

A Támogatáskezelő

- informatikai környezetének és annak elemeinek, valamint az informatikai eszközeinek a karbantartása akkor engedélyezett, ha arra az IOV előzetesen, írásban engedélyt adott vagy azt kérte, elrendelte;
- a karbantartó szervezetekről és személyekről naprakész nyilvántartást vezet;
- megköveteli a hozzáférési jogosultság igazolását az elektronikus információs rendszeren karbantartást végzőktől (az igazolás meglétének és megfelelőségének ellenőrzése a személyes használatra átadott eszközöknél az eszköz használójának a kötelessége, egyéb esetekben a karbantartást végző személyt az IO részéről fogadó és kísérő közalkalmazott feladata);
- felhatalmazást ad a kívánt hozzáférési jogosultságokkal és műszaki szakértelemmel rendelkező közalkalmazottaknak, hogy felügyeljék az általuk használt eszközre vonatkozó, külső partnerek által végzett karbantartási tevékenységet.

Amennyiben a karbantartás során a Támogatáskezelő informatikai környezetéhez, vagy elektronikus információs rendszeréhez hozzá kell férni, és a karbantartást végző hozzáférési jogosultsággal nem rendelkezik, az IO az IOV által kijelölt, megfelelő jogosultsággal és műszaki szakértelemmel rendelkező személy útján köteles támogatni a karbantartást oly módon, hogy a karbantartó által kért műveleteket, tesztelést a Támogatáskezelő informatikai környezetében, elektronikus információs rendszerében elvégzi. A karbantartást támogató személy nem végezhet olyan műveletet, amellyel kárt okoz a Támogatáskezelőnek, vagy közalkalmazottjának, partnerének, vagy amelyet a Támogatáskezelő szabályzatai, vagy jogszabály, hatósági előírás tilt.

Minden olyan esetben, amikor a Támogatáskezelő elektronikus információs rendszerét nem a Támogatáskezelő, hanem megbízásából külső partner üzemelteti, a pontban leírtak érvényesítését a Támogatáskezelő elektronikus információs rendszerét üzemeltető partnernek kell biztosítani. Az erre

vonatkozó szerződéses elvárást a kapcsolódó szerződésekbe be kell építeni, amely elvárás érvényesítése a JI feladata.

3.3. LOGIKAI VÉDELMI INTÉZKEDÉSEK

3.3.1. ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK

3.3.1.1. Általános védelmi intézkedésekkel kapcsolatos alapvető elvárások

A Támogatáskezelő informatikai infrastruktúrájához, informatikai rendszerelemeihez történő hozzáférések ellenőrzése során a jelen eljárásrendben foglaltak szerint kell eljárni.

A Támogatáskezelő az elektronikus információbiztonsággal kapcsolatos (ideértve a rendszer- és felhasználói, külső és belső hozzáférési) engedélyezési eljárási folyamatokat az *„Az infokommunikációs eszközök használatáról szóló szabályzat"* dokumentumban határozta meg. Jelen szabályzatban leírtak ezért az Infokommunikációs *eszközök használatáról szóló* szabályzattal együtt értelmezendők, az elvárásokat együttesen kell alkalmazni.

A Támogatáskezelő célul tűzte ki és törekszik rá, hogy az elektronikus információs rendszer és környezet biztonsági állapota feleljen meg a jelen szabályzatban meghatározott elvárásoknak és közalkalmazottjaitól, partnereitől elvárja, hogy mindenkor ennek megfelelően járjanak el.

A Támogatáskezelő információbiztonsággal összefüggő szerepköreit és felelősségi köreit ezen szabályzatban megfogalmazottak szerint rendeli alkalmazni.

Amennyiben e szabályzat adott pontja máshogyan nem rendeli,

- a Támogatáskezelő informatikai infrastruktúrájához, elektronikus információs rendszereihez hozzáférő valamennyi felhasználó feladata és felelőssége a jelen szabályzatban megfogalmazott védelmi intézkedések alkalmazása, viselkedési elvárások betartása az általa betöltött munkakör keretein belül;
- az új megoldások előkészítése, kidolgozása, bevezetésének koordinálása és ellenőrzése az IO feladata,
- a Támogatáskezelő meglévő elektronikus információs rendszerének üzemeltetésével kapcsolatos tevékenység végrehajtása, illetve annak támogatása az IO feladata,
- a Támogatáskezelő informatikai infrastruktúrájának és elektronikus információs rendszereinek a védelmi elvárásainak ezen szabályzat keretein belüli megfogalmazása és a megvalósítást ellenőrzése az IBF feladata.

A Támogatáskezelő elektronikus információbiztonsági engedélyezési folyamatait integrálni kell a szervezeti szintű kockázatkezelési eljárásba összhangban ezen szabályzattal.

A hozzáférések ellenőrzését az ott leírt személyeknek kell elvégezniük, legalább éves gyakorisággal. Az ellenőrzések megtörténtét és megfelelőségét az IBF feladata legalább éves gyakorisággal ellenőrizni.

3.3.1.2. Elektronikus információbiztonsággal kapcsolatos engedélyezés

Az elektronikus információbiztonsággal kapcsolatos engedélyezést ki kell terjeszteni a Támogatáskezelő hatókörébe tartozó valamennyi

- emberi, fizikai és logikai erőforrásra;
- eljárási és védelmi szintre és folyamatra.

A Támogatáskezelő informatikai architektúrájával, elektronikus információs rendszereivel, erőforrásaival, folyamataival kapcsolatos, elektronikus információbiztonságot érintő engedélyezést ezen szabályzat alapján kell végezni.

Amennyiben bármely, Támogatáskezelőn belül alkalmazott, illetve a Támogatáskezelő működése során felmerülő ilyen jellegű engedélyezés a szabályzatban nincsen meghatározva, az engedélyezést a szabályzat legközelebbi felülvizsgálata során az IOV és az IBF által be kell emelni a szabályzatba.

A Támogatáskezelőben újonnan alkalmazott, elektronikus információbiztonságot érintő engedélyezést úgy kell bevezetni, hogy az engedélyezés az ezen szabályzatban megfogalmazott követelményeknek megfelelően történjen.

3.3.1.3. Az elektronikus információs rendszer kapcsolódásai

3.3.1.3.1. Elektronikus információs rendszerek kapcsolódására vonatkozó alapvető elvárások

A Támogatáskezelő elektronikus információs rendszerét más elektronikus információs rendszerekhez csak szabályozott módon szabad összekapcsolni, az FI, az IOV és az IBF előzetes, írásos hozzájárulásával.

A Támogatáskezelő az ilyen kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát dokumentálni rendeli. A dokumentációt az összekapcsolásban érintett elektronikus információs rendszer üzemeltetőjének, illetve az üzemeltetést támogató külső szervezetnek kell az összekapcsolást megelőzően elkészíteni, az IO koordinálásával.

A Támogatáskezelő elektronikus információs rendszereinek a szabályzat kiadásakor fennálló kapcsolatait az IBF koordinálásával fel kell mérni (a rendszerek üzemeltetését támogató és fejlesztő külső szervezetek bevonásával).

3.3.1.3.2. Belső rendszerkapcsolatok

A Támogatáskezelő elektronikus információs rendszereinek Támogatáskezelőn belüli összekapcsolása szabályozott módon történhet, az FI az IOV és az IBF előzetes, írásos hozzájárulásával.

3.3.1.3.3. Külső kapcsolódásokra vonatkozó korlátozások

A Támogatáskezelő FI-ja a külső elektronikus információs rendszerekhez való kapcsolódásokat az informatikai biztonsági szabályzatban, valamint az IOV és az IBF által egyedileg meghatározott elvárások alapján engedélyezi; amelynek eredménye lehet

- az összes kapcsolat engedélyezése vagy tiltása,
- meghatározott kapcsolatok engedélyezése, illetve
- meghatározott kapcsolatok tiltása.

A külső kapcsolatra vonatkozó korlátozásokat az IOV feladata nyilvántartani és változás esetén aktualizálni. A nyilvántartás meglétét és naprakészségét az IBF-nek legalább évente ellenőriznie szükséges.

3.3.1.4. Személybiztonság

A személybiztonsággal kapcsolatban a Támogatáskezelő által alkalmazott valamennyi eljárást vagy elvárást ki kell terjeszteni a Támogatáskezelő teljes személyi állományára, valamint minden olyan természetes személyre, aki a Támogatáskezelő elektronikus információs rendszereivel (kivéve a Támogatáskezelő honlapjával látogatóként) kapcsolatba kerül, vagy kerülhet.

Azokban az esetekben, amikor a Támogatáskezelő elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem a Támogatáskezelő közalkalmazottja, a személyi biztonsággal kapcsolatos elvárásokat a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell, mint dokumentált kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).

3.3.2. TERVEZÉS

3.3.2.1. Rendszerbiztonsági terv

A Támogatáskezelőnek, ha az elektronikus információs rendszer tervezése a hatáskörébe tartozik, az elektronikus információs rendszerhez rendszerbiztonsági tervet kell készítenie, amely

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

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

3.3.2.1. Cselekvési terv

A Támogatáskezelőnek cselekvési tervet kell készítenie, ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg (azaz valamely elvárás nem, vagy részben teljesül).

A cselekvési tervben dokumentálni kell a megállapított hiányosságok javítására, valamint az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányuló tervezett tevékenységeket.

Az elkészített, meglévő cselekvési terveket legalább éves gyakorisággal frissíteni kell, a biztonsági értékelések, biztonsági hatáselemzések és a folyamatos felügyelet eredményei alapján.

A cselekvési terv készítésének és végrehajtásának, valamint frissítésének koordinálása az IBF feladata, akit az IO támogat ebben a tevékenységében.

3.3.2.2. Személyi biztonság

A személyi biztonsági eljárásrendet rendszeresen, de legalább évente felül kell vizsgálni, aktualizálni kell. A felülvizsgálat és aktualizálás, valamint az eljárásrendnek megfelelő működés ellenőrzés az IBF feladata.

Az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt a hozzáférési jogosultságot igénylő személynek írásban nyilatkoznia kell, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, megértette; és azok betartását, az azoknak való megfelelést vállalja. A nyilatkozatot a közalkalmazottak esetében a HOV, a szerződéses partnerek esetében az adott szerződésben a Támogatáskezelő oldaláról kijelölt kapcsolattartó feladata a hozzáférést igénylővel aláíratni, majd a nyilatkozatot a közalkalmazottak esetében az érintett személy Támogatáskezelőn belüli közalkalmazotti 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 elektronikus információs rendszerhez 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 elektronikus információs rendszerekkel 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 IO feladata mindez.

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

3.3.2.3. Információbiztonsági architektúra leírás

3.3.2.3.1. Információbiztonsági architektúra leírásra vonatkozó alapvető elvárások

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

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

A Támogatáskezelő elektronikus információs rendszerének az információbiztonsági architektúra leírásának elkészítését az IBF koordinálja, a készítést az IO támogatja, és az IOV ellenőrzi az elkészült architektúra leírásokat.

3.3.2.3.2. Az információbiztonsági architektúra leírás tartalma

A z információbiztonsági architektúra leírásnak

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

3.3.3. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS

3.3.3.1. A rendszer fejlesztési életciklusa

3.3.3.1.1. Rendszerfejlesztési életciklussal kapcsolatos alapvető elvárások

A Támogatáskezelő a rendszerek fejlesztési életciklusa kapcsán elrendeli, hogy

- a Támogatáskezelőben alkalmazott elektronikus információs rendszerek teljes életútján, azok minden (alábbiakban meghatározott) életciklus-szakaszában figyelemmel kell kísérni az elektronikus információs rendszerek informatikai biztonsági helyzetét és meg kell tenni a megfelelő intézkedéseket, hogy az elektronikus információs rendszerrel kapcsolatban támasztott információbiztonsági elvárások teljesüljenek;

- a fejlesztési életciklus egészére meg kell határozni és dokumentálni szükséges az információbiztonsági szerepköröket és felelősségeket (*lásd a következő 3.3.3.1.2. pontot*).

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

- milyen információbiztonsági előnyöket/veszélyeket jelentenek a Támogatáskezelő 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 Támogatáskezelőtől 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, elektronikus információs rendszerhez 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 Támogatáskezelő 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 elektronikus információs rendszer(elem) tulajdon- és használati jogával kapcsolatos elvárásokat,
- garanciális és teljesítési követelményeket, továbbá
- azon intézkedéseket, amelyek az információbiztonsági incidensek megelőzését, megakadályozását, hatásának csökkentését szolgálják.

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

Az átvenni tervezett elektronikus információs rendszer(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 IOV 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, elektronikus információs rendszer(elem) szerezhető be (függetlenül annak későbbi használójától, funkciójától és üzemeltetési módjától, körülményeitől), amely megfelel a Támogatáskezelő szabályzataiban, valamint a vonatkozó jogszabályokban, jogforrásokban megfogalmazott követelményeknek. Az elvárásoknak való megfelelésről a szállítót először nyilatkoztatni kell (a következő bekezdésben leírt módon), illetve kétség esetén a követelményeknek megfelelést elbírálását az IO végzi, információbiztonsági funkcionalitású rendszer(elem) esetén az IBF bevonásával.

A Támogatáskezelőnek a szerződéses kötelezettségek keretében a szerződéses partnereitől a szerződéses kapcsolat kezdetekor, a szerződés aláírásával egyidőben meg kell követelnie, hogy a szerződéses partner nyilatkozzon róla, hogy a szolgáltatási szerződés alapján a Támogatáskezelő által igénybe venni/kifejlesztetni szándékozott elektronikus információs rendszer, szolgáltatás megfelel a Támogatáskezelő által elvárt elektronikus információbiztonsági követelményeknek (az *„5. sz. melléklet – Igénybe vett szolgáltatások, megvásárolt, valamint kifejlesztett rendszerek kapcsán elvárt elektronikus információ-biztonsági követelmények betartásának* vállalása*”* aláírásával);.

A partnerektől elvárás a Támogatáskezelő értékrendjének vállalása, valamint az informatikai biztonsággal kapcsolatos alapvető elvárások betartásának vállalása, ezért a szerződéses kapcsolat kezdetén, a szerződés aláírásával egyidejűleg nyilatkoztatni kell őket ezen (*„6. sz. melléklet – Információbiztonsági házirend és nyilatkozat”* dokumentumban részletezett) alapelvek, elvárások elfogadásáról, betartásáról. A szerződés ezen nyilatkozat aláírásának elmaradása vagy megtagadása esetén nem léptethető életbe.

3.3.3.1.2. Rendszerek életciklusa

A Támogatáskezelő a rendszer alábbi életciklus szakaszait határozza, különbözteti meg:

- követelmény meghatározás (amelynek keretében a szakmai (funkcionális) elvárások mellett az IO és az IBF meghatározza a rendszerrel kapcsolatos információbiztonsági elvárásokat);
- fejlesztés vagy beszerzés (amelynek keretében a szállítók felkérésekor, az ajánlatkérés során, valamint az ajánlatok értékelése és a szerződéskötés során az az információbiztonsági szempontokat megfelelően figyelembe kell venni – amelyért az IOV, a JCI vezetője valamint az OI vezetője és az információbiztonsági elemek esetében az IBF a felelős);
- megvalósítás vagy értékelés (amelynek során a fejlesztők, szolgáltatók a korábban megfogalmazott információbiztonsági elvárásokat is megvalósítják, bevezetik – amelyet az IO és információbiztonsági funkcionalitású rendszer(elem) esetén az IBF ellenőriz, kontrollál);
- üzemeltetés és fenntartás (amelynek során az üzemeltetést végző személyeknek, szervezeteknek a Támogatáskezelő általános, és a rendszerrel kapcsolatos egzakt információbiztonsági elvárásait betartva garantálniuk kell a rendszer megfelelő bizalmasságát, integritását és rendelkezésre állását – amelyet az IO rendszeresen, az IBF esetenként, mintavétellel ellenőriz);
- kivonás (archiválás, megsemmisítés) (amelynek keretében az üzemeltetést végző személyeknek, szervezeteknek a Támogatáskezelő általános, és a rendszerrel kapcsolatos egzakt információbiztonsági elvárásait betartva a rendszer beállításait és/vagy üzemeltetési környezetét oly módon kell módosítaniuk, hogy a rendszer legfeljebb csak lekérdezésre legyen használható, az erre meghatározott módon és esetekben, a kijelölt személyek számára – amelyet az IO a kivonást követően majd utána rendszeresen ellenőrzi, az ellenőrzések megtörténtét pedig az IBF esetenként, mintavétellel ellenőrzi).

3.3.3.2. Funkciók, portok, protokollok, szolgáltatások

Ha a Támogatáskezelő külső partnertől informatikai vagy információbiztonsági szolgáltatást tervez igénybe venni, a külső partnernek a „fejlesztés vagy beszerzés” életciklus-szakaszban az ajánlatadás során meg kell határoznia a szolgáltatások igénybevételéhez a Támogatáskezelőtől vagy a

Támogatáskezelő másik szolgáltatójától elvárt, szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat. A követelménynek való megfelelés ellenőrzése az IOV feladata.

3.3.4. BIZTONSÁGI ELEMZÉS

3.3.4.1. Biztonságelemzési eljárásrend

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

A „*Biztonsági elemzés*" pontban meghatározott, biztonságelemzéssel és a biztonságelemzési eljárásrenddel, biztonsági értékeléssel kapcsolatos feladatokat az IBF koordinálja, illetve esetenként végzi, valamint számon kéri a feladatoknak a Támogatáskezelő közalkalmazottjainak vagy támogatást végző külső partnerek általi elvégzését.

A „*Biztonsági elemzés*" pontban meghatározott elvárások teljesülésének, feladatok végrehajtásának az ellenőrzése a Támogatáskezelő Főigazgatójának feladata, amelyet legalább éves gyakorisággal el kell végeznie.

3.3.4.2. Biztonsági értékelések

3.3.4.2.1. Biztonsági értékelések alapvető elvárásai

A Támogatáskezelőnek a biztonsági elemzés keretében

- legalább évente átfogó informatikai auditot kell végeztetnie ,
- legalább évente sérülékenység vizsgálatot kell végeztetnie (ennek keretében ún. black box, grey box és white box vizsgálatot, behatolási teszteket végeztetve);
- legalább évente a biztonsági elemzés keretében gyűjtött információ alapján értékelnie kell az elektronikus információs rendszer és működési környezete védelmi intézkedéseit, kontrollálnia kell a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelő működést;
- el kell készítenie vagy el kell készíttetnie a biztonságértékelés eredményét összefoglaló jelentést;
- gondoskodnia kell róla, hogy a biztonságértékelés eredményét összefoglaló jelentést a Támogatáskezelő vezetése megismerje.

3.3.4.2.2. Biztonsági értékelés tartalma

A biztonsági értékelésnek tartalmaznia kell

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

3.3.4.3. A biztonsági teljesítmény mérése

A Támogatáskezelőnek ki kell fejlesztenie, alkalmaznia és felügyelnie kell az elektronikus információs rendszerei biztonsági mérésének rendszerét, amelybe beleértendő az alkalmazott információbiztonsági megoldások hatékonyságának rendszeres értékelése és az eredményekről a Támogatáskezelő vezetésének a rendszeres tájékoztatása.

3.3.5. TESZTELÉS, KÉPZÉS ÉS FELÜGYELET

A Támogatáskezelő informatikai infrastruktúrájával, elektronikus informatikai rendszerelemeivel kapcsolatos tesztelési, képzési és felügyeleti tevékenységet a Támogatáskezelő jelen szabályzatban, eljárásrendben határozza meg.

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

Az IO feladata elvégezni illetve az elvégzést koordinálni, továbbá (koordinálás esetén) az elvégzést számon kéri a Támogatáskezelő közalkalmazottjaitól vagy támogatást végző külső partnereitől. A feladatok elvégzését, az elvárások teljesülését az IBF-nek támogatnia kell.

A „*Tesztelés, képzés és felügyelet*" pontban meghatározott elvárások teljesülésének, feladatok végrehajtásának az ellenőrzése az IBF feladata, amelyet legalább éves gyakorisággal el kell végeznie.

3.3.5.1. Tesztelés, képzés és felügyelet általános elvárásai

A Támogatáskezelő ezen pontban fogalmazza meg, dokumentálja és hirdeti ki az elektronikus információs rendszer tesztelésével, kapcsolódó képzésével és felügyeletével kapcsolatos eljárásokat, terveket, amelyek támogatják a tesztelési, képzési és felügyeleti tevékenységek

- fejlesztését és fenntartását, valamint azok
- folyamatos időbeni végrehajtását.

A Támogatáskezelőnek a tesztelési, képzési és ellenőrzési terveket a kockázatkezelési stratégia és a lehetséges, vagy bekövetkezett biztonsági események, valamint azon súlyossága alapján legalább évente, de súlyos súlyosságú biztonsági eseményt követően egy hónapon belül felül kell vizsgálnia.

3.3.5.2. A biztonsági teljesítmény mérése

A Támogatáskezelőnek ki kell fejlesztenie, alkalmaznia és felügyelnie kell az elektronikus információs rendszerei biztonsági mérésének rendszerét, amelybe beleértendő az alkalmazott információbiztonsági megoldások hatékonyságának rendszeres értékelése és az eredményekről a Támogatáskezelő vezetésének a legalább negyedéves rendszerességű, írásos és szóbeli tájékoztatása. A tájékoztatás során a mérés módját, menetét és eredményét olyan módon kell bemutatni, hogy azok informatikai és információbiztonsági szakmai végzettség nélkül is érthetők legyenek.

A biztonsági teljesítmény mérése során törekedni kell rá, hogy a mérés

- objektív,
- szubjektív adatokat és értékelést mellőző,
- számszerűsíthető eredményt adó,
- megismételhető, reprodukálható legyen.

A biztonsági teljesítmény mérése során mérni szükséges legalább:

- a hibákhoz kapcsolódóan a vezetői tájékoztatás gyakoriságának kétszeri időtartama alatt
    - az azonosított hibákat havi és súlyosság szerinti bontásban,
    - a hibajavításokat havi és javítási stádium szerinti bontásban,
    - a javítások átlagos és teljes idő- és (ha mérhető) pénzbeli ráfordítás szükségletét havi bontásban,
    - az SLA-t befolyásoló és nem befolyásoló hibák számát havi és információs rendszer(elem) szerinti bontásban,
    - a meghibásodások, javítások miatti SLA sértések teljes időtartamát havi bontásban;
- a karbantartásokhoz kapcsolódóan a vezetői tájékoztatás gyakoriságának időtartama alatt
    - a tervezett és elvégzett karbantartásokat havi és információs rendszer(elem) szerinti bontásban,
    - a karbantartások átlagos és teljes idő- és pénzbeli ráfordításait terv/tény adatokkal, havi bontásban,
    - az SLA-t befolyásoló és nem befolyásoló karbantartások számát havi és információs rendszer(elem) szerinti bontásban,
    - a karbantartások miatti SLA sértések teljes időtartamát havi bontásban;
- a mentésekhez kapcsolódóan a vezetői tájékoztatás gyakoriságának időtartama alatt

- a sikertelen mentések számát
  - online és offline mentések, valamint
  - érintett rendszerelemenkénti bontásban,
- a sikeres és sikertelen visszatöltések számát rendszerelemenkénti bontásban,
- a mentésre felhasznált és a mentésre felhasználható tárterület méretét,
- a mentésre használható tárterület várható használati időtartamát (azaz azt, meddig elegendő a mentésre az ennek rendelkezésére álló tárterület),

- a sérülékenységekhez kapcsolódóan a vezetői tájékoztatás gyakoriságának kétszeri időtartama alatt
  - az azonosított sérülékenységek számát havi és súlyosság szerinti bontásban,
    - az azonosított és a Támogatáskezelőt érintő sérülékenységek számát
      - havi és súlyosság szerinti, valamint,
      - érintett elektronikus információs rendszerelem száma szerinti bontásban,
      - kezelt, megszüntetett és fennálló sérülékenység szerinti bontásban,
  - a sérülékenység publikálásától a sérülékenység kezelésének, megszüntetésének befejezéséig eltelt átlagos és teljes idő- és pénzbeli ráfordítás szükségletét havi bontásban,

- a határvédelmi megoldásokhoz kapcsolódóan a vezetői tájékoztatás gyakoriságának időtartama alatt, havi bontásban
  - a tűzfal által veszélyesnek ítélt és korlátozott kommunikációs kérések számát,
  - a sikertelen VPN kapcsolódások számát felhasználói bontásban,
  - a hálózati hiba miatti kiesések idejét,

- a vírusvédelmi megoldásokhoz kapcsolódóan a vezetői tájékoztatás gyakoriságának időtartama alatt, havi bontásban
  - szerverek, munkaállomások, tabletek és telefonok száma, amelyek
    - rendelkeznek/nem rendelkeznek vírusvédelemmel,
    - aktív/nem aktív a vírusvédelmük,
    - naprakész/nem naprakész a vírusvédelmük,
  - vírusfertőzések száma, ahol
    - vírusmentesítés vagy
    - karanténba helyezés történt,

- a felhasználói azonosítókhoz kapcsolódóan a vezetői tájékoztatás gyakoriságának kétszeri időtartama alatt, havi bontásban
  - a felhasználó azonosítók karbantartásának számát, karbantartási eseménytípusonként (felhasználói azonosító létrehozása, módosítása, zárolása), elektronikus információs rendszerelemek és hónap szerinti bontásban

- a jogosultsági beállításokhoz kapcsolódóan a vezetői tájékoztatás gyakoriságának kétszeri időtartama alatt, havi bontásban

  a jogosultság módosítások számát, módosítási eseménytípusonként (új jogosultság létrehozása, meglévő jogosultság módosítása, jogosultság zárolása, jogosultság visszavonása), elektronikus információs rendszerelemek és hónap szerinti bontásban

3.3.5.3. Sérülékenység teszt

3.3.5.3.1. Sérülékenységi tesztre vonatkozó alapkövetelmények

A Támogatáskezelő elektronikus információs rendszereire és alkalmazásaira sérülékenység vizsgálatot kell végezni vagy végeztetni, ha azt az elektronikus információs rendszerfejlesztési, üzemeltetési és használati körülményei lehetővé teszik.

A sérülékenységi vizsgálatot legalább évente el kell végezni. Ha új lehetséges sérülékenység merül fel az elektronikus információs rendszerrel vagy alkalmazásaival kapcsolatban és annak teljes mértékű megszüntetése nem mondható ki egyértelműen, meg kell ismételni / ismételtetni a sérülékenység tesztet.

A sérülékenység tesztet sérülékenység-vizsgálati eszközök és technikák alkalmazásával, illetve a Kormányzati Eseménykezelő Központ vagy a jogszabályban erre kijelölt, engedélyezett szervezet bevonásával azon elektronikus információs rendszerek kapcsán kell elvégezni, amelyek a Támogatáskezelő felügyelete, irányítása alatt állnak.

A sérülékenységi tesztet végzőnek

- kimutatást kell készítenie a feltárt hibákról és a nem megfelelő konfigurációs beállításokról;
- végre kell hajtania az ellenőrzési listákat és tesztelési eljárásokat;
- fel kell mérnie a sérülékenység lehetséges hatásait;
- elemeznie kell a sérülékenység teszt eredményét;
- meg kell osztania a sérülékenység teszt eredményét az IOV-vel és az IBF-fel, valamint a szervezet kérése esetén a Támogatáskezelő vezetésével.

A sérülékenységi vizsgálat eredménye alapján az IOV-nek a feltárt sérülékenységek kezelésére intézkedési tervet kell készítenie, amelyet az IBF-fel egyeztetést követően be kell mutatnia a Támogatáskezelő vezetésének, amely dönt az intézkedési terv egészének vagy egyes részeinek végrehajtásáról, vagy vállalja a feltárt sérülékenységek jelentette kockázatot, illetve dönt az intézkedési terv Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) részére továbbításáról.

Az elfogadott intézkedési terv (elemek) végrehajtásának koordinálása az IO feladata, amelyet az IOV rendszeresen ellenőriz és támogat. Az intézkedési terv végrehajtását a Támogatáskezelő valamennyi közalkalmazottja és szerződött partnere támogatni köteles, munkaköre, illetve szerződéses tevékenysége keretei között.

3.3.5.3.2. Frissítési képesség

A Támogatáskezelőnek illetve a sérülékenységek feltárását végző partnerének olyan sérülékenység azonosító, felmérő, értékelő eszközt kell alkalmaznia, melynek sérülékenység feltáró képessége könnyen bővíthető az ismertté váló sérülékenységekkel.

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

A Támogatáskezelőnek illetve a sérülékenységek feltárását végző partnerének az elektronikus információs rendszerre vizsgált sérülékenység körét aktualizálnia kell az új tesztet megelőzően, vagy a sérülékenység feltárását követően azonnal.

3.3.5.3.4. Privilegizált hozzáférés

A Támogatáskezelőnek az általa sérülékenység vizsgálatra kijelölt rendszerelemeihez az elektronikus információs rendszer különleges jogosultsághoz kötött - úgynevezett privilegizált - hozzáférést kell biztosítania.

3.3.5.3.5. Felfedhető információk

A sérülékenységet végző szervezetnek, szakembernek, vagy a Támogatáskezelőnek meg kell határoznia, hogy egy támadó milyen információkat képes elérni az elektronikus információs rendszerben, és ennek elhárítására javításokat kell megfogalmaznia, végrehajtania. A javaslatokat a sérülékenységeket feltáró

személynek vagy partnernek az IOV-vel közösen kell elkészítenie, amelyet az IBF-el való egyeztetést követően be kell mutatnia a Támogatáskezelő vezetésének, amely dönt a javaslatok teljes vagy részleges végrehajtásáról, vagy vállalja a feltárt sérülékenységek jelentette kockázatot, kitettséget.

Az elfogadott javaslatok végrehajtásának koordinálása az IOV feladata. A javaslatok végrehajtását kiemelten az IBF, de a Támogatáskezelő valamennyi közalkalmazottja és szerződött partnere támogatni köteles, munkaköre illetve szerződéses tevékenysége keretei között.

3.3.6. KONFIGURÁCIÓKEZELÉS

A konfigurációkezeléssel kapcsolatos elvárások teljesülését az IOV koordinálja.

3.3.6.1. Konfigurációkezelési eljárásrend

3.3.6.1.1. Konfigurációkezelési alapkövetelmények

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

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

A *„3.3.6. KONFIGURÁCIÓKEZELÉS”* pontban meghatározott elvárások teljesülésének, feladatok végrehajtásának az ellenőrzése az IBF feladata, amelyet legalább éves gyakorisággal el kell végeznie.

3.3.6.2. Alapkonfiguráció

3.3.6.2.1. Alapkonfiguráció létrehozása

A Támogatáskezelő az elektronikus információs rendszereihez egy-egy alapkonfigurációt fejleszt ki, dokumentálja és karbantartja azt, valamint leltárba foglalja a rendszer lényeges elemeit.

A Támogatáskezelő elektronikus információs rendszereihez készített alapkonfiguráció dokumentált leírását, telepítőkészleteit biztonságos helyen kell tárolni, ahol csak a telepítést végző közalkalmazott és/vagy külső támogató, valamint az IOV és az IBF fér hozzá. A telepítőkészletek kapcsán a ” *3.3.6.8. 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 legalább évente felül kell vizsgálni és a módosításokat át kell vezetni. A felülvizsgálat és a módosítások átvezetése az IOV feladata, felelőssége. A felülvizsgálatot az IBF-nek ellenőriznie kell.

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

3.3.6.3. A konfigurációváltozások felügyelete (változáskezelés)

3.3.6.3.1. Változáskezelés alapkövetelményei

A Támogatáskezelő informatikai infrastruktúrájában, elektronikus információs rendszerelemei 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 korábbi gyártású eszközére,
    - szerver operációs rendszerének és a kliensek tömeges operációs rendszer cseréje,
    - a szakmai rendszerek működésének jelentős módosítása,
    - a gyártó által kiadott frissítések telepítése,

illetve a gyártó által kiadott frissítések vizsgálata, telepítése valamint a rosszindulatú szoftverek elleni védelmet biztosító rendszer 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 IOV és az adatgazda előzetes, írásos engedélye szükséges
- Az egyes információs rendszerek, rendszerelemek esetében az azok üzemeltetését végző szervezet, szakember feladata a változtatás kezdeményezése, de változtatást kezdeményezhet az IOV 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 IOV számára, aki a kapott információ alapján dönt a változtatás elfogadásáról és arról, szükséges-a biztonsági hatásvizsgálat. Amennyiben igen, azt az IO 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 Támogatáskezelő vállalja, az IOV feladata dönteni róla, hogy a tervezett változtatás tesztelésre kerülhet-e.
- A módosítást az üzemi rendszerekben való alkalmazás előtt tesztkörnyezetben ki kell próbálni (lásd a következő pontot). A tesztelést az érintett elektronikus információs rendszer(elem) üzemeltetést végzőnek kell végeznie, szükség esetén az IO, illetve az IBF bevonásával.
- Az előzetes információ és a teszteredmények alapján az IOV 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 IOV 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 IOV illetve az általa megbízottak feladata nyilvántartásba venni és visszakereshető formában tárolni.

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

3.3.6.3.2. Előzetes tesztelés és megerősítés

A konfiguráció, illetve az elektronikus információs rendszer 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 IOV végzi.

3.3.6.4. Biztonsági hatásvizsgálat

3.3.6.4.1. Biztonsági hatásvizsgálat végrehajtási kötelezettség.

A Támogatáskezelőnek az elektronikus információs rendszerben tervezett változtatásoknak az információbiztonságra való hatását meg kell vizsgálnia és értékelnie kell, még a változtatások megvalósítására vonatkozó döntést megelőzően. Az értékelést az IO végzi, amelyet kérésére az IBF támogat. Az értékelés eredményét az IOV köteles megosztani a változást kezdeményezővel, a tesztelést végzőkkel és az IBF-fel.

3.3.6.5. Konfigurációs beállítások

3.3.6.5.1. Konfigurációs beállításra vonatkozó alapkövetelmények

A Támogatáskezelő informatikai infrastruktúrája, elektronikus információs rendszerei kapcsán az IOV koordinálásával meg kell határozni a működési követelményeknek még megfelelő, de biztonsági szempontból a lehető leginkább korlátozott funkcionalitást (legszűkebb funkcionalitást, a "szükséges minimum" elv alapján), valamint az ehhez tartozó konfigurációs beállítást, amelyet kötelezően alkalmazandó konfigurációként elő kell írni.

Az így meghatározott konfiguráció elemeit az IO tartja nyilván és tájékoztatja arról a Támogatáskezelőn belül az érintetteket, valamint szintén az IO 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 elektronikus információs rendszer valamennyi elemében az adott elemet üzemeltető szervezet, szakember,
- a szakmai üzemeltetést érintő konfigurációs beállításokat az elektronikus információs rendszer valamennyi elemében az adott elem legfőbb szakmai felhasználójának

feladata elvégezni.

Amennyiben a meghatározott elemek konfigurációs beállításaiban eltérés szükséges, az erre vonatkozó írásos igényt az IOV számára kell eljuttatni, aki dönt az eltérés alkalmazhatóságáról. A döntés eredményéről az IOV-nek írásban értesíteni kell a kérelmezőt és a kérelemben érintett rendszerelem üzemeltetőjét. A kérelmet és a döntést, az értesítésekkel együtt az IOV-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.

3.3.6.6. Legszűkebb funkcionalitás

3.3.6.6.1. Legszűkebb funkcionalitás alapkövetelményei

A Támogatáskezelő informatikai infrastruktúráját, úgy kell konfigurálni, hogy csak azok a szolgáltatások, portok, protokollok legyenek engedélyezve, melyek a rendszer biztonságos működéséhez, a szolgáltatások megfelelő igénybe vételéhez szükségesek; minden további szolgáltatást, portot, protokollt tiltani szükséges.

A konfiguráció megváltoztatása változtatásnak minősül, ezért annak végrehajtása során a *„3.3.6.3. A konfigurációváltozások felügyelete (változáskezelés)”* fejezetben leírtakat kell alkalmazni.

A beállítások rendszeres (legalább éves gyakoriságú) ellenőrzése az IBF feladata.

3.3.6.7. Elektronikus információs rendszerelem leltár

3.3.6.7.1. Rendszerelem leltárra vonatkozó alapkövetelmények

A Támogatáskezelő által használt elektronikus információs rendszer 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 és 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 „3. sz. melléklet – Rendszernyilvántartás" dokumentumnak megfelelően.

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 a z IOV feladata.

3.3.6.8. A szoftverhasználat korlátozásai

3.3.6.8.1. Szoftverhasználat alapkövetelményei

A Támogatáskezelő informatikai infrastruktúrájában kizárólag az IOV által engedélyezett, jogtiszta szoftver használható, amelynek használatára vonatkozó licenccel vagy más engedéllyel a Támogatáskezelő rendelkezik.

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

A Szabadon használható vagy nyílt forráskódú szoftverek használatbavételét az IOV 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 IOV illetve a Támogatáskezelő informatikai támogatását végző szervezet képviselője férhet hozzá.

3.3.6.9. A felhasználó által telepített szoftverek

3.3.6.9.1. Felhasználó által telepített szoftverekre vonatkozó alapvető elvárások

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

Erre nem feljogosított felhasználó szoftvert a Támogatáskezelő informatikai infrastruktúrájába nem telepíthet, és ott telepítést nem igénylő, a Támogatáskezelő 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 IOV feladata.

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

3.3.7. KARBANTARTÁS

3.3.7.1.Rendszerkarbantartási eljárásrend

3.3.7.1.1. Rendszerkarbantartási alapkövetelmények

A Támogatáskezelő 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 IOV feladata.

A rendszerkarbantartással kapcsolatos elvárások teljesülését az IOV koordinálja.

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

3.3.7.2. Rendszeres karbantartás

3.3.7.2.1. Rendszeres karbantartás alapkövetelményei

A Támogatáskezelő 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 IOV éves karbantartási tervet készít, az ütemezésbe a szakmai területek képviselőit is bevonva.

Ha a Támogatáskezelő a karbantartást belső erőforrással nem tudja elvégezni, az IOV feladata kezdeményezni a Támogatáskezelő 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 Támogatáskezelő által készített titoktartási nyilatkozatot és dokumentált formában megismerte a Támogatáskezelő 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 IOV feladata kijelölni azt a közalkalmazott 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 IOV előzetes jóváhagyásával szabad elkezdeni.

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

Amennyiben a karbantartáshoz szükséges az elektronikus információs rendszer vagy a rendszerelemek kiszállítása a Támogatáskezelő által kontrollált területről, a kiszállítást előzetesen, írásban engedélyezni szükséges. Az engedélyt az IOV adhatja meg.

Az elektronikus információs rendszer vagy a rendszerelemek kiszállítása előtt azokról valamennyi adatot és információt – ellenőrzött, sikeres mentést követően – visszaállíthatatlan módon törölni kell (a *„3.3.8.3. Adathordozók törlése, megsemmisítése”* 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 IOV 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.

3.3.8. ADATHORDOZÓK VÉDELME

3.3.8.1. Adathordozók védelmére vonatkozó eljárásrend

3.3.8.1.1. Adathordozók védelmére vonatkozó alapkövetelmények.

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

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

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

A Támogatáskezelőben adathordozók beszerzésére kizárólag az IO jogosult.

A közalkalmazottak adathordozó iránti igényét az érintett szervezeti egység vezetőjének írásban kell jeleznie az IOV 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 Támogatáskezelő adathordozóin csak a Támogatáskezelő által jóváhagyott, az adathordozó felelős megőrzőjének feladatainak végrehajtásához szükséges adat tárolható.

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

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

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

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

3.3.8.2. Hozzáférés az adathordozókhoz

A Támogatáskezelő 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, polgári jogi szerződésnek, szabályzatoknak megfelelően
szerverek merevlemezei, a Támogatáskezelő informatikai rendszerein és megosztásain keresztül	informatikai felhasználók	felhasználó által kontrollált adatok írása, módosítása, törlése, a kinevezési okiratnak, polgári jogi szerződésnek, szabályzatoknak megfelelően
hordozható adathordozók	hordozható adathordozó felelős megőrzője	felhasználó által kontrollált adatok írása, módosítása, törlése, a kinevezési okiratnak, polgári jogi szerződésnek, , szabályzatoknak megfelelően
számítógépek adathordozói	a Támogatáskezelő informatikai üzemeltetését támogató szakemberek, szervezetek	az üzemeltetéshez szükséges műveletek, a szerződéseknek, szabályzatoknak megfelelően
számítógépek adathordozói és hordozható adathordozók	IO, IBF	adattartalom ellenőrzése
számítógépek adathordozói és hordozható adathordozók	IO	adattartalom törlése, a szabályzatoknak megfelelően

3.3.8.3. Adathordozók törlése, megsemmisítése

3.3.8.3.1. Adathordozók törlésére, megsemmisítésére vonatkozó alapkövetelmények

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 IOV dönt az eszköz cserére történő kiadhatóságáról vagy megsemmisítéséről.

Az adatok megfelelő módon történő eltávolításáért az adatgazda a felelős. Az adatok eltávolítását az IO végzi, az adatgazda és a felelős megőrző (elérhetetlensége esetén az IOV vagy az IBF) jelenlétében. Az adattörlés az Eraser alkalmazással történik, az alábbiaknak megfelelően:

Adattárolón tárolt információ típusa	Törlési mechanizmus
nem nyilvános információ	a teljes tárterület legalább ötszöri, véletlen adatokkal feltöltése és felülírása
üzleti titok, személyes adat	a teljes tárterület legalább hétszeri, véletlen adatokkal feltöltése és felülírása

Adattárolón tárolt információ típusa	Törlési mechanizmus
nemzetbiztonság által védeni rendelt információ	a teljes tárterület legalább kilencszeres, véletlen adatokkal feltöltése és felülírása

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 IOV-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, erre szolgáló, hitelesített eszközzel (legalább DIN 66399 szabvány szerinti P-3 vágásra alkalmas eszközzel).

3.3.8.4. Adathordozók használata

3.3.8.4.1. Adathordozó használatára vonatkozó alapkövetelmények

A Támogatáskezelő 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, polgári jogi szerződés), és a Támogatáskezelő belső szabályzatai ezt engedélyezik; olyan mértékben és módon, ahogyan az a Támogatáskezelő által elvárt feladatai teljesítéséhez szükséges.

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

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

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

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

Az adathordozók használatát a Támogatáskezelő által megbízott közalkalmazott vagy külső személy, Támogatáskezelő előzetes bejelentés nélkül ellenőrizheti.

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

3.3.9. AZONOSÍTÁS ÉS HITELESÍTÉS

3.3.9.1. Azonosítási és hitelesítési eljárásrend

3.3.9.1.1. Azonosításra és hitelesítésre vonatkozó alapkövetelmények

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

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

3.3.9.2. Azonosítás és hitelesítés

3.3.9.2.1. Egyedi azonosítás és hitelesítés

A Támogatáskezelő elektronikus információs rendszereinek egyedileg azonosítani és hitelesíteni kell a Támogatáskezelő felhasználóit, és a felhasználók által végzett tevékenységet, ennek érdekében a Támogatáskezelő informatikai infrastruktúrájához, elektronikus információs rendszereihez 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. Amennyiben az így képzett felhasználónév megegyezne egy korábbi felhasználónévvel, a vezetéknév első és második karakterét is be kell vonni a felhasználói azonosítóba és így tovább. Azonos neveknél, vagy azonos felhasználói azonosítónál a fent leírt módon képzett felhasználói azonosító végét folytonosan növekvő sorszámmal kell kiegészíteni.

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

A jelszószéfben tárolt jelszavak mentéséről gondoskodni szükséges.

3.3.9.2.2. Hálózati hozzáférés privilegizált fiókokhoz

A Támogatáskezelő elektronikus információs rendszereinek többtényezős hitelesítést kell alkalmazniuk a különleges jogosultsághoz kötött (úgynevezett privilegizált) felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

3.3.9.3. Azonosító kezelés

3.3.9.3.1. Azonosító kezelés alapkövetelményei

A Támogatáskezelő informatikai infrastruktúrájában használt azonosítóknak egyedinek kell lenniük.

A külső partnerek, támogatók, diákmunkások (általánosságban: közalkalmazottakon túli felhasználók) felhasználói azonosítójának tartalmaznia kell az arra vonatkozó jelzést, hogy a felhasználó nem közalkalmazott, hanem külső partner. A felhasználói azonosító Támogatáskezelő 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 IOV feladata.

Az azonosítók ismételt felhasználása tilos.

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

3.3.9.4. A hitelesítésre szolgáló eszközök kezelése

3.3.9.4.1. Hitelesítésre szolgáló eszközök kezelésének alapkövetelményei

A Támogatáskezelő 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.

3.3.9.5.1. Jelszó (tudás) alapú hitelesítés

3.3.9.5.1.1. Jelszó (tudás) alapú hitelesítés alapkövetelményei

A Támogatáskezelő

- 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 60 napig 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).

A Támogatáskezelő informatikai infrastruktúrájában

- az azonosítóhoz tartozó jelszót az IO hozza létre oly módon, hogy kezdeti jelszót állít be az azonosítóhoz;
- az azonosítóhoz tartozó kezdeti jelszót az IO átadja az érintett felhasználónak, amelyet az az első bejelentkezéskor kötelezően megváltoztat VAGY az érintett felhasználó jelenlétében az IO közalkalmazottja belép az eredeti jelszóval, amelyet a felhasználó az IO közalkalmazottja 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, a Támogatáskezelő 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 IOV-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, Qwertzu1, 1Qay2Wsx stb. kerülendő).

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

A Támogatáskezelő 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.

3.3.9.5.2. Birtoklás alapú hitelesítés

3.3.9.5.2.1. Birtoklás alapú hitelesítés alapkövetelményei

A Támogatáskezelő elektronikus információs rendszerében hardver token alapú hitelesítés esetén olyan mechanizmusokat kell alkalmazni, amely megfelel a Támogatáskezelő által meghatározott minőségi követelményeknek, további intézkedésig minimálisan az ezen pontban meghatározott elvárásoknak.

A Támogatáskezelő 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.

3.3.9.5.3. Tulajdonság alapú hitelesítés

Tulajdonság alapú hitelesítés esetén a Támogatáskezelő a felhasználó egyedi azonosítást lehetővé tevő tulajdonságai (arcmás, ujjlenyomat, billentyűzethasználati sajátosság stb.) alapján köteles elvégezni a felhasználó azonosítását és hitelesítését.

Tulajdonság alapú hitelesítés akkor alkalmazható, ha a Támogatáskezelő az általa használt eszközökön a felhasználói bevonásával előzetesen tesztelte és megfelelőnek minősítette az adott tulajdonság alapján való hitelesítést. A megfelelő minősítés során kiemelt figyelmet kell fordítani a false pozitív azonosítások arányára.

Tulajdonság alapú hitelesítés alkalmazása esetén kötelező minden felhasználónak lehetővé tenni a megfelelő felhasználói azonosító-jelszó alapú hitelesítési megoldásokat, a tulajdonság alapú hitelesítést megelőzően vagy legfeljebb azzal egyező időben.

3.3.9.4. A hitelesítésre szolgáló eszköz visszacsatolása

A Támogatáskezelő elektronikus információs rendszerében 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 birtoklásón alapuló eszköz jellegéről, állapotáról.

3.3.9.5. Hitelesítés kriptográfiai modul esetén

A Támogatáskezelő elektronikus információs rendszerének 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.

3.3.9.6. Azonosítás és hitelesítés (Támogatáskezelőn kívüli felhasználók)

3.3.9.6.1. Támogatáskezelőn kívüli felhasználók azonosításával és hitelesítésével kapcsolatos alapkövetelmények

A Támogatáskezelőn kívüli felhasználók elektronikus információs rendszerhez történő hozzáférése során a Támogatáskezelőn belüli felhasználók kapcsán leírtaknak megfelelően kell eljárni, azzal a különbséggel, hogy Támogatáskezelőn kívüli személy részére csak akkor hozható létre felhasználói azonosító, ha

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

3.3.9.6.2. Hitelesítésszolgáltatók tanúsítványának elfogadása

A Támogatáskezelő elektronikus információs rendszerei csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványokat fogadhatják el a Támogatáskezelőn kívüli felhasználók hitelesítéséhez.

3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE

3.3.10.1. Hozzáférés ellenőrzési eljárásrend

3.3.10.1.1. Hozzáférés ellenőrzési eljárásrend alapelvárásai

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

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

3.3.10.2. Felhasználói fiókok kezelése

3.3.10.2.1. Felhasználói fiókok kezelésének alapvető elvárásai

A Támogatáskezelő az informatikai infrastruktúrájában az alábbi fióktípusokat határozza meg:

- Felhasználó (A szokásos ügymenet végrehajtásához szükséges, arra használt felhasználói fiók. A legtöbb közalkalmazott 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 közalkalmazottak tevékenységének eredményét is látják, ellenőrizhetik, monitorozhatják.)
- Adminisztrátor (A kiemelt jogosultságot igénylő, jellemzően informatikai szakértelmet követelő tevékenység elvégzéséhez. Csak az IO néhány közalkalmazottja, valamint a Támogatáskezelő 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.)

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

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

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

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

A felhasználói fiókokat és azonosítókat az IOV-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 Támogatáskezelő elektronikus információs rendszerében felhasználói csoport, levelezőlista vagy új jogosultság (szerepkör) létrehozását kiemelt felhasználó, szervezeti egység vezető vagy adminisztrátor kezdeményezheti, a csoportot, jogosultságot (szerepkört) pedig

- az FI,
- a Főigazgató-helyettesek,

- az Igazgatók,
- az IOV 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).

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.

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.

3.3.10.2.2. Felhasználói jogosultság beállítás és eszközellátás folyamata

Az állásajánlat elfogadását követően a Támogatáskezelő az Infokommunikációs szabályzatban meghatározott módon biztosítja a leendő közalkalmazott számára a felhasználói jogosultságot és a szükséges eszközöket (számítógép és tartozékai, mobiltelefon, SIM kártya).

Az új közalkalmazott fizikai belépőkártyáját a HOV adja ki.

3.3.10.3. Hozzáférés ellenőrzés érvényesítése

A Támogatáskezelő elektronikus információs rendszerének 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 IOV feladata.

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

3.3.10.4. Sikertelen bejelentkezési kísérletek

3.3.10.4.1. Sikertelen bejelentkezési kísérletekre vonatkozó alapkövetelmények

A Támogatáskezelő informatikai infrastruktúrájában a következő fiókzárolási házirendet kell alkalmazni sikertelen bejelentkezési kísérletek esetén:

Szabály megnevezése	Beállított érték
Fiókzárolás küszöbe	3 sikertelen próbálkozás
Fiókzárolás időtartama	30 perc időtartamra
Fiókzárolási számláló nullázása	sikeres bejelentkezést követően

3.3.10.5. A rendszerhasználat jelzése

A Támogatáskezelő informatikai infrastruktúrájába bejelentkező képernyőkön (beleértve az operációs rendszerbe belépést, a távoli kapcsolattal való kapcsolódást és az egyes szakmai informatikai rendszerekbe, alkalmazásokba belépést) a Támogatáskezelő által meghatározott rendszer használatra vonatkozó figyelmeztető üzenetet vagy jelzést kell megjeleníteni, amely jelzi, hogy

- a felhasználó a Támogatáskezelő elektronikus információs rendszerét tervezi használni;
- a rendszerhasználatot a Támogatáskezelő 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 Felhasználói Informatikai Biztonsági Házirendben foglaltakat is.

Az elektronikus információs rendszernek 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 Támogatáskezelő által üzemeltetett, nyilvánosan elérhető elektronikus információs rendszer 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.

3.3.10.6. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

3.3.10.6.1. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek alapkövetelményei

A Támogatáskezelő informatikai infrastruktúrájában, elektronikus információs rendszerében általában nem engedélyezett az azonosítás vagy hitelesítés nélküli tevékenység, kivéve

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

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

Információs rendszerelem	Azonosítás vagy hitelesítés nélkül is végrehajtható felhasználói tevékenység
vendégek számára telepített Wi-Fi használata	a Wi-Fi csak jogszerű, és a Támogatáskezelő szabályzatával megegyező módon használható, ésszerű keretek között, etikus és jó erkölcsbe tartozó tevékenységre
nyilvános honlap használata	a honlapon keresztül publikált információ megismerése, kapcsolattartási adatok alapján kapcsolat felvétele, visszajelzés a Támogatáskezelő tevékenységével kapcsolatban

3.3.10.7. Távoli hozzáférés

3.3.10.7.1. Távoli hozzáférés alapkövetelményei

A Támogatáskezelő informatikai infrastruktúrájához, elektronikus információs rendszeréhez történő távoli hozzáférés a Támogatáskezelő valamennyi közalkalmazottja számára megengedett. A Támogatáskezelőn kívüli felhasználók számára a távoli hozzáférésről a Támogatáskezelő és a külső szervezet közötti szerződésben kell rendelkezni.

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

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

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

A Támogatáskezelő informatikai infrastruktúrájához, elektronikus információs rendszeréhez történő távoli hozzáférés kizárólag olyan informatikai eszköztől megengedett, amely

- a Támogatáskezelő 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.

3.3.10.8. Vezeték nélküli hozzáférés

3.3.10.8.1. Vezeték nélküli hozzáférés alapkövetelményei

A Támogatáskezelő által üzemeltetett vezetéknélküli hálózat

- neve nem utalhat a Támogatáskezelőre, név alapján nem lehet a Támogatáskezelőhöz kapcsolható,
- jelszavát legalább havonta cserélni szükséges és csak a használatra jogosultakkal szabad megosztani.

A Támogatáskezelő közalkalmazottjai a Támogatáskezelő által a vendégek számára biztosított Wi-Fi hálózatot nem használhatják, csak hordozható számítógéppel. A vendég Wi-Fi hálózat nevét és hozzáférési kódját az IO biztosítja az érintett közalkalmazottak 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 IO kérésre támogatást nyújt.

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

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

3.3.10.9. Mobil eszközök hozzáférés ellenőrzése

3.3.10.9. Mobil eszközök hozzáférés ellenőrzésére vonatkozó alapkövetelmények

A Támogatáskezelő valamennyi közalkalmazottja számára megengedett a Támogatáskezelő által nekik használatra adott mobiltelefonról a Támogatáskezelő levelező rendszeréhez való hozzáférés.

A Támogatáskezelőn kívüli felhasználók számára a mobiltelefonnal a Támogatáskezelő levelező rendszeréhez való hozzáférésről a Támogatáskezelő és a külső szervezet közötti szerződésben kell rendelkezni.

A levelezés mobiltelefonon való elérését a Támogatáskezelő valamennyi közalkalmazottja számára biztosítja. A levelezés mobiltelefonnal való eléréséhez szükséges beállításokat az IO végzi el, a mobiltelefon érintett közalkalmazottnak átadása előtt.

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

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

A Támogatáskezelő levelező rendszerének elérésére használt mobiltelefonon kötelező beállítani a legalább négy karakter hosszúságú képernyőzárat.

A mobiltelefonon legfeljebb egy hónapnyi levélmennyiség tárolható, amelyet a megfelelő beállítással kell biztosítani.

A mobiltelefonokról a levelek távoli törlésének lehetőségét meg kell valósítani, és a leveleket az ellopott vagy elhagyott telefonokról törölni kell. Szintén törölni kell a mobiltelefonokon levő vállalati leveleket, ha a mobiltelefont használó közalkalmazott kilép a Támogatáskezelőtől.

3.3.10.10. Külső elektronikus információs rendszerek használata

3.3.10.10.1. Külső elektronikus információs rendszerek használatára vonatkozó alapkövetelmények

A Támogatáskezelő elektronikus információs rendszereihez külső informatikai rendszerből nem engedélyezett hozzáférni.

Amennyiben a Támogatáskezelő elektronikus információs rendszereihez külső informatikai rendszerből való hozzáférési igény a későbbiekben felmerül, az IOV és az IBF bevonásával ki kell dolgozni, hogy milyen feltételek és szabályok betartása mellett biztonságos és engedélyezett a hozzáférés.

3.3.10.11. Nyilvánosan elérhető tartalom

3.3.10.11.1. Nyilvánosan elérhető tartalomra vonatkozó alapkövetelmények

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

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

A Támogatáskezelő honlapján való információ közzétételéről a Támogatáskezelő kabinetvezetője, illetve a szakmai tartalmakért felelős szervezeti egység vezetői döntenek.

A Támogatáskezelő honlapjára a FK keretében tevékenykedő, erre írásban feljogosított közalkalmazottak töltik fel a tartalmat (akiket a szervezeti egység vezetőjének kérésére az IO közalkalmazottjai támogatnak).

A nyilvánosan hozzáférhető elektronikus információs rendszertartalmat a DPO-nak rendszeresen, de legalább félévente 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.

3.3.11. RENDSZER- ÉS INFORMÁCIÓ SÉRTETLENSÉG

3.3.11.1. Rendszer- és információ sértetlenségre vonatkozó alapkövetelmények

A „Rendszer-és információ sértetlenség" fejezetben leírtakat adott elektronikus információs rendszer tekintetében akkor kell alkalmazni, ha az adott elektronikus információs rendszert a Támogatáskezelő üzemelteti.

Amennyiben a Támogatáskezelő adott elektronikus információs rendszerét külső szervezet üzemelteti, az ebben a fejezetben leírtakat a rendszerüzemeltetést végző külső szervezet és a Támogatáskezelő közötti szerződésben szerződéses kötelemként kell érvényesíteni oly módon, hogy az e fejezetben leírt elvárásoknak való megfelelést a külső szervezet biztosítsa.

3.3.11.2. Rendszer- és információsértetlenségre vonatkozó eljárásrend

3.3.11.2.1. Rendszer- és információsértetlenségre vonatkozó eljárásrend alapkövetelményei

A Támogatáskezelő 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.

3.3.11.3. Hibajavítás

3.3.11.3.1. Hibajavításra vonatkozó alapkövetelmények

A Támogatáskezelő informatikai infrastruktúrájában, elektronikus információs rendszereiben 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, a változáskezelés és hibajavítás közötti természetes különbségekre tekintettel.

A hibajavítás nem eredményezhet súlyosabb hibát, mint az elhárítani tervezett hiba.

A hibajavítás adminisztrációjának mértéke enyhíthető, amennyiben a hiba csekély súlyú.

A hibák javítását és kezelését a Támogatáskezelő informatikai támogatását végző külső partnerek végzik oly módon, hogy az egyes partnerek az általuk támogatott informatikai rendszerelemmel kapcsolatos hibákat kötelesek javítani.

A hibajavítást az IOV 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 IO nyilvántartást vezet, amely tartalmazza legalább a hiba leírását és azonosításának idejét, körülményeit.

Javítási tevékenységet csak olyan külső támogató végezhet, amely/aki érvényes szerződéssel vagy megbízással rendelkezik; adathordozóval is kapcsolatos javítás esetén pedig aláírta a Támogatáskezelő által készített titoktartási nyilatkozatot és dokumentált formában megismerte a Támogatáskezelő 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 IOV feladata kijelölni azt a közalkalmazott 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 IOV 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 elektronikus információs rendszer vagy a rendszerelemek kiszállítása a Támogatáskezelő által kontrollált területről, a kiszállítást előzetesen, írásban engedélyezni szükséges. Az engedélyt az IOV adhatja meg.

Az elektronikus információs rendszer 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 IOV 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 Támogatáskezelő üzemi rendszerébe, környezetébe telepítés előtt tesztelni kell annak érdekében, hogy a szoftverfrissítésnek a Támogatáskezelő 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 IOV által.

A biztonsági szoftverfrissítéseket a frissítés kiadását követő egy hónapon belül, a kritikus szoftverfrissítéseket 14 napon belül telepíteni, telepíttetni szükséges. A funkcionális javítást, bővítést tartalmazó szoftverfrissítések telepítéséről az IOV dönt, az adott rendszert, rendszerelemet üzemeltető IO közalkalmazottjának javaslata alapján.

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 IO közalkalmazottnak kell javaslatot tennie, illetve azt az IOV 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 IO közalkalmazott, az IOV és a Támogatáskezelő 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 IOV tájékoztatja a FI-t, aki dönt a további lépésekről.

3.3.11.4. Kártékony kódok elleni védelem

3.3.11.4.1. Kártékony kódok elleni védelem alapkövetelményei

A Támogatáskezelőnek meg kell őriznie az informatikai infrastruktúrájának és az elektronikus információs rendszereinek, valamint a bennük tárolt adatoknak, információnak a bizalmasságát, sértetlenségét és rendelkezésre állását a kártékony kódok és a kéretlen üzenetek támadásaival szemben is.

A Támogatáskezelőnek az informatikai infrastruktúráját és elektronikus információs rendszereit 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 Támogatáskezelő 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 IO közalkalmazott javaslatára, az IOV előzetes, írásos jóváhagyását követően, előzetesen tesztelt módon, az elektronikus 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 figyelembe vételével 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 „*3.3.6. 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 „*3.1.5.5 Biztonsági eseménykezelési terv*" fejezet tartalmazza azzal a kiegészítéssel, hogy a kártékony kódirtó rendszert úgy kell konfigurálni, hogy riasztás esetén automatikusan elektronikus levélben értesítse a Támogatáskezelő helyszíni informatikai támogatását végző szervezet képviselőit és az IOV-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.

3.3.11.5. Az elektronikus információs rendszer felügyelete

3.3.11.5.1. Az elektronikus információs rendszer felügyeletére vonatkozó alapkövetelmény

A Támogatáskezelő informatikai infrastruktúrájának, elektronikus információs rendszereinek üzemeltetésébe beleértendő a működés felügyelete, a mentések elvégzése, illetve hiba esetén az eszközök javítását végzők bevonása.

A Támogatáskezelő informatikai infrastruktúrájának, elektronikus információs rendszereinek 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 Támogatáskezelőnek

- 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 elektronikus információs rendszer jogosulatlan használatát;
- erősíteni kell az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelet észlel;
- meghatározott gyakorisággal biztosítani kell az elektronikus információs rendszer felügyeleti információkat az IOV és az IBF, valamint a Támogatáskezelő informatikai infrastruktúráját, illetve elektronikus információs rendszereit üzemeltetők felé, továbbá (az IOV és az IBF bevonásával, közvetítésével) rendszeresen a Támogatáskezelő felső vezetése számára.

3.3.11.6. Biztonsági riasztások és tájékoztatások

3.3.11.6.1. Biztonsági riasztásokra és tájékoztatásokra vonatkozó alapkövetelmények

A Támogatáskezelőnek

- folyamatosan figyelnie kell a Kormányzati Eseménykezelő Központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;
- folyamatosan figyelemmel kell kísérni a Nemzeti Elektronikus Információbiztonsági Hatóságtól 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.

3.3.11.7. A kimeneti 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 IOV-vel és az IBF-fel közösen javaslatot tesz FI-nak, aki dönt a bevezetendő, alkalmazandó folyamatról és kontroll intézkedésekről. A folyamat véglegesítése, szabályozása és a kontroll intézkedések kidolgozása, bevezetése a javaslatot tevő, valamint az IOV és az IBF feladata, akik saját hatáskörben kötelesen intézkedni az általuk elvégezni jogosult feladatokat, a további feladatok végrehajtását pedig kötelesek megfelelően koordinálni.

3.3.12. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG

3.3.12.1. Naplózási eljárásrend

3.3.12.1.1. Naplózási eljárásrendre vonatkozó alapkövetelmények

A Támogatáskezelő informatikai infrastruktúrájában, elektronikus informatikai rendszerelemeinek 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 IO közalkalmazottjai és az IOV támogatnak.

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

3.3.12.2. Naplózható események

3.3.12.2.1. Naplózható eseményekre vonatkozó alapkövetelmények

A Támogatáskezelő informatikai infrastruktúrájában, elektronikus információs rendszereiben 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 IOV és az IBF évente felülvizsgálja abból a szempontból, hogy a tapasztalatok alapján a naplózott információ elengedő és megfelelő-e a biztonsági események kivizsgálásához.

3.3.12.3. Naplóbejegyzések tartalma

3.3.12.3.1. Naplóbejegyzések tartalmára vonatkozó alapkövetelmények

A Támogatáskezelő elektronikus információs rendszerének 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.

3.3.12.4. Napló tárkapacitás

A naplók tárkapacitását a Támogatáskezelő informatikai infrastruktúrájának, elektronikus információs rendszereinek 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 *„3.3.12.9. A naplóbejegyzések megőrzése”* pontban).

A napló tárkapacitás figyelését az informatikai infrastruktúra, és az elektronikus információs rendszerek 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.

3.3.12.5. Naplózási hiba kezelése

3.3.12.5.1. Naplózási hiba kezelésére vonatkozó alapkövetelmények

A Támogatáskezelő elektronikus információs rendszerét, valamint ennek a naplózási funkcióját úgy kell kialakítani, hogy naplózási hiba esetén riasztást küldjön az IOV 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).

3.3.12.6. Naplóvizsgálat és jelentéskészítés

3.3.12.6.1. Naplóvizsgálatra és jelentéskészítésre vonatkozó alapkövetelmények

A Támogatáskezelő informatikai infrastruktúrájának és elektronikus információs rendszereinek a naplóállományait

- az általános napi üzemeltetési feladatok során az üzemeltetést végzőnek,
- esetenként (de legalább negyedévente az IOV-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 IO közalkalmazott feladata kivizsgálni és kezelni, illetve az IOV-t és az IBF-et tájékoztatni, a „*3.3.11.3. Hibajavítás*” fejezetben leírtak alapján.

A naplóban levő biztonsági eseményeket az érintett rendszer(elem) üzemeltetését végző IO közalkalmazott feladata kivizsgálni és kezelni, illetve az IOV-t és az IBF-et tájékoztatni. A szokatlan működésre és biztonsági eseményre utaló jeleket a „*3.1.5.5 Biztonsági eseménykezelési terv*” fejezetben leírtak alapján kell kezelni.

3.3.12.7. Időbélyegek

3.3.12.7.1. Időbélyegekre vonatkozó alapkövetelmények

A Támogatáskezelő informatikai környezetének és elektronikus információs rendszereinek 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 Támogatáskezelő informatikai környezetét és elektronikus információs rendszereit 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.

3.3.12.8. A naplóinformációk védelme

3.3.12.8.1. Naplóinformáció védelmével kapcsolatos alapkövetelmények

A Támogatáskezelő informatikai infrastruktúráját, elektronikus információs rendszereit és az ezek eseményeit naplózó megoldásokat úgy kell kialakítani, hogy az elektronikus információs rendszer 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, csak adminisztrátor férhet hozzá olvasási jogosultsággal a rögzített naplóinformációhoz (törlésre nem szabad jogosultságot adni számára sem).

3.3.12.9. A naplóbejegyzések megőrzése

A Támogatáskezelő informatikai infrastruktúrájában, elektronikus információs rendszereiben képződött naplóinformációit rendszeresen menteni kell a Támogatáskezelő szokásos mentési rendszere segítségével. A napló tárkapacitással összhangban a mentéseket úgy kell kialakítani, hogy naplóbejegyzések ne vesszenek el.

A központi szerverek naplóállományait félévente legalább egyszer külső, offline tárhelyre kell menteni.

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

A naplóbejegyzéseket legalább 180 naptári napig meg kell őrizni, a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

3.3.12.10. Naplógenerálás

3.3.12.10.1. Naplógenerálásra vonatkozó alapkövetelmények

A Támogatáskezelő informatikai infrastruktúráját, elektronikus információs rendszereit fel kell készíteni a naplózással kapcsolatos alábbi követelmények teljesítésére:

- biztosítania kell a naplóbejegyzések előállítási lehetőségét a „3.3.12.2. Naplózható események” pontban meghatározott naplózható eseményekre, a „3.3.12.3. Naplóbejegyzések tartalma” módon;
- lehetővé kell tennie az üzemeltetésért felelős személyeknek és az IOV, valamint az IBF számára, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az elektronikus információs rendszer egyes elemei esetében;
- naplóbejegyzéseket kell tudnia megőriznie a „3.3.12.9. A naplóbejegyzések megőrzése” és megvédenie a „3.3.12.8. A naplóinformációk védelme” pontban meghatározottak szerint.

3.3.13. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM

3.3.13.1. Rendszer- és kommunikációvédelmi eljárásrend

3.3.13.1.1. Rendszer- és kommunikációvédelmi eljárásrend alapkövetelményei

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

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

3.3.13.2. A határok védelme

3.3.13.2.1. A határok védelmére vonatkozó alapkövetelmények

A Támogatáskezelő informatikai infrastruktúrájának, valamint elektronikus információs rendszereinek határvédelmét tűzfalakkal kell biztosítani oly módon, hogy az informatikai infrastruktúrája és az elektronikus információs rendszerek ne legyenek jogosulatlanul elérhetőek a Támogatáskezelőn

kívülről, az Internet irányából, illetve róluk csak a tűzfalakon keresztül legyen elérhető az Internet vagy más külső hálózat.

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

- a Támogatáskezelő honlapja,
- a szerverek,
- az irodai környezet,
- a szakmai rendszerek (szakrendszerek),
- a mentésre szolgáló rendszerelemek,
- a naplóállományok központi gyűjtését és elemzését biztosító rendszerelemek,
- a rosszindulatú kódok elleni védelmet biztosító központi rendszerelemek,
- a patchelést végző 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 Támogatáskezelő honlapját, illetve a vendég Wi-Fi annak Internet kijáratával együtt a Támogatáskezelő belső informatikai hálózatától elkülönített, de tűzfalakkal szintén védett hálózaton kell üzemeltetni.

A külső és belső tűzfalakat úgy kell konfigurálni, hogy csak a minimálisan szükséges portok, protokollok és szolgáltatások legyenek engedélyezve.

A tűzfalak felügyeletét folyamatosan biztosítani kell.

3.3.13.3. Kriptográfiai kulcs (tanúsítvány) előállítása és kezelése

A Támogatáskezelő informatikai infrastruktúrájában, elektronikus információs rendszereiben alkalmazott kriptográfiához szükséges kriptográfiai kulcsokat, tanúsítványokat a Támogatáskezelőnek a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés-szolgáltatótól kell vásárolnia.

A NISZ által kibocsátott személyi aláíró tanúsítvány igénylését az IO koordinálja, a NISZ erre szolgáló telefonszámát felhívva és a kapott utasításokat követve.

Az IO által igényelt/generált kulcsok szétosztását az IO végzi. A szétosztást dokumentálni és jegyzőkönyvezni kell. A jegyzőkönyvet a kulcsok szétosztását végző személynek, az érintettnek és az IOV-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 IO közös területén kell tárolni, más által nem hozzáférhetően, de valamennyi hozzáférést naplózva,
- a GIRO Zrt. által adott kártyát a Gazdasági igazgató feladata megfelelően tárolni és kezelni,
- minden további típusú tanúsítványt és a használatához szükséges jelszót, kódot, azonosítót stb. az adott személy tanúsítványt használó személy feladata megfelelően tárolni és kezelni.

A Támogatáskezelő 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 Támogatáskezelő 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 Támogatáskezelő kivizsgál és szankcionálhat, a *„3.1.6.7. Munkajogi intézkedések”* fejezetben leírtaknak megfelelően.

A NISZ által kibocsátott, elvesztett vagy ellopott token, 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 IO felé, akik incidensként nyilvántartásba veszik a történteket.

A szükségtelen tanúsítványt dokumentáltan és helyre nem állítható módon meg kell semmisíteni (pl. a megszűnt munkaviszonyú közalkalmazott személyi tanúsítványát vissza kell vonni a NISZ oldalon, a kapcsolódó tokent és kártyát pedig vágással működésképtelenné kell tenni). A megsemmisítésről készített jegyzőkönyvet az IO megsemmisítést végző közalkalmazottja mellett legalább egy másik IO közalkalmazottnak is ellen kell jegyeznie.

A jegyzőkönyvekből valamennyi aláíró számára egy-egy eredeti aláírásokkal ellátott példányt kell biztosítani. A jegyzőkönyveket az azt kapó személynek 8 évig meg kell őriznie.

3.3.13.4. Kriptográfiai védelem

A Támogatáskezelő informatikai infrastruktúrája, elektronikus információs rendszere működtetése során csak olyan kriptográfiai megoldás alkalmazható, mely megfelel az elektronikus aláírásról szóló 2001. évi XXXV. törvény előírásainak, illetve az elektronikus aláírást felügyelő hatóság ajánlásainak és állásfoglalásainak (azaz az elektronikus ügyintézés és bizalmi szolgáltatások általános szabályiról szóló 2015. évi CCXXII. törvény XIX. Fejezetében meghatározott bizalmi listán megtalálható szolgáltató, az ott megadott szolgáltatásra vonatkozóan bocsátotta ki).

3.3.13.5. Együttműködésen alapuló számítástechnikai eszközök

A Támogatáskezelő informatikai infrastruktúrájában, elektronikus információs rendszerei kapcsán az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválása nem engedélyezett, és a távoli aktiválást az elektronikus információs rendszerek beállításai meg kell, hogy akadályozzák.

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

A Támogatáskezelő elektronikus információs rendszerének a név/cím feloldási kérésekre a hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozó kiegészítő adatokat is biztosítania kell.

A Támogatáskezelőn elektronikus információs rendszerének jeleznie kell az utódtartományok biztonsági állapotát is, valamint (ha azok támogatják a biztonságos feloldási szolgáltatásokat) hitelesítenie kell az utód- és elődtartományok közötti bizalmi láncot.

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

A Támogatáskezelő elektronikus információs rendszerének ellenőriznie kell, hogy a név/cím feloldási kérésre a válasz attól a forrástól érkezik-e, amelyhez a feloldási kérést a Támogatáskezelő elküldte (eredethitelesítést és adatsértetlenség ellenőrzést kell kérnie és végrehajtania).

3.3.13.8. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

A Támogatáskezelő név/cím feloldási szolgáltatást nyújtó elektronikus információs rendszerének hibatűrőnek, redundánsnak kell lennie, és meg kell valósítania a belső/külső szerepkör szétválasztást.

3.3.13.9. A maradványinformáció védelme

A Támogatáskezelő elektronikus információs rendszerének védenie kell a Támogatáskezelő által meghatározott maradvány információk bizalmasságát, sértetlenségét.

A Támogatáskezelő ennek keretében védeni rendeli az átmeneti fájlokat és a kimeneti információ véglegest megelőző állapotait, komponenseit.

3.3.13.10. A folyamatok elkülönítése

A Támogatáskezelő elektronikus információs rendszereinek elkülönített végrehajtási tartományt kell fenntartaniuk minden végrehajtó folyamat számára.

Budapest, 2022. május 5.

1.A. SZ. MELLÉKLET – ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGI OSZTÁLYA
Nem publikus melléklet!

A melléklethez kizárólag a következő személyek számára engedélyezett a hozzáférés:

- Főigazgató,
- Általános Főigazgató-helyettes,
- Főigazgatói kabinetvezető,
- Stratégiai és humánpolitikai igazgató,
- Operatív igazgató,
- Jogi igazgató,
- Informatikai osztályvezető ,
- Elektronikus információbiztonsági felelős,
- Belső ellenőr,
- Védelmi referens,
- Integritás tanácsadó

Elektronikus információs rendszer neve	Elektronikus információs rendszer biztonsági osztálya

1.B. SZ. MELLÉKLET – TÁMOGATÁSKEZELŐ BIZTONSÁGI SZINTJE
Nem publikus melléklet!

A melléklethez kizárólag a következő személyek számára engedélyezett a hozzáférés:

- Főigazgató,
- Általános Főigazgató-helyettes,
- Főigazgatói kabinetvezető,
- Stratégiai és humánpolitikai igazgató,
- Operatív igazgató,
- Jogiigazgató,
- Informatikai osztályvezető,
- Elektronikus információbiztonsági felelős,
- Belső ellenőr,
- Védelmi referens,
- Integritás tanácsadó

A Támogatáskezelő

- jelenlegi biztonsági szintje:
- elvárt biztonsági szintje:

2. SZ. MELLÉKLET – INTÉZKEDÉSI TERV
Nem publikus melléklet!

A melléklethez kizárólag a következő személyek számára engedélyezett a hozzáférés:

- Főigazgató,
- Általános Főigazgató-helyettes,
- Főigazgatói kabinetvezető,
- Stratégiai és humánpolitikai igazgató,
- Operatív igazgató,
- Jogi igazgató,
- Informatikai osztályvezető ,
- Elektronikus információbiztonsági felelős,
- Belső ellenőr,
- Védelmi referens,
- Integritás tanácsadó

Szükséges intézkedések:

ID	Érintett pont	Teendő	Felelős	Határidő
1				
2				
3				
4				
5				
6				
7				

Az intézkedési terv felépítése eltérhet a mellékletben bemutatottól, ha a mellékletben szereplő tartalmi elemek megtalálhatóak benne.

3. SZ. MELLÉKLET – RENDSZERNYILVÁNTARTÁS
Nem publikus melléklet!

A melléklethez kizárólag a következő személyek számára engedélyezett a hozzáférés:

- Főigazgató,
- Általános Főigazgató-helyettes,
- Főigazgatói kabinetvezető,
- Stratégiai és humánpolitikai igazgató,
- Operatív igazgató,
- Jogi igazgató,
- Informatikai osztályvezető,
- Elektronikus információbiztonsági felelős,
- Belső ellenőr,
- Védelmi referens,
- Integritás tanácsadó

Rendszernév	
Rendszer alapfeladatai	
Rendszer szolgáltatásai	
Felhasználható licencszám	
Felhasznált licencszám	
Rendszerfelügyelő	
neve	
beosztása	
telefonszáma	
e-mail címe	
Rendszer ***fejlesztője***	
neve	
címe	
cégjegyzékszáma	
adószáma	
kapcsolattartó	
neve	
beosztása	
telefonszáma	
e-mail címe	
Rendszer ***szállítója***	
neve	
címe	
cégjegyzékszáma	
adószáma	
kapcsolattartó	
neve	
beosztása	
telefonszáma	
e-mail címe	
Rendszer ***karbantartója***	
neve	
címe	
cégjegyzékszáma	
adószáma	
kapcsolattartó	
neve	

beosztása	
telefonszáma	
e-mail címe	
Rendszer ***üzemeltetője***	
neve	
címe	
cégjegyzékszáma	
adószáma	
kapcsolattartó	
neve	
beosztása	
telefonszáma	
e-mail címe	

A rendszernyilvántartáshoz használható a mellékletben szereplő táblázatnál bővebb adattartalmú alkalmazásfelmérő Excel táblázat („EMET_applications_20210414_01A.xlsx”) is.

4. SZ. MELLÉKLET – INFORMATIKAI KOCKÁZATFELMÉRÉSI ÉS KOCKÁZATKEZELÉSI ELJÁRÁSREND

Nem publikus melléklet!

A melléklethez kizárólag a következő személyek számára engedélyezett a hozzáférés:

- Főigazgató,
- Általános Főigazgató-helyettes,
- Főigazgatói kabinetvezető,
- Stratégiai és humánpolitikai igazgató,
- Operatív igazgató,
- Jogi igazgató,
- Informatikai osztályvezető,
- Elektronikus információbiztonsági felelős,
- Belső ellenőr,
- Védelmi referens,
- Integritás tanácsadó

M4.1. AZ INFORMATIKAI KOCKÁZATFELMÉRÉS ÉS ÉRTÉKELÉS ALAPELVEI

Az informatikai kockázatfelmérés és értékelés (a továbbiakban együttesen: „***kockázatelemzés***”) tervezése során az alábbi elveket kell követni:

a) 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.
b) A kockázatfelmérés során elsősorban a Támogatáskezelő számára legfontosabb tevékenységekre és az azokat támogató informatikai rendszerelemekre kell fókuszálni, az ilyen tevékenységeket és rendszerelemeket akár a többi rendszerelemnél gyakrabban felmérve, értékelve.
c) 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 (például magas kockázatúnak minősített) tevékenységeket, rendszerelemeket ismételten vizsgálni szükséges.
d) A tervezésnek rugalmasnak kell lennie, azaz a Támogatáskezelő 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.
e) A kockázatfelmérésfelmérés és értékelés tervezésének a Támogatáskezelőre 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 Főigazgatóval egyeztetni, jóváhagyatni szükséges.

M4.2. AZ INFORMATIKAI KOCKÁZATFELMÉRÉS ÉS ÉRTÉKELÉS TERVEZÉSE, ELŐKÉSZÍTÉSE

Az informatikai kockázatfelmérés és értékelés tervezése, valamint a tevékenység során

a) elemezni kell a külső és belső kontrollkörnyezetet annak érdekében, hogy azonosításra kerüljenek az informatikai kockázatfelmérésre és értékelésre vonatkozó elvárások, különösen
    i. a hazai, Európai Unió-n belüli és egyéb nemzetközi *jogszabályi* elvárások,
    ii. a hazai, Európai Unió-n belüli és egyéb nemzetközi *szabványelvárások*,
    iii. a Nemzeti Kulturális Alap stratégiája, célkitűzései, rövid- és hosszú távú feladatai,
    iv. a Támogatáskezelő stratégiája, célkitűzései, rövid- és hosszú távú feladatai,
    v. a Támogatáskezelő működési környezete,

vi. a gazdasági-politikai környezet elvárásai,
vii. a Főigazgató elvárásai.

b) azonosítani kell a lényegi folyamatokat és folyamatgazdákat (az adott folyamat irányításáért, működtetéséért felelős személy),
c) azonosítani kell a releváns informatikai rendszerelemeket és szerepüket a Támogatáskezelő 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. INFORMATIKAI KOCKÁZATFELMÉRÉSI ÉS ÉRTÉKELÉSI CIKLUS

A Támogatáskezelő létfontosságú rendszerelem besorolása (és az emiatt a Támogatáskezelőre vonatkozó jogszabályi követelmények) miatt legalább 2 évente a Támogatáskezelő 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 Támogatáskezelő valamennyi lényegi tevékenységét, rendszerelemét felmérni és értékelni, döntést kell hozni róla, hogy

a) 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),
b) 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,
c) a Támogatáskezelő pótlólagos erőforrást von be a szükséges kockázatfelmérésbe és értékelésbe, intézkedési terv készítésbe.

A döntést az IBF-nek és az IOV-nek kell előkészíteni és a FI elé terjeszteni, aki meghozza a szükséges döntést.

M4.4. INFORMATIKAI KOCKÁZATFELMÉRÉS ÉS ÉRTÉKELÉS TÍPUSAI

A **41/2015. évi BM rendelet** (továbbiakban: BM rendelet) egyik oldalról előírja a rendszeres kockázatelemzés elvégzését, és meghatározza a kockázatelemzés alapelveit, azonban a részletekben nem köti meg az érintett Támogatáskezelő kezét.

A Támogatáskezelő többféle célú és módszerű informatikai kockázatfelmérést és értékelést végezhet; ezekből néhány példa:

a) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) és BM rendelet által meghatározott követelményeknek megfelelés elemzése (compliance jellegű felmérés és értékelés, azaz a valószínűségek nem kerülnek értékelésre) a Támogatáskezelő létfontosságú rendszerelem minősítése miatt,
b) az Ibtv., a BM rendelet által meghatározott követelmények alapján meghatározott nem-megfelelések miatti sérülékenységek értékelése, elemzése (nem compliance jellegű felmérés és értékelés, a sérülékenységek miatt bekövetkező következmények valószínűségeit is figyelembe veszi),
c) az ISO27001 információbiztonsági szabványnak megfelelő kockázatfelmérés és értékelés,
d) egyedi kockázatértékelések (pl. a Főigazgató által meghatározott területek vagy az IBF, esetleg a belső ellenőr által végzett vizsgálatokon azonosított nem-megfelelőségek kockázatfelmérése és értékelése)

M4.4.A LÉTFONTOSSÁGÚ RENDSZERELEM MINŐSÍTÉS MIATTI ELVÁRÁSOKNAK MEGFELELÉS ÉRTÉKELÉSE

A Támogatáskezelő a megfelelés szintjének minél könnyebb követhetősége érdekében a Rendeletben előírt kockázatelemzés mellett megfelelőségi vizsgálatot is végeztethet, amely számszerűsíti, hogy a Rendeletben meghatározott öt biztonsági szint elvárásainak milyen mértékben felel meg az Alap, azaz

a) az adott időszakban mely biztonsági szintnek kell megfelelnie,
b) az elvárt biztonsági szint elvárásai közül melyeknek felelt meg és melyeknek nem,
c) a magasabb (adott időszakban nem kötelezően elérendő) biztonsági szintek elvárásaiból melyeknek felelt meg a Támogatáskezelő (az elvártnál korábban)

A vizsgálat a megfelelőségi kockázatot méri, azaz nem valószínűségalapú.

Az elemzés során az ún. OVI táblázatokat kell használni és az azok alapján azonosított nem-megfelelőségeket kell megfelelően értékelni.

Az ilyen elemzést az IBF feladata elvégezni.

M4.4.B LÉTFONTOSSÁGÚ RENDSZERELEM MINŐSÍTÉS MIATTI KOCKÁZATELEMZÉS

A Támogatáskezelő 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 Létfontosságú rendszerelem minősítés miatti 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.

M4.4.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.

M4.4.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.

M4.5. ADMINISZTRATÍV FELKÉSZÜLÉS

Az egyes kockázatértékelések előtt

a) egyeztetni szükséges a tervezett kockázatértékelés módszerét, időzítését és területét a FI-val és ha az FI egyetért vele, az érintett terület vezetőjével,
b) meg kell határozni a szükséges közreműködőket és a tőlük elvárt közreműködés módját, időszükségletét,
c) el kell kérni és tanulmányozni szükséges a kapcsolódó belső szabályozásokat,
d) el kell kérni és tanulmányozni a kapcsolódó egyéb dokumentációt (munkaköri leírások, nyilvántartások, folyamatleírások, naplók stb. – ezeket az adott ellenőrzés alapján meghatározva)

e) tanulmányozni szükséges a kapcsolódó hazai és nemzetközi jogszabályok aktuális tartalmát,
f) tanulmányozni szükséges a kapcsolódó hazai és nemzetközi szabványok aktuális tartalmát,
g) el kell kérni és tanulmányozni a korábbi informatikai kockázatértékelések és külső/belső ellenőri megállapításokat, valamint a kapcsolódó intézkedési terveket, továbbá azok megvalósítási állapotát,
h) meg kell határozni a kockázatértékeléshez szükséges összegyűjtendő adatokat és azok időtávját, mennyiségét.

M4.6. 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

a) 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
b) a kockázatértékelésben érintett szervezeti egység, külső közreműködő, szolgáltató szabálytalanság vagy csalás gyanújában érintett, vagy
c) az értékelendő tevékenységért felelős szervezeti egység, külső közreműködő, szolgáltató vezetői várhatóan meghiúsítanák az eredményes kockázatértékelést.

M4.7. A KOCKÁZATÉRTÉKELÉS MÓDSZEREINEK MEGHATÁROZÁSA

Az informatikai kockázatértékelés során törekedni kell az egyszerű, áttekinthető módszerek alkalmazására, amely jellemzően

a) előzetes adatgyűjtésen,
b) személyes interjúkon,
c) adatok elemzésén, értékelésén
d) belőlük következtetések levonásán,
e) az értékelésnek az érintett területtel való egyeztetésén és
f) 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.

M4.8. KIEMELT KOCKÁZAT ÉSZLELÉSE ESETÉN KÖVETENDŐ ELJÁRÁS

Amennyiben a kockázatétékelés során kiemelt besorolású kockázatra derül fény, a kockázatértékelést végzőnek

a) haladéktalanul kezdeményeznie kell a tevékenységért felelős személynél a megfelelő kockázatkezelési intézkedés megkezdését,
a) 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).

M4.9. 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 nem-megfeleléseket 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, „mindössze" 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 akceptálható okokból – a késések tényén nem változtatva.)

Egy példa a megállapításra:

- A Támogatáskezelő székházát 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 Támogatáskezelő számára a nem-megfelelés.

Példa: a hiányzó villámhárító (mint nem-megfelelés) lehetséges következménye, hogy

- a Támogatáskezelő székházát villámcsapás érheti,
- ha a Támogatáskezelő székházát 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 a *„M4.11.1.* Nem-megfelelések lehetséges következményének *"* pontban kerülnek bemutatásra.

Lehetséges következmény bekövetkezési valószínűsége

Az azonosított nem-megfelelés nem feltétlenül okoz azonnali következménykárt a Támogatáskezelő számára.

Példa: a hiányzó villámhárító (mint nem-megfelelés) nem jelenti automatikusan, hogy

- a Támogatáskezelő székházát feltétlenül villámcsapás éri, illetve
- ha a Támogatáskezelő székházát villámcsapás éri, ez azonnal vagy néhány napon belül be fog következni,
- a Támogatáskezelő székházát esetlegesen érő villámcsapás feltétlenül tüzet fog okozni vagy valamennyi elektromos készülék teljes és helyreállíthatatlan tönkremeneteléhez vezet, illetőleg a Támogatáskezelő 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 Támogatáskezelő székháza környékén az elmúlt három év során minden nyáron volt vihar és villámcsapás, az nem jelenti automatikusan azt, hogy

- a Támogatáskezelő székháza 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%,
- és hasonlóan:
- a bizonyított megfelelés valószínűsége szintén 100%.

A könnyebb besorolhatóság ás áttekinthetőség érdekében a lehetséges következmény bekövetkezési valószínűségét ötfokozatú skálán határozzuk meg, amelynek részletei a *„M4.11.2. 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 *„M4.11.3*. 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 Támogatáskezelő székházának 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 a *„M4.11.4. Elvárt intézkedés osztályozása a* megvalósítás javasolt időtávja alapján*"* pontban leírtak szerint kell meghatározni.

Ráfordításigény

A javasolt intézkedés ráfordításigényét a „M4.11.5. Elvárt intézkedés osztályozása a megvalósítás várható ráfordításigénye alapján" pontban leírtak szerint kell meghatározni.

Törekedni kell a minél kisebb külső és belső ráfordítást igénylő megoldások javasolására, 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.

M4.10. ELVÁRT INTÉZKEDÉS KEZELÉSE

Az elvárt intézkedés megvalósításáért felelős személyt az intézkedés végrehajtásában a Támogatáskezelő valamennyi közalkalmazottjának és partnerének támogatnia kell, munkakörük és szerződésük mértékéig.

Az elvárt intézkedéseket az IOV nyilvántartja.

Az egyed elvárt intézkedések végrehajtásáért felelős személy a határidő lejáratát megelőzően legfeljebb egy alkalommal írásban, megfelelő indoklással, az IOV-vel és az IBF-fel végzett egyeztetést követően a

FI-tól határidő, illetve feladat módosítást kérhet. A kérelem elfogadásáról vagy elutasításáról a Főigazgató az IOV és az IBF véleményének kikérését követően dönt, és erről tájékoztatja a felelős személyt és az érintett Támogatáskezelői egység vezetőjét is.

A határidő, illetve feladat módosítására vonatkozó kérelem elbírálásának jogát a FI átruházhatja az IOV-re vagy az IBF-re. Az így meghatalmazott személy köteles a FI-nak rendszeresen (de legalább félévente) beszámolni a feladat- és határidő módosítási kérelmekről, valamint azok elfogadásáról vagy elutasításáról.

Az egyes elvárt intézkedések megvalósítását az IOV rendszeresen, de legalább félévente ellenőrzi. A határidőre meg nem valósított elvárt intézkedés végrehajtására az IOV 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 IOV felé.

A felelős az elvárt intézkedés lezárását az elvégzett feladatok megfelelő, írásos, dokumentált igazolásával (bizonyításával) köteles haladéktalanul jelenteni az IOV felé.

A sikeresen teljesítettnek jelentett elvárt intézkedéseket az IOV 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 IOV 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 IOV felé.

Az IBF az elvárt intézkedések kezelése kapcsán gyűjtött tapasztalatairól rendszeresen, de legalább évente köteles beszámolni a FI számára.

M4.11. KOCKÁZATÉRTÉKELÉS SORÁN ALKALMAZOTT OSZTÁLYOZÁSOK

M4.11.1. 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

a) nem várható közvetlen vagy közvetett anyagi kár,
b) nincs külső bizalomvesztés, a probléma kisebb, a Támogatáskezelőn belül marad, és Támogatáskezelőn belül meg is oldható,
c) az érintett elektronikus információs rendszer nem kezel jogszabályok által védett (pl.: személyes) adatot;
d) a hiányosság nem jelent közvetlen veszélyt szakmai célra használt elektronikus információs rendszerre, illetve abban tárolt adatra.

Alacsony besorolású a megállapításban említett állapot, gyakorlat, hiányosság, ha a lehetséges hatásaként

a) a közvetlen és közvetett anyagi kár a Támogatáskezelő költségvetéséhez, szellemi és anyagi erőforrásaihoz képest alacsony,
b) az esetlegesen lehetséges társadalmi-politikai hatás a Támogatáskezelőn belül kezelhető;
c) az üzlet-, vagy ügymenet szempontjából csekély értékű, és/vagy csak belső (Támogatáskezelőre vonatkozó) szabályzattal védett adat vagy elektronikus információs rendszer elérése, rendelkezése állása, bizalmassága sérülhet,
d) téves belső következtetés levonásához vezethet a Támogatáskezelő által használt elektronikus információs rendszer jellemzőiről.

Közepes besorolású a megállapításban említett állapot, gyakorlat, hiányosság, ha a lehetséges hatásaként

a) a közvetlen és közvetett anyagi kár a Támogatáskezelő költségvetéséhez, szellemi és anyagi erőforrásaihoz képest erősen érzékelhető (a közvetlen és közvetett anyagi kár eléri vagy meghaladja a Támogatáskezelő költségvetésének 5%-át),
a) bizalomvesztés állhat elő a Támogatáskezelőn belül vagy a Támogatáskezelővel kapcsolatban, esetlegesen Támogatáskezelő szabályzatában foglalt kötelezettségek sérülhetnek;
b) az üzlet-, vagy ügymenet szempontjából közepes értékű, vagy a Támogatáskezelő szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat elérése, rendelkezésre állása sérülhet,
c) téves külső következtetés levonásához vezethet a Támogatáskezelő által használt elektronikus információs rendszer jellemzőiről.

Magas besorolású a megállapításban említett állapot, gyakorlat, hiányosság, ha a lehetséges hatásaként

a) a közvetlen és közvetett anyagi kár a Támogatáskezelő költségvetéséhez, szellemi és anyagi erőforrásaihoz képest jelentős (a közvetlen és közvetett anyagi kár eléri vagy meghaladja a Támogatáskezelő költségvetésének 10%-át),
b) személyi sérülések esélye megnőhet (ideértve például a káresemény miatti szolgáltatás kimaradását, illetve a rendszer irányítatlansága miatti veszélyeket);
c) az üzlet-, vagy ügymenet szempontjából nagy értékű, üzleti titkot, vagy a Támogatáskezelő szempontjából különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat elérése, rendelkezése állása, bizalmassága tömegesen, vagy jelentősen sérülhet;
d) a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, illetve bekövetkezhet a bizalomvesztés a Támogatáskezelőn belül vagy a Támogatáskezelővel kapcsolatosan,
e) jelentősen téves külső következtetés levonásához vezethet a Támogatáskezelő által használt elektronikus információs rendszer jellemzőiről.

Kiemelt besorolású a megállapításban említett állapot, gyakorlat, hiányosság, ha a lehetséges hatásaként

a) különösen nagy értékű üzleti titok, a Támogatáskezelő szempontjából kiemelten érzékeny információt képező adat sérülhet,
b) a közvetlen és közvetett anyagi kár eléri vagy meghaladja a Támogatáskezelő költségvetésének 15%-át,

c) a Támogatáskezelő iránti társadalmi, politikai bizalom sérülhet,
d) alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;
e) az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;
f) a Támogatáskezelői adatvagyon helyreállíthatatlanul megsérülhet;
g) 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 Támogatáskezelő sajátosságaira tekintettel kerültek meghatározásra, más szervezet, társaság, informatikai környezet esetében az egyes kategóriákhoz eltérő követelmények lehetségesek.

M4.11.2. 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:

Előfordulási valószínűség	Lehetséges következmény előfordulási valószínűségének jelentése
Elenyésző	A megállapításban említett állapot, gyakorlat, hiányosság hatásaként előforduló lehetséges következmény (káresemény) *várhatóan három éves túl, vagy három éves 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).

M4.11.3. 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:

Előford. val.sz. / 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

M4.11.4. 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 részletes leírása
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.
Rövidtávon 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.

M4.11.5. ELVÁRT INTÉZKEDÉS OSZTÁLYOZÁSA A MEGVALÓSÍTÁS VÁRHATÓ RÁFORDÍTÁSIGÉNYE ALAPJÁN

Javaslatainkat, a végrehajtani ajánlott intézkedéseket a megvalósítás várható ráfordításigénye alapján az alábbi kategóriákba soroltuk:

Ráfordításigény	Várható ráfordítás részletes magyarázata
Elenyésző	A megvalósítás várható időigénye legfeljebb 4 munkaóra. A megvalósítás jellemzően belső erőforrás /közalkalmazott 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 /közalkalmazott 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 /közalkalmazott 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 /közalkalmazott 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 /közalkalmazottak 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 Támogatáskezelő sajátosságaira tekintettel kerültek meghatározásra, más szervezet, társaság, informatikai környezet esetében az egyes jellemzőkhöz megadott számértékek más nagyságot vehetnek fel.

5. SZ. MELLÉKLET – IGÉNYBE VETT SZOLGÁLTATÁSOK, MEGVÁSÁROLT, VALAMINT KIFEJLESZTETT RENDSZEREK KAPCSÁN ELVÁRT ELEKTRONIKUS INFORMÁCIÓ-BIZTONSÁGI KÖVETELMÉNYEK BETARTÁSÁNAK VÁLLALÁSA

Nem publikus melléklet!

Alulírott mint a … [Szállító] teljes jogú 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, a Támogatáskezelő 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 Támogatáskezelő által elvárt biztonsági osztályhoz és szinthez tartozó, a 41/2015 (VII. 15.) BM rendeletben meghatározott funkcionális és biztonsági követelmények teljesítésére.
b) A nem a Támogatáskezelő számára egyedileg fejlesztett Rendszer esetében a fejlesztési dokumentációval kapcsolatos elvárások teljesítése alól egyedileg felmentés adható, amelyet az IOV 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 Támogatáskezelőnek 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 Támogatáskezelő (IOV, 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 elvárás-részletekkel egyetemben. A Szállító nyilatkozatát a Szakmai Követelmények kapcsán a Szakmai Területnek, a Biztonsági Követelmények kapcsán az IOV-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 41/2015 (VII. 15.) BM rendelet 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 Támogatáskezelő 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, Támogatáskezelőt projektkeretek között, megfelelő szerepkörök, felhatalmazások kialakításával, a felelősségek elkülönítésével és alkalmas személyek kijelölésével, ellenőrzötten és dokumentáltan végzi.
i) A Szállító gondoskodik róla, hogy a Támogatáskezelő IOV-je és IBF-e már a fejlesztés tervezésétől kezdődően (by design), annak teljes életciklusába folyamatosan bevonásra kerüljön. A legfontosabb fejlesztési szakaszok lezárása a Szakmai Terület képviselőjének, valamint az IOV 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 Támogatáskezelő képviselőjének bevonásával) köteles a fejlesztés megkezdése, hardver összeállítása, szolgáltatás megkezdése előtt azonosítani a Támogatáskezelő 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 Támogatáskezelő 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 Támogatáskezelő 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, magyar nyelvű megjegyzésekkel, 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 Támogatáskezelőnél üzemelő és bevezetni tervezett további biztonsági és jogosultságkezelési architektúrába, különös tekintettel az alkalmazott authentikációs eljárásra, az AD alkalmazására (a Támogatáskezelő közalkalmazottjai 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. 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 támadásokat),
s. a Rendszer, mind backup, mind nagy rendelkezésre állást biztosító funkcióiban támogassa a Támogatáskezelő 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 Támogatáskezelőnek 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 Támogatáskezelőnek 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 és a pénzügyi 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 Támogatáskezelő 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 Támogatáskezelő 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 Támogatáskezelő 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 Támogatáskezelő bizonyosságot szerezzen

   a. a feltárt sérülékenységek megfelelő módon és határidőre végzett kezeléséről,
   b. arról, hogy a korábban azonosított sérülékenységek kezelése nem generált újabb sérülékenységet.

dd) A Szállító a fejlesztési folyamat végén köteles átadni a Támogatáskezelő 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 Támogatáskezelő a továbbiakban jogszerűen és teljeskörűen rendelkezhessen – ezek hiányában a teljesítési igazolás nem adható ki és a kapcsolódó számlát a Támogatáskezelő 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 Támogatáskezelőhez 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 Támogatáskezelő 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 Támogatáskezelő utasításai szerint jár el.

ff) A Támogatáskezelő a szerződés teljes időtartama alatt annak tárgyában tájékoztatást kérhet, továbbá a fejlesztési folyamatot helyszíni ellenőrzés keretében jogosult vizsgálni. A Támogatáskezelő 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 Támogatáskezelő kezdeményezésére köteles igazolni.

hh) A Szállító részéről alvállalkozó igénybevétele a szerződés teljesítése során nem tiltott, azonban ennek tényéről és a bevonni kívánt alvállalkozókról a Támogatáskezelőt előzetesen írásban értesíteni kell szerződéskötés előtt, hozzájárulását kérve. Amely alvállalkozó alkalmazásához a Támogatáskezelő 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 Támogatáskezelőn 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 kerülhessen sor.

jj) A Szállító fenntartja a jogot az elkészült Rendszer saját hatáskörben végzett biztonsági vizsgálatára. Amennyiben a Támogatáskezelő 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 Támogatáskezelő-specifikus követelmények jelentése:

- IOV: 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, a Támogatáskezelő 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 a Támogatáskezelővel megegyezett módon és határidőre történő helyreállításának hiányában) a Támogatáskezelő 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.

……..	……..
X Y [név],	X Y [név],
édesanyám neve:	édesanyám neve:
születési helyem és születésem ideje:	születési helyem és születésem ideje:
személyi azonosító iratom típusa és azonosítója/száma:	személyi azonosító iratom típusa és azonosítója/száma:

6. SZ. MELLÉKLET – INFORMÁCIÓBIZTONSÁGI HÁZIREND ÉS NYILATKOZAT

Publikus melléklet!

A Támogatáskezelő elkötelezett a közalkalmazottak / foglalkoztatottak (együtt: munkatársak) 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 Támogatáskezelő elkötelezett a kölcsönös bizalmon alapuló munkakörnyezet megteremtésében, ahol mindenkit, aki a Támogatáskezelőnek dolgozik, megbecsülnek és mindenki emberi méltóságát tiszteletben tartják.

A Támogatáskezelő és a vele kapcsolatba kerülő belső és külső érintettek között bizalmi kapcsolat van, ennek megfelelően elvárt, hogy valamennyi foglalkoztatott, tisztségviselő és partner (továbbiakban együtt: munkatárs) adja meg a megfelelő tiszteletet egymásnak és a Támogatáskezelő felhasználóinak.

A Támogatáskezelő felelős a vagyonát képező tárgyi eszközök, üzleti titkok, szellemi tulajdon megfelelő kezeléséért, védelméért és biztosítja a megfelelő adatbiztonságot a papíralapon és elektronikusan tárolt információ vonatkozásában egyaránt.

A Támogatáskezelő 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 munkatárs kötelessége és felelőssége.

A Támogatáskezelői vagyon és erőforrások helytelen, vagy gondatlan kezelése sérti az állampolgárok érdekét és rontja a felhasználók számára nyújtott szolgáltatás színvonalát, ezért kerülendő.

A munkatársak 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 munkatárs.

Különös gondot szükséges fordítani arra is, hogy az irodai eszközöket, berendezéseket (írószer, papír, fénymásoló, nyomtató, számítógép, telefon stb.) magáncélra ne használják a munkatársak. 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 Támogatáskezelő és felhasználói, partnerei számára.

A Támogatáskezelő kizárólag jogszerű módon gyűjt adatokat, valamint nyilvánosan hozzáférhető információforrásokat használ a szakmai/gazdasági i, felhasználói, beszállítói és technológiai tendenciák és magatartásminták, illetve többek között jogszabálytervezetek, egyéb szabályozói intézkedések és kommunikációs kampányok értékelése során.

A Támogatáskezelő elkötelezett munkatársai, illetve valamennyi ember magánélethez való jogának tiszteletben tartása és személyes adataik bizalmas kezelése mellett.

A Támogatáskezelő megelőző biztonsági intézkedéseket tesz az adatbázisokban tárolt személyes adatok védelmére, hogy elkerülje a megsemmisülés, adatvesztés és a jogosulatlan hozzáférés kockázatát.

A Támogatáskezelő kizárólag a hatékony működéséhez szükséges személyes adatokat gyűjt, tárol és kezel a jogszabályoknak megfelelően.

A Támogatáskezelő elvárja, hogy munkatársai

- ismerjék meg a személyes adatok védelmére vonatkozó törvényi és jogszabályi előírásokat;
- ismerjék meg és alkalmazzák a Támogatáskezelő megoldásait az üzleti titok és üzleti információ védelme érdekében;
- megfelelő körültekintéssel járjanak el mind a külső, mind a belső kommunikáció tekintetében;
- tartsák be a titoktartási és az egyéb vonatkozó szabályzatokat;
- korlátozzák az üzleti 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 munkatársai rendelkezzenek aláírt titoktartási nyilatkozattal.

A Támogatáskezelő munkatársai felelősek a Támogatáskezelőn belül, vagy a Támogatáskezelővel fennálló szakmai/gazdasági 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 Támogatáskezelő 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 Támogatáskezelő digitális rendszerein tárolt információk, valamint a foglalkozatottak otthoni vagy egyéb, nem a Támogatáskezelő tulajdonban lévő digitális rendszerein tárolt, a Támogatáskezelővel kapcsolatos információk szervezeti tulajdonnak minősülnek és ennek megfelelően szükséges kezelni őket.

A Támogatáskezelő szellemi tulajdonának védelme megköveteli, illetve lehetővé teszi, hogy a Támogatáskezelő megakadályozza, hogy azt bárki engedély nélkül használja, valamint díjat számítson fel ezek használati jogáért.

A munkatársaknak 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 munkatársnak 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 munkatársak saját anyagi vagy más haszonszerzésük céljára.

Az adatok jogszabályok szerinti védetté (pl.: szigorúan titkossá, titkossá, bizalmassá, korlátozott terjesztésűvé) minősítésének eszközét csak akkor lehet alkalmazni, ha a közjó szempontjából valamely, a közpénzek felhasználására vagy a közhatalom gyakorlására vonatkozó információk nyilvánosságához fűződő érdeknél súlyosabb érdek fűződik az adatok bizalmas kezeléséhez, és az a hozzáférhetőség kisebb fokú korlátozásával nem valósítható meg.

A Támogatáskezelő elkötelezett a kiberbiztonsági kultúra kialakítása, fenntartása, fejlesztése mellett, amelyet teljes tevékenysége, annak minden résztvevője esetében ösztönöz.

A Támogatáskezelő elkötelezett az elektronikusan tárolt adatok bizalmas kezelése, sértetlenségének és hozzáférhetőségének megőrzése iránt saját informatikai megoldások és belső szabályzatok alkalmazásával az adatok teljes életciklusa, azok tárolása, feldolgozása és továbbítása során. Ennek megfelelően:

- valamennyi, a Támogatáskezelői informatikai infrastruktúra 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 Támogatáskezelő informatikai vagy telekommunikációs eszközeire végzett adatletöltés, vagy magánjellegű adatoknak a Támogatáskezelő eszközein tárolása ekkor sem engedélyezett.

A megfelelő biztonság érdekében (a magánélet tiszteletben tartására vonatkozó és az adatvédelmi jogszabályok által biztosított kereteken belül) a Támogatáskezelő fenntartja a jogot, hogy a karbantartási-, gazdasági-, és jogszabályi követelmények teljesítése érdekében hozzáférjen az eszközökhöz és a rajtuk tárolt adatokhoz.

A Támogatáskezelő elvárja, hogy foglalkoztatottjai, tisztségviselői, partnerei

- ismerjék meg és alkalmazzák a Támogatáskezelő 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 Támogatáskezelő tulajdonát képező, vagy általa kezelt elektronikusan tárolt adatokat érintő káreseményeket, helytelen használatot és egyéb problémákat.

A Támogatáskezelő 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 Támogatáskezelő egészére vonatkozóan értelmezik, de az jogvita során fel is használható.

A Támogatáskezelő elvárja, hogy munkatársai

- 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 Támogatáskezelő álláspontjával, és még látszatát sem kelthetik annak, hogy a Támogatáskezelő nevében nyilvánulnak meg, a Támogatáskezelő álláspontját közlik.

A Támogatáskezelő nyílt, átlátható és kiegyensúlyozott kétirányú kommunikációt folytat a külső érintettekkel.

A Támogatáskezelő 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 Támogatáskezelő nevében a tulajdonosok és a média, valamint a további 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 Támogatáskezelő nem tűri és nem tolerálja a nyilvánosság félrevezetését.

A Támogatáskezelő foglalkoztatottjainak, gondoskodniuk kell róla, hogy a Támogatáskezelő működésére vonatkozó tartalmú, nyilvános közleménynek minősülő külső, például szakmai fórumokon tartandó előadással kapcsolatban rendelkezzenek a megfelelő vezetői jóváhagyással.

A Támogatáskezelő közösségi médiában történő megjelenéseit az erre kijelölt szervezeti egység, személyek koordinálják. A foglalkoztatottak, partnerek közösségi médiában való jelenléte a magánszférába tartozik, és ezt a Támogatáskezelő tiszteletben tartja, ugyanakkor a foglalkoztatottak, partnerek nem léphetnek fel a Támogatáskezelő 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 Támogatáskezelőre, nem jeleníthetik meg a Támogatáskezelőt 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]

Tanúsítom, hogy X Y ezt a nyilatkozatot tiszta tudattal, döntéshozatalra képes állapotban, minden kényszer nélkül, saját kezűleg, jelenlétemben írta alá.

…….. ……..

X Y [név], X Y [név],

édesanyám neve: édesanyám neve:

születési helyem és születésem ideje: születési helyem és születésem ideje:

személyi azonosító iratom típusa és azonosítója/száma: személyi azonosító iratom típusa és azonosítója/száma:

7. SZ. MELLÉKLET – TERVEZETT ELLENŐRZÉSEK RENDJE

Nem publikus melléklet!

Nr.	Ellenőrizendő terület	Ellenőrzött jellegzetesség, tevékenység, állapot	Megfelelő (elfogadható) érték	Nem megfelelő (nem elfogadható) érték	Ellenőrzés gyakorisága	Ellenőrzés módja	Elenőrzést végzi	Nem-megfelelés esetén teendő	Nem-megfelelés szankciója
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									

18									
19									
20									
21									
22									
23									
24									
25									

A tervezett ellenőrzések rendjének nyilvántartásához a mellékletben szereplő táblázat tetszőleges formázással használható annak érdekében, hogy a szükséges tartalom a legkedvezőbb módon nyilvántartható és formázható legyen.

A melléklethez kizárólag a következő személyek számára engedélyezett a hozzáférés:

- Főigazgató,
- Általános Főigazgató-helyettes,
- Főigazgatói kabinetvezető,
- Stratégiai és humánpolitikai igazgató,
- Operatív igazgató,
- Jogi igazgató,
- Informatikai osztályvezető ,
- Elektronikus információbiztonsági felelős,
- Belső ellenőr,
- Védelmi referens,
- Integritás tanácsadó

8.1. SZ. MELLÉKLET – TEVÉKENYSÉG (SZOLGÁLTATÁS) KATALÓGUS

Nem publikus melléklet!

Nr.	Szolg. neve	Szolg. leírása	Szolg nyújtja (EMET/külső sz.)	Szolg. belső felelőse	Szolg. felhasználói	SLA kritériumok					
						Rendelkezésre állás	Lehetséges max. kiesés		Elvárt minőségi kritérium		
							óra	%/hó	neve	értéke	méri
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											

19											
20											
21											
22											
23											
24											
25											

A melléklethez kizárólag a következő személyek számára engedélyezett a hozzáférés:

- Főigazgató,
- Általános Főigazgató-helyettes,
- Főigazgatói kabinetvezető,
- Stratégiai és humánpolitikai igazgató,
- Operatív igazgató,
- Jogi igazgató,
- Informatikai osztályvezető ,
- Elektronikus információbiztonsági felelős,
- Belső ellenőr,
- Védelmi referens,
- Integritás tanácsadó

Az elvárt SLA kritériumok nemteljesítése biztonsági eseménynek számít, amelyet ennek megfelelően kell kezelni.

8.2. SZ. MELLÉKLET – INFORMATIKAI TEVÉKENYSÉG (SZOLGÁLTATÁS) KATALÓGUS

Nem publikus melléklet!

Nr.	Szolg. neve	Szolg. leírása	Szolg nyújtja (EMET/külső sz.)	Szolg. belső felelőse	Szolg. felhasználói	SLA kritériumok					
						Rendelkezésre állás	Lehetséges max. kiesés		Elvárt minőségi kritérium		
							óra	%/hó	neve	értéke	méri
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											

19											
20											
21											
22											
23											
24											
25											

A melléklethez kizárólag a következő személyek számára engedélyezett a hozzáférés:

- Főigazgató,
- Általános Főigazgató-helyettes,
- Főigazgatói kabinetvezető,
- Stratégiai és humánpolitikai igazgató,
- Operatív igazgató,
- Jogi igazgató,
- Informatikai osztályvezető ,
- Elektronikus információbiztonsági felelős,
- Belső ellenőr,
- Védelmi referens,
- Integritás tanácsadó

Az elvárt SLA kritériumok nemteljesítése biztonsági eseménynek számít, amelyet ennek megfelelően kell kezelni.

9. SZ. MELLÉKLET – INFORMATIKAI RENDSZEREK FOLYAMATOS MŰKÖDÉSÉVEL KAPCSOLATOS LEGFONTOSABB TUDNIVALÓK SZERKEZETE
Publikus melléklet!

Informatikai rendszer neve

Informatikai rendszer fő funkciói:

- …
- …
- …

Informatikai rendszer használatára jogosultak:

- …
- …
- …

Informatikai rendszer innen indítható (elérési út):

Informatikai rendszer felhasználói kézikönyvének elérési útja:

Az informatikai rendszer szakmairendszergazdája (támogatója) és az ő elérhetősége:

- név, beosztás
- telefonszám:
- e-mail cím:

Az informatikai rendszer informatikai támogatója és az ő elérhetősége:

- név, beosztás
- telefonszám:
- e-mail cím:

Az informatikai rendszer helyes működését jelzi:

- …
- …
- …

Az informatikai rendszer nem megfelelő működését jelzi:

- …
- …
- …

Ha az informatikai rendszer nem megfelelő működését tapasztalja, akkor a következőt tegye:

- …
- …
- …

10. SZ. MELLÉKLET – MENTÉSI TERV

Nem publikus melléklet!

Nr.	Rendszerelem	Mentett állapot	Mentési		Mentő-rendszer neve	Mentésre használt média		Job neve	Mentés ellenőrzési módja
			gyakoriság	mód		neve	tárolása		
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									
23									
24									
25									
26									

A melléklethez kizárólag a következő személyek számára engedélyezett a hozzáférés:

- Főigazgató,
- Általános Főigazgató-helyettes,
- Főigazgatói kabinetvezető,
- Stratégiai és humánpolitikai igazgató,
- Operatív igazgató,
- Jogi igazgató,
- Informatikai osztályvezető,
- Elektronikus információbiztonsági felelős,
- Belső ellenőr,
- Védelmi referens,
- Integritás tanácsadó

11. SZ. MELLÉKLET – BIZTONSÁGI ESEMÉNYKEZELÉSI TERV
Publikus melléklet!

Az Emberi Erőforrás Támogatáskezelőben (továbbiakban: Támogatáskezelő) biztonsági eseménynek (incidensnek) számít minden olyan történés, cselekvés, vagy ezek elmaradása, amely a Támogatáskezelő informatikai vagy telekommunikációs infrastruktúrájának, felhasználóinak, illetve az ebben tárolt adatoknak a bizalmasságát, sértetlenségét vagy rendelkezésre állását a Támogatáskezelő által nem kívánt módon befolyásolja.

Biztonsági eseményre példa:

- jogosulatlan hozzáférést eredményezhet, például:
    - jelszó felírása, különösen, ha a felírt jelszót a felhasználó „elhagyja”
    - 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 Támogatáskezelő 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 Támogatáskezelő szakmai/gazdasági 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 Támogatáskezelő által elvárttól eltérő tárolása, szállítása stb.

- a Támogatáskezelő 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 Támogatáskezelő elektronikus információs rendszerének 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 Támogatáskezelő 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 IO felé, az Informatikai Help Desk bármely 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 mellékletben leírtak szerint kell eljárni.

Az IO 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 IO-nak haladéktalanul nyilvántartásba kell vennie, majd ki kell vizsgálnia, amelynek során a bejelentést kapó IO közalkalmazottnak haladéktalanul értesítenie kell az IOV-t és a valószínűsíthetően érintett rendszerelem működtetéséért felelős

közalkalmazott, külső szervezetet (II. szintű Help Desk), 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 *„M4.11.1. Nem-megfelelések lehetséges következményének osztályozása”* pont alapján kell elvégezni. Az osztályozást az IOV feladata elvégezni.

Amennyiben a biztonsági esemény (incidens) lehetséges következménye

- közepes vagy magasabb besorolású, haladéktalanul értesíteni kell az eseményről az Operatív igazgatót, 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 IOV dönt, illetve erre az IBF tehet javaslatot.

Az értesítéseket az IOV-nek kell elvégeznie.

A biztonsági esemény további kezelésébe a II. szintű Help Desk tagjain 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 IOV-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 lényegi(nek tűnő) körülményekkel, tapasztalatokkal együtt,
- a biztonsági esemény kiváltó okát,
- a biztonsági esemény lezárási idejével,

a biztonsági esemény által okozott tényleges kárral együtt.

Az IOV-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 (azok azonosításából, kezeléséből - lessons learn), annak érdekében, hogy a később előforduló hasonló események kezelése magasabb színvonalú lehessen.

A biztonsági eseményekről az IOV-nek évente összefoglaló tájékoztatást kell adnia a FI, az OI, 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 közalkalmazottak /foglalkoztatottak számára a biztonsági események felismerésére és megfelelő kezelésére.

A biztonsági eseménykezelés hatékonyságának növelésére az IBF is javaslatot tehet.

12. SZ. MELLÉKLET – MUNKAKÖRÖK BIZTONSÁGI SZEMPONTÚ BESOROLÁSA
Nem publikus melléklet!

Szervezeti egység	Munkakör	Besorolás

A besorolásokat a Stratégiai és humánpolitikai igazgató hajtja végre és küldi a FI-nak jóváhagyásra. A jóváhagyott besorolást a humánpolitikai osztályvezető továbbítja az IBF és IOV felé (ezen szabályzat előző bekezdésben említett mellékletének frissítése érdekében).

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

A melléklethez kizárólag a következő személyek számára engedélyezett a hozzáférés:

- Főigazgató,
- Általános Főigazgató-helyettes,
- Főigazgatói kabinetvezető,
- Stratégiai és humánpolitikai igazgató,
- Operatív igazgató,
- Jogi igazgató,
- Informatikai osztályvezető,
- Elektronikus információbiztonsági felelős,
- Belső ellenőr,
- Védelmi referens,
- Integritás tanácsadó

13. SZ. MELLÉKLET – NETIKETT: A SZÁMÍTÓGÉPES KOMMUNIKÁCIÓ ILLEMSZABÁLYAI, KÜLÖNÖS TEKINTETTEL AZ INTERNETRE

Publikus melléklet!

ETIKETT

Etikettnek nevezzük a társadalmi érintkezés formáinak elfogadott rendszerét. Az informatika fejlődése új kultúrát teremtett saját szokásokkal, viselkedési normákkal, illemszabályokkal. Aki részesévé akar válni ennek a világnak, annak meg kell ismernie, és be kell tartania ezeket a szabályokat.

NETIKETT

Az Internetre vonatkozó illemszabályokat, szokásokat, viselkedési formákat hálózati etikettnek, röviden netikettnek (Internet zsargon a network (hálózat) és az etiquette (illemtan) összevonásából) nevezzük. A szokásos netikettek erkölcsi, etikai normákat és használati tanácsokat vegyesen tartalmaznak. A netikett célja barátságos légkör megteremtése és megőrzése az Internetes kommunikációban.

A NETIKETT 3 FŐ RÉSZE

A netikett 3 fő részre osztható:

- „egy-egynek” kommunikáció,
- „egy-sokaknak” kommunikáció, és az
- „információs szolgáltatások”

„EGY-EGYNEK” KOMMUNIKÁCIÓ,

Az egy-egynek kommunikáció során egy ember kommunikál egy másik emberrel, ilyen a levelezés. Általában a valós társalgás szabályai érvényesek, csak ez az Interneten még fontosabb, hiszen hiányzik a metakommunikáció, és a hangszín.

„EGY-SOKAKNAK” KOMMUNIKÁCIÓ

„Egy-sokaknak” kommunikáció (levelezési listák, hírlevelek, fórumok, IRC) során egy ember sok másikkal kommunikál. Az e-mailre vonatkozó szabályok itt is érvényesek, sőt még fontosabbak, hiszen több emberrel kommunikálunk egyszerre.

INFORMÁCIÓS SZOLGÁLTATÁSOK

Információs szolgáltatások (WWW, FTP) sokan – sokaknak helyeznek el információt.

LEVELEZÉSSEL KAPCSOLATOS ETIKAI ALAPOK

A levél tartalmára vonatkozó alapvető etikai szabály, hogy e-mail-ben ne írjunk olyasmit, amit nem küldenénk el levelezőlapon (ez a szabály valamennyi Internetes szolgáltatásra érvényes). Titkosítás nélkül az Interneten minden nyilvános, az ember magáról állítja ki a bizonyítványt egy nem megfelelő stílusú levéllel.

Vannak tabutémák, amire nem szabad rákérdezni sem szóban, sem levélben (pl. mennyi a havi illetménye, mely párthoz tartozik, van-e családja, milyen vallású stb.) Mindenki annyit mond el és ír le magáról, amennyit jónak tart.

Legyünk konzervatívak a küldésben és liberálisak a fogadásban: Ne küldjünk indulatos leveleket (flame-ket), akkor sem, ha provokálnak, viszont ne legyünk meglepve, ha ilyet kapunk. Ne válaszoljunk rá és ne küldjük tovább!

Mindig ellenőrizzük a levél címét: vannak címek melyek úgy néznek ki, mintha egy ember lenne, pedig csoportot jelentenek.

Mindig töltsük ki a levél *„Subject”(*Tárgy) rovatát, így tájékoztatjuk a címzettet a levél tartalmáról, és olvassuk el a saját leveleink *„Tárgy”* rovatát is. (Pl.: az, aki segítséget kért tőlünk, egy következő levélben, értesített minket, hogy már „Nem érdekes”.)

Ha hosszú eszmecserét kezdeményezünk, ellenőrizzük a címet, és a hosszú levél Tárgy sorába kerüljön be a „*Long*” szó.

Ne küldjünk lánclevelet, kéretlenül nagy mennyiségű információt.

Célszerű a levél végén egy-két sorban ismertetni saját elérhetőségünket. (Signature, aláírás fájl)

A levél tartalmára vonatkozó néhány formai szabály: használjunk kis- és nagybetűt vegyesen, szimbólumokat hangsúlyozásra, kiemelésre, „Emoji”-kat (Smiley és társai).

A levél legyen tömör anélkül, hogy túlságosan lényegre törő lenne.

LEVELEZÉSI LISTÁK NÉHÁNY ETIKAI SZABÁLYA

A fel- és leiratkozó üzeneteket a megfelelő címre küldjük, és mentsük el a feliratkozásra kapott választ (tartalmazza a leiratkozáshoz szükséges információkat).

Mielőtt levelezési listára postázunk valamit, olvassunk el legalább néhány tucat üzenetet az adott levelezési listán, ismerjük meg a közösség szokásait, szóhasználatát, „tolerancia-szintjét”.

Amit írunk, – elképzelhető – széles közönség olvassa majd. Vigyázzunk a levél tartalmára.

Mielőtt elküldünk egy levelet, ellenőrizzük azt. Az elküldött levelet nem lehet visszavonni (ha látszólag sikerül is az elküldött üzenet visszahívása, nem lehetünk bizonyosak benne, hogy annak egy vagy több példánya nem maradt a címzett informatikai infrastruktúrájában továbbra is elérhető, kívül a kontroll-lehetőségeinken).

Az üzenet címét mindig ellenőrizzük: a csoportnak, vagy csak egy személynek szeretnénk küldeni.

Válaszüzenet esetén idézzünk csak annyit az eredetiből, hogy a válasz érthető legyen.

Helytelen nagy fájlokat küldeni egy listára.

Ha kérdést teszünk fel, akkor készítsünk a válaszokból egy gondos összegzést és küldjük el a listára.

Privát levelezési listára csak akkor küldjünk levelet, ha oda korábban meghívtak bennünket. Privát levelezési listán olvasott üzenetet ne küldjük tovább szélesebb körben.

Tilos listás leveleket tovább küldeni a küldő engedélye nélkül.

A CHAT NÉHÁNY ETIKAI SZABÁLYA

Ismerjük meg a csoport kultúráját.

Nem szükséges mindenkit személyesen üdvözölni, egy egyszerű „Szia” is elegendő.

Ha valaki becenevet, alias-t vagy álnevet használ, tiszteljük az anonimitását.

Nyomdafestéket nem tűrő kifejezéseket ne használjunk.

INFORMÁCIÓS SZOLGÁLTATÁSOK (WWW, FTP)

Az Interneten lévő anyagnak a közízlésnek megfelelőnek kell lennie - uszító, rasszista, fasiszta, vallási, politikai anyag nem lehet.

Törvénybe ütköző anyag elhelyezése TILOS.

Az Interneten elhelyezett anyagokért a web oldal készítője a felelős és nem a szolgáltató.

Az oldal alján el kell helyezni a készítő nevét és e-mail címét.

Az Interneten elhelyezett információk egy része ingyenes, másik része nem. Ezekről érdemes informálódni.

Ne használjuk más FTP site-ját arra, hogy egy harmadik személynek szánt fájl-t oda helyezzünk el.

14. SZ. MELLÉKLET – LÁTOGATÓK NYILVÁNTARTÁSA

Nem publikus melléklet!

Létesítmény neve és címe:

Érintettek	Név (nyomtatott betűkkel)	Támogatáskezelő	Beosztás	Belépés ideje	Aláírás	Kilépés ideje	Aláírás
Látogató:							
Meghívó:							
Kísérő:							

Érintettek	Név (nyomtatott betűkkel)	Támogatáskezelő	Beosztás	Belépés ideje	Aláírás	Kilépés ideje	Aláírás
Látogató:							
Meghívó:							
Kísérő:							

Érintettek	Név (nyomtatott betűkkel)	Támogatáskezelő	Beosztás	Belépés ideje	Aláírás	Kilépés ideje	Aláírás
Látogató:							
Meghívó:							
Kísérő:							

A Támogatáskezelő elektronikus információs rendszereknek helyt adó, általa felügyelt létesítményeibe (szerverszoba, informatikai raktár stb.) belépő, nem informatikai osztályon dolgozó közalkalmazottakról kötelező a melléklet adattartalmának megfelelő nyilvántartást vezetni.
A nyilvántartást 8 (nyolc) évig meg kell őrizni, amely az IOV feladata.

A nyilvántartáshoz kizárólag a következő személyek számára engedélyezett a hozzáférés:

- Főigazgató,
- Általános Főigazgató-helyettes,
- Főigazgatói kabinetvezető,
- Stratégiai és humánpolitikai igazgató,
- Operatív igazgató,
- Jogi igazgató,
- Informatikai osztályvezető,
- Elektronikus információbiztonsági felelős,
- Belső ellenőr,
- Védelmi referens,
- Integritás tanácsadó