EMBERI ERŐFORRÁS
TÁMOGATÁSKEZELŐ

Melléklet a(z) ...../2019. ( ) EMET főigazgatói utasításhoz

Az Emberi Erőforrás Támogatáskezelő Elektronikus Információbiztonsági Szabályzata

témafelelős:

……

Juhász Sándor

elektronikus információbiztonsági felelős

jóváhagyta:

……..

dr. Mészáros Karina

főigazgató

TARTALOM

I. ÁLTALÁNOS RENDELKEZÉSEK

1. § Jelen Elektronikus Információbiztonsági Szabályzat (a továbbiakban: IBSZ) az Emberi Erőforrás Támogatáskezelő (a továbbiakban: Támogatáskezelő) által kezelt információkra, illetve a Támogatáskezelő üzemeltetésében álló informatikai rendszerekre vonatkozóan szabályozza a biztonsági intézkedéseket, meghatározza a számítástechnikai eszközök használatának, valamint az információkezelés folyamatának biztonsági szabályait, az információbiztonsággal kapcsolatos szerepköröket, és előírja az egyes szereplők információbiztonságot érintő feladatait, függetlenül attól, hogy az információ elektronikus vagy papíralapon keletkezett, került tárolásra, illetve kezelésre.

1. JOGSZABÁLYI HÁTTÉR, JOGI LEHATÁROLÁS

2. § (1) Az IBSZ a jogszabályok előírásainak alkalmazásán alapul, és az információvédelemre vonatkozó jogszabályi szintű rendelkezésekkel – különösen az alábbiakban felsorolt törvényekben és a végrehajtásukra kiadott jogszabályokban foglaltakkal – együtt értelmezendő:

a) az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény;

b) a közadatok újrahasznosításáról szóló 2012. évi LXIII. törvény;

c) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.);

d) az államháztartásról szóló 2011. évi CXCV. törvény;

e) a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény;

f) a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény;

g) a közpénzekből nyújtott támogatások átláthatóságáról szóló 2007. évi CLXXXI. törvény;

h) a minősített adat védelméről szóló 2009. évi CLV. törvény;

i) a számvitelről szóló 2000. évi C. törvény;

j) a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény;

k) a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény;

l) az államháztartásról szóló törvény végrehajtásáról szóló 368/2011. (XII. 31.) Korm. rendelet;

m) a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet;

n) a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet;

o) a közérdekű adatok elektronikus közzétételére, az egységes közadatkereső rendszerre, valamint a központi jegyzék adattartalmára, az adatintegrációra vonatkozó részletes szabályokról szóló 305/2005. (XII. 25.) Korm. rendelet;

p) az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról szóló 466/2017. (XII. 28.) Korm. rendelet;

q) a támogatásból megvalósuló fejlesztések központi monitoringjáról és nyilvántartásáról szóló 60/2014. (III. 6.) Korm. rendelet;

r) 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: Vhr.);

s) a közzétételi listákon szereplő adatok közzétételéhez szükséges közzétételi mintákról szóló 18/2005. (XII. 27.) IHM rendelet.

3. § Az IBSZ-ben nem rendezett kérdésekben a fentiekben említett hatályos jogszabályok rendelkezéseit, továbbá a Támogatáskezelő egyéb belső szabályzataiban, így különösen a Szervezeti és Működési Szabályzatban, az Egyedi Iratkezelési Szabályzatban, az Infokommunikációs Eszközökről Szóló Szabályzatban, az EMET Közérdekű adatok megismerésére irányuló kérelmek eljárásrendjéről, továbbá a kötelezően közzéteendő adatok nyilvánosságra hozatalának rendjéről szóló Szabályzatban, a Tűzvédelmi Szabályzatban és a Szociális juttatásokról szóló szabályzatban, az Adatvédelmi Szabályzatban foglaltak az irányadók.

4. § Az IBSZ nem foglalkozik a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló Európa Parlament és a Tanács 2016/679 rendelet (GDPR) hatálya alá tartozó adatok kezelésének szabályaival. A GDPR hatálya alá tartozó adatok kezelésének részletező szabályait a Támogatáskezelő Adatvédelmi Szabályzata tartalmazza.

2. AZ INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT CÉLJA, HATÁLYA

2.1 Az Információbiztonsági Szabályzat célja

5. § (1) Az IBSZ célja, hogy a Támogatáskezelőnél a szervezeti egységek és munkatársaik egymás közötti és a Támogatáskezelőhöz nem tartozó külső szervekkel, személyekkel fenntartott kapcsolatokban biztosítható legyen:

a Támogatáskezelő informatikai rendszereinek (a továbbiakban: rendszerek) és a rendszerekben tárolt információk megfelelő rendelkezésre állása;

a) az adatállományok formai és tartalmi helyességének, épségének megőrzése;

b) az adatok és információk bizalmassága, megfelelő védelme;

c) a Támogatáskezelő tevékenysége során keletkezett információk védelme;

d) a számítógépes feldolgozások és az eredményadatok további hasznosítása során az illetéktelen hozzáférésből és felhasználásból eredő hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése;

e) az informatikai szoftvereszközökkel kapcsolatos jogbiztonság, jogtisztaság;

f) a jogszabályi szinten rögzített információbiztonsági elvárásoknak való megfelelés.

(2) A célok elérése érdekében a védelemnek működnie kell a rendszerek fennállásának teljes ciklusa alatt – a megtervezéstől az alkalmazáson (üzemeltetésen) keresztül – a felszámolásukig. Az IBSZ alkalmazásánál figyelembe kell venni, hogy a Támogatáskezelő különböző szervezeti egységei használatában működő telekommunikációs és informatikai rendszerek tervezése, bevezetése, üzemeltetése és ellenőrzése vonatkozásában meghatározott feladatok elsősorban a törvényesség betartásával, másodsorban a védelem hiányából eredő lehetséges károk értékével legyenek arányosak.

6. § Az IBSZ rendelkezéseit minden informatikai rendszer esetében, teljes körűen kell alkalmazni. A vonatkozó informatikai biztonsági követelményeket az egyes rendszerek fejlesztési és alkalmazási dokumentációiban is meg kell jeleníteni.

2.2 Az IBSZ személyi hatálya

7. § Az IBSZ személyi hatálya kiterjed a Támogatáskezelő valamennyi foglalkoztatottjára. Az IBSZ személyi hatálya kiterjed továbbá minden személyre, aki a Támogatáskezelő informatikai vagy azzal összefüggő rendszerét, szolgáltatásait igénybe veszi, informatikai struktúráját és annak eszközeit üzemelteti vagy használja, függetlenül a Támogatáskezelőhöz kapcsolódó jogviszonyától. Más természetes személyeket az IBSZ csak a külön megállapodásokban (pl. adatvédelmi nyilatkozat, adatszolgáltatási megállapodás, titoktartási nyilatkozat, stb.) rögzítettek szerint érint.

2.3 Az IBSZ tárgyi hatálya

8. § (1) Az IBSZ tárgyi hatálya kiterjed:

a) valamennyi (a Támogatáskezelő tulajdonában lévő, vagy általa bérelt, kezelésében levő) informatikai és telekommunikációs berendezésre, vagy a Támogatáskezelő használatában álló épületben található, leltári jelzéssel ellátott, továbbá a Támogatáskezelő megbízásából a Támogatáskezelő munkatársai számára harmadik személy által biztosított informatikai eszközre, beleértve az eszközök, berendezések műszaki dokumentációját is;

b) a Támogatáskezelő eszközein működtetett rendszerprogramokra és a felhasználói programokra;

c) a Támogatáskezelő tulajdonában, vagy bérleményében, továbbá üzemeltetésében álló valamennyi informatikai szakrendszerre;

d) az adatkommunikációra, a Támogatáskezelő számítógépes kábelhálózatára, a Támogatáskezelő számára, illetve a Támogatáskezelő által üzemeltetett hálózati elemekre;

e) amennyiben a Támogatáskezelő működésére irányadó egyéb szabályzat – így különösen az Egyedi Iratkezelési Szabályzat, az Infokommunikációs Eszközökről szóló Szabályzat, az EMET Közérdekű adatok megismerésére irányuló kérelmek eljárásrendjéről, továbbá a kötelezően közzéteendő adatok nyilvánosságra hozatalának rendjéről szóló Szabályzata, az Adatvédelmi Szabályzat, a Tűzvédelmi Szabályzat és a Szociális juttatásokról szóló szabályzat – eltérően nem rendelkezik:

ea) az informatikai folyamatot leíró valamennyi dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési dokumentációk);

eb) az adathordozók tárolására és felhasználására, beleértve a feldolgozásra és a felhasználókhoz történő eljuttatás folyamatait is;

ec) az információk felhasználására;

ed) az információk teljes körére, keletkezésük és felhasználásuk, valamint feldolgozásuk helyétől, továbbá a megjelenési formájuktól (bizonylatok, tablók, mágneses adathordozók, stb.) függetlenül;

9. § Az IBSZ rendelkezéseit alkalmazni kell minden olyan adat- és információkezelésre, amelyet a Támogatáskezelő, mint kezelő szerv meghatalmazása alapján külső szervezet végez.

10. § Az IBSZ hatálya nem terjed ki a Nemzeti Infokommunikációs Szolgáltató Zrt. (NISZ) által szolgáltatott rendszerekre, hálózatokra, melyekre vonatkozóan a biztonsági kérdéseket a NISZ-szel kötött megállapodásban kell rögzíteni.

2.4 A Támogatáskezelő működése szempontjából kiemelt és normál rendszerek és azok ismérvei

11. § (1) A Támogatáskezelő működése szempontjából kiemelt az a rendszer, amely összefügg a Támogatáskezelő alaptevékenységével, vagy amely nagy mennyiségű személyes adatot, vagy különleges adatot tartalmaz. A kiemelt rendszerek közé tartoznak továbbá azok az – elsősorban technikai jellegű – rendszerek, amelyek a Támogatáskezelő napi működéséhez és feladatellátásához nélkülözhetetlenek. A kiemelt rendszerek információbiztonsági szempontból fokozott védelmet igényelnek. E körbe tartoznak különösen az alábbi rendszerek:

a) bér- és munkaügyi rendszer;

b) gazdasági, ügyviteli rendszer;

c) iratkezeléssel összefüggő rendszerek;

d) támogatással, pályáztatással összefüggő rendszerek;

e) EU információs rendszer;

f) központi levelező kiszolgálók;

g) központi tárhely kiszolgálók;

h) intézményi autentikációs rendszerek;

i) telekommunikációs rendszer és hálózat;

j) kommunikációs rendszerek;

k) technológiai rendszerek.

(2) Normál rendszerek a kiemelt rendszerek körébe nem sorolt, a Támogatáskezelő egészére nem, csak egyes részeire kiterjedő olyan rendszerek, amelyek használatához szükséges a személyes autentikáció.

3. ÉRTELMEZŐ RENDELKEZÉSEK

12. § (1) Az IBSZ alkalmazása során:

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

b) adatállomány: adathordozón tárolt, logikailag összetartozó adatok összessége;

c) adatátvitel: adatok informatikai rendszerek, rendszerelemek közti továbbítása;

d) adatbázis: szoftverrel rendszerbe szervezett, egy vagy több adatállomány;

e) adatbiztonság: az adatok jogosulatlan kezelése, megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni technikai, szervezési megoldások és eljárási szabályok összessége, az adatkezelésnek azon állapota, amelyben a fenyegetettséget jelentő kockázati tényezőket különböző műszaki, szervezési megoldások és intézkedések a lehető legkisebb mértékűre csökkentik;

f) 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;

g) adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése;

h) adathordozó: bármely alakban, bármilyen eszköz felhasználásával és bármilyen eljárással előállított, adat tárolására alkalmas, vagy adatot tartalmazó anyag;

i) adatvédelem: Az adatok jogosulatlan megszerzésének, illetve manipulálásának megakadályozására irányuló intézkedések összessége.

j) alapszolgáltatások: azok az informatikai szolgáltatások, amelyek minden felhasználó számára rendelkezésre állnak;

k) alkalmazás (alkalmazói program, alkalmazói szoftver): a szoftver és minden egyéb olyan számítógépes program, amelyet egy feladat vagy feladatkör végrehajtására terveztek, és amely a hardver és az üzemi rendszer funkcióit használja;

l) auditálás: előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;

m) autentikáció: az elektronikus kommunikációban résztvevő felek identitásának megállapítása és ellenőrzése;

n) azonosító eszköz: olyan eszköz, amely a felhasználó egyértelmű azonosítására szolgál (pl. mágneskártya);

o) 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;

p) biztonsági esemény: bármilyen olyan esemény, ami az érvényben lévő biztonsági szabályokat sérti, vagy a biztonsági szabályok sérülésének gyanúját vetik fel, így különösen az informatikai rendszer biztonságában beállt olyan kedvezőtlen változás, melynek hatására az informatikai rendszerben tárolt adatok bizalmassága, sértetlensége, vagy rendelkezésre állása megsérült, vagy megsérülhet;

q) 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;

r) biztonsági osztály: az elektronikus információs rendszer védelmének elvárt, a Vhr-ben meghatározott kritériumok alapján számolt erőssége;

s) biztonsági osztályba sorolás: a Vhr-ben felsorolt kritériumok és a kockázatelemzés alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;

t) biztonsági rendszer: az épületek betörés és vagyonvédelmi rendszere;

u) biztonsági szint: az Ibtv-ben, illetve a Vhr-ben meghatározott kritériumok szerint az elektronikus információs rendszert használó, üzemeltető, fejlesztő szervezeti egység, vagy a szervezet felkészültségének foka, az azzal kapcsolatos elvárások kötelező teljesülésének mértéke az elektronikus információs rendszert érintő biztonsági feladatok kezelésére;

v) biztonsági szintbe sorolás: a szervezet, vagy az elektronikus információs rendszer fejlesztő, üzemeltető, kezelő szervezeti egység felkészültségének meghatározása az Ibtv-ben és a Vhr-ben meghatározott biztonsági feladatok kezelésére;

w) elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben az adatokhoz minden felhasználó kizárólag jogosultsága mértékében képes hozzáférni oly módon, hogy 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;

x) fájl: számítógépen tárolt információtárolási egység. Egy fájl tartalma a gép szempontjából vagy adat, vagy program, amely végrehajtandó utasításokat tartalmaz;

y) felhasználó: meghatározott jogosultságokkal bíró olyan személy, aki a Támogatás-kezelő informatikai rendszerét, hálózatát, szolgáltatásait autentikációt követően igénybe veszi;

z) hardver: az informatikai rendszer fizikai eleme;

aa) hálózat: informatikai eszközök, rendszerek közti adatátvitelt megvalósító logikai és fizikai eszközök összessége, amely adatcserét tesz lehetővé;

bb) hozzáférés: olyan eljárás, amely a felhasználó számára, jogosultsága függvényében elérhetővé teszi az informatikai rendszer erőforrásait;

cc) időbélyegzés-szolgáltatás: Az időbélyeg az elektronikus dokumentumhoz végérvényesen hozzárendelt, vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikus dokumentum az időbélyegzés időpontjában változatlan formában létezett. Az időbélyeg másodperc pontossággal tartalmazza a bélyegzés időpontját és ezzel a dokumentum egy adott időpontban meglévő állapotát rögzíti; az időbélyegzővel ellátott elektronikus dokumentumon minden utólagosan végrehajtott módosítás érzékelhető;

dd) informatikai szolgáltatások: a Támogatáskezelő által biztosított számítástechnikai, információ-feldolgozási és kommunikációs szolgáltatások;

ee) informatikai támadás: minden olyan hardver vagy szoftver elem működését befolyásoló tényező, amely kihasználva azok sérülékenységét szándékosan akadályozza azok működését vagy kárt tesz azokban;

ff) kapcsolószekrény: a Támogatáskezelő informatikai és telekommunikációs hálózatának működtetéséhez szükséges eszközök elhelyezésére szolgáló szekrények;

gg) központi rendszer: a Támogatáskezelő szerverei, kommunikációs eszközei, központi nyomtatói;

hh) működőképesség: az elektronikus információs rendszernek és elemeinek az elvárt és igényelt üzemelési állapota;

ii) PKI technológia: a PKI technológia (Public Key Infrastructure, magyarul: Nyilvános Kulcsú Infrastruktúra) alkalmazása lehetővé teszi, hogy minden elektronikusan aláírt dokumentum vagy üzenet olvasója ellenőrizni tudja az üzenetet küldő személy azonosságát és az üzenet sértetlenségét. Az elektronikus aláírás az aláíró magánkulcsával készül és kizárólag annak párjával, a nyilvános kulccsal lehet ellenőrizni az aláírás eredetiségét, az aláírt elektronikus dokumentum sértetlenségét. A PKI alapú titkosítás során a feladó az általa elkészített üzenethez vagy dokumentumhoz a címzett nyilvános kulcsát kapcsolja, vagyis a kódolás a nyilvános kulccsal történik. A címzett a hozzá küldött dokumentumot vagy üzenetet kizárólag a nyilvános kulcs párjával, azaz a saját tulajdonában lévő magánkulcsával tudja dekódolni, vagyis elolvasni;

jj) PKI alapú autentikáció: A PKI alapú autentikáció során egy személy vagy szervezet, illetve egy informatikai eszköz (pl. webszerver) tanúsítványa segítségével azonosítja magát és igazolja, bizonyítja kilétét távoli szerverekre/rendszerekbe történő belépés céljából (felhasználónév és jelszó helyett).

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

ll) rosszindulatú alkalmazás: a rosszindulatú számítógépes programok összefoglaló neve. Ide tartoznak a vírusok, férgek (worm), kémprogramok (spyware), agresszív reklámprogramok (adware), a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközök (rootkit);

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

nn) 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;

oo) SPAM: kéretlen e-mail, vagy SMS. Jobbára kereskedelmi célú és nagy mennyiségben kiküldött üzenet;

pp) személyes adat: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés;

qq) szerverterem: a központi informatikai rendszereket, szolgáltatásokat működtető számítógépek elhelyezésére szolgáló elkülönített helyiség(ek);

rr) tartomány: a hálózaton lévő szerverek és számítógépek logikai csoportja, amelyek egy közös biztonsági és bejelentkezési nyilvántartó rendszert használnak;

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

tt) tűzfal (firewall): a belső hálózatot a külső hálózattól védő szoftver és/vagy hardver eszköz. Szabályozza a két oldal közötti információáramlást, biztosítja, hogy az alkalmazások csak a számukra engedélyezett erőforrásokat érhessék el.

uu) zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem

II. AZ INFORMÁCIÓVÉDELEMMEL ÉRINTETT SZEREPLŐK FELADATKÖRE ÉS FELELŐSSÉGE

1. A FŐIGAZGATÓ FELADATKÖRE ÉS FELELŐSSÉGE

13. § (1) A Támogatáskezelő főigazgatója gondoskodik az elektronikus információs rendszerek védelméről a következők szerint:

a) jóváhagyja a Támogatáskezelő elektronikus információs rendszerei tekintetében a biztonsági osztályokba sorolást,

b) jóváhagyja a Támogatáskezelő elektronikus információs rendszereit kezelő/üzemeltető/fejlesztő felelős szervezeti egységek biztonsági szintbe sorolását,

c) az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,

d) meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,

e) jóváhagyja az információbiztonsági oktatási tervet,

f) jóváhagyja a Támogatáskezelő információbiztonsági cselekvési tervét,

g) biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,

h) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az Ibtv-ben foglaltak szerződéses kötelemként teljesüljenek,

i) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az Ibtv-ben foglaltak szerződéses kötelemként teljesüljenek,

j) együttműködik a hatósággal, amelynek során:

k) tájékoztatást nyújt a Támogatáskezelő elektronikus információbiztonságáért felelős személyéről,

l) tájékoztatás céljából megküldi a szervezet informatikai biztonsági szabályzatát,

m) az ellenőrzés lefolytatásához szükséges feltételeket biztosítja,

n) a Támogatáskezelő információbiztonsági politikáját,

o) a Támogatáskezelő információbiztonsági stratégiáját,

p) jóváhagyja az információbiztonsággal kapcsolatos szabályzatokat,

q) irányítja a vezetők informatikával összefüggő, illetve az elektronikus információbiztonsági felelős tevékenységét,

r) döntést hoz az információbiztonsággal kapcsolatos beruházások, fejlesztések tekintetében,

s) döntést hoz az informatikai biztonságot meghatározó, befolyásoló területek, tevékenységének összehangolása tekintetében.

2. AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI FELELŐS FELADATKÖRE ÉS FELELŐSSÉGE

14. § (1) A Támogatáskezelő elektronikus információbiztonsági felelőse gondoskodik az elektronikus információs rendszerek védelméről a következők szerint:

a) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek összehangolásáról, tervezéséről, szervezéséről, koordinálásáról és elvégzéséről, vagy irányításáról és ellenőrzéséről;

b) gondoskodik a Támogatáskezelő jogszabályoknak megfelelő működéséről;

c) elkészíti az információbiztonsági szabályzatot;

d) elkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezeti egységek biztonsági szintbe történő besorolását;

e) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit, rendelkezéseit;

f) kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal;

g) tájékoztatja a jogszabályban meghatározott szervet bármely elektronikus információs rendszert érintő biztonsági eseményről;

h) biztosítja a jogszabályokban megfogalmazott követelmények teljesülését a Támogatáskezelő valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában;

i) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért;

j) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről.

3. A GAZDASÁGI IGAZGATÓ FELADATKÖRE ÉS FELELŐSSÉGE

a) közvetlenül irányítja az Informatikai Osztályvezetőjének tevékenységét

b) dönt a jogosultság-igény kielégítéséről, megtagadásáról, vagy módosításáról és döntéséről tájékoztatja az igénylőt és az Informatikai Osztályt (Infokommunikációs Szabályzat 14. § d) pontja szerint)

c) benyújtott kérelem alapján dönt mobil számítógép használatának engedélyezéséről (Infokommunikációs Szabályzat 81. § (3) pont), illetve jogosult a használati idő lejárta előtt az engedélyt visszavonni és az eszköz visszaszállítását elrendelni (Infokommunikációs Szabályzat 88. §)

4. AZ INFORMATIKAI OSZTÁLY VEZETŐJÉNEK FELADATKÖRE ÉS FELELŐSSÉGE

15. § (1) A Támogatáskezelő gazdasági igazgatójának irányításával ellátja az Informatikai Osztály vezetését. Legfontosabb feladatkörei:

a) felel a Támogatáskezelő informatikai rendszereinek folyamatos és egységes működtetéséért;

b) irányítja az Osztály munkatársainak munkáját;

c) felel az üzemeltetést, illetve fejlesztést végző külső cégek, megbízottak munkájának koordinációjárt, ellenőrzéséért, ellenőrzi és igazolja a teljesítéseket,

d) az informatikai eszközökkel, szolgáltatásokkal kapcsolatos javítási, karbantartási, üzemeltetési szerződéseket megkötésre előkészíti;

e) felel az Informatikai Osztály által üzemeltetett informatikai eszközök, szoftverek, alkalmazások jogosultsági beállításaiért;

f) elkészíti és folyamatosan karbantartja a Támogatáskezelő informatikai szabályzatait.

5. A RENDSZERGAZDÁK ÉS AZ INFORMATIKAI OSZTÁLY MUNKATÁRSAINAK FELADATKÖRE ÉS FELELŐSSÉGE

16. § (1) A Támogatáskezelő informatikai üzemeltetési feladatait az Informatikai Osztály látja el az alábbiak szerint:

a) gondoskodik a szerverek és a rajtuk futó alkalmazások felügyeletéről;

b) gondoskodik a Támogatáskezelő számítógépeinek, informatikai eszközeinek és szoftvereinek, kommunikációs rendszereinek előkészítéséről és beüzemeléséről, üzemeltetéséről, a hibák elhárításáról;

c) gondoskodik a kiemelt szakrendszerek kivételével a jogosultsági szintek beállításáról és gondozásáról;

d) gondoskodik az informatikai biztonsági hiányosságok felszámolásáról az információbiztonsági vezető jelzése alapján;

e) a működéshez szükséges kiemelt, folyamatos üzemelést igénylő feladatok esetén gondoskodik az esetleges áramkimaradás, vagy feszültségingadozás elleni védelem biztosításáról;

f) gondoskodik a szoftverfrissítések (hibajavítások, verziókövetés) telepítéséről;

g) gondoskodik az informatikai eszközök, szoftverek karbantartásáról, javíttatásáról, beszerzéséről;

h) gondoskodik a szoftverek nyilvántartásáról,

i) gondoskodik a dokumentációk, leírások megőrzéséről, tárolásáról, selejtezteséről;

j) gondoskodik az eseti, egyedi felhasználói igények kezelése során felmerülő informatikai problémák megoldásáról;

k) gondoskodik az intézményi adatbázisok frissítéséről, a kiemelt szakrendszerek kivételével a rendszerek adatainak, beállításainak rendszeres mentéséről és archiválásáról, a tárolt adatok aktualizálásáról;

l) ellátja az intézményi és projekt rendszergazdai feladatokat;

m) javaslatot tesz az informatikai fejlesztésekre, megvalósítása esetén közreműködik annak lebonyolításában;

n) részt vesz az internetes felületek működtetésében;

o) a felügyelete alá tartozó teljes rendszer komplex biztonságával összefüggésben minden üzemeltető és felhasználó felé jogosult intézkedni, tevékenységüket jogosult korlátozni.

6. AZ ALKALMAZÁSGAZDÁK FELADATKÖRE ÉS FELELŐSSÉGE

17. § (1) A Gazdasági Igazgatóság Informatikai Osztálya a Támogatáskezelőnél használt valamennyi kiemelt informatikai rendszerhez alkalmazásgazdát nevez meg. Az alkalmazásgazda feladata a rábízott rendszer olyan mélységű ismerete, hogy zavartalan működését szakmai oldalról ellenőrizni tudja, illetve szükség esetén intézkedni tudjon a biztonságos működés érdekében.

(2) Az alkalmazásgazda feladatkörében:

a) feladatának ellátásához szükséges hozzáféréssel rendelkezik a megfelelő szoftverrendszer vonatkozásában;

b) a szakrendszer által biztosított lehetőségek alapján, a jogosultsági struktúra szerint beállítja az adott szakrendszerben a felhasználói jogosultságokat. A jogosultsági beállításokat dokumentálja;

c) informatikai és szakmai támogatást nyújt a felhasználóknak a szoftverrendszer használatát illetően;

d) az adott szakrendszert illetően meghatározza az adatmentések, archiválások gyakoriságát, módját, a visszaállítási tesztek gyakoriságát és metódusát;

e) specifikációt, dokumentációt készít a fejlesztésekhez,

f) részt vesz a fejlesztések tesztelésében,

g) hiba esetén közreműködik a szakrendszer helyreállításában, tesztelésében.

7. FELHASZNÁLÓK FELADATKÖRE ÉS FELELŐSSÉGE

18. § (1) A Támogatáskezelő informatikai rendszereinek felhasználói kötelesek az informatikai és biztonsági szabályokat betartani, illetve ezek betartásában az informatikai rendszer használatát irányító személyekkel együttműködni.

(2) Előbbiek alapján a felhasználók feladata:

a) az adatok elvárható és a vonatkozó szabályzásoknak megfelelő gondossággal való kezelése;

b) a rendelkezésre bocsátott számítástechnikai eszközök megóvása;

c) a belépési jelszavának (jelszavainak) az előírt, vagy javasolt időben történő megváltoztatása, titkosságának megőrzése;

d) a gépen tárolt információk védelme.

e) Ha elhagyja a munkaállomást, köteles azt olyan állapotban hagyni (például a számítógép zárolása funkcióval), hogy más ne használhassa, segítségével semmilyen információhoz hozzá ne férhessen, azokat ne módosíthassa, illetve a rendszerbe semmilyen információt be ne juttathasson;

f) a munkatársak adatállományaik biztonságáért felelősek, ezért kötelesek a munkaállomásukon létrehozott adataikat, dokumentumaikat a hálózati meghajtókra menteni;

g) az üzemeltető személyzettel való együttműködés;

h) az esetlegesen felfedezett biztonsági vagy működési problémák jelentése az illetékes üzemeltető személyzetnek;

i) a számukra szervezett informatikai oktatásokon részt venni;

j) a feladatainak elvégzéséhez szükséges eszközök, alkalmazói programok kezelésének megfelelő szintű ismerete.

(3) A felhasználóknak a biztonságos munkavégzés érdekében tilos:

a) az informatikai eszközök megbontása, a hardver konfigurációk megváltoztatása;

b) más felhasználók munkájának akadályozása, dokumentumainak illetéktelen megtekintése, másolása;

c) a hálózat megbontása, átstrukturálása, számítógépek, eszközök engedély nélküli csatlakoztatása, áthelyezése;

d) a Támogatáskezelő informatikai rendszerében nem alkalmazott szoftver installálása;

e) modem, vagy egyéb telekommunikációs eszköz beszerelése és használata.

8. KÜLSŐ PARTNEREK FELADATKÖRE ÉS FELELŐSSÉGE

19. § (1) A speciális informatikai vagy szakmai ismereteket igénylő folyamatok, munkák ellátásához a Támogatáskezelő külső partnereket bízhat meg. A külső partnerek típusuk munkavégzésük és jogi státuszuk szerint a következők lehetnek:

a) szerződéssel foglalkoztatott természetes személyek,

b) a felügyeleti szerv által delegált természetes személyek,

c) vállalkozói szerződéssel foglalkoztatott jogi személyek.

20. § (2) A Támogatáskezelő informatikai rendszereit használó külső partnereket ugyanazon kötelezettségek terhelik, mint a Támogatáskezelő alkalmazottait a következő megkötésekkel:

a) amennyiben jogosultsága szerint a természetes személy külső partner a Támogatáskezelő bármely informatikai, vagy szakrendszerének adatállományához hozzáféréssel rendelkezik, úgy titoktartási nyilatkozat kitöltésére kötelezett;

b) a jogi személyiséggel rendelkező külső partner munkavégzésének feltétele a partner biztonsági osztályba sorolása. Amíg a kívánt biztonsági osztály kritériumait a külső partner nem teljesítette, számára nem adható jogosultság;

c) a b) pontban megfogalmazottakat szerződésben kell rögzíteni;

d) a jogi személyiséggel rendelkező külső partnerrel kötött szerződésnek tartalmaznia kell az adatvédelmi és információbiztonsági garanciákat, nevezetesen:

da) a Támogatáskezelő hálózatát, hardver és szoftverállományát érintő bármiféle információ felhasználásának tiltása,

db) a Támogatáskezelő védelmi rendelkezéseiről szóló bármiféle információ felhasználásának tiltása,

dc) a Támogatáskezelő által kezelt adatok minőségére, mennyiségére, szerkezetére, logikai felépítésére vonatkozó bármiféle információ felhasználásának tilalma;

e) a Támogatáskezelő szerverszobájában külső partner kizárólag az Informatikai Osztály vezetőjének írásos engedélyével írásos módon indokolt esetben és kizárólag a Támogatáskezelő Informatikai Osztályának munkatársa jelenlétében és felügyelete mellett tartózkodhat, végezhet bármiféle tevékenységet. A tevékenység leírását a belépés és a kilépés időpontjának rögzítésével, a felügyelet ellátó munkatárs megnevezésével írásos formában kell rögzíteni.

III. AZ INFORMÁCIÓBIZTONSÁGHOZ KAPCSOLÓDÓ RENDELKEZÉSEK

1. KOCKÁZATELEMZÉS

21. § A III/1.1. fejezetben meghatározottak kivételével minden rendszer esetében rendelkezni kell olyan kockázatelemzéssel, ami a rendszer által nyújtott szolgáltatások részleges vagy teljes kimaradásának a Támogatáskezelő működőképességére tett hatásait tartalmazza. Külön kell kezelni a szolgáltatás elérhetetlenségéből, illetőleg az adatbázis sérülésből származó hatásokat. A kockázatelemzési dokumentum előállítása és karbantartása a Támogatáskezelő információbiztonsági felelősének és a szolgáltatás üzemeltetőjének, illetve alkalmazásgazdáinak a feladata. Az elektronikus információs rendszerek kockázatait a Vhr. által meghatározott követelményrendszer szerint is értékelni kell.

1.1 Információvagyon leltár

22. § (1) A kockázatelemzés alapját a Támogatáskezelő információvagyon leltára képezi. Az információvagyon leltár két komponensből áll:

a) adatvagyon leltár,

b) szoftverleltár.

(2) Az adatvagyon leltár előállítása és karbantartása a Támogatáskezelő adatvédelmi felelősének és alkalmazásgazdáinak feladata.

23. § A szoftverleltár tartalmazza a Támogatáskezelő tulajdonában vagy bérleményében álló összes szoftvert, beleértve az operációs rendszereket, az irodai szoftvercsomagokat, illetve a hardver- és hálózatüzemeltetéshez használt programokat, valamint a funkcionális szakrendszerek szoftvereit is.

24. § Nem szükséges kockázatelemzést végezni azon szoftverek esetén, amelyek licence, szerződése garantálja a szoftver sérülékenységeinek fejlesztő általi folyamatos monitorozását és a javítócsomagok automatikus közzétételét.

25. § A szoftverleltár elkészítéséért és naprakészen tartásáért az Informatikai Osztály felel

1.2 Biztonsági osztályba sorolás

26. § (1) Az Ibtv. és a Vhr. alapján a Támogatáskezelő az elektronikus információs rendszereit köteles biztonsági osztályba sorolni az információs rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának követelményei alapján. Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást a Támogatáskezelő főigazgatója hagyja jóvá. A biztonsági osztályba sorolást kockázatelemzés alapján kell elvégezni. A biztonsági osztályba sorolás eredményét jelen IBSZ tartalmazza. A biztonsági osztályba sorolást legtöbbször 3 évente, de új rendszer bevezetésekor azonnal el kell végezni. A Vhr. szerint a nemzeti adatvagyont kezelő rendszerek esetében a biztonsági osztályba sorolás során a legfőbb szempont az elektronikus információs rendszer sértetlensége, a különleges személyes adatokat kezelő rendszerek esetén pedig alapvető igény a bizalmasság fenntartása.

(2) A megállapítások alapján az EMET rendszerei az alábbi biztonsági osztályba tartoznak:

Alkalmazás azonosítója	Biztonsági osztály	Funkció	Tranzakciók típusa	Kezelt adatok jellege
EMET honlap	**2**	**weboldal /www.emet.gov.hu/**	**tartalomfrissítés**	**tájékoztató**
NKA honlap	**2**	**weboldal /www.nka.hu/**	**tartalomfrissítés**	**tájékoztató**
Intranet	**2**	**Ügyviteli rendszer**	**tartalomfrissítés**	**nyilvántartási adatok**
EPER	**3**	**Pályázatkezelési rendszer**	**Pályázatkezelési**	**nyilvántartási, személyes, pénzügyi adatok, különleges adatok**
EPER BURSA	**3**	**Pályázatkezelési rendszer**	**Pályázatkezelési**	**nyilvántartási, személyes adatok, pénzügyi adatok**

Effector	**2**	**Pályázatkezelési rendszer**	**Pályázatkezelési**	**nyilvántartási, személyes adatok, pénzügyi adatok**
Grantsys	**2**	**Pályázatkezelési rendszer**	**Pályázatkezelési**	**nyilvántartási, személyes adatok, pénzügyi adatok**
NKPR (Nemzeti Kiválóság Program) Pályázatkezelő Rendszer	**3**	**Pályázatkezelési rendszer**	**Pályázatkezelési**	**nyilvántartási, személyes adatok, pénzügyi adatok**
UKIR (Útravaló Ösztöndíjprogram) Pályázatkezelő Rendszer	**4**	**Pályázatkezelési rendszer**	**Pályázatkezelési**	**nyilvántartási, személyes, pénzügyi adatok, különleges adatok**
SBNT (Fejezeti Kulturális Pályázatok) Pályázatkezelő Rendszer	**2**	**Pályázatkezelési rendszer**	**Pályázatkezelési**	**nyilvántartási, személyes adatok, pénzügyi adatok**
KAB (Kábítószer-prevenciós programok) pályázatkezelő rendszer	**2**	**Pályázatkezelési rendszer**	**Pályázatkezelési**	**nyilvántartási, személyes adatok, pénzügyi adatok**
CSINI-PR (Család-, Ifjúság és Népesedéspolitikai Intézet – Pályázatkezelő Rendszer)	**2**	**Pályázatkezelési rendszer**	**Pályázatkezelési**	**nyilvántartási, személyes adatok, pénzügyi adatok**

Forrás KGR (Költségvetési Gazdálkodási Rendszer)	**2**	**Pénzügyi nyilvántartó program**	**pénzügyi**	**pénzügyi adatok**
KIR3	**2**	**Bérszámfejtő program**	**bérszámfejtési**	**pénzügyi adatok**
KIRA (Központosított Illetményszámfejtő Rendszer Alkalmazás)	**2**	**Munkaügyi és bérszámfejtő program**	**személyügyi és bérszámfejtési**	**nyilvántartási, személyes adatok, pénzügyi adatok**
Poszeidon EKEIDR Irat és Dokumentumkezelő Rendszer	**2**	**Ügyviteli és Iktató program**	**iratkezelési**	**iratkezelési adatok**
Spiceworks Hibabejelentő és Rendszerfelügyeleti Alkalmazás	**2**	**Ügyviteli rendszer**	**ügyviteli, hibabejelentő**	**nyilvántartási adatok**
Wintiszt	**2**	**Személyügyi nyilvántartó program**	**személyügyi**	**személyes adatok**
eLearning	**2**	**Oktató rendszer**	**tartalomfrissítés, online vizsga**	**tájékoztató, nyilvántartási**
UKIR oktató	**2**	**Oktató rendszer**	**tartalomfrissítés, beszámoló kezelés**	**személyes adatok, nyilvántartási adatok**
Winaccess Beléptető Rendszer	**2**	**beléptető rendszer**	**belépési adatok**	**személyes adatok, nyilvántartási adatok**

1.3 Szintbe sorolás

27. § (1) A Vhr. meghatározza a hatálya alá tartozó szervezetek, köztük a Támogatáskezelő szervezeti egységei számára előírt biztonsági szint besorolásának szabályait. Eszerint az elektronikus információs rendszert üzemeltetői, illetve alkalmazásgazdai szinten kezelő szervezeti egység biztonsági szintbe sorolása megegyezik az elektronikus információs rendszer biztonsági osztályával:

Alkalmazás azonosítója	Biztonsági osztály	Funkció	Tranzakciók típusa	Kezelt adatok jellege
EMET honlap	2	weboldal /www.emet.gov.hu/	tartalomfrissítés	tájékoztató
NKA honlap	2	weboldal /www.nka.hu/	tartalomfrissítés	tájékoztató
Intranet	2	Ügyviteli rendszer	tartalomfrissítés	nyilvántartási adatok
EPER	3	Pályázatkezelési rendszer	Pályázatkezelési	nyilvántartási, személyes, pénzügyi adatok, különleges adatok
EPER BURSA	3	Pályázatkezelési rendszer	Pályázatkezelési	nyilvántartási, személyes adatok, pénzügyi adatok
Effector	2	Pályázatkezelési rendszer	Pályázatkezelési	nyilvántartási, személyes adatok, pénzügyi adatok
Grantsys	2	Pályázatkezelési rendszer	Pályázatkezelési	nyilvántartási, személyes adatok, pénzügyi adatok
NKPR (Nemzeti Kiválóság Program) Pályázatkezelő Rendszer	3	Pályázatkezelési rendszer	Pályázatkezelési	nyilvántartási, személyes adatok, pénzügyi adatok
UKIR (Útravaló Ösztöndíjprogram) Pályázatkezelő Rendszer	4	Pályázatkezelési rendszer	Pályázatkezelési	nyilvántartási, személyes, pénzügyi adatok, különleges adatok
SBNT (Fejezeti Kulturális Pályázatok) Pályázatkezelő Rendszer	2	Pályázatkezelési rendszer	Pályázatkezelési	nyilvántartási, személyes adatok, pénzügyi adatok
KAB (Kábítószer-prevenciós programok) pályázatkezelő rendszer	2	Pályázatkezelési rendszer	Pályázatkezelési	nyilvántartási, személyes adatok, pénzügyi adatok

CSINI-PR (Család-, Ifijúság és Népesedéspolitikai Intézet –Pályázatkezelő Rendszer)	2	Pályázatkezelési rendszer	Pályázatkezelési	nyilvántartási, személyes adatok, pénzügyi adatok
Forrás KGR (Költségvetési Gazdálkodási Rendszer)	2	Pénzügyi nyilvántartó program	pénzügyi	pénzügyi adatok
KIR3	2	Bérszámfejtő program	bérszámfejtési	pénzügyi adatok
KIRA (Központosított Illetményszámfejtő Rendszer Alkalmazás)	2	Munkaügyi és bérszámfejtő program	személyügyi és bérszámfejtési	nyilvántartási, személyes adatok, pénzügyi adatok
Poszeidon EKEIDR Irat és Dokumentumkezelő Rendszer	2	Ügyviteli és Iktató program	iratkezelési	iratkezelési adatok
Spiceworks Hibabejelentő és Rendszerfelügyeleti Alkalmazás	2	Ügyviteli rendszer	ügyviteli, hibabejelentő	nyilvántartási adatok
Wintiszt	2	Személyügyi nyilvántartó program	személyügyi	személyes adatok
eLearning	2	Oktató rendszer	tartalomfrissítés, online vizsga	tájékoztató, nyilvántartási
UKIR oktató	2	Oktató rendszer	tartalomfrissítés, beszámoló kezelés	személyes adatok, nyilvántartási adatok
Winaccess Beléptető Rendszer	2	beléptető rendszer	belépési adatok	személyes adatok, nyilvántartási adatok

2. ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK

2.1 Biztonsági zónák

28. § (1) Az elektronikus információbiztonsági felelős, a Támogatáskezelő által használt épületekben az alábbi biztonsági zónákat hozta létre:

a) Számítógépterem, kapcsolószekrények (kiemelt védelem)

b) Raktárak, szerviz helyiségek területe (fokozott védelem)

c) Nyilvános helységek (pl.: irodák, folyosók) (alap védelem)

Az egyes biztonsági zónák követelményeit a **2.2.2 Elektronikus védelmi intézkedések** **33. §**-a tartalmazza.

2.2. Élőerős védelmi intézkedések

29. § A Támogatáskezelő épületeiben biztonsági szolgálat működik. A Támogatáskezelőnél a munkatársak belépéskor történő azonosítása a biztonsági szolgálat feladata. A biztonsági szolgálat látja el a látogatók, vendégek, külső szolgáltatók adatainak felvételét, ellenőrzését és rögzítését, továbbá a zárt láncú kamerarendszer által továbbított képek ellenőrzését.

2.2 Fizikai (mechanikai és elektronikus) védelmi intézkedések

30. § (1) A Támogatáskezelő által használt fizikai védelmi intézkedések két csoportra oszthatóak:

a) mechanikai védelmi intézkedések,

b) elektronikus védelmi intézkedések.

2.2.1 Mechanikai védelmi intézkedések

31. § (1) A mechanikai védelmi intézkedéseknek a kockázatokkal arányosak kell lenniük. A védelmi intézkedéseket megelőző kockázatleltárt a Támogatáskezelő elektronikus információbiztonsági felelőse és üzemeltetési osztályvezetője végzi el szükség esetén külső szakértő bevonásával.

(2) A Támogatáskezelő székhelyén és telephelyein a 3 méternél alacsonyabban levő ablakokat mechanikai védelemmel szükséges ellátni (rács, fólia, stb.). A mechanikai védelem tervezése és kivitelezése során figyelembe kell venni a MABISZ ajánlásait.

2.2.2 Elektronikus védelmi intézkedések

32. § A Támogatáskezelő proximity kártya alapú beléptető rendszert üzemeltet. A beléptető rendszer adatai alapján a biztonsági szolgálat feladata a Támogatáskezelő dolgozóinak, vendégeinek, látogatóinak beazonosítása a III/2.2. fejezet szerint.

33. § A fokozott és kiemelt védelemmel ellátott biztonsági zónákba csak az arra jogosult személyek kapnak belépési jogosultságot. A kiemelt védelemmel ellátott biztonsági zónákba a

belépési jogosultsággal rendelkező munkatársak mágneskártya vagy Proximity kártya használatával léphetnek be (belépéseket a biztonsági rendszer naplózza).

34. § A biztonsági rendszer riasztást ad, ha a biztonsági zónában, annak élesített állapotában bárki tartózkodik. Riasztás esetén a biztonsági szolgálat a számára kiadott szolgálati utasításban meghatározott módon jár el. A Támogatáskezelő területére a belépési kódot az Informatikai Osztály vezetőjenek a munkatárs kilépésekor azonnal meg kell vonnia, a jogosultságot azonnal le kell tiltatni a beléptető rendszerben, a kártyát pedig a kilépő munkatársnak az Üzemeltetési és Dokumentumkezelési Osztályon le kell adnia. A kiadott, letiltott jogosultságokat és azonosító eszközöket az Informatikai Osztály vezetője dokumentálja.

35. § Figyelemmel a Támogatáskezelő papíralapú iratforgalmára, a Támogatáskezelő székhelyén és telephelyein tűzjelző rendszer telepítése szükséges. A dohányzásra kijelölt helyek kivételével tilos a Támogatáskezelő bármely saját tulajdonú épületében, vagy bérleményében a dohányzás és a nyílt láng használata.

36. § A fokozott papír forgalmú helyiségekben (pl. irattár, iktató) önálló tűz- és/vagy füstérzékelő berendezéseket és tűzoltó készülékeket kell elhelyezni.

37. § A tűzvédelemre vonatkozó részletes szabályozást a Támogatáskezelő Tűzvédelmi szabályzata, az egyéb mechanikai védelmi intézkedésekkel és a beléptető rendszerrel kapcsolatos részletes szabályozást a Támogatáskezelő Vagyonvédelmi szabályzata tartalmazza.

2.4. Logikai védelmi intézkedések

38. § A Támogatáskezelő munkatársai a feladatuk ellátáshoz szükséges információkhoz történő hozzáférési szintjük szerint jogosultságmátrix alapján a kialakított jogosultságcsoportokhoz vannak rendelve. A jogosultságcsoportok a hálózati meghajtókon és szervereken tárolt információk típusa, fajtája és mennyisége alapján kerülnek kialakításra. Az egyes jogosultságcsoportokhoz tartozó jogosultságokról, azok tartalmáról és a kiosztott, továbbá megvont jogosultságokról az Informatikai Osztály nyilvántartást vezet. A jogosultságigénylés és -megvonás eljárásrendjét a Támogatáskezelő Infokommunikációs eszközökről szóló szabályzata tartalmazza.

39. § A Támogatáskezelő által üzemeltetett vagy használt szakrendszerek jogosultságtípusait, azok leírását, a kiosztott, illetve megvont jogosultságokat, továbbá a jogosultságigénylés és -megvonás eljárásrendjét a Támogatáskezelő egyes szakrendszereinek jogosultságigénylő belső utasítása tartalmazza. Az utasítások és nyilvántartások naprakészen tartásáért a szakrendszerek alkalmazásgazdái a felelősek.

40. § (1) A Támogatáskezelő alkalmazza a lefojtó útvonal irányítás eszközei közül a következőket:

a) hely szerint szűrt hozzáférés-védelem: publikus hálózatról csak a webfelület frontendjei érhetőek el, a demilitarizált zóna mögött elhelyezkedő elemek kizárólag engedélyezett IP címekről látogathatóak;

b) viselkedés alapú szűrés: intruder detection system alkalmazásával naprakész szabályrendszer alapján a felhasználói viselkedés szűrése, anomália esetén a felhasználó kitiltása a hálózatról.

c) Izoláció: a különböző rendszerek különböző zónákban helyezkednek el, amely zónák közt nincs átjárás.

3. SZERVERTEREM

41. § A Támogatáskezelő a központi rendszerei védelmére szervertermet alakít ki és a számítástechnikai folyamatok üzemeltetéséhez szükséges fontos eszközöket oda telepíti. A szerverterem kialakításának szabályai:

3.1 A szerverterem kialakításának szempontjai

42. § (1) Kiemelten **fontos szempontok** a szerverterem tervezésénél, kialakításánál és átalakításánál:

a) a statikai követelmények (várható maximális födémterhelés, eszközök száma, azok várható súlya) figyelembe vétele;

b) a környezetből adódó rezgések, környezeti zavarok (pl. nagy-frekvenciás hálózat) figyelembe vétele;

c) a klimatizálás biztosítása;

d) a szünetmentes tápellátás biztosítása;

e) a géptermet kerüljék el a közműhálózati vezetékek (víz, gáz, csatorna, stb.); a szerverterem felett és a határoló falfelületei mellett vizesblokkot tartalmazó helyiség nem lehet, felette és mellette a falban gáz- vagy vízcsövek nem haladhatnak;

f) a szerverterem ajtói rendelkezzenek legalább 30 perces (mű. bizonylatolt) tűzállósággal;

g) a géptermen belül automatikus betörés- és tűzjelző rendszert kell telepíteni, ami mozgás-, nyitás-, füst-, üvegtörés és vízérzékelőkkel rendelkezzen; az érzékelők és a jeleket feldolgozó központ feleljen meg az MSZ 9785, valamint az EN 54 szabványsorozatok előírásainak, rendelkezzenek a hazai minősítő intézetek forgalomba-hozatali engedélyével;

h) törekedni kell a szerverteremben az ablakok elfalazásáról, de ha ablakok mégis megmaradnak, akkor azokon legyen belülről átlátszó fólia;

i) a padlóburkolatok, berendezési tárgyak tűzálló és antisztatikus anyagból legyenek;

j) az épület villámvédelme elégítse ki a kommunális- és lakóépületekre vonatkozó előírásokat; az MSZ 274-5T:1993 szabvány szerint az LPZ 0B - LPZ 1 zónahatáron túlfeszültség elleni védelembe be kell vonni az árnyékolást megtestesítő, a helységhez tartozó összes fémszerkezetet (az elektromos hálózatot, víz, gáz, távfűtés, csatornahálózatokat, antenna bevezetéseket, adatátviteli és távbeszélő hálózatokat stb.);

k) a szerverszobán kívül legyen kialakítva külön operátor szoba, és szervizszoba.

3.2 A szerverteremmel kapcsolatos minimális követelmények

43. § (1) A szerverterem védelmének kialakításában és fenntartásában részvevők kötelesek, a tervezés és megvalósítás, majd üzemeltetés során az alábbi követelmények betartására és betartatására:

a) a nyílászárók (ajtók, ablakok) rendelkezzenek nyitottság és zártság ellenőrző eszközzel;

b) a belső terek védelme mozgásérzékelővel legyen biztosított; a védelem ki- és bekapcsolása a bejáraton kívül elhelyezett minimum 6 számjegyes kóddal működtetett tasztatúráról történjék;

c) megfelelő kapacitású klíma és szünetmentes tápellátó rendszer álljon rendelkezésre;

d) automatikus tűzjelző és halonnal oltó tűzoltórendszer folyamatosan álljon rendelkezésre;

e) a szerverterembe belépni szándékozók belépés előtti automatikus azonosításának lehetősége (pl. mágneskártya, proximity kártya) álljon rendelkezésre.

3.3 A szerverterembe történő be- és kilépés rendjének szabályozása

44. § (1) A szerverterembe való belépésre jogosultak kötelesek az alábbi követelmények betartására és betartatására:

a) A szerverterembe történő belépéshez szükséges kártyák vagy kódazonosítók kiadását és visszavonását az Informatikai Osztály vezetője engedélyezi.

b) Látogató kizárólag csak a benntartózkodáshoz engedéllyel rendelkező személy jelenlétében tartózkodhat a szerverteremben, és a belépését a szerverterem vendégkönyvében regisztrálnia kell.

c) Külső munkatárs csak a benntartózkodáshoz engedéllyel rendelkező személy jelenlétében és felügyelete mellett végezhet munkát. A külső munkatárs ilyen esetben a végzett munkát (pl. hibajavítás, takarítás) a Géptermi eseménynaplóban dokumentálni köteles.

d) Az Informatikai Osztály vezetője nyilvántartást köteles vezetni az aktuálisan érvényes géptermi belépési jogosultságokról.

3.4 A szervertermi munkavégzés, a terem zárása/nyitása

45. § (1) A szerverteremben történő biztonságos munkavégzés érdekében, az ott munkát végzők kötelesek az alábbi követelmények betartására és azt betartatására:

a) A szerverterem biztonságilag kiemelten védett terület, munkaszünet esetén a szerverterem zárását/nyitását csak a terem üzemeltetését végző felelős személyek végezhetik.

b) A géptermi munka befejezése után a szerverterem zárása saját kulccsal, majd a biztonsági rendszer élesítésével történik. A biztonsági rendszert csak a szerverteremben munkát végző és felhatalmazott operátor élesítheti.

c) A szerverterem nyitására ugyanez vonatkozik, csak fordított sorrendben.

d) A számítógépeket és a kisegítő berendezéseket (perifériák) munkaszünet alkalmával bekapcsolt állapotban lehet hagyni.

e) A szerverek zárási és indítási eljárásait munkautasítás (Üzemeltetés rendje) tartalmazza.

(2) A szerverterem bezárása előtt:

a) ellenőrizni kell a klíma hőfokszabályzó állását (max. 24 °C-ra lehet állítva),

b) az ablakokat zárt állapotban kell hagyni,

c) a szalagfüggönyöket a belátás megakadályozására el kell fordítani.

d) A szerverterem biztonsági (tartalék) kulcsát és a belépő kódot lezárt és aláírt borítékban a biztonsági szolgálat őrzi.

e) A szerverterem zárásakor, ill. nyitásakor észlelt bármilyen rendellenességet az Osztály vezetője felé azonnal jelenteni kell.

f) A szerverterem zárására/nyitására jogosultsággal rendelkező munkatársakról nyilvántartást kell vezetni. Minden ilyen jogosultság megadását az Informatikai Osztály vezetője engedélyezi.

3.5 Szerverteremre vonatkozó egyéb előírások

46. § (1) A szerverterem üzemeltetésében részvevők kötelesek az alábbi követelmények betartására és betartatására:

47. § A szerverterem biztonsági (betörés- és tűzjelző) rendszere szünetmentes áramellátásról működjön, eseménykor az épület biztonsági szolgálatára, valamint a Rendőrségre, ill. a Tűzoltóságra adjon riasztást.

a) A szerverterem összes ajtaját folyamatosan – munkavégzés alatt is – csukva kell tartani. Ennek érdekében az ajtókat automatikus csukó szerkezettel kell ellátni.

b) A szerverterembe történő ki- és bejárás céljára egy és csakis egy ajtó álljon rendelkezésre.

c) A szerverteremben üzemelő informatikai eszközök legyenek ellátva a villámlás másodlagos hatásai elleni védelemmel.

4. HARDVEREKRE ÉS SZOFTVEREKRE VONATKOZÓ ELŐÍRÁSOK

4.1 A központi rendszerekkel kapcsolatos szabályozás

48. § A Támogatáskezelő a *központi rendszer*ekhez kiemelt védelmet biztosít. Minden esetben, amikor a szerverteremben, illetve vele, egyenrangú védelemmel rendelkező más területen szerverek és kommunikációs eszközök telepítése történik, biztosítani kell ezen eszközök biztonságos elkülönítését és védelmét (pl. szerver szoba és operátori szoba kialakításával).

49. § A szervereket és a kommunikációs eszközöket (router, switch), azok fizikai védelme céljából erre a célra kialakított jól szellőző, zárható szekrényben elzárva kell üzemeltetni. A szervereknél

és a kommunikációs eszközöknél (router, switch) biztosítani kell a személyre szóló azonosítás alapján történő logikai hozzáférést.

50. § A központi rendszer elemei telepítésének, áttelepítésének végrehajtása minden esetben az Informatikai Osztály vezetőjének a felelőssége. Szerver vagy kommunikációs eszköz nem az IBSZ által előírt körülmények közötti elhelyezésére csak az Informatikai Osztály vezetője előzetes és egyedi engedélye mellett van lehetőség, és csak átmeneti jelleggel. A központi rendszerek telepítésénél az Informatikai Osztálynak minden esetben kiemelten kell gondoskodni a berendezések biztonságáról, az illetéktelen hozzáférés megelőzéséről, megakadályozásáról. A központi rendszerekhez sem a rendszereket szállítók, sem a rendszert fejlesztők nem rendelkezhetnek közvetlen hozzáférési jogosultsággal. Minden egyes külső beavatkozás (verziófrissítés, programhiba javítás, egyedi fejlesztés stb.) során dokumentálni kell a programváltozásokat, az elvégzett ellenőrzéseket, teszteléseket.

51. § A központi rendszerekhez tartozó helyi hálózat megbízhatóságának növelésére, annak túlterhelését, hálózatrészek kiesését megelőző, a helyi adottságoknak megfelelően kiválasztott rendszertechnikai megoldásokat (redundáns átviteli utak, illetve aktív elemek, dinamikus átkonfigurálás, osztott hálózatvezérlés stb.) kell alkalmazni.

52. § A számítástechnikai eszköz telepítésének részét képezi az eszköz verifikálása (ellenőrzés). A verifikálás eredményét, azaz hogy az eszköz a meghatározott biztonsági követelményeknek eleget tesz, az Informatikai Osztály köteles írásban rögzíteni.

4.2 Munkaállomások, laptopok

53. § (1) Munkaállomások, laptopok telepítése, konfigurációkezelése során az alábbiakat kell figyelembe venni:

a) Minden munkaállomás telepítést, módosítást, cserét az Infokommunikációs eszközökről szóló szabályzatban foglalt eljárásrend szerint kell kezdeményezni.

b) A munkaállomásokról nyilvántartását kell vezetni. A nyilvántartás tartalmazza a munkaállomás hardver konfigurációját és a munkaállomásra telepített szoftvereket. A nyilvántartások vezetése, azok aktualizálása az Informatikai Osztály feladata.

c) A munkaállomásokat csak a feladat ellátásához szükséges beállításokkal és programokkal szabad telepíteni.

d) A munkaállomások elhelyezésénél (fizikai telepítés) minden esetben kiemelten kell gondoskodni a berendezések biztonságáról, az illetéktelen hozzáférés megelőzéséről, megakadályozásáról. Azon irodahelyiségeket, ahol munkaállomás működik, tilos felügyelet nélkül hagyni, ha a helyiségben senki sem tartózkodik, azt be kell zárni.

e) A munkaállomáson egyedi hozzáférést kell biztosítani, ezáltal lehetővé téve, hogy a munkaállomást csak az arra jogosult Felhasználók használhassák.

4.3 Vírusellenőrzés

54. § A Támogatáskezelő biztosítja az informatikai rendszerének egészére kiterjedő rend-szeres és folyamatos vírusvédelmet. Vírusellenőrzés történik a helyi hálózaton, a levelező szerveren, valamint az összes munkaállomáson.

55. § Az Informatikai Osztály gondoskodik arról, hogy a vírusellenőrző programnak mindig a legújabb verziója működjön. A frissítéseknek maximum 1 munkanapon belül meg kell történniük.

56. § Csak jogtiszta és megfelelő dokumentációval ellátott vírusellenőrző program használata megengedett.

57. § A vírusellenőrző programot csak speciális esetekben, csak az Informatikai Osztály vezetőjének utasítására lehet kikapcsolni. A rendszergazda kötelessége, hogy a vírusvédelmet a lehető legrövidebb időn belül visszakapcsolja. A vírusirtó leállítását és újraindítását az Informatikai Osztálynak űrlapon dokumentálnia kell. A felhasználók a vírusvédelmet semmilyen körülmények között sem kapcsolhatják ki.

58. § A hatékony vírusvédelem érdekében a Támogatáskezelő munkatársaihoz kívülről érkező leveleken kiterjesztés és tartalom szerinti szűrést kell végezni és a vírusgyanús leveleket azonnal karanténba kell helyezni.

59. § (1) Amennyiben a vírusellenőrzések ellenére a felhasználók vírusra utaló hibás, vagy furcsa működést tapasztalnak, a vírusfertőzés gyanújáról azonnal értesíteni kell az Informatikai Osztályt. Rosszindulatú alkalmazás jelenlétére utaló jelek különösen:

a) rosszindulatú alkalmazás elleni védelemről gondoskodó alkalmazás névvel azonosított rosszindulatú alkalmazást jelez;

b) fájl másolása esetén a forrásfájl és a célfájl mérete, neve eltérő;

c) szokatlan és váratlan képernyő tevékenység;

d) szokatlan alkalmazás-tevékenység: felhasználói beavatkozás nélkül elinduló alkalmazások, a megszokottól eltérően viselkedő alkalmazások, elérhetetlen funkciók, stb.;

e) jelentősen lassult működés, amely többszöri újraindítás során sem javul.

60. § Külső adathordozó használata előtt az adathordozó adatállományát a rosszindulatú alkalmazás elleni védelemről gondoskodó alkalmazás használatával ellenőrizni kell.

61. § A vírus-detektálás (vagy vírusgyanú felmerülése) és a víruseltávolítás biztonsági eseménynek számít, ezért minden vírusdetektálást és víruseltávolítást haladéktalanul jelenteni kell az Informatikai Osztály vezetője és az elektronikus információbiztonsági felelős felé. Az ilyen eseményt az Informatikai Osztálynak ki kell vizsgálnia, és dokumentálnia, illetve az Ibtv-ben meghatározott jelentési kötelezettségnek eleget tennie.

62. § Az Informatikai Osztály vezetője időszakosan ellenőrizni köteles, hogy az aktuálisan használt vírusellenőrző program megegyezik a kiadott legfrissebb változattal.

63. § A biztonsági kockázatot jelentő elektronikus küldemények kezelése során az Iratkezelési Szabályzat rendelkezéseit is figyelembe kell venni.

4.4 Rendszerek fejlesztése, továbbfejlesztése, verzióváltások

64. § A Támogatáskezelőbe új rendszer fejlesztésével, létező rendszerek tovább fejlesztésével, az új rendszerek, verziók bevezetésével és szükséges dokumentációival kapcsolatos biztonsági elvárásokat az Informatikai Osztály által készített és évente karbantartott követelményjegyzék tartalmazza. A követelményjegyzéket a Támogatáskezelő minden rendszerfejlesztés, rendszerbevezetés tartalmú pályázatának, szerződésének mellékleteként csatolni kell, a benne foglaltakat a szállítóktól meg kell követelni.

65. § Külső és belső ellenőrzési eszközökkel ellenőrizni kell, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

66. § (1) Az elektronikus információbiztonsági felelős valamennyi rendszer vagy rendszerelem, hardver és szoftver beszerzése során meghatározza és szerződéses követelményként megkövetelheti az alábbiakat:

a) a funkcionális biztonsági követelményeket;

b) a garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint);

c) a biztonsággal kapcsolatos dokumentációs követelményeket;

d) a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket;

e) az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat;

f) az elfogadási kritériumokat.

67. § A rendszerfejlesztésekben résztvevő munkatársak, a rendszer valamennyi életciklusában értékeli és érvényesíti a biztonsági követelményeket. Az elektronikus információbiztonsági felelőssel együttműködve meghatározzák a rendszerhez kapcsolódó információbiztonsági szerepköröket és felelősségeket.

68. § (1) A rendszer életciklus szakaszokat a következők szerint kell meghatározni:

a) követelmény-meghatározás;

b) fejlesztés vagy beszerzés;

c) megvalósítás vagy értékelés;

d) üzemeltetés és fenntartás;

e) kivonás (archiválás, megsemmisítés).

69. § Az elektronikus információs rendszerek beszerzése és fejlesztése során az elektronikus információbiztonsági felelős megköveteli a rendszer adminisztrátori és fejlesztői

dokumentációjának az elkészítését, melyeknek tartalmazniuk kell rendszer biztonsági vonatkozásait, a biztonságos konfigurálását, telepítését és üzemeltetését, a biztonsági funkciók hatékony alkalmazását és fenntartását, ismert sérülékenységeket, továbbá a felhasználó által elérhető biztonsági funkciókat és a felhasználó kötelezettségeit a biztonság fenntartásához;

4.5 Rendszerkarbantartások

70. § (1) Az Informatikai Osztály, az elektronikus információbiztonsági felelőssel együttműködve, a rendszerkarbantartások és az azokhoz kapcsolódó ellenőrzések elvégzése érdekében rendszerkarbantartási eljárásokat alakít ki. Az elvégzett karbantartási tevékenységekről nyilvántartást vezetnek. A karbantartások tervezése és végrehajtása során:

a) a gyártói vagy a forgalmazó specifikációknak megfelelően, továbbá a szervezeti igények szerint a karbantartásokat és javításokat ütemezetten hajtja végre;

b) dokumentálja és felülvizsgálja a karbantartásokról és javításokról készült feljegyzéseket;

c) jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban;

d) külső karbantartó személyzet esetén minden esetben ellenőrizni kell karbantartást végzők, szervezetek vagy személyek jogosultságát a munka elvégzésére;

e) az Informatikai Osztály vezetőjének, vagy az általa meghatalmazott felelős munkatársak jóváhagyása szükséges az elektronikus információs rendszer vagy a rendszerelemek Támogatáskezelő létesítményeiből történő kiszállításhoz;

f) gondoskodik arról, hogy az elszállítás előtt minden adat és információ – mentést követően – a berendezésről törlésre kerüljön;

g) a javítási tevékenységek után ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat;

h) csatolja a meghatározott, karbantartással kapcsolatos információkat a karbantartási nyilvántartáshoz.

(2) A karbantartási terveket és eljárásokat évente felül kell vizsgálni és szükség szerint aktualizálni.

5. AZ ADATHORDOZÓK KEZELÉSE ÉS BIZTONSÁGA

71. § Az adatok sérülésének elkerülése és a működésfolytonosság fenntartása érdekében, az Informatikai Osztály és az információbiztonsági felelős, üzemeltetési eljárásokat hoz létre, az elektronikus dokumentumokhoz, számítógép médiumokhoz, adathordozókhoz történő jogosulatlan hozzáférés, módosítás, ellopás megakadályozása érdekében. A védelem szabályozási, logikai és fizikai eljárásokat tartalmaz a 4. alfejezetben, a Támogatáskezelő Vagyonvédelmi szabályzatában és az Infokommunikációs eszközökről szóló szabályzatban foglaltaknak megfelelően.

5.1 Az eltávolítható adathordozók kezelése

72. § (1) A hordozható adathordozók – más terminológia szerint eltávolítható adathordozók – jellegükből adódóan jelentős információbiztonsági kockázatot hordoznak.

(2) Az eltávolítható adathordozók közé tartoznak az adatkazetták, CD-k, DVD-k, külső merevlemezek, pendrive-ok, de ebbe a kategóriába kell sorolni hozzáférhetőségük és felépítésük miatt a mobiltelefonok és fényképezőgépek memóriáját is. (Általában használatos még az „USB mass storage" elnevezés is.)

(3) A legnagyobb veszélyt az eltávolítható adathordozók jogosulatlan használata jelenti. A Támogatáskezelő hálózatához ilyen eszközt kapcsolva fennáll a rosszindulatú kódok (vírusok) bejutásának veszélye, másrészről pedig fennáll az adatok jogosulatlan elvitelének veszélye, ezért a dolgozók saját **eltávolítható adathordozóikat külön feljogosítás nélkül a hálózathoz nem csatlakoztathatják!**

5.2 Az eltávolítható adathordozókkal kapcsolatos irányelvek

73. § (1) Az eltávolítható adathordozókkal kapcsolatos irányelvek a következők:

a) bizalmas információ csak titkosítva írható fel rájuk;

b) biztosítani kell hardver titkosítással ellátott pendrive-okat azon üzleti munkatársak számára, akiknek munkájához indokolt;

c) a titkosítatlan optikai adathordozókat, amennyiben már nem szükségesek, helyreállíthatatlanul fizikailag meg kell semmisíteni;

d) a megőrzendő adatok esetében figyelembe kell venni az eszköz várható élettartamát és ennek megfelelően időközönként át kell másolni az adatokat vagy több helyen kell azokat tárolni.

5.3 Adathordozók újrahasznosítása és selejtezése

74. § (1) Az adathordozók újrahasznosítása és selejtezése során, az adatok kiszivárgásának megakadályozására, az Informatikai Osztály az alábbi utasításokat betartva jár el:

a) A már szükségtelenné vált adatot tartalmazó, de újrafelhasználható adathordozókat – tipikusan munkaállomások, laptopok merevlemezei, új felhasználóhoz történő kiadásuk előtt –szokásos formázási vagy törlési eljárással törli, majd az eszközt újra használatba adja. Ez kizárólag a szervezeten belül történő újrafelhasználás esetén érvényes.

b) A használaton kívüli adathordozókat osztályozza aszerint, hogy tartalmaznak-e érzékeny adatot. Amennyiben ez nem megállapítható, akkor az adathordozót úgy kezeli, mint ami érzékeny adatot tartalmaz.

c) Az érzékeny adatokat tartalmazó mágneses adathordozókat (merevlemezeket) le-mágnesezéssel vagy speciális felülírással törli.

d) Azokat az adathordozókat, amelyek már további használatra nem alkalmasak, selejtezi. A selejtezésre szánt adathordozókról jegyzőkönyvet vesz fel, és az adatmegsemmisítést bizottságilag jegyzőkönyvezi.

e) Valamennyi adathordozó típus esetén igénybe veheti a speciális, adatmegsemmisítéssel foglalkozó cégek szolgáltatását, amelyek bezúzással, vagy égetéssel, jegyzőkönyvezés mellett végzik a megsemmisítést.

f) A nem elektronikus – jellemzően papír alapú – adathordozók esetében is hasonlóan kell eljárni, a használatból kivont adathordozókat első sorban fizikailag kell megsemmisíteni az Iratkezelési Szabályzatban foglaltak szerint.

5.4 Az adathordozók tárolása és védelme

75. § (1) Az adathordozók tárolása és védelme érdekében az alábbi utasításokat kell követni:

a) Az adathordozókat a rajtuk lévő adatok érzékenységének megfelelően védeni kell, használaton kívül el kell zárni.

b) Adathordozó (adat) a Támogatáskezelő területéről csak a főigazgató írásos engedélyével, az 1. számú mellékletben található kérelem alapján kerülhet ki. Ez vonatkozik az adathordozókon történő kivitelre, vagy az egyéb, elektronikus úton történő továbbításra, mint az Internet vagy a (mobil)telefonos adattovábbítás.

c) A központi infrastruktúrán (kiszolgálók, csoportkönyvtárak, fájl szerverek stb.) kívül például felhasználói munkaállomásokon, laptopokon csak olyan adatot szabad tárolni, melyek sérülése, elvesztése vagy illetéktelenek kezébe történő kerülése nem okozhat a Támogatáskezelő számára kárt vagy bizalomvesztést. Az ilyen adatok nem kerülnek központi mentésre, ezért a mentési igényt minden esetben az Informatikai Osztály vezetője felé kell jelezni.

d) A személyi használatra kiadott laptopokon bizalmas információt csak titkosítva szabad tárolni.

6. DOKUMENTÁCIÓKHOZ KAPCSOLÓDÓ VÉDELMI INTÉZKEDÉSEK

76. § (1) Minden nyilvántartott szoftverhez nyilván kell tartani a szoftver dokumentációját, ami magában foglalja az alábbiakat**:**

a) felépítésének, funkcióinak és adatkapcsolatainak felső szintű leírását, valamint alapvető jellemzőit (mérete, nyelve, működési környezet, készítője);

b) felhasználói és üzemeltetői kézikönyveket, különösképpen a felhasználói jogosultság rendszer leírását, továbbá a felhasználó kötelezettségeit a biztonság fenntartásához;

c) a rendszer telepítőkészletét, telepítési segédleteit;

d) a tesztelést igazoló, valamint az üzemeltetésre átvétel jegyzőkönyveit;

e) az üzemi, konfigurációs beállítások leírását;

f) a rendszer üzemeltetésével, támogatásával kapcsolatos partneri megállapodásokat (pl.: licencek, szerződések, elérhetőségek);

g) a rendszer biztonsági vonatkozásait, az ismert sérülékenységeket, biztonsági funkciók hatékony alkalmazását és fenntartását.

77. § A felsorolt dokumentumok őrzése az Informatikai Osztály feladata. A rendszerleírási és rendszerprogram dokumentációinak első példányát az Informatikai Osztály informatikai könyvtárában kell tárolni elektronikus formában. A leírások és dokumentációk másodpéldányát papíron (és lehetőség szerint elektronikus formában is) tűzbiztos lemezszekrényben kell tárolni. A dokumentációkat minden esetben úgy kell elhelyezni, hogy azok a tárolás közben ne sérüljenek vagy károsodjanak.

78. § Gondoskodni kell arról, hogy az információs rendszerre vonatkozó – különösen az adminisztrátori és fejlesztői – dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható.

79. § Gondoskodni kell a dokumentációknak az érintett szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről.

80. § A rendszerleírások és rendszerprogram dokumentációinak frissítését minden olyan esetben, amikor a rendszeren változtatás (rendszerkonfiguráció változtatás, javítás, verzióváltás, stb.) történik, az üzembe állítás (üzemeltetésre átadás) előtt frissíteni kell. A dokumentációk naprakészségért az Informatikai Osztály a felelős.

81. § A rendszerleírásokról és rendszerprogram dokumentációkról űrlapon kell pontos nyilvántartást vezetni, a verziószámoknak és a telepítés időpontjainak a feltüntetésével. A nyilvántartásnak biztosítania kell, hogy legalább 1 évre visszamenőleg meghatározható legyen minden, az egyes rendszerekkel kapcsolatos változás ideje, oka, mibenléte. A nyilvántartás vezetése és annak folyamatos aktualizálása az Informatikai Osztály feladata.

82. § A felhasználói dokumentációk folyamatos rendelkezésre állása megköveteli, hogy a dokumentumokat gyorsan és egyszerűen el lehessen érni. A felhasználói dokumentációkat javasolt elektronikusan, nyilvános mappában, vagy intraneten tárolni.

7. ELEKTRONIKUS KOMMUNIKÁCIÓHOZ KAPCSOLÓDÓ VÉDELMI INTÉZKEDÉSEK

7.1 Általános rendelkezések

83. § A Támogatáskezelő hálózatát, vagy munkaállomásait csak ellenőrzött kapcsolaton keresztül lehet más hálózatokhoz csatlakoztatni. Engedély nélkül tilos bármilyen egyéni kommunikációs eszköz (pl. mobiltelefon, másik hálózathoz csatlakozni képes számítógép) csatlakoztatása a Támogatáskezelői munkaállomásokhoz. A fentiek biztosítása érdekében a Támogatáskezelő munkaállomásainak technikai beállításait úgy kell elvégezni, hogy a mindennapi munkához nem szükséges kommunikációs lehetőségek tiltva legyenek.

7.2 E-mail használattal kapcsolatos előírások

84. § (1) Az e-mail használatával kapcsolatos, jelen paragrafus alatti előírásokat akkor kell alkalmazni, ha a Támogatáskezelő működésére irányadó egyéb szabályzat, így különösen az Iratkezelési Szabályzat másként nem rendelkezik. Az elektronikus levelezés célja a gyors ügyintézés és a papír alapú dokumentumok mennyiségének csökkentése. A Támogatáskezelő minden munkatársával szemben elvárás az elektronikus levelezéssel kapcsolatban a körültekintő és etikus viselkedés.

(2) A Támogatáskezelő munkatársaira az alábbi, az elektronikus levelező rendszerre vonatkozó jogok és kötelezettségek vonatkoznak:

a) a belső elektronikus levelező rendszerben továbbított üzenet, levél vagy csatolt fájl egyenértékű az üzenet, levél vagy csatolt fájl személyes, papír alapon történő átadásával;

b) az elektronikus levelező rendszerből kifelé továbbított üzenet nem vonatkozhat kötelezettségvállalásra;

c) az elektronikus levelező rendszerből kifelé továbbított bizalmasan kezelendő üzenet csak titkosítva küldhető;

d) az elektronikus levelező rendszerből kifelé továbbított levélben vagy üzenetben tilos a Támogatáskezelő rossz hírét kelteni;

e) elektronikus levelezéskor az elektronikus levelezési címet csak az arra jogosult személy használhatja, más nevében elektronikus levél küldése nem engedélyezett;

f) az elektronikus levelező rendszer használata során minimálisra kell csökkenteni annak személyes célokra történő használatát, az elektronikus levelező rendszerrel személyes üzleti tevékenység nem végezhető;

g) a téves címzés miatt megkapott levelet bizalmasan kell kezelni, és azt haladéktalanul az eredeti címzettjének vagy a feladójának kell továbbítani;

h) a Támogatáskezelő elektronikus levelező rendszerében továbbított üzenetben vagy levélben nem alkalmazható kézi aláírás szkennelt változata;

i) a Támogatáskezelő elektronikus levelező rendszerében továbbított üzenetben vagy levélben a Támogatáskezelő Arculati Kézikönyvében meghatározott formát kell alkalmazni.

j) a postafiók tárhelye beosztástól függően korlátozott, így ennek felszabadítására szükséges archiválást egy lokális archív fájlba (továbbiakba: *.pst) kell megtenni, amelyet a munkatárs a saját hálózati meghajtóján köteles tárolni. A *.pst fájl megengedett maximális mérete 5 GB, így ennek az adatmennyiségnek az elérése után, a fent említett szabályok szerint új *.pst fájlba kell folytatni a levelek archiválását.

7.3 Vezeték nélküli hozzáférés

85. § (1) A Támogatáskezelő a mobileszközökkel rendelkező felhasználói számára egyedi engedélyezési eljárás után vezeték nélküli (WiFi) hozzáférési lehetőséget biztosíthat elektronikus információs rendszereihez. Az igénylő munkahelyi vezetője javaslatával ellátott kérelmet juttat el a Támogatáskezelő főigazgatójához. A Főigazgató jóváhagyását követően adható a felhasználó számára WiFi hozzáférési jogosultság.

(2) A vezeték nélküli hálózat létesítése és üzemeltetése során az alábbi feltételeknek kell teljesülniük:

a) A vezeték nélküli hozzáférést titkosítással és a felhasználók, vagy eszközök hitelesítésével kell védeni;

b) A vezeték nélküli hálózat konfigurálását a rendszergazdák csak közvetlen jogosultság birtokában, a védett hálózaton kialakított vezetékes kapcsolaton keresztül végezhetik;

c) A vezeték nélküli hálózat üzemeltetése során megfelelő karakterisztikájú és teljesítményszintű antennák, vagy egyéb technikák alkalmazásával gondoskodni kell arról, hogy a szervezet fizikai határain kívülről a jelek észlelésének a valószínűsége minimális legyen;

d) A belső hálózatra irányuló nyílt WiFi alkalmazása a Támogatáskezelő területén tilos. Nyílt, ún. vendég WiFi kizárólag külön zónában elhelyezett, a belső hálózattól szeparált módon lehetséges.

7.4 Behatolásvédelmi szabályok és tűzfalak

86. § (1) Behatolásvédelmi szabályokra és tűzfalakra vonatkozó rendelkezések a következők:

a) Az Informatikai Osztály, a Támogatáskezelő a Központi rendszereit tűzfallal vagy azzal egyenértékű tűzfal jellegű berendezéssel (továbbiakban: Tűzfal) védi, annak megakadályozására, hogy kívülről illetéktelen személy a rendszerbe behatolhasson. Az ilyen védelmi feladatot ellátó berendezést a Központi rendszerek részének kell tekinteni.

b) A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban kell elhelyezni, elkülönítve a belső szervezeti hálózattól.

c) A Támogatáskezelő hálózatáról szigorúan tilos bármilyen, a tűzfalat megkerülő kapcsolatot létesíteni nyilvános hálózatokkal (pl.: Internetet modemen keresztül használni).

d) Nem nyilvános hálózatokat (pl. banki átutalásokhoz bankterminál használata, BM hálózata) csak ellenőrzött kapcsolaton keresztül szabad használni.

e) Az alkalmazott tűzfal auditáltatását annak üzembe helyezését követően külső szakértővel el kell végeztetni.

f) Az alkalmazott tűzfalon változtatást csak a hálózati eszközök rendszergazdája végezhet, ha azt az Informatikai Osztály vezetője előzetesen engedélyezte.

g) Az alkalmazott tűzfal berendezésen végrehajtott változásokat a rendszergazdának dokumentálnia kell (ki és mikor végezte a beavatkozást, mit módosított), és erről az Informatikai Osztály vezetőjét haladéktalanul értesíteni köteles.

h) Az alkalmazott tűzfal működőképes konfigurációjáról a módosítás előtt olyan biztonsági másolatot kell készíteni, amelynek segítségével a korábbi működő állapot – szükség esetén – gyorsan előállítható. A legutolsó biztonsági másolatot a normál mentésekkel együtt tűzbiztos széfben kell eltárolni.

i) A központi rendszereken végzett bármilyen olyan beállítás, amihez rendszergazdai jogosultság szükséges, csak a Támogatáskezelő területén végezhető.

j) Ha a központi rendszerekhez - rendkívüli esetben - távoli helyről válik szükségessé rendszergazdai beavatkozás, akkor ez a megfelelő óvintézkedések (egyszeri jelszó, hívás-visszahívás eljárás, stb.) megtétele mellett végezhető el.

k) Biztosítani kell, hogy a Támogatáskezelő informatikai rendszerének bármely elemén kizárólag csak az arra felhatalmazott rendszergazda végezhessen rendszergazdai jogosultsághoz kötött módosításokat.

l) Az elektronikus információs rendszerben elkülönített végrehajtási tartományt kell fenntartani minden végrehajtó folyamat számára.

7.5 Elektronikus aláírás

87. § A Támogatáskezelő rendelkezik PKI alapú elektronikus aláírással.

7.5.1 Az elektronikus aláírás igénylése

88. § Elektronikus aláírás szolgáltatást a Támogatáskezelő munkavállalója kizárólag a Nemzeti Infokommunikációs és Szolgáltató Zrt.-től veheti igénybe. Az aláírást igénylését minden esetben az igénylő munkatárs kezdeményezi a https://hiteles.gov.hu/cikk/13/tanusitvanyok linkről letölthető *„Tanúsítvány-megrendelő és regisztrációs űrlap”* kitöltésével. A kitöltött űrlapot további ügyintézésre megküldi az elektronikus információbiztonsági felelősnek. Az igénylést a Támogatáskezelő főigazgatója hagyja jóvá.

89. § Az elkészített tanúsítványt az igénylő helyszíni átadás során vagy személyesen az Ügyfélkapcsolati irodában veszi át a szolgáltatótól.

90. § Az Informatikai Osztály telepíti az tanúsítványt kezelő programot, illetve elvégzi a használathoz szükséges szoftvermódosításokat a kezelő számítógépén. A program telepítését és a szoftvermódosítások elvégzését kizárólag az Informatikai Osztály munkatársa végezheti el az Osztály vezetőjének írásos utasítása alapján.

91. § A tanúsítvány birtokosának a telepítés és a módosítások után haladéktalanul meg kell változtatnia a tanúsítvány alapértelmezett jelszavát a NISZ Zrt. által meghatározott jelszószabályoknak megfelelően.

92. § Az Informatikai Osztálynak naprakész nyilvántartást kell vezetnie a kiadott, illetve kompromittálódott vagy lejárt tanúsítványokról.

7.5.2 Eljárás az aláírás sérülése esetén

93. § Amennyiben a kompromittálódás gyanúja felmerül, a tanúsítványt a továbbiakban tilos használni. A kompromittálódás gyanújáról a tanúsítvány kiadóját és az Ibtv-ben meghatározott szerveket az Informatikai Osztály haladéktalanul értesíti.

7.5.3 Kilépő munkatársak elektronikus aláírása

94. § A kilépő munkatársak jogviszonyuk megszűnésekor kötelesek az aláírás tokent leadni az Informatikai Osztályon. Az átvételt az Informatikai Osztály vezetője aláírásával igazolja. A kilépő munkatárs tanúsítványának visszavonásáról az Informatikai Osztály vezetője haladéktalanul intézkedik.

8. SZEMÉLYEKHEZ KAPCSOLÓDÓ VÉDELMI INTÉZKEDÉSEK, AZONOSÍTÁS ÉS HITELESÍTÉS

8.1 Általános előírások

95. § A Támogatáskezelő biztosítja, hogy minden munkatársa megfelelő hozzáféréssel rendelkezzen a munkaköréhez szükséges informatikai alapszolgáltatásokhoz. A Támogatáskezelő minden munkatársa számára biztosítja a munkakör ellátásához szükséges alkalmazói szoftverek, illetve az alkalmazói szoftverek meghatározott részeinek rendeltetésszerű használatát.

96. § A jogosultságok felhasználókhoz kötődnek. A felhasználó számára biztosított jogosultság alapján az adatokon végzett minden tevékenységgel és az adatok felhasználásával kapcsolatos minden felelősség a felhasználót terheli.

97. § Azon alkalmazói szoftverek esetében, ahol a szolgáltató egy intézmény részére csak egy (általában az intézmény vezetőjéhez kapcsolt) hozzáférési jogosultságot biztosít, ott a jogosultság továbbadásával érintett felhasználót terhel minden felelősség az adatokon végzett minden tevékenységgel és az adatok felhasználásával kapcsolatban.

98. § A Támogatáskezelő gondoskodik arról, hogy az informatikai rendszerében tárolt adatokhoz illetéktelen ne férjen hozzá, adatolvasást, adatmegsemmisítést, adatmódosítást ne tudjon végrehajtani.

8.2 A felhasználó azonosítása és hitelesítése, hozzáférés szabályozás, név és jelszó konvenciók

99. § Minden felhasználó saját, kizárólagos használatú egyedi azonosítóval (User ID) rendelkezik, mely használatával, magát jelszavával hitelesítve, hozzáfér a rendszer erőforrásaihoz. Az egyedi azonosító alkalmas arra, hogy a végzett tevékenységek nyomon követhetőek legyenek és hozzájuk egyéni felelősség legyen rendelhető.

100. § A felhasználói azonosító nem utalhat a szerepkör esetleges privilégiumára (például rendszergazda vagy üzemeltető stb.).

101. § Csoportos felhasználói azonosító nem engedélyezett. Szerződött partnerek, külső támogatók (harmadik fél) valamennyi, a Támogatáskezelő rendszereihez hozzáférési jogosultsággal rendelkező munkatársának saját azonosítót kell igényelnie, amelynek kezelése a belső alkalmazotti azonosítókkal azonos módon történik.

102. § Különleges jogosultságokkal rendelkező (privilegizált) felhasználó regisztrálását minden esetben az Informatikai Osztály vezetője hagyja jóvá a kezdeményező szervezeti egység indokolással ellátott javaslata alapján. Az Informatikai Osztály vezetőjének jogában áll a privilegizált felhasználó regisztrálását elutasítani. Az elutasítást indokolni szükséges. Privilegizált fiókokhoz történő távoli hozzáféréshez többfaktoros autentikáció szükséges.

103. § Az azonosítók ismételt felhasználása – mivel személyhez kötött, egyedi azonosítókról van szó – nem engedélyezett, kivéve abban az esetben, amennyiben a korábban kilépett munkatárssal létesít újra munkaviszonyt a Támogatáskezelő.

104. § Három hónapos inaktivitás után a nem használt azonosítókat le kell tiltani.

105. § A felhasználó név megadását (felhasználónév) minden alaprendszernél a munkatárs vezetéknevéből és a keresztnevének első karakteréből kell létrehozni, több azonos keresztnevű munkatárs esetében a szükséges megkülönböztetés érdekében a keresztnév további karaktereit kell használni. Ettől az előírástól csak indokolt esetben szabad eltérni.

106. § A jelszavakkal kapcsolatos rendelkezéseket (jelszavakkal kapcsolatos biztonsági feltételek, elfelejtett jelszó esetén követendő szabályok) az Infokommunikációs Eszközökről szóló Szabályzat tartalmazza.

9. SZEMÉLYI BIZTONSÁG

107. § (1) A felhasználók tevékenységének ellenőrzése és szabályozása érdekében az Informatikai Osztály és az elektronikus információbiztonsági felelős:

a) szabályzataiban rögzíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő munkatársakkal, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet;

b) az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja;

c) a követelmények változásáról az érintett külső, vagy belső munkatársakat értesíti.

9.1 A felhasználók kötelezettségeként előírt védelmi intézkedések

108. § (1) A Támogatáskezelő informatikai eszközein és hálózati meghajtóin kizárólag a felhasználó munkakörével és munkájával kapcsolatos adatok tárolhatók. A felhasználó saját, munkájával összefüggésbe nem hozható adatait az Informatikai Osztály előzetes felszólítás nélkül törölheti. A felhasználó felel az általa használt informatikai eszközökön tárolt adatok védelméért az alábbiak szerint:

a) a bizalmasan kezelendő és belső használatú információk nem tárolhatóak hordozható eszközön, amennyiben a munkavégzés helyszíne szükségessé teszi az ezekhez való hozzáférést, úgy a 152. §-ban meghatározottak szerint VPN kapcsolaton érhetőek el a felhasználó számára;

b) a felhasználó tartózkodni köteles a bizalmasan kezelendő és belső használatú információk kódolatlan külső hálózaton történő küldésétől;

c) a felhasználó tartózkodni köteles a jelszavak titkosítás nélküli tárolásától;

d) a felhasználó köteles a mobileszközök valamennyi biztonsági szolgáltatását használni;

e) a felhasználó köteles az asztali számítógépet és a hordozható számítógépet jelszóval védeni;

f) a felhasználó köteles a felügyelet nélkül hagyott asztali számítógépet és a hordozható számítógépet zárolni.

(2) A felhasználó adatkezelését, ideértve különösen az adatok másolását, áthelyezését, továbbítását, fel- és letöltését az Informatikai Osztály a Támogatáskezelő adatbiztonsága érdekében naplófájlban rögzítheti és tárolhatja.

9.2 Jogosultságcsoportok, jogosultságkezelés

(1) A Támogatáskezelő informatikai rendszereihez az alábbi hozzáférési csoportokat határozza meg:

a) Az alapszolgáltatás hozzáférés a Támogatáskezelő által meghatározott irodarendszerekhez való hozzáférést biztosítja, ami minden felhasználói munkaállomáson rendelkezésre áll.

b) Az alkalmazói szoftver hozzáférés az alkalmazói szoftver használatát biztosítja, ami a felhasználói terület erre jogosult munkatársának munkaállomásán rendelkezésre áll.

c) A speciális IT szolgáltatás hozzáférés a speciális informatikai szolgáltatások (pl. laptop használat) igénybe vételét biztosítja.

d) A rendszergazda hozzáférés a rendszerszoftverekhez (operációs rendszerek), az alkalmazásgazda hozzáférés a célszoftverekhez (adatbázis-kezelők, szakrendszerek) való hozzáférést biztosítja, ilyen jogosultsággal a kinevezett rendszergazdák, illetve alkalmazásgazdák rendelkeznek;

e) A Támogatáskezelő munkatársai számára az egyes rendszerekhez történő hozzáférési jogosultságokat – amennyiben a szakrendszer jogosultságkezelési utasítása ettől eltérő módon nem rendelkezik – a Támogatáskezelő Hibabejelentőjén keresztül kell igényelni. A jogosultságok kiadásával, módosításával, letiltásával, illetve törlésével kapcsolatos részletes rendelkezéseket az Infokommunikációs eszközökről szóló szabályzat tartalmazza.

9.3 Információbiztonsági tudatosság és képzés

109. § Annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést kell nyújtani, amit az elektronikus információbiztonsági felelős, vagy külső, erre a célra szakosodott megbízott partner biztosít a rendszer felhasználói számára. Az informatikai biztonság tudatosítására irányuló tevékenység és képzés a Támogatáskezelő összes közalkalmazotti-, munka-, vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottjának tekintetében kötelező.

110. § Az információbiztonsági oktatást először munkába álláskor, illetve a szerepkör átvételét megelőzően kell megtartani.

111. § (1) Az információbiztonsági oktatásnak a munkakör igényei szerint:

a) alkalmazkodnia kell az alkalmazott által betöltött feladatkörhöz,

b) tartalmaznia kell az ismert fenyegetésekre történő felkészülést,

c) ismertetnie kell az információbiztonság belső szervezetét,

d) ismertetnie kell az információbiztonsági fenyegetések felismerésének módját és a szükséges intézkedéseket.

112. § A munkatársak információbiztonsági képzésen történő részvételt követően tesztet töltenek ki, mellyel igazolják, hogy elsajátították tudnivalókat.

113. § (1) Az információbiztonsági tudatosságot frissítő képzést éves rendszerességgel meg kell ismételni, a 109. § szerint. A képzésen minden, számítógépet használó munkatársnak részt kell vennie. Az éves frissítő képzések során:

a) ellenőrizni és frissíteni kell az alapvető információbiztonsági tudatossággal kapcsolatos ismereteket

b) tájékoztatni kell a munkatársakat az újabb fenyegetésekről és az azok elleni védekezésről,

c) ismertetni kell az információ-feldolgozó eszközök helyes használatára vonatkozó tudnivalókat és változásokat,

d) tájékoztatást kell adni a szoftverjogi követelmények alapjairól,

e) frissíteni kell az információbiztonsági incidensek kezelésével kapcsolatos tudnivalókat,

f) ismételten tesztet kell kitölteniük a munkatársaknak.

114. § A képzések megtörténtét és az ellenőrző teszt eredményeit dokumentálni kell.

115. § A képzéshez tananyagot és vizsga anyagot kell összeállítani. A képzés formája nem kötött, lehet csoportos, vagy egyéni képzés és számonkérés, de történhet elektronikus (e-learning) formában is.

9.4 A Nemzeti Kibervédelmi Intézet tájékoztatói

116. § Az információbiztonsági felelős a felhasználókat a Nemzeti Kibervédelmi Intézet szabad terjesztésű tájékoztatójának továbbításával, vagy annak kivonatolásával, Intraneten történő közzétételével folyamatosan tájékoztatjaaz információbiztonsággal kapcsolatos felmerülő újabb hírekről, trendekről.

117. § A Nemzeti Kibervédelmi Intézet által megküldött riasztásokat kiemelt prioritású levélként – azok tartalmától függően – azonnal továbbítani kell az Informatikai Osztály, vagy a Támogatáskezelő összes munkatársa részére.

9.5 Eljárás a jogviszony megszüntetése esetén

118. § A kilépő munkatárs a közvetlen vezetőjének gondoskodnia kell arról, hogy az elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátása továbbra is biztosított legyen, ezt a munkaköri feladatok és dokumentumok átadás-átvételi folyamatával biztosítja. Az átvevő személyét szintén a kilépő munkatárs munkahelyi vezetője jelöli ki.

119. § A Támogatáskezelő Infokommunikációs Szabályzatában foglaltaknak *(II. fejezet Hozzáférés és használat, 2. pontja Jogosultságok igénylése és visszavonásának folyamata)* megfelelően, meg kell előzni azt, hogy a jogviszonyt megszüntető munkatárs esetlegesen az elektronikus információs rendszert, illetve abban tárolt adatokat bármilyen formában jogosulatlanul törölje, módosítsa, vagy másolatot készítsen azokról, vagy más módon megsérthesse az elektronikus információbiztonsági szabályokat. Tájékoztatni kell a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről.

120. § (1) A kilépés során, a jogviszony megszűnését megelőzően az Informatikai Osztály munkatársai gondoskodnak a kilépő:

a) elektronikus információs rendszerekhez történő hozzáférési jogosultságainak megszüntetéséről;

b) egyéni hitelesítő eszközeinek visszavételéről vagy megszüntetéséről;

c) a Támogatáskezelő tulajdonában álló informatikai eszközök visszavételéről.

121. § A Támogatáskezelő szükség esetén tájékoztatja a jogviszony megszűnéséről a kilépő munkatárssal munkakapcsolatban lévő belső és külső munkatársakat.

122. § A kilépés további részletes szabályait, illetve a kilépéskezeléssel kapcsolatos eljárási szabályokat részletezően a Szociális juttatásokról szóló szabályzat és az Infokommunikációs eszközökről szóló szabályzat tartalmazza.

9.6 Elektronikus információbiztonsági szabályok megsértése

123. § A Támogatáskezelő Főigazgatója írásbeli figyelmeztetésben részesíti az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben. Amennyiben az elektronikus információbiztonsági szabályokat nem a Támogatáskezelő személyi állományába tartozó személy sérti meg, érvényesíteni kell a vonatkozó jogszabályokban, illetve szerződés(ek)ben meghatározott következményeket és meg kell tenni a szükséges jogi lépéseket.

10. MENTÉS, ARCHIVÁLÁS

124. § A hálózati meghajtókon tárolt adatok biztonsága érdekében az adatokról az Informatikai Osztály napi rendszerességgel mentést végez, és/vagy redundáns merevlemezekkel működő szervereket üzemeltet.

125. § (1) Az Informatikai Osztály meghatározott gyakorisággal mentést végez az elektronikus információs rendszerben tárolt felhasználói szintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal:

a) meg kell határozni minden elektronikus információs rendszerre vonatkozóan a mentések szükséges gyakoriságát, a mentendő adatok körét;

b) a mentésekre vonatkozó igényeket összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal (RPO, RTO) a szakmai területekkel egyeztetve kell kialakítani.

126. § (1) Az Informatikai Osztály meghatározott gyakorisággal elmenti az elektronikus információs rendszerek dokumentációját, köztük a biztonságra vonatkozókat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal:

a) megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen;

b) a legfontosabb adatokról az Informatikai Osztály a szakmai igények szerinti gyakorisággal és részletezettséggel archiválást végez.

127. § (1) A mentési és archiválási adathordozókat azonosító sorszámmal látja el és azokról nyilvántartást vezet. Az archiválásokat és mentéseket tartalmazó adathordozókon jól láthatóan és azonosíthatóan fel kell tüntetni az adathordozó azonosítóját. A mentések és archiválások típusát és idejét az eszközöktől függő módon, manuálisan vagy elektronikusan nyilván kell tartani.

(2) Az archiválásokat és mentéseket tartalmazó adathordozókat a hálózati meghajtóktól és szerverektől elkülönített épületben, zárt helyiségben vagy szekrényben kell őrizni. Rendszeresen ellenőrizni kell a mentések és archiválások helyreállíthatóságát, tesztelni kell a mentett információkat, az adathordozók megbízhatóságának és az információ sértetlenségének garantálása érdekében.

128. § A mentési rend részletes szabályait a Támogatáskezelő Archiválási szabályzata, illetve az egyes szakrendszerekre vonatkozó külön mentési utasítások tartalmazzák. A szakrendszerek mentési utasításai az Archiválási szabályzat mellékletét képezik.

11. NAPLÓZÁS

11.1 Naplózási eljárásrend

129. § Az Informatikai Osztály feladatai közé tartozik az elektronikus információs rendszerek figyelemmel kísérése és a a technikai események naplózási adatainak gyűjtése és feldolgozása.

130. § A naplógyűjtést és feldolgozást oly mértékben automatizálni kell, hogy a kritikus események nyomán riasztás keletkezzen és a rendszeradminisztrátorok haladéktalanul tudjanak intézkedni.

131. § Az informatikai infrastruktúra működésének és felhasználásának ellenőrzésére felügyeleti eszközöket kell alkalmazni, amelyek probléma esetén meghatározott módon riasztást adnak az illetékes rendszergazda számára. A megfigyelendő paramétereket és riasztási értékeket kockázatértékelés alapján kell meghatározni, meg kell határozni a naplózható és naplózandó eseményeket és erre fel kell készíteni az elektronikus információs rendszert.

132. § A napló funkciókat az Informatikai Osztály technikai és rendszer-hozzáférési oldalról tervezi meg, az alkalmazásgazdák pedig az általuk felügyelt információs rendszer sajátosságainak figyelembe vételével állítják össze igényüket a naplózandó eseményekre. A megfigyelések ki kell terjedjenek a technikai paraméterek ellenőrzésére, továbbá az eszközökhöz és szolgáltatásokhoz történő hozzáférésre is.

133. § (1) Az alábbi események naplózását feltétlenül be kell állítani, amennyiben az alkalmazás ezt lehetővé teszi:

a) a felhasználók tevékenysége,

b) az adatállományok (adatbázisok) módosítása az alkalmazói rendszerekben,

c) lekérdezések és jogosulatlan lekérdezési kísérletek,

d) az üzemeltetők operációs rendszerbe történő be-és kijelentkezése,

e) az üzemeltetők tevékenysége az operációs rendszerben,

f) a hozzáférési jogosultságok módosítása,

g) operációs rendszer események, esetleges hibák,

h) hálózati menedzsment riasztások,

i) konfigurációs beállítások módosítása,

j) jogosulatlan hozzáférési kísérletek, az egyes rendszerek detektálási képességein belül.

134. § Amennyiben az alkalmazás az a)-j) pontban megjelölteket nem teszi lehetővé, úgy a biztonság fenntartása érdekében meg kell határozni a listából azokat a pontokat, amelyek az alkalmazás biztonságának szempontjából kiemeltek és – legalább – az ezeknek a pontoknak megfelelő rendszerfejlesztés szükséges.

135. § A naplózható eseményeknek le kell fedniük az alkalmazások működését és az alapinfrastruktúrát oly mélységben, hogy megfelelőek legyenek a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

136. § A naplóbejegyzésekben kell, hogy legyen elegendő információ ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

137. § Létre kell hozni a naplózás részletszabályait tartalmazó naplózási eljárásrendet, amely a naplózás és a hozzá tartozó ellenőrzések megvalósulását segíti.

11.2 Napló információk védelme

138. § A naplóinformációk keletkezésük után is szükségesek lehetnek az üzemeltetési vagy információbiztonsági incidensek utólagos kiértékelése céljából, továbbá illegális beavatkozások esetén azok bizonyítására is felhasználhatók.

139. § A naplóinformációkat a naplókezelő eszközöket meg kell védeni a jogosulatlan hozzáféréstől. Meg kell oldani, hogy a rendszeradminisztrátorok ne tudják utólagosan módosítani a naplóbejegyzéseket.

140. § A naplóbejegyzéseket napi gyakorisággal ellenőrizni és elemezni kell a nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából. Rendellenes jelenség esetén azt jelenteni kell az illetékes vezetőknek (informatikai, gazdasági).

141. § Amennyiben jogszabály másképp nem rendelkezik, a naplóállományokat legalább egy évig meg kell őrizni.

11.3 Naplógenerálás és ellenőrzés

142. § A naplózó funkcionalitásnak biztosítania kell naplóbejegyzés generálását az előre meghatározott, naplózható eseményekre. A naplózandó eseményeket az arra feljogosított rendszeradminisztrátorok állíthatják be.

143. § A normálistól eltérő működési jellemzők megállapítása az üzemeltető feladata.

144. § Az egyes naplók tartalmának ellenőrzését, kiértékelését előre meghatározott ütemtervnek megfelelően kell végezni. Az ellenőrzéseket az adott rendszerek üzemeltetői végzik. Az ellenőrzések elvégzését dokumentálni kell. Az ellenőrzés végrehajtását az informatikai vezető háromhavonta felülvizsgálja. A felülvizsgálat tényét, és az esetleges megállapításokat jegyzőkönyvben kell rögzíteni.

11.4 Naplózási hibák kezelése

145. § Az elektronikus információs rendszerek naplózó funkciójának alkalmasnak kell lennie arra, hogy az informatikai alkalmazás és infrastruktúra naplózási hibája esetén riasztást küldjön az illetékes rendszergazdának, s ezzel párhuzamosan végrehajtsa azokat a tevékenységeket, amelyeket a rendszer biztonságának fenntartása érdekében el kell végezni (például rendszer leállítás, régi naplóbejegyzések felülírása, naplózás leállítása).

11.5 Időszinkronizálás

146. § A Támogatáskezelő információ-feldolgozó rendszerének óráit egymással, illetve egy hiteles külső időforrással szinkronizálni kell. A rendszeres szinkronizálás – a szakrendszerek speciális jogszabályi kötelezettségein túl – azért szükséges, mert más módon nem biztosítható a berendezések együttes működése, ami feltétele az üzemeltetési esemény kivizsgálásának, illetve bizonyíték jogi, vagy fegyelmi esetekben. A nem szinkronizált bejegyzések akadályozzák ezeket a kivizsgálásokat és ártanak a bizonyíték hitelességének.

147. § A szervezeten belül ki kell jelölni egy pontosidő-szervert, ami a többi berendezés szinkronizálásának alapja. Az időszerver a pontos időt valamelyik hitelesített külső NTP szerverről kérje le.

12. MONITOROZÁS

148. § A monitorozást a Támogatáskezelő minden központi szolgáltatást futtató eszközén, valamint a határvédelmi eszközökön alaphelyzetben engedélyezni kell.

149. § A szerverek, hálózati eszközök, valamint a biztonsági rendszer elemeinek naplóállományait rendszeresen ellenőrizni kell, és a biztonsági megfontolásokat figyelembe véve meghatározott ideig tárolásáról gondoskodni kell.

150. § (1) A naplózási funkciónak rögzítenie kell legalább a következőket:

a) a rendszer leállását és újraindulását,

b) a rendszerben fellépő hibákat,

c) felhasználó bejelentkezést, vagy sikertelen bejelentkezési kísérleteket,

d) tranzakció végrehajtását,

e) új felhasználó felvételét, törlését,

f) a naplóállományok törlését.

151. § A központi szolgáltatások, és a határvédelmi eszközök, valamint kritikus informatikai eszközök egy riasztórendszerhez kapcsolódnak. A riasztórendszer automatikus SMS és e-mail küldéssel reagál a rendszerhibákra, és minden olyan eseményre, ami a normális működéstől eltér. Az SMS-ek a felügyelettel megbízott rendszergazdák mobiltelefonjára érkeznek munkaidőben és munkaidőn kívül is. Az SMS-ek érkezése után a rendszergazdának haladéktalanul meg kell kezdenie a hiba felderítését, és elhárítását.

13. KÜLSŐ ELÉRÉSEKHEZ KAPCSOLÓDÓ VÉDELMI INTÉZKEDÉSEK

152. § (1) A Támogatáskezelő hálózatát elérhetővé kell tenni külső telephelyekről, hogy az itt alkalmazott szoftvereket a fejlesztők, adminisztrátorok elérhessék és a különböző akadályokat, problémákat, hibákat elhárítsák, megoldhassák. VPN felhasználó létrehozásának rendje a következő:

a) A támogatáskezelői hálózathoz való kapcsolódási szándékot belső felhasználó esetén a munkahelyi vezetőnek, külső felhasználó esetén a kapcsolattartónak, illetve a külső felhasználónak kell jeleznie az elektronikus információbiztonsági felelős felé.

b) a VPN hozzáférés alaphelyzetben le van tiltva, az engedélyezést belső- és külső felhasználók egyaránt az ibf@emet.gov.hu címen, igényelhetik az elvégzendő munka leírásával és a hozzáférés szükséges időintervallum meghatározásával.

c) a VPN jogosultság engedélyezéséről a Főigazgató dönt, az elektronikus információbiztonsági felelős javaslata alapján, aki a beérkezett igényt a Támogatáskezelő elektronikus információs rendszereinek biztonsága és az azokban tárolt adatok bizalmassága, sértetlensége és rendelkezésre állása alapján javasolja a hozzáférés megadását.

d) a VPN jogosultság engedélyezését követően az Informatikai Osztály erre kijelölt adminisztrátora létrehozza a VPN felhasználót/ jelszót és megosztja az igénylővel.

e) Többtényezős hitelesítést kell alkalmazni a különleges jogosultsághoz kötött – úgynevezett privilegizált – felhasználói fiókokhoz való, hálózaton keresztüli hozzáféréshez.

14. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉGRE VONATKOZÓ VÉDELMI INTÉZKEDÉSEK

14.1 Általános rendelkezések

153. § Rendszer- és információsértetlenségre vonatkozó védelmi intézkedéseket a Támogatáskezelő saját üzemeltetésű elektronikus információs rendszerein be kell vezetni. Amennyiben az érintett rendszert külső szervezet üzemelteti, jelen védelmi intézkedésekre vonatkozó követelményeket a szolgáltatási szerződés esetén szerződéses kötelemként kell érvényesíteni és azokat a szolgáltatónak kell biztosítania.

154. § A rendszer- és információsértetlenségre vonatkozó eljárások részletszabályozásait az Informatikai Osztály vezetője, az osztályra vonatkozó belső munkadokumentumként fogalmazza meg. Az általános alapelvek az IBSZ részét képezik.

155. § (1) Az elektronikus információs rendszerek hibáit fel kell tárni és tervezetten meg kell javítani. Ennek kapcsán:

a) a Támogatáskezelő valamennyi munkatársának kötelezettsége, hogy az elektronikus információs rendszerek észlelt hibáit az Informatikai Osztály felé a Hibabejelentőn bejelentsék.

b) Az Informatikai Osztály a bejelentéseket értékeli, a hibák javítását azok súlyossága alapján priorizálja, majd megtervezi, megrendeli, vagy saját hatáskörben elvégzi a hibajavítást.

c) Telepítés előtt a hibajavítással kapcsolatos szoftverfrissítéseket tesztelni kell a feladatellátás hatékonysága és a szóba jöhető következmények szempontjából.

156. § Minden alkalmazott és külső munkatárs kötelessége, hogy az informatikai rendszerekben általa észlelt rendellenességet, gyaníthatóan gyenge pontot vagy sérülékenységet jelentse az Informatikai Osztálynak. Ezek a gyenge pontok támadásra, visszaélésre adhatnak lehetőséget, védelmi intézkedések meghozatala válhat szükségessé.

157. § A munkatársak felé elvárás, hogy jelentsék az észlelt problémát, azonban a feltárt probléma ellenőrzése, vagy javítása – az esetleges vétlen károkozás, vagy a bizonyítékok sérülésének lehetősége miatt – tilos.

14.2 Rendszerfrissítések kezelése

158. § Az operációs rendszerek, hálózatkezelő eszközök szoftverei, adatbázis-kezelők, egyéb dobozos és egyedi fejlesztésű szoftverek biztonsági frissítéseit a gyártó által történő kiadáskor az elektronikus információbiztonsági felelős kockázati értékelésnek veti alá. Meg kell állapítania a valós fenyegetettség mértékét és annak függvényében kell dönteni a frissítések bevezetéséről. A kiemelt kockázatú sérülékenységet javító frissítést a tesztelést követően azonnal telepíteni kell.

159. § A kiszolgálók és a munkaállomások operációs rendszereinek frissítései ütemezhetőek, azaz a kockázatkezelést és tesztelést követően tervezett határidőn belül telepítésre kell, hogy kerüljenek. Kiemelt kockázatú sérülékenységet javító frissítést a tesztelést követően azonnal telepíteni kell.

160. § Egyedi és dobozos feldolgozó szoftverek (számviteli alkalmazások, bérprogram stb.) frissítéseit a szoftver fejlesztőjével/támogatójával egyeztetett módon kell bevezetni.

161. § Nagyobb, több rendszert érintő rendszerfrissítéseket – például adatbázis-kezelők frissítései – körültekintően meg kell tervezni, figyelembe véve az összes kapcsolódó rendszerre gyakorolt esetleges hatásait. Amennyiben inkompatibilitási okokból nem valósítható meg a frissítés rövid határidőn belüli telepítése, akkor helyettesítő intézkedéseket (kompenzációs kontrollt) kell bevezetni a végleges megoldásig (például alkalmazás tűzfal telepítése).

162. § A hibajavítást a konfigurációkezelési folyamatba be kell építeni és annak szabályai szerint kell kezelni.

14.3 Kártékony kódok, vírusok elleni védelem

163. § A kártékony kódok elleni védelmet olyan módon kell kialakítani, hogy az elektronikus információs rendszert annak belépési és kilépési pontjain védje a kártékony kódok ellen, derítse fel és semmisítse meg azokat.

164. § A kártékony kódok elleni védelmi mechanizmusokat frissíteni kell minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg. A frissítéseket a konfigurációkezelés szabályaival és eljárásaival összhangban kell elvégezni.

165. § (1) A kártékony kódok elleni védelmi mechanizmusokat úgy kell konfigurálni, hogy a védelem eszköze:

a) rendszeres ellenőrzéseket hajtson végre az elektronikus információs rendszeren, és hajtsa végre a külső forrásokból származó fájlok valós idejű ellenőrzését a végpontokon, a hálózati belépési vagy kilépési pontokon, a biztonsági szabályzatnak megfelelően, amikor a fájlokat letöltik, megnyitják, vagy elindítják,

b) a kártékony kód észlelése esetén blokkolja vagy helyezze karanténba azt, riassza a kijelölt rendszeradminisztrátort és a meghatározott további személy(eke)t.

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

14.4 Az elektronikus információs rendszer felügyelete

166. § (1) Ki kell alakítani az elektronikus információs rendszer felügyeleti rendszerét, amely alkalmas arra, hogy észlelje a kibertámadásokat, vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat;

a) azonosítani kell az elektronikus információs rendszer jogosulatlan használatát;

b) felügyeleti eszközöket kell alkalmazni a meghatározott alapvető információk gyűjtésére;

c) a behatolás-felügyeleti eszközökből nyert információkat védeni kell a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;

d) meg kell erősíteni az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelek észlelhetők;

e) biztosítani kell, hogy az elektronikus információs rendszer felügyeleti információkat a kijelölt felelős személyek meghatározott gyakorisággal megkapják.

14.5 Biztonsági riasztások és tájékoztatások

167. § (1) A kiberbiztonság fenntartása, a biztonsági események és sérülékenységek hatékony kezelése érdekében az elektronikus információbiztonsági felelős együttműködik a kormányzat elektronikus biztonságért felelős szerveivel:

a) folyamatosan figyeli a Kormányzati Eseménykezelő Központ (GovCsirt) által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseit;

b) folyamatosan figyelemmel kíséri a Nemzeti Elektronikus Információbiztonsági Hatóságtól (NEIH) érkező értesítéseit;

c) szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki, melyet el juttat a szervezeten belül illetékes személyekhez;

d) kialakítja és működteti a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, folyamatosankapcsolatot tart fenn a jogszabályban meghatározott szervekkel (GovCsirt, NEIH);

e) meghozza a megfelelő ellenintézkedéseket és válaszlépéseket.

14.6 Jelentés biztonsági eseményekről

168. § (1) Az információbiztonsági eseményeket észlelő felhasználó(k)nak a lehető leggyorsabban jelenteni kell azt az Informatikai Osztálynak és az elektronikus infomrációbiztonsági felelősnek. Biztonsági eseményre utalhat, melyet a felhasználóknak azonnal jelenteniük kell, ha

a) szolgáltatás, a berendezés vagy az eszközök elvesztése történik,

b) rendszer rendellenes működését észlelik,

c) a szabályzatoknak vagy irányelveknek való nem-megfelelés válik nyilvánvalóvá,

d) észlelhető a fizikai biztonsági rendelkezések megsértése,

e) nem ellenőrzött rendszerbeli változásokat tapasztalnak,

f) a szoftver vagy hardver hibás működése lép fel,

g) jogosulatlan hozzáférést tapasztalnak.

(2) A felhasználók tudatossági oktatásában ki kell térni arra, hogy hogyan kell válaszolniuk egy-egy felmerült incidensre és milyen módon kell elősegíteniük a bizonyítékok gyűjtését.

14.7 A biztonsági eseményekre és incidensekre adott válasz és fejlesztés

169. § (1) Az észlelt információbiztonsági eseményekre és gyengeségekre mielőbb válaszintézkedéseket kell hozni. Az események követését és a megoldási javaslatok, fejlesztések kidolgozását az Informatikai Osztály végzi. Amennyiben az esemény komplexebb és speciális szakértelmet igényel, a megoldás kidolgozásához külső szakértőt kell igénybe venni.

(2) Tipikusan információbiztonsági incidensek közé kell sorolni:

a) információs rendszer hibáit és a szolgáltatás megszakadását,

b) rosszindulatú kód, vírustámadás fellépését,

c) DOS, DDOS támadást,

d) a nem teljes vagy nem pontos működési adatokból eredő hibákat,

e) a bizalmasság és sértetlenség megsértését,

f) az információs rendszerekkel való visszaélést.

(3) Információbiztonsági incidensek esetén az elektronikus információs rendszerek biztonságáért felelős személy irányítja az intézkedéseket:

a) incidensmegoldó team összehívása – rendszergazdák, alkalmazásgazdák és az érintett területi vezetők bevonása;

b) incidens okának felderítése,

c) bizonyítékok gyűjtése,

d) incidens behatárolása és megszüntetése, helyreállítás,

e) előfordulás okának meghatározása és megszüntetése,

f) helyesbítő tevékenység az újbóli előfordulás megakadályozására,

g) tevékenységek dokumentálása,

h) adatközlés az érintettek felé,

i) jelentés a főigazgató felé

170. § A biztonsági események elemzése alkalmas arra, hogy a fennálló védelmi intézkedéseket hatékonyan felül lehessen vizsgálni és javítani. A kiértékelés jelezheti az ellenőrzések és eszközök kiegészítésének szükségességét, hogy a jövőbeni előfordulások valószínűségét csökkenteni lehessen, megelőzve az anyagi és erkölcsi károkozást.

171. § Az információbiztonsági események, visszaélések esetén hiteles és megváltoztathatatlan módon meg kell őrizni a vonatkozó naplóbejegyzéseket, adathordozókat és a papíralapú dokumentumokat, gondoskodva a bizonyítékok megváltoztathatatlanságáról a későbbi esetleges felelősségre vonás, polgári vagy büntetőjogi eljárás kezdeményezése érdekében.

IV. ÜZLETMENET-FOLYTONOSSÁG TERVEZÉSE

172. § Az informatikai szolgáltatások, vagy azok egy részének elvesztése a Támogatáskezelő számára katasztrófát jelenthet. Az egyes szakrendszerek esetén lehetőség van önálló, szakrendszer-specifikus katasztrófa elhárítási terv elkészítésére.

1. KATASZTRÓFA LEÍRÁSA

173. § Az informatikai katasztrófa egy olyan nem tervezett esemény, amely az adatfeldolgozó képesség elvesztését okozza legalább 1 munkanap időre. Az üzletmenet-folytonosság tervezésének az a feladata, hogy a szervezet kritikus információ-feldolgozó képességeit helyre lehessen állítani elfogadhatóan rövid idő alatt a szükséges aktuális adatokkal egy informatikai katasztrófa után. Tekintettel a Támogatáskezelő munkafolyamatainak informatikai támogatottságára, az informatikai szolgáltatások elvesztése az érintett munkafolyamatok szinte teljes leállásával jár. Katasztrófa esetén a Támogatáskezelő adatvagyona is sérülhet. Elsődleges

prioritás az adatvagyon megőrzése, másodlagos az ügyfélfogadás és az azzal kapcsolatos üzletmenet biztosítása. Minden további feladat harmadlagos jellegű.

1.1 Tevékenység-sorozat katasztrófa esetén:

174. § (1) Tevékenység-sorozat katasztrófa esetén a következő az eljárás:

a) az esemény bekövetkezte;

b) a katasztrófa-elhárítási csapat riasztása; főigazgató, igazgatók, Informatikai Osztály, külső szolgáltatók (amennyiben érintettek);

c) a károk enyhítése;

d) a helyreállítási folyamat megindítása;

e) az alaptevékenység visszaállítása;

f) tényleges helyreállítás;

g) jelentések a jogszabályokban meghatározott módon;

h) a tanulságok levonása.

1.2 Kritikussá válás eseti kritériumai

175. § (1) A kritikus informatikai alkalmazások ismérveit Az IBSZ tárgyi hatálya című fejezet tartalmazza. Informatikai szolgáltatás-kimaradás időlegesen kritikussá válhat továbbá – besorolásától függetlenül – az alábbiesetekben.

(2)Ha leállása esetén egyes ügyfelekkel kapcsolatos ügyek nem bonyolíthatók még papír alapú nyilvántartások segítségével sem az előírt határidőn belül. Egy ilyen alkalmazás leállása akkor informatikai katasztrófa, ha:

a) nem tervezett a leállása;

b) tervezett leállása túllépte a maximális 1 nap vagy 1 hétvége időtartamot.

(3) Kritikus informatikai szolgáltatás továbbá az, mely az 176. § (2) bekezdésbe nem tartozik, de nyilvántartása a Támogatáskezelői adatvagyon részét képezi és ez az adatvagyon rész nem érhető el legalább 3 napon keresztül. Ekkor a 3. nap után a szolgáltatás leállása szintén informatikai katasztrófának minősül.

1.3 Az informatikai szolgáltatás visszaállításának időtávja

176. § Informatikai katasztrófa bekövetkezése esetén a katasztrófa elhárítását azonnal meg kell kezdeni. Amennyiben az informatikai szolgáltatás nem állítható helyre 2 napon belül, abban az esetben további 3 napon belül meg kell oldani az informatikai, vagy papír alapú ideiglenes szolgáltatást. Az ideiglenes szolgáltatás időtávja addig tart, amíg az informatikai szolgáltatás helyreállítása be nem fejeződik, melynél törekedni kell arra, hogy 2 héten belül fejeződjön be.

2. A SZOLGÁLTATÁS FENNTARTÁSÁNAK/HELYREÁLLÍTÁSÁNAK ESZKÖZEI

2.1 Munkaerő

177. § Informatikai katasztrófa bekövetkezése esetén a főigazgatónak, az igazgatóknak, az Informatikai Osztály minden munkatársának, az elektronikus információbiztonsági felelősnek, az adatvédelmi felelősnek és az érintett szervezeti egységek vezetőinek munkaidőn kívül és munkaszüneti napokon is azonnal be kell jönnie a Támogatáskezelő székhelyére és meg kell kezdenie a szolgáltatás fenntartását/helyreállítását. A helyreállítási munka vezetője az Informatikai Osztály vezetője. Szükség esetén az érintett szervezeti egységek vezetői a vezetésük alatt lévő szervezeti egység személyi állományából további munkatársakat is behívhatnak, akiknek ez esetben szintén kötelező megjelenni. A katasztrófa elhárításáig a munkatársak munkaideje napi 10 óra, munkaszüneti napokon is. Ez alól felmentést vagy engedményt csak a főigazgató adhat.

2.2 Ideiglenes nyilvántartások

178. § A katasztrófa elhárításának elhúzódó időtartama alatt – amennyiben lehetséges és nem veszélyezteti a leállt szolgáltatás adatvagyonának jövőbeli integritását – ideiglenes nyilvántartást kell létrehozni a szolgáltatás helyettesítésére, mely lehet informatikai, de papíralapú is. Az elhárítás befejezése után az ideiglenes nyilvántartás adatainak a helyreállított szolgáltatásba történő integrálását azonnal meg kell kezdeni.

179. § Az iktatórendszer üzemzavara esetén követendő eljárásrendet, így különösen az ideiglenes nyilvántartás vezetésére vonatkozó részletes szabályokat a Támogatáskezelő Iratkezelési Szabályzata tartalmazza.

3. KATASZTRÓFA ELHÁRÍTÁSI GYAKORLAT

180. § Az Informatikai Osztály évente egyszer, a főigazgatóval előre egyeztetett időpontban katasztrófa elhárítási gyakorlatot tart. A gyakorlat nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

V. ZÁRÓ RENDELKEZÉSEK

181. § (1) Az IBSZ felülvizsgálatát el kell végezni

a) az IBSZ tárgykörét érintő jogszabály módosítása esetén,

b) minden olyan esetben, amikor az elektronikus információs rendszerekben, vagy a működési környezetben jelentős változás történik,

c) három évente, tervezetten.

1. sz. melléklet a(z) …/2019. ( ) EMET főigazgatói utasításhoz

1. SZÁMÚ MELLÉKLET

ENGEDÉLYKÉRELEM ADATOK, ADATHORDOZÓN TÖRTÉNŐ KIVITELÉRE/ELEKTRONIKUS ÚTON TÖRTÉNŐ TOVÁBBÍTÁSÁRA

_____(név)

a _____ (szervezeti egység)

munkatársának engedélyezem, hogy az alább felsorolt adatokat, az Elektronikus Információbiztonsági Szabályzat, Adatvédelmi Szabályzat és Infokommunikációs Szabályzat vonatkozó rendelkezéseit betartva, a Támogatáskezelő területéről adathordozón kivigye vagy az egyéb, elektronikus úton továbbítsa.

Adathordozón vagy az egyéb, elektronikus úton továbbítani kívánt adatok:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____

Budapest,

_____

főigazgató