HUNGARY HELPS

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

Iktatószám: VIG/83.-1.../2023

19/2023. Vig. utasítás

a Hungary Helps Ügynökség Nonprofit Zrt.
Elektronikus információbiztonsági szabályzatáról szóló 9/2022 Vig. utasítással kiadott szabályzat módosításáról - ***a módosítást vastag és dőlt betű jelzi***

Készítette: .....
Dr. Kovács Mariann
jogtanácsos

Ellenőrizte: .....
Dr. Schifter-Kiss Virág
jogi vezető

Kiadta: .....
Kovács Péter
vezérigazgató

Hungary Helps Ügynökség Nonprofit Zrt. • HUNGARY HELPS • Adószám: 26705231-2-41 Bank: 10023002-00356152-00000017 1011 BUDAPEST, Szilágyi Dezső tér 1.

Hatályos: 2023. augusztus 4.

HUNGARY HELPS

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

TARTALOMJEGYZÉK

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

I. ÁLTALÁNOS RENDELKEZÉSEK

1. § Jelen Elektronikus Információbiztonsági Szabályzat (a továbbiakban: IBSZ) a Hungary Helps Ügynökség Nonprofit Zrt. (a továbbiakban: Társaság) által kezelt információkra, illetve a Társaság 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 adatvagyonról szóló 2021. évi XCI. 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,

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

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 Társaság egyéb belső szabályzataiban, így különösen a Szervezeti és Működési Szabályzatban, az Iratkezelési Szabályzatban, az a Társaság Közérdekű adatok megismerésére irányuló kérelmek eljárásrendjéről, továbbá a kötelezően közzéteendő adatok nyilvánosságra hozatalának rendjéről 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 Társaság Adatvédelmi Szabályzata tartalmazza.

2. AZ INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT CÉLJA, HATÁLYA

2.1 Az Információbiztonsági Szabályzat célja

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

a Társaság 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 Társaság 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;

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

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 Társaság 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 Társaság valamennyi foglalkoztatottjára. Az IBSZ személyi hatálya kiterjed továbbá minden személyre, aki a Társaság informatikai vagy azzal összefüggő rendszerét, szolgáltatásait igénybe veszi, informatikai struktúráját és annak eszközeit üzemelteti vagy használja, függetlenül a Társasághoz 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 Társaság tulajdonában lévő, vagy általa bérelt, kezelésében levő) informatikai és telekommunikációs berendezésre, vagy a Társaság használatában álló épületben található, leltári jelzéssel ellátott, továbbá a Társaság megbízásából a Társaság munkatársai számára harmadik személy által biztosított informatikai eszközre, beleértve az eszközök, berendezések műszaki dokumentációját is;

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

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

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

e) minden olyan eszközre, amelyet a Társaság foglalkoztatottjai a munkavégzés során a Társasággal kapcsolatos kommunikációra használnak

f) amennyiben a Társaság működésére irányadó egyéb szabályzat - így különösen az Iratkezelési Szabályzat, ***A Hungary Helps Ügynökség Nonprofit Zrt. közérdekű adatai megismerésének és közzétételének rendjéről valamint a beérkező panaszok kezeléséről szóló szabályzat***, az Adatvédelmi Szabályzat, a - eltérően nem rendelkezik:

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

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

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

fc) az információk felhasználására;

fd) 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 Társaság, 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 Társaság működése szempontjából kiemelt és normál rendszerek és azok ismérvei

11. § (1) A Társaság működése szempontjából kiemelt az a rendszer, amely összefügg a Társaság 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 Társaság napi működéséhez és feladatellátásához nélkülözhetetlenek. A kiemelt rendszerek információbiztonsági szempontból fokozott védelmet igényelnek. E körbe tartoznak különösen az alábbi rendszerek:

a) iratkezeléssel összefüggő rendszerek;

b) támogatással, pályáztatással összefüggő rendszerek;

(2) Normál rendszerek a kiemelt rendszerek körébe nem sorolt, a Társaság 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,

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

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;

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

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 Társaság által biztosított számítástechnikai, információ-feldolgozási és kommunikációs szolgáltatások;

ee) informatikai támadás: minden olyan hardver vagy szoftver elem működését befolyásoló

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

tényező, amely kihasználva azok sérülékenységét szándékosan akadályozza azok működését vagy kárt tesz azokban;

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

gg) központi rendszer: a Társaság 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;

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

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

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

II. AZ INFORMÁCIÓVÉDELEMMEL ÉRINTETT SZEREPLŐK FELADATKÖRE ÉS FELELŐSSÉGE

1. A VEZÉRIGAZGATÓ FELADATKÖRE ÉS FELELŐSSÉGE

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

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

b) jóváhagyja a Társaság 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 Társaság 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 Társaság elektronikus információbiztonságáért felelős személyéről,

l) tájékoztatás céljából megküldi a szervezet informatikai biztonsági szabályzatát,

m) az ellenőrzés lefolytatásához szükséges feltételeket biztosítja,

n) a Társaság információbiztonsági politikáját,

o) a Társaság információbiztonsági stratégiáját,

p) jóváhagyja az információbiztonsággal kapcsolatos szabályzatokat,

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

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

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 Társaság elektronikus információbiztonsági felelőse gondoskodik az elektronikus információs rendszerek védelméről a következők szerint. A Társaság gazdasági és szolgáltatási igazgatójának irányításával ellátja az Informatikai feladatokat. Legfontosabb feladatkörei:

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

b) gondoskodik a Társaság jogszabályoknak megfelelő működéséről;

c) elkészíti és folyamatosan karbantartja 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 Társaság 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, felel a Társaság informatikai rendszereinek folyamatos és egységes működtetéséért;

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

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

m) felel Társaság által üzemeltetett informatikai eszközök, szoftverek, alkalmazások

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

jogosultsági beállításaiért;

2. A GAZDASÁGI ÉS SZOLGÁLTATÁSI IGAZGATÓ FELADATKÖRE ÉS FELELŐSSÉGE

15. § (1) Feladatkörei:

a) közvetlenül irányítja az elektronikus Információbiztonsági felelős tevékenységét
b) dönt a jogosultság-igény kielégítéséről, megtagadásáról, vagy módosításáról és döntéséről tájékoztatja az igénylőt

3. AZ ALKALMAZÁSGAZDÁK FELADATKÖRE ÉS FELELŐSSÉGE

16. § (1) A Gazdasági és Szolgáltatási Igazgatóság a Társaságnál használt valamennyi kiemelt informatikai rendszerhez alkalmazásgazdá(ka)t 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) specifikációt, dokumentációt készít a fejlesztésekhez,

e) részt vesz a fejlesztések tesztelésében,

f) hiba esetén közreműködik a szakrendszer helyreállításában, tesztelésében.

4. FELHASZNÁLÓK FELADATKÖRE ÉS FELELŐSSÉGE

17. § (1) A Társaság 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;

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

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 Társaság informatikai rendszerében nem alkalmazott szoftver installálása;

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

5. KÜLSŐ PARTNEREK FELADATKÖRE ÉS FELELŐSSÉGE

18. § (1) A speciális informatikai vagy szakmai ismereteket igénylő folyamatok, munkák ellátásához a Társaság 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.

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

a) amennyiben jogosultsága szerint a természetes személy külső partner a Társaság bármely informatikai, vagy szakrendszerének adatállományához hozzáféréssel rendelkezik, úgy

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

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 Társaság hálózatát, hardver és szoftverállományát érintő bármiféle információ felhasználásának tiltása,

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

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

III. AZ INFORMÁCIÓBIZTONSÁGHOZ KAPCSOLÓDÓ RENDELKEZÉSEK

1. KOCKÁZATELEMZÉS

20. § 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 Társaság működőképességére tett hatásait tartalmazza. Külön kell kezelni a szolgáltatás elérhetetlenségéből, illetőleg az adatbázis sérülésből származó hatásokat. A kockázatelemzési dokumentum előállítása és karbantartása a Társaság 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

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

a) adatvagyon leltár,

b) szoftverleltár.

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

22. § A szoftverleltár tartalmazza a Társaság 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.

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

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

24. § A szoftverleltár elkészítéséért és naprakészen tartásáért az GSZI felel

1.2 Biztonsági osztályba sorolás

25. § (1) Az Ibtv. és a Vhr. alapján a Társaság 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 Társaság vezérigazgatója 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 a Társaság rendszerei az alábbi biztonsági osztályba tartoznak:

Alkalmazás azonosítója	Biztonsági osztály	Funkció	Tranzakciók típusa	Kezelt adatok jellege
Hungary Helps Ügynökség honlap	2	weboldal /hungaryhelps.gov.hu/	tartalomfrissítés	tájékoztató, személyes és pénzügyi adatok
Intranet	2	Ügyviteli rendszer	tartalomfrissítés	nyilvántartási adatok
DoTo	4	Pályázatkezelési rendszer	Pályázatkezelési	nyilvántartási, személyes, pénzügyi adatok, különleges adatok

1.3 Szintbe sorolás

26. § (1) A Vhr. meghatározza a hatálya alá tartozó szervezetek, köztük a Társaság 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
DoTo Rendszer	4	Pályázatkezelési rendszer	Pályázatkezelési	nyilvántartási, személyes, pénzügyi adatok, különleges adatok

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

1.3 Logikai védelmi intézkedések

27. § A Társaság 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 GSZI nyilvántartást vezet. A jogosultságigénylés és - megvonás eljárásrendjét a Társaság Infokommunikációs eszközökről szóló szabályzata tartalmazza.

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

29. § (1) A Társaság 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.

1.4 Rendszerek fejlesztése, továbbfejlesztése, verzióváltások

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

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

32. § (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

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

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.

33. § 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.

34. § (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).

35. § 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;

2. AZ ADATHORDOZÓK KEZELÉSE ÉS BIZTONSÁGA

36. § Az adatok sérülésének elkerülése és a működésfolytonosság fenntartása érdekében, az GSZI és az információbiztonsági felelős, üzemeltetési eljárásokat hoz létre, az elektronikus dokumentumokhoz, számítógép médiumokhoz, adathordozókhoz történő jogosulatlan hozzáférés, módosítás, ellopás megakadályozása érdekében.

2.1 Az eltávolítható adathordozók kezelése

37. § (1) A hordozható adathordozók - más terminológia szerint eltávolítható adathordozók - jellegükből adódóan jelentős információbiztonsági kockázatot hordoznak. Külső adathordozó használata előtt az adathordozó adatállományát a rosszindulatú alkalmazás elleni védelemről gondoskodó alkalmazás használatával ellenőrizni kell.

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

(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 Társaság 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!**

2.2 Az eltávolítható adathordozókkal kapcsolatos irányelvek

38. § (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.

2.3 Adathordozók újrahasznosítása és selejtezése

39. § (1) Az adathordozók újrahasznosítása és selejtezése során, az adatok kiszivárgásának megakadályozására, az GSZI 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

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

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.

2.4 Az adathordozók tárolása és védelme

40. § (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 Társaság területéről csak a vezérigazgató 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 Társaság számára kárt vagy bizalomvesztést. Az ilyen adatok nem kerülnek központi mentésre, ezért a mentési igényt minden esetben az Gazdasági és Szolgáltatási Igazgató GSZI felé kell jelezni.

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

3. DOKUMENTÁCIÓKHOZ KAPCSOLÓDÓ VÉDELMI INTÉZKEDÉSEK

41. § (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);

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

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

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

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

44. § 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 a GSZI a felelős.

45. § 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 GSZI feladata.

46. § 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.

4. ELEKTRONIKUS KOMMUNIKÁCIÓHOZ KAPCSOLÓDÓ VÉDELMI INTÉZKEDÉSEK

4.1 Általános rendelkezések

47. § A Társaság 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 Társasági munkaállomásokhoz. A fentiek biztosítása érdekében a Társaság munkaállomásainak technikai beállításait úgy kell elvégezni, hogy a mindennapi munkához nem szükséges kommunikációs lehetőségek tiltva legyenek.

4.2 E-mail használattal kapcsolatos előírások

48. § (1) Az e-mail használatával kapcsolatos, jelen paragrafus alatti előírásokat akkor kell alkalmazni, ha a Társaság 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 Társaság minden munkatársával szemben elvárás az elektronikus levelezéssel kapcsolatban a körültekintő és etikus viselkedés.

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

kolással ellátott
ó regisztrálását
hozzáféréshez

onosítókról van
tt munkatárssal

el a munkatárs
os keresztnevű
ábbi karaktereit

en az GSZI és

e előtt írásbeli
lhasználót, aki
használatához
gismerte, saját

rtesíti.

ek
a felhasználó
t, munkájával
A felhasználó
szerint:

ik hordozható
ezekhez való

tú információk

használni;

épet jelszóval

a hordozható

ső elektronikus levelező rendszerben továbbított üzenet, levél vagy csatolt fájl
iértékű az üzenet, levél vagy csatolt fájl személyes, papír alapon történő átadásával;

lektronikus levelező rendszerből kifelé továbbított üzenet nem vonatkozhat
ezettségvállalásra;

ektronikus levelező rendszerből kifelé továbbított bizalmasan kezelendő üzenet csak
ítva küldhető;

ektronikus levelező rendszerből kifelé továbbított levélben vagy üzenetben tilos a
ság rossz hírét kelteni;

onikus levelezéskor az elektronikus levelezési címet csak az arra jogosult személy
álhatja, más nevében elektronikus levél küldése nem engedélyezett;

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

es címzés miatt megkapott levelet bizalmasan kell kezelni, és azt haladéktalanul az
eti címzettjének vagy a feladójának kell továbbítani;

rsaság elektronikus levelező rendszerében továbbított üzenetben vagy levélben a
aság Arculati Kézikönyvében meghatározott formát kell alkalmazni.

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

4.3 Vezeték nélküli hozzáférés

Társaság a mobileszközökkel rendelkező felhasználói számára egyedi engedélyezési
vezeték nélküli (WiFi) hozzáférési lehetőséget biztosíthat elektronikus információs
ez.

ték nélküli hálózat létesítése és üzemeltetése során az alábbi feltételeknek kell
:

ezeték nélküli hozzáférést titkosítással és a felhasználók, vagy eszközök hitelesítésével
védeni

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

számítógépet zárolni.

A felhasználó adatkezelését, ideértve különösen az adatok másolását, áthelyezését, továbbítását, fel- és letöltését az GSZI a Társaság adatbiztonsága érdekében naplófájlban rögzítheti és tárolhatja.

Az elvárható gondosság elve alapján a mobiltelefonos alkalmazás(ok) telepítése előtt győződjünk meg annak nem káros voltáról. Időközönként illetve telepítés előtt látogassuk meg információkért a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet honlapját: https://nki.gov.hu/

6.2 Jogosultságcsoportok, jogosultságkezelés

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

a) Az alapszolgáltatás hozzáférés a Társaság 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;

63. A Társaság munkatársai számára az egyes rendszerekhez történő hozzáférési jogosultságokat - amennyiben a szakrendszer jogosultságkezelési utasítása ettől eltérő módon nem rendelkezik - a hibabejelentőn keresztül kell igényelni. § 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 Társaság valamennyi munkavállalója, vagy munkavégzésre irányuló egyéb jogviszonyban állók tekintetében kötelező.

6.3 Eljárás a jogviszony megszüntetése esetén

64. § A kilépő munkatárs 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.

65. § A Társaságnak 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

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről.

66. § (1) A kilépés során, a jogviszony megszűnését megelőzően az GSZI munkatársai gondoskodnak a kilépő:

a) elektronikus információs rendszerekhez történő hozzáférési jogosultságainak megszüntetéséről;

b) egyéni hitelesítő eszközeinek visszavételéről vagy megszüntetéséről;

c) a Társaság tulajdonában álló informatikai eszközök visszavételéről.

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

6.4 Elektronikus információbiztonsági szabályok megsértése

68. § A Társaság Vezérigazgatója írásbeli figyelmeztetésben részesíti az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben. Amennyiben az elektronikus információbiztonsági szabályokat nem a Társaság 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.

7. MENTÉS, ARCHIVÁLÁS

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

70. § (1) A GSZI 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.

71. § (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 zárt helyiségben vagy szekrényben kell őrizni. Rendszeresen ellenőrizni kell a mentések és archiválások helyreállíthatóságát, tesztelni kell a mentett információkat, az adathordozók megbízhatóságának

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

és az információ sértetlenségének garantálása érdekében.

8. NAPLÓZÁS

8.1 Naplózási eljárásrend

72. § A GSZI feladatai közé tartozik az elektronikus információs rendszerek figyelemmel kísérése és a technikai események naplózási adatainak gyűjtése és feldolgozása.

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

74. § 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.

75. § A napló funkciókat a GSZI 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.

76. § (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.

77. § 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.

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

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

79. § 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.

8.2 Napló információk védelme

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

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

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

8.3 Naplógenerálás és ellenőrzés

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

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

8.4 Naplózási hibák kezelése

85. § 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).

8.5 Időszinkronizálás

86. § A Társaság 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.

87. § 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.

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

9. MONITOROZÁS

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

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

90. § (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.

10. KÜLSŐ ELÉRÉSEKHEZ KAPCSOLÓDÓ VÉDELMI INTÉZKEDÉSEK

91. § (1) A Társaság 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 Társasági 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 jogosultság engedélyezéséről a Vezérigazgató dönt, az elektronikus információbiztonsági felelős javaslata alapján, aki a beérkezett igényt a Társaság elektronikus információs rendszereinek biztonsága és az azokban tárolt adatok bizalmassága, sértetlensége és rendelkezésre állása alapján javasolja a hozzáférés megadását.

c) a VPN jogosultság engedélyezését követően a GSZI erre kijelölt munkatársa létrehozza a VPN felhasználót/ jelszót és megosztja az igénylővel.

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

11. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉGRE VONATKOZÓ VÉDELMI INTÉZKEDÉSEK

11.1 Általános rendelkezések

92. § Rendszer- és információsértetlenségre vonatkozó védelmi intézkedéseket a Társaság saját üzemeltetésű elektronikus információs rendszerein be kell vezetni.

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

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

a) a Társaság valamennyi munkatársának kötelezettsége, hogy az elektronikus információs rendszerek észlelt hibáit a GSZI felé írásban bejelentsék.

b) A GSZI 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.

94. § Minden alkalmazott és külső munkatárs kötelessége, hogy az informatikai rendszerekben általa észlelt rendellenességet, gyaníthatóan gyenge pontot vagy sérülékenységet jelentse a GSZI-nek.

95. § 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.

11.2 Rendszerfrissítések kezelése

96. § 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.

97. § 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.

98. § Egyedi és dobozos feldolgozó szoftverek frissítéseit a szoftver fejlesztőjével/támogatójával egyeztetett módon kell bevezetni.

99. § 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.

11.3 Kártékony kódok, vírusok elleni védelem

100. § 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.

101. § 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.

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

102. § (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.

11.4 Az elektronikus információs rendszer felügyelete

103. § (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.

11.5 Biztonsági riasztások és tájékoztatások

104. § (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 eljuttat a szervezeten belül illetékes személyekhez;

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

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

e) meghozza a megfelelő ellenintézkedéseket és válaszlépéseket.

11.6 Jelentés biztonsági eseményekről

105. § (1) Az információbiztonsági eseményeket észlelő felhasználó(k)nak a lehető leggyorsabban jelenteni kell a GSZI-nek és az elektronikus információbiztonsági 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.

11.7 A biztonsági eseményekre és incidensekre adott válasz és fejlesztés

106. § (1) Az észlelt információbiztonsági eseményekre és gyengeségekre mielőbb válaszintézkedéseket kell hozni. Az események követését és a megoldási javaslatok, fejlesztések kidolgozását a GSZI 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.

107. § 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.

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

108. § 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

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

1. KATASZTRÓFA LEÍRÁSA

110. § 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 Társaság munkafolyamatainak informatikai támogatottságára, az informatikai szolgáltatások elvesztése az érintett munkafolyamatok szinte teljes leállásával jár. Katasztrófa esetén a Társaság adatvagyona is sérülhet. Elsődleges prioritás az adatvagyon megőrzése, minden további feladat másodlagos jellegű.

1.1 Tevékenység-sorozat katasztrófa esetén:

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

a) az esemény bekövetkezte;

b) a katasztrófa-elhárítási csapat riasztása; vezérigazgató, gazdasági és szolgáltatási igazgató, 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

112. § **(1)** A kritikus informatikai alkalmazások ismérveit jelen szabályzat tárgyi hatálya című fejezete tartalmazza. Informatikai szolgáltatás-kimaradás időlegesen kritikussá válhat továbbá - besorolásától függetlenül - az alábbi esetekben.

(2) Ha leállása esetén a folyamatban lévő 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;

Hungary Helps Ügynökség Nonprofit Zrt.
1011 Budapest, Szilágyi Dezső tér 1.
+36 1 896 6344
hungaryhelps@hungaryhelps.gov.hu

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

(3) Kritikus informatikai szolgáltatás továbbá az, amely nem tartozik a 154. §-ban körülírt informatikai katasztrófa körébe, de nyilvántartása a Társasági 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

113. § 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, de törekedni kell a 2 héten belül befejezésre.

2. A SZOLGÁLTATÁS FENNTARTÁSÁNAK/HELYREÁLLÍTÁSÁNAK ESZKÖZEI

2.1 Munkaerő

114. § Informatikai katasztrófa bekövetkezése esetén a vezérigazgatónak, a gazdasági és szolgáltatási igazgatónak, a GSZI 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 Társaság székhelyére és meg kell kezdeniük a szolgáltatás fenntartását/helyreállítását. A helyreállítási munka vezetője a gazdasági és szolgáltatási igazgató. 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 vezérigazgató adhat.

2.2 Ideiglenes nyilvántartások

115. § 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.

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

V. ZÁRÓ RENDELKEZÉSEK

117. § (1) Jelen szabályzat felülvizsgálatát el kell végezni

a) a tárgykörét érintő jogszabály módosítása esetén,
b) minden olyan esetben, amikor az elektronikus információs rendszerekben, vagy a működési környezetben jelentős változás történik,
c) Háromévente, tervezetten

(2) Jelen szabályzat 2023. augusztus 4. napján lép hatályba.