KIVONAT

A Nemzeti Védelmi Szolgálat Informatikai[1] Biztonsági Szabályzata

- Nemzeti Védelmi Szolgálat főigazgatójának 28/2013. utasítása -

Általános rendelkezések

1. Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) alapvető célja, hogy a Nemzeti Védelmi Szolgálat (a továbbiakban: NVSZ) informatikai rendszerének használata során biztosítsa az adatvédelem és az adatbiztonság jogszabályi követelményeinek az érvényesülését. Az adatokat védeni kell a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

2. Az IBSZ személyi hatálya kiterjed az NVSZ teljes személyi állományára, valamint az NVSZ informatikai rendszerével, szolgáltatásaival szerződéses, vagy más módon kapcsolatba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetek képviselőire, munkatársaira (a továbbiakban: külső személy) a velük kötött szerződésben rögzített mértékben, illetve a titoktartási nyilatkozat alapján.

3. Az IBSZ tárgyi hatálya az NVSZ használatában lévő, vagy az általa üzemeltetett valamennyi informatikai rendszerre, illetve azok környezetét alkotó rendszerelemekre terjed ki, azok teljes életciklusában (tervezés, bevezetés, fejlesztés, üzemeltetés, selejtezés). A minősített adatokat kezelő rendszerekre (függetlenül, hogy önállóan vagy hálózatban működik) a minősített adat védelmére vonatkozó jogszabályokat és a speciális szabályokat tartalmazó belső normát (rendszerbiztonsági követelmények) kell alkalmazni.

3/A. [1]Az információs rendszerekkel kapcsolatos információbiztonsági kockázati tényezők felmérésével, a kockázati tényezők meghatározásával és azok kezelésével kapcsolatos eljárási szabályokat, a károk kezelése érdekében szükséges lépéseket és eljárások körét a Nemzeti Védelmi Szolgálat Belső Kontroll Kézikönyve, valamint az NVSZ kockázatkezelési rendszerének működtetéséről szóló főigazgatói utasítás tartalmazza, összhangban az NVSZ elektronikus információbiztonságának védelméről szóló főigazgatói utasítás 2. melléklet, „informatikai biztonsági események észlelése és kezelése” cím alatt meghatározottakkal.

4. Az IBSZ alkalmazásában használt fontosabb fogalmak

a) **adat:** az információnak olyan új formában való ábrázolása, amely alkalmas közlésre, értelmezésre, vagy feldolgozásra. Tények, fogalmak vagy utasítások formalizált ábrázolása, amely alkalmas az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra (MSZ ISO 2382-1). A számítástechnikában adat a számítógépes állományok meghatározott része (minden, ami nem program), illetve mindaz, amivel a számítógépek a kommunikációjuk során foglalkoznak (kimenő és bemenő adat);

b) **adatállomány:** az informatikai rendszerben logikailag összetartozó, együtt kezelt adatok;

c) **adatátvitel:** az adatok informatikai rendszerek, rendszerelemek közötti továbbítása;

d) **adatkezelés:** az alkalmazott eljárástól függetlenül az adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása;

---

[1] Megállapította a 16/2017. NVSZ Főigazgatói utasítás 1. pontja. Hatályos 2017. 04. 21-től.

e) **adatvédelem:** az adatkezelés során érintett természetes személyek jogainak és érdekeinek védelmére és az adatkezelés során felmerülő eljárásokra vonatkozó szabályozások és eljárások;
f) **bejelentkezés:** a felhasználó által kezdeményezett olyan logikai kapcsolat, amelynek eredményeképpen az informatikai rendszer funkcióinak használata lehetővé válik;
g) **bizalmasság:** az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak, és csak a jogosultságuk szerint ismerhetik meg, használhatják fel, és rendelkezhetnek a felhasználásáról;
h) **biztonság:** a védelmi rendszer olyan, a szervezet számára kielégítő mértékű állapota, amely zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet valósít meg;
i) **elektronikus aláírás:** az informatikai rendszerben kezelt adathoz csatolt, kódolással előállított jelsorozat, amely az adat, illetve az eljáró személy azonosságának, hitelességének és sértetlenségének bizonyítására használható;
j) **engedélyezett program:** az Informatikai Osztály (a továbbiakban: IO) által a felhasználó részére átadott számítógépen lévő programok, továbbá az IO vezetőjének vagy a helyettesének az egyetértésével feltelepíthető programok;
k) **felhasználó:** személy vagy szervezet, aki (amely) egy adott számítástechnikai eszközt igénybe vesz;
l) **hálózat:** informatikai eszközök közötti adatátvitelt megvalósító logikai és fizikai eszközök összessége;
m) **hozzáférés:** olyan eljárás, amely valamely informatikai rendszer használója számára elérhetővé tesz a rendszerben adatokként tárolt információkat;
n) **információ:** tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret (adat), amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságot csökkent vagy szüntet meg;
o) **információvédelem:** az informatikai rendszerekben kezelt adatok által hordozott információk bizalmasságának, hitelességének és sértetlenségének védelme;
p) **informatikai biztonság:** az informatikai biztonság az informatikai rendszer olyan – az érintett számára kielégítő mértékű - állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;
q) **Internet:** a TCP/IP-protokollon alapuló, nyilvános, világméretű számítógépes hálózat. Az Internet a szolgáltatások széles skáláját nyújtja felhasználóinak (FTP, Gopher, IRC, e-mail, Telnet, http, WWW stb.);
r) **jelszó:** védett karakterfüzér, amelyet a felhasználói névvel együtt használva a belépni szándékozót azonosítja;
s)[2] **megbízott rendszergazda:** olyan az adott hálózaton/számítógépen felhasználóknál többlet jogosultsággal rendelkező felhasználó, aki meghatározott számítógépeken illetve hálózati szegmensben és/vagy meghatározott ideig rendszergazda feladatott lát el a részére biztosított egyedi rendszergazdai felhasználó név használatával;
t) **program:** a számítógépes utasítások logikailag és funkcionálisan összetartozó sorozata;
u) **rendelkezésre állás:** az adat, és az informatikai rendszer elemeinek tulajdonsága, amely arra vonatkozik, hogy az arra jogosultak által a szükséges időben és időtartamra használható;
v) **rendszerelemek:** az adatokat körülvevő, az informatikai rendszer részét képző elemek;
w) **rendszergazda:** a számítógépes rendszerek üzemeltetését végző szakember;
x) **rendszerbiztonsági felügyelő:** a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

[2] Beiktatta: 2/2016. (I. 11.) NVSZ főigazgatói utasítás 1. pontja. Hatályos: 2016.01.12-től.

szóló 161/2010. (V. 6.) Korm. rendelet értelmező rendelkezésében meghatározott személy;

y) **sértetlenség:** az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség), és a származás megtörténtének bizonyosságát (letagadhatatlanság) is; a rendszerelem tulajdonsága, amely arra vonatkozik, hogy a rendszerelem rendeltetésének megfelelően használható;[3]

z)[3] **szolgáltatás felhasználó:** olyan az adott hálózaton futó szolgáltatás vagy segédprogram által használt, egyedi felhasználónévvel rendelkező technikai felhasználó, mely személyhez nem köthetően kizárólag az adott hálózati szolgáltatás vagy segédprogram működéshez kerül létrehozásra és használatra;

zs)[4] **technikai felhasználó:** olyan az adott hálózaton vagy számítógépen felhasználóknál többlet jogosultsággal rendelkező felhasználó, aki a részére biztosított egyedi technikai felhasználónév használatával, előre meghatározott feladatot vagy feladatokat lát el a rendszergazda jogosultsággal rendelkező felhasználó távolléte esetén.

zsa)[5] ***üzemeltetés:*** az NVSZ elektronikus információs rendszereinek használatát lehetővé tevő, különböző szintű szolgáltatások technikai biztosításának és hibaelhárításának összetett folyamata;

zsb**)** ***üzemeltető:*** az NVSZ elektronikus információs rendszereinek vagy annak részeinek működtetését végző és a működésért felelős szervezeti elem;"

zsc)[6] ***vírus*****:** olyan programtörzs, amely a megfertőzött program alkalmazása során másolja, esetleg mutálja is önmagát. Valamilyen beépített feltétel bekövetkezésekor többnyire romboló, néha csak figyelmeztető vagy „tréfás" hatású kódja is elindul. Többnyire komoly károkat okoz, adatot töröl, formázza a merevlemezt, vagy adatállományokat küld szét e- mailben;

zsd) **Warez-oldal:** illegális szoftvermásolatok (az eredeti programba épített másolásvédelmet vagy regisztrációt kijátszva/semlegesítve, és ez által bárki számára használhatóvá téve azt) közzétételére fenntartott internetes oldal - warez-site -, ahonnan e programok ingyenesen letölthetők;

zse) **zárt hálózat:** fizikailag teljesen leválasztott, önálló hálózat;

zsf)[7] **informatikai biztonsági incidens:** olyan biztonsági esemény, amely nem része az informatikai szolgáltatás normális működésének és a szolgáltatás kiesését, vagy minőségének romlását eredményezi. Az incidenskezelési megbízott: az Informatikai Osztály vezetője.

Alapelvek

5. Az informatikai biztonsági kérdések tekintetében a bizalmasság, sértetlenség és rendelkezésre állás alapelveit kell érvényesíteni.

6. Az NVSZ objektumaiban az NVSZ számára létrehozott logikai hálózathoz csatlakozó, vagy az NVSZ által engedélyezett hálózatba nem kötött eszközök (a továbbiakban: eszközök) rendeltetésszerűen, munkavégzés céljából, az NVSZ érdekeinek szem előtt tartásával, az NVSZ által meghatározott módon használhatóak.

7. A felhasználó felelősséggel tartozik a munkavégzés céljából átvett eszközért, köteles megőrizni annak hardver és szoftver integritását. Az integritás sérelmének minősül a

---

[3] Beiktatta: 2/2016. (I. 11.) NVSZ főigazgatói utasítás 1. pontja. Hatályos: 2016.01.12-től.

[4] Beiktatta: 2/2016. (I. 11.) NVSZ főigazgatói utasítás 1. pontja. Hatályos: 2016.01.12-től.

[5] Beiktatta a 23/2017. (07.14.) NVSZ főigazgatói utasítás 1. pontja. Hatályos: 2017. 07.15.-től

[6] A számozást módosította a 23/2017. (07.14.) NVSZ főigazgatói utasítás 1. pontja. Hatályos: 2017. 07.15-től

[7] Beiktatta: 16/2018. NVSZ főigazgatói utasítás 1. pontja. Hatályos: 2018.06.05-től.

felhasználó részéről elvégzett hardveres (pl.: az informatikai eszközből illetve eszközbe alkatrész eltávolítása illetve behelyezése) vagy szoftveres (pl.: nem engedélyezett program telepítése, biztonsági beállítások[4] módosítása) módosítás.

8. Tilos más felhasználó azonosítójával az NVSZ informatikai rendszerébe bejelentkezni, más részére a bejelentkezési hozzáférést átadni.

9. [8]Az NVSZ tulajdonát nem képező, idegen információs, számítástechnikai és telekommunikációs eszközt az NVSZ informatikai struktúrájába csatlakoztatni tilos. Ettől eltérni csak kivételes esetben a hálózatot üzemeltető IO rendszergazdájával való technikai egyeztetés után, az IO vezetőjének előzetes, írásbeli jóváhagyása után lehetséges.

Azok az adathordozók, amelyek szakmai tevékenységgel kapcsolatban, az NVSZ tevékenységével összefüggő feladatokat ellátó társszervek által előállított adatokat tartalmaznak, mentesülnek az írásbeli jóváhagyás beszerzése alól.

9/A.[9] Csak és kizárólag olyan, az NVSZ informatikai rendszereivel kapcsolat létesítésére alkalmas, vagy azzal kapcsolatban adatcserére/feltöltésre felhasználni kívánt eszközt lehet beszerezni, vagy használni (mind központi forrás, mind egyéb ellátmány terhére) amit az IO előzetesen jóváhagyott és rendszer-integritás vizsgálata megtörtént. Amennyiben erre nem kerül sor, az IO az adatok és eszközök esetleges további felhasználásának lehetetlenné válása vagy megsemmisülésért felelősséget nem tud vállalni.

9/B.[10] **Az NVSZ hálózata nem használható az alábbi tevékenységekre:**

a) a mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése (pl. rágalmazás), tiltott haszonszerzésre irányuló tevékenység (pl. piramisjáték), szerzői jogok megsértése (pl. szoftver nem jogszerű terjesztése),

b) profitszerzést célzó, direkt üzleti célú tevékenység és reklám,

c) [11]a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenységre, ilyen információknak és programoknak a terjesztésére,

d) a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybevevő tevékenység (pl. nem hivatali körlevelek, hálózati játékok, kéretlen reklámok),

e) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használatra, gépek/szolgáltatások — akár tesztelés céljából történő - túlzott mértékben való szisztematikus próbálgatása (pl. TCP port scan),

f) a hálózat erőforrásainak a hálózaton elérhető adatoknak illetéktelen kezelése, módosítása, megrongálása, megsemmisítése vagy bármely károkozásra irányuló tevékenység,

g) másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységét bántó, zaklató tevékenység (pl. pornográf anyagok közzététele),

h) hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet

---

[8] Módosította a 16/2017. NVSZ főigazgatói utasítás 2. pontja. Hatályos: 2017. 04.21.

[9] Beiktatta: 26/2014. (VIII. 15.) NVSZ főigazgatói utasítás 1. pontja. Hatályos: 2014.08.16-tól.

[10] Beiktatta: 26/2014. (VIII. 15.) NVSZ főigazgatói utasítás 1. pontja. Hatályos: 2014.08.16-tól.

[11] Módosította: 16/2018. NVSZ főigazgatói utasítás 2. pontja. Hatályos: 2018.06.05-től.

más gépről vagy más felhasználótól származna (spoofing).

9/C.[12] A 9/C. pontban felsoroltak elkerülésének érdekében az NVSZ nyílt, illetve zárt informatikai hálózatának használatára vonatkozó figyelmeztető üzenetet vagy jelzést küld a felhasználó számára a rendszerhez való hozzáférés engedélyezése előtt az alábbi szöveggel:

„A felhasználó az NVSZ rendszerét használja. Az informatikai rendszer jogosulatlan használata tilos. A rendszer használat során végzett tevékenységek rögzítésre, naplózásra kerülhetnek. ”

Az elektronikus informatikai rendszer a fenti figyelmeztető üzenetet vagy jelzést mindaddig a képernyőn tarja, amíg a felhasználó közvetlen műveletet nem végez a rendszerbe való bejelentkezéshez vagy további rendszer hozzáféréshez.

9/D.[13] Az új informatikai eszközök beszerzésénél – különös tekintettel a biztonságkritikus termékekre (pl.: szerver, storage, mentőegység, switch, tűzfal, stb.) – a minimális garanciális idő 3 év.

9/E.[14] A hardver és szoftver elemek biztonsági dokumentációinak, sebezhetőségének, konfigurációval és az adminisztratív funkciók használatával kapcsolatos ismert sérülékenységek nyomon követése a Kormányzati Eseménykezelő Központ (GovCERT) heti rendszerességű tájékoztatása alapján történik.

9/F.[15] A biztonságelemzési eljárásrendet, annak időszakos felülvizsgálatát, valamint frissítését a bizalmas minősítési szintű adatok elektronikus feldolgozása és rejtjelező eszközön történő továbbítására készített számítógépes rendszer rendszerbiztonsági követelményei, illetve ezen rendszer központi szervereinek üzemeltetés biztonsági szabályzata tartalmazza.

9/G.[16] A biztonsági előírásokat megsértőkkel szemben a biztonsági vezető javaslatára fegyelmi eljárást kell kezdeményezni. Fegyelmi eljárást a biztonsági vezető értesítésével egy időben az érintett dolgozó közvetlen vezetője is kezdeményezhet.

Ha nem az NVSZ személyi állományába tartozó személy sérti meg az elektronikus információbiztonsági szabályokat, a biztonsági vezető érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések fennállásának lehetőségét, szükség szerint kezdeményezi ezeket az eljárásokat.”

Védelmi intézkedések

10. Szervezeti biztonság

a) [17] Az Ibtv. 11. § c) pontjában foglaltak alapján kinevezett Informatikai Biztonsági Felügyelő (a továbbiakban: IBF) alapvető feladata az informatikai biztonsággal kapcsolatos biztonsági követelmények teljesülésének felügyelete és ellenőrzése, valamint az informatikai

---

[12] Beiktatta: 26/2014. (VIII. 15.) NVSZ főigazgatói utasítás 1. pontja. Hatályos: 2014.08.16-tól.
[13] Beiktatta: 39/2015. (VI. 30.) NVSZ főigazgatói utasítás 1. pontja. Hatályos: 2015.07.01-től.
[14] Beiktatta: 39/2015. (VI. 30.) NVSZ főigazgatói utasítás 1. pontja. Hatályos: 2015.07.01-től.
[15] Beiktatta: 39/2015. (VI. 30.) NVSZ főigazgatói utasítás 1. pontja. Hatályos: 2015.07.01-től.
[16] Beiktatta a 23/2017. (07.14.) NVSZ Főigazgatói utasítás 3. pontja. Hatályos: 2017. 07. 15-től
[17] Módosította a 16/2017. (IV. 20.) NVSZ főigazgatói utasítás 5. pontja. Hatályos: 2017. 04.21.-től.

biztonság megsértését eredményező valós vagy feltételezett események kivizsgálása. Évente értékeli az NVSZ informatikai biztonsági helyzetét, felülvizsgálja az IBSZ-t. Az értékelő jelentést minden év március 31-ig a Hivatalon keresztül felterjeszti az NVSZ főigazgatójának. Az NVSZ hálózati infrastruktúráját és a folyamatos üzemmenetet veszélyeztető hálózati műveletek korlátozására vagy letiltására javaslatot tesz az IO vezetőjének.

b) Az IBF szerepkörét el kell különíteni az informatikai rendszerek mindennapos üzemeltetési feladataitól, és a feladatait a munkaköri leírásában rögzíteni kell. Az IBF nem lehet az IO állományába tartozó személy. [18]

c) Az informatikai biztonsággal kapcsolatos üzemeltetési tevékenység ellátása az IO feladatkörébe tartozik.

d) [19]Az IO vezetője összehangolja és irányítja az NVSZ által nyújtott informatikai szolgáltatásokat. Tervezi, szervezi, irányítja, és koordinálja az NVSZ-nél üzemeltetett informatikai rendszerek védelmével összefüggő tevékenységeket. Az informatikai biztonság szempontjából véleményezi az NVSZ szabályzatait. Véleményezi az informatikai eszközök és alkalmazások beszerzési és fejlesztési igényeit, melybe bevonja az IBF-t. Az IO vezetője valamint az IBF a feladatai ellátásához külső munkatársakat, szakértőket vonhat be.

e) Az informatikai rendszerek üzemeltetését az IO munkatársai végzik.

11. [20]Az NVSZ informatikai rendszereiben tárolt adatok védelmének módszereit és az adatbiztonsági intézkedéseket az NVSZ Adatvédelmi Szabályzata tartalmazza. Az adatvédelmi incidens kivizsgálása során, amennyiben megállapításra került, hogy az incidens elektronikus információs rendszert érintett, akkor az incidenskezelési megbízott haladéktalan értesítése szükséges, akinek feladata a 11/A. pontban foglaltak végrehajtása.

11/A. [21]Informatikai biztonsági incidenssel kapcsolatos eljárásrend

a) Az incidenskezelés elsődleges célja a normál szolgáltatási körülmények soron kívüli visszaállítása, minimalizálva az elektronikus információs rendszerre gyakorolt káros hatást, így biztosítva a szolgáltatás minőségének színvonalát.

b) Amennyiben az elektronikus információs rendszer felhasználója informatikai biztonsági incidensről szerez tudomást, azt haladéktalanul bejelenti az incidenskezelési megbízottnak. Az incidenskezelési megbízott az IBF értesítése mellett megkezdi a felhasználó és a felhasználó szervezeti elem vezetője által készített jelentés alapján az incidens kivizsgálását.

c) Az IBF feladata az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálya alá tartozó bármely elektronikus információs rendszert érintő informatikai biztonsági incidensről a meghatározottak szerint tájékoztatni az év bármelyik napján, a nap 24 órájában a Kormányzati Eseménykezelő Központot, amely szerv a kivizsgálásban segítséget, támogatást nyújthat.

d) Az incidens kivizsgálásáról szóló jelentés tartalmazza:

---

[18] A 10. b) alpont harmadik mondatát hatályon kívül helyezte a 16/2017. (IV. 20.) NVSZ főigazgatói utasítás 12. pontja. Hatályát vesztette: 2017. 04. 21-én.

[19] Módosította: 16/2018. NVSZ főigazgatói utasítás 4. pontja. Hatályos: 2018.06.05-től.

[20] Módosította: 16/2018. NVSZ főigazgatói utasítás 6. pontja. Hatályos: 2018.06.05-től.

[21] Beiktatta: 16/2018. NVSZ főigazgatói utasítás 7. pontja. Hatályos: 2018.06.05-től.

da) az incidens észlelőjének nevét, elérhetőségét;
db) az incidens jellegét, pontos leírását;
dc) az incidens által érintett szolgáltatás pontos megnevezését;
dd) az incidenssel érintett rendszert, rendszerelemet;
de) telephely megnevezését (telephely neve, pontos címe, emelet);
df) a hibabehatárolás esetén szerzett információkat, a hiba leírását;
dg) a hibás eszköz fajtáját, típusát, gyári számát;
dh) egyéb, a hibaelhárítást megkönnyítő információkat (pl. áramszünet stb);
di) az incidens következményeit, és várható hatását;
dj) az incidens megszüntetésével, hátrányos következményeinek mérséklésével kapcsolatban megtett, illetve javasolt intézkedéseket.

e) A kivizsgálást követően az incidenst bejelentő részére visszacsatolás szükséges és amennyiben a bejelentő a hiba további fennállását igazolja vissza, az incidens elhárítási folyamatot elölről kell kezdeni.

f) Az elektronikus információs rendszert érintő informatikai biztonsági incidens kivizsgálásában részt vevő személy csak az lehet, aki előzetesen részt vett a biztonságiesemény-kezelő eljárásról szóló, kormányzati eseménykezelő központ által tartott tájékoztató előadáson.

12. Az informatikai rendszer áramellátásának biztonsága

a) A megbízható működés szempontjából biztosítani szükséges, hogy az elektromos hálózat a szünetmentességre, az áthidalási és újratöltési időre vonatkozó követelményeknek megfeleljen. Ha egy nem szerverszobának kijelölt hivatali helyiségben szerver üzemel, gondoskodni kell lokális szünetmentes tápáramellátásról.

b) Az elektromos hálózatnak meg kell felelnie az MSZ 1600 sorozatú szabványoknak. Az érintésvédelemnek meg kell felelnie az MSZ 172 sorozatú szabványoknak.

c) A túlfeszültség- és villámvédelemnek meg kell felelnie a kommunális és lakóépületekre vonatkozó előírásoknak.

d) Az elektromos hálózat meghibásodása, az energiaellátás megszűnése esetén gondoskodni kell az informatikai berendezések védelméről (lehetőség szerint szünetmentes áramforrást illetve alternatív áramszolgáltatási lehetőséget kell igénybe venni).

e) Az adatátviteli (távközlési) kábelt el kell különíteni az energiaellátás kábeleitől.

13. Hálózatmenedzsment

a) Az NVSZ közvetlen szervezeti és fizikai felügyeletén kívül eső kapcsolatok esetében a kriptográfiai módszerek (pl.: kódolás, digitális aláírás, SSL/TSL, https) használata kötelező.

b) Az illetéktelen hozzáférés megelőzése érdekében:

ba) gondoskodni kell a rendszerdokumentációk biztonságos tárolásáról;
bb) minimálisra kell csökkenteni a rendszerdokumentációkhoz hozzáférők számát;
bc) gondoskodni kell a nyilvános hálózaton keresztül elérhető, vagy azon keresztül továbbított dokumentáció védelméről.

c) Az IO az NVSZ hálózati infrastruktúráját és a folyamatos üzemmenetet veszélyeztető hálózati műveleteket korlátozhatja, vagy letilthatja.

d) Az IO kizárólag az NVSZ szerverein tárolt az NVSZ adatvagyonát képező adatok védelmét biztosítja. A munkaállomásokon hálózatra kapcsolt vagy önálló gépeken tárolt adatokért a

számítógépet használó a felelős. Az ilyen jellegű adatok mentésére a Gazdasági és Humán Igazgatónak benyújtott kérelem alapján az IO külső mentőeszközöket (pl.: pendrive, USB winchester) biztosít. Az NVSZ informatikai eszközein kizárólag a szolgálati feladatokhoz tartozó adatokat lehet tárolni.

e) [22] Az NVSZ Informatikai rendszerébe kapcsolt munkaállomásokhoz tilos külső Internet elérést illetve egyéb külső hálózati kapcsolatot elérhetővé tevő, továbbá ezen kapcsolatokat akár vezetékkel akár vezeték nélkül megosztani képes eszközt csatlakoztatni (mobiltelefon, mobil stick, wifi és nem wifi router, stb.). Ezen tiltás alól kizárólag az IO előzetes hozzájárulásával és szakmai felügyelete mellett lehet eltérni.

f) [23] Az önálló munkaállomásokra (továbbiakban: offline gép) tilos külső Internet elérést, illetve egyéb külső hálózati kapcsolatot elérhetővé tevő, valamint ezen kapcsolatokat akár vezetékkel akár vezeték nélkül megosztani képes eszközt csatlakoztatni (mobiltelefon, mobil stick, wifi és nem wifi router, stb.). Ezen tiltás alól kizárólag az IO előzetes hozzájárulásával és szakmai felügyelete mellett lehet eltérni. Operatív munka során keletkezett adatokat tároló szolgálati mobiltelefont úgynevezett „repülő" vagy „offline" állapotba kell kapcsolni, melynek következtében nem képes a GSM hálózathoz csatlakozni, így nem tud a készülék a modemként funkcionálni, tehát adatokat sem tud küldeni/fogadni. Az offline gépeken a vírusirtó szoftvert napra készen kell tartani. A szolgálati pendrive-ok, külső adattároló merevlemezekről csak az IO által jóváhagyott és telepített vírusirtó védelmi szoftverrel ellátott offline gépekhez lehet csatlakoztatni.

g) [24] Minősített adatok feldolgozására használt rendszerek esetében a minősített adat védelméről szóló 2009. évi CLV. törvény és a végrehajtására kiadott kormányrendeletek (különös tekintettel a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendeletre) rendelkezései az irányadóak. A változástípusok, változáskezelési vizsgálat kötelező és nem kötelező elemeit, előfeltételeit, valamint az ezzel kapcsolatos változtatásokat és kockázatelemzéseket a rendszerengedélyhez szükséges rendszerbiztonsági követelmények, valamint az üzemeltetési biztonsági szabályzat határozza meg.

h) [25] Munkaállomás hálózatból történő kivételét (tartományi kiléptetés) illetve munkaállomás hálózatba történő betételét (tartományi beléptetés) az IO-tól kell kérni szolgálati jegyen, aki ellenőrzi a ki/beléptetéshez szükséges feltételek meglétét és szükségességét, intézkedik ezek végrehajtására az érintett szervezeti elemek felé. A szolgálati jegy másodpéldányát egyidejűleg meg kell küldeni az NVSZ Hivatal Ügyviteli Osztály rendszerbiztonsági felügyelője részére a szükséges rendszerengedély-módosítás előkészítése érdekében.

14. Az elektronikus levelezés biztonsága

a) A levelezőrendszer vírusvédelmét folyamatosan frissíteni kell, valamint követni kell az új email vírusok megjelenését.

b) Az elektronikus levelező eszközök, elsősorban a szerverek fizikai és logikai védelméről folyamatosan gondoskodni kell (pl. nyomon kell követni az új szoftverfrissítések, service packok és security-patch fájlok megjelenését).

---

[22] Beiktatta: 26/2014. (VIII. 15.) NVSZ főigazgatói utasítás 4. pontja. Hatályos: 2014.08.16-tól.

[23] Beiktatta: 26/2014. (VIII. 15.) NVSZ főigazgatói utasítás 4. pontja. Hatályos: 2014.08.16-tól.

[24] Módosította a 16/2017. (IV. 20.) NVSZ főigazgatói utasítás 8. pontja. Hatályos: 2017. 04.21-től.

[25] Beiktatta: 2/2016. (I. 11.) NVSZ főigazgatói utasítás 2. pontja. Hatályos: 2016.01.12-től.

c) [26]A kétes forrásból származó üzeneteket, az elektronikus levelezés forgalmát - a technikai lehetőségek szerint - tartalmilag szűrni kell, a szenzitív adatok kiszivárgásának elkerülése érdekében. Az NVSZ levelezőrendszerén tárolt és továbbított levelek az NVSZ tulajdonát képezik, ezért az NVSZ szabályzatokban és utasításokban feljogosított ellenőrző szerveinek ezekhez az állományokhoz, a vizsgálathoz szükséges mértékig betekintési joga van.

d) Az NVSZ levelezőrendszere reklám, valamint egyéb üzleti célokra nem használható.

15. Az Internet használatának rendje

a) Az Internet szolgáltatás a felhasználói jogosultság része.

b) Az internetes hozzáférés csak a munkaköri feladatok ellátására használható.

c) Az ORFK-n keresztüli Internet igénybevételét az ORFK Gazdasági Főigazgatóság Informatikai Infrastruktúra Üzemeltetési Főosztálya ellenőrzi. Az ORFK havi kerethasználat- túllépésre irányuló értesítése alapján - az Ellenőrzési Osztály közreműködésével - a szervezeti egység vezetőjének ki kell vizsgálnia az Internethasználat jogosultságát.

d) [27] A mindenkori érvényes letöltési keretre vonatkozó adat a http://cimtar.police.hu belső intranetes címen, a „korlátozások” címszó alatt található. Az aktuális letöltési értéket a *https://statistic.police.hu/kvota* oldal betöltése után megadva az e-mail címet és a hozzá tartozó jelszót, lehet figyelemmel kísérni.

e) Az igénybevétel jogszerűségének, illetve jogszerűtlenségének megállapítására irányuló eljárás során az érintettnek lehetőséget kell adni arra, hogy az Internethasználat indokoltságát bizonyítsa.

f) Tilos az NVSZ hálózati infrastruktúráját veszélyeztető oldalakat (felnőtt tartalmú-, warez-, fájlcserélő weboldalak stb.) látogatni.

g) [28] Azoknak a felhasználóknak, akiknek a munkaköréhez tartozóan indokolt az 15/f) pontban meghatározott oldalak látogatása, külön engedély alapján lehet hozzáférést igényelni.

16. Védelem a rosszindulatú programok ellen

a) [29]Törekedni kell arra, hogy megfelelő intézkedésekkel megakadályozzuk, illetve kiszűrjük a rosszindulatú programokat (vírusokkal fertőzött termékek, a hálózati férgek, Trójai programok, logikai bombák stb.).

b) A rosszindulatú programokkal szembeni védekezést szűréssel és a programok bevezetése előtti ellenőrzéssel kell megvalósítani. A rosszindulatú program elleni védekezés részét képezi a felhasználók tájékoztatása, a hozzáférés-védelem, továbbá a változtatások felügyelete és ellenőrzése.

c) [30]Ha a felhasználó bármilyen rendellenességet, vírusra utaló jelenséget észlel, akkor a munkafolyamat felfüggesztésével egyidejűleg az IO vezetőjét, a kijelölt rendszergazdát, vagy az NVSZ rendszeradminisztrátort azonnal telefonon értesíteni köteles. A szolgálati helyen kívül használt informatikai eszközöknél az észlelést követően a további használat mellőzésével, a fenti értesítési rend mellett, az informatikai eszközt az IO-ra ellenőrzésre is

---

[26] Módosította: 16/2018. NVSZ főigazgatói utasítás 8. pontja. Hatályos: 2018.06.05-től.
[27] Megállapította: 26/2014. (VIII. 15.) NVSZ főigazgatói utasítás 5. pontja. Hatályos: 2014.08.16-tól.
[28] Megállapította: 26/2014. (VIII. 15.) NVSZ főigazgatói utasítás 6. pontja. Hatályos: 2014.08.16-tól.
[29] Módosította: 16/2018. NVSZ főigazgatói utasítás 9. pontja. Hatályos: 2018.06.05-től.
[30] Módosította a 16/2017. (IV. 20.) NVSZ főigazgatói utasítás 10. pontja. Hatályos: 2017. 04.21-től.

el kell juttatni.

17. Az adatok mentése

a) A biztonsági mentéseket ha az a mentő rendszerből kikerült, lehetőség szerint külön telephelyen, vagy helyiségben, de minimum elkülönülten, elzárva a mentett adat biztonsági szintjének megfelelő védelemmel ellátott helyen kell tárolni. A mentések adathordozóit nyilvántartásba kell venni, és azok meglétét rendszeresen ellenőrizni kell.

b) [31] Az időszakos mentéseket, archiválásokat - ha jogszabály, vagy belső norma másként nem rendelkezik - minimum három hónapig meg kell őrizni.

c) A mentések végrehajtásáért az IO vezetője által kijelölt rendszergazda a felelős.

d) [32] A készített mentések célja a katasztrófa illetve egyéb vis major jellegű rendszerhiba esetén történő adat visszaállás. Az adatok megőrzési ideje a mentési háttértárolók kapacitásának figyelembe vételével három hónap. Felhasználói figyelmetlenség következtében történő adat törlés esetén, visszamenőlegesen maximum három hónap időtartamra tud az IO adatokat visszaállítani. A mentési időszakok között létrehozott és ugyanabban a ciklusban megsemmisült adatok visszaállítására technikailag nincs lehetőség. A visszaállítás minimum 1-2 órát vesz igénybe, a mentőrendszer és az informatikai hálózat aktuális terheltségi szintjétől függően.

e) [33]Rendkívüli események által okozott károk elkerülésére, enyhítésére - a hálózati meghibásodások, adatvesztések utáni helyreállításra - a rendszer üzemeltetője köteles intézkedni. Ennek érdekében a helyreállításhoz alkalmazható napi, heti mentéseknek rendelkezésre kell állnia. A mentések elkészítése, karbantartása és a tárolása a kapcsolódó biztonsági szabályok betartása mellett az üzemeltető feladata. Az NVSZ IO gondoskodik az elektronikus információs rendszer utolsó mentett állapotba történő helyreállításáról és újraindításáról egy esetleges összeomlást, kompromittálódást vagy hibát követően

f) [34]Az elektronikus ügyintézési kötelezettség teljesítésével összefüggő nem minősített adatok sérüléséből eredő működési zavar esetén a működési képesség helyreállítása és az adatvesztés minimalizálása okán az NVSZ az adatok biztonságát szolgáló Kormányzati Adattrezorhoz csatlakozott, mely részleteiről az Archiválási szabályzat rendelkezik.

18. A rendszerek és a programok működési zavarainak kezelése

a) Az NVSZ minden szerverén és munkaállomásán folyamatosan figyelni kell a rendszerek esetleges hibaüzeneteit.

b) Rendszer-, illetve alkalmazáshiba esetén:

ba) figyelemmel kell kísérni a működési zavar tüneteit, a képernyőn megjelenő üzeneteket,

bb) amennyiben a rendszerhibát vélhetően külső, illetéktelen beavatkozás, vagy vírustámadás okozta, az érintett munkaállomást, számítógépet le kell választani a hálózat(ok)ról, szükség esetén ki kell kapcsolni. Ilyen esetekben fokozottan figyelni kell a hordozható adathordozókra is (Pen drive, CD-ROM, mentési médiák), melyeket az IO-nak vizsgálat céljára át kell adni,

---

31 Megállapította: 26/2014. (VIII. 15.) NVSZ főigazgatói utasítás 7. pontja. Hatályos: 2014.08.16-tól.

32 Beiktatta: 26/2014. (VIII. 15.) NVSZ főigazgatói utasítás 8. pontja. Hatályos: 2014.08.16-tól.

33 Beiktatta a 23/2017. (VII. 14.) NVSZ főigazgatói utasítás 4. pontja. Hatályos: 2017. 07.15-től.

34 Beiktatta: 16/2018. NVSZ főigazgatói utasítás 10. pontja. Hatályos: 2018.06.05-től.

bc) a meghibásodott számítógépben használt adathordozók kizárólag a biztonsági ellenőrzést követően használhatók más számítógépekben.

c)[35] Az amortizációs csere az alkalmazott hardver és szoftver követelmények alkalmazhatóságának függvényében történik.

d)[36] Az ügymenet folytonosságának fenntartása érdekében minimum öt darab tartalék munkaállomás, hálózati aktív eszközökből típusonként egy-egy darab tartalék rendelkezésre állása szükséges. Szerver gépek esetén szükséges a nagy rendelkezésre állás biztosítása (failover, HA, stb.).

e)[37] Az ügymenet-folytonosság felülvizsgálata az elektronikus információs rendszer, vagy a működési környezet változása esetén vagy minimum 5 évente szükséges. Az alkalmazott elektronikus információs rendszer fizika sérülése esetén a helyreállítás az informatikai osztályvezető utasításainak megfelelően – szükség esetén külső szakértő bevonásával – történik, úgy, hogy a helyreállítás nem ronthatja le az eredetileg terezett és megvalósított biztonsági védelmeket.

19. Fejlesztési alapelvek

a) Minden új program-tervezetet meg kell küldeni az IO-nak véleményezésre.

b) Minden program bevezetésének feltétele, hogy rendelkeznie kell programtervvel, az informatikai rendszerhez kapcsolódó leírással, kezelői útmutatással és oktatói dokumentációval.

c) A fejlesztői és teszt rendszereket ha a technikai lehetőség biztosított, akkor el kell választani az éles rendszerektől.

d) Az NVSZ által fejlesztett programok forráskódjához csak az a személy férhet hozzá, akinek az alkalmazásért felelős vezető írásos engedélyt adott. A program forrásának minden változását dokumentálni kell.

e) A programok forráskódjainak korábbi verzióit archiválni kell. A program forráskönyvtárainak karbantartását és másolását a változtatásokra vonatkozó szigorú ellenőrzési eljárások alá kell vonni.

20. A felhasználói hozzáférés általános szabályai

a) Az információs rendszerek illetéktelen elérésének megakadályozása érdekében megfelelő hozzáférési rendszert kell kialakítani. Hozzáférési jogosultság csak írásban kérhető.

b) Olyan be- és kijelentkezési eljárást kell működtetni, amely alapján mindegyik több felhasználós rendszerben és szolgáltatásnál szabályozni lehet a felhasználók hozzáférését.

c) A felhasználó azonosító az informatikai rendszert használó identitásának egyedi, jellemző, ellenőrizhető és hitelesítésre alkalmas megjelenítése kell, hogy legyen az informatikai rendszerben, nem adható ki különböző felhasználók részére megegyező azonosító. Az egyedi felhasználói azonosítót a hozzáférés szabályozására, az adatok és az információk védelmére, valamint a hitelesítés támogatására kell felhasználni. Biztosítani kell, hogy a felhasználó azonosítója az egyes erőforrásokhoz, folyamatokhoz és az adatokhoz való hozzáférést megfelelően szabályozza (korlátozza).

---

[35] Beiktatta: 39/2015. (VI. 30.) NVSZ főigazgatói utasítás 3. pontja. Hatályos: 2015.07.01-től.

[36] Beiktatta: 39/2015. (VI. 30.) NVSZ főigazgatói utasítás 3. pontja. Hatályos: 2015.07.01-től.

[37] Beiktatta: 39/2015. (VI. 30.) NVSZ főigazgatói utasítás 3. pontja. Hatályos: 2015.07.01-től.

d) Az egyes felhasználói azonosítókhoz rendelt jogosultságok minden esetben csak az adott munkakör ellátásához szükséges minimális funkcióelérést biztosíthatják.

e) A felhasználói azonosítók vonatkozásában a következő szabályokat kell alkalmazni:

ea) az NVSZ munkatárs, illetve külső személyek - amennyiben munkakörük, illetve beosztásuk alapján az informatikai rendszer szolgáltatásait igénybe vehetik -, munkába állásuk után kapják meg felhasználói azonosítójukat. A szervezeti egység vezetője megigényli a felhasználói azonosítót a hozzáférési jogosultságok megjelölésével. Más azonosítója átmenetileg sem használható;

eb) [38] A dolgozó jogviszonyának megszűnése esetén a felettes vezetője gondoskodik az információs rendszerrel kapcsolatos jogosultságok megszüntetéséről. Az IO a Leszerelő lap aláírásával a kilépő számára igazolja, hogy az IO által kezelt hozzáférési jogosultságait visszavonja, illetve visszavonásukat kezdeményezi, valamint az NVSZ elektronikus információs rendszerein létrehozott, profiljához tartozó és az abban tárolt adatokat törli, vagy a megbízott rendszergazdák útján törölteti, legkésőbb a jogviszony megszűnését követő 1 hónapon belül. Kivételt képeznek ez alól a szerveken létrehozott jogosultságok kezeléséhez kapcsolódó profilok (pl: AD account);

ec) a jogviszonyukat huzamosabb ideig szüneteltető (pl.: képviselőjelölt, gyermek szülése stb.), illetve a más okból tartósan távollévő (pl.: külföldi kiküldetés, elhúzódó gyógykezelés) NVSZ munkatársak felhasználói azonosítóját le kell tiltani, illetve munkába állásukkal egyidőben ismét engedélyezni kell. Erről a munkatárs mindenkori vezetője írásban tájékoztatja az IO-t;

ed) külső személyek, akik valamilyen okból igénybe vehetik az NVSZ bármelyik rendszerének szolgáltatásait, csak meghatározott időre, és korlátozott lehetőségeket biztosító (pl. egy adott projekt keretein belül érvényes) felhasználói azonosítót kaphatnak, ami szerkezetileg megfelel a szervezeten belüli NVSZ munkatársak azonosítójának, de egyértelműen és könnyen megállapítható, hogy az adott felhasználói azonosító külső személyé.

f) **[39]** Az elektronikus információs rendszer tíz egymást követő sikertelen bejelentkezési kísérletet követően legalább 1 percig a felhasználói fiókot automatikusan zárolja vagy más módon késlelteti a következő bejelentkezési kísérletet.

21. A jogosultságok kezelése

a) Standard jogosultságok:

aa) olvasási jog (betekintés),
ab) módosítási jog.

b) A hozzáférés-jogosultság vezérlésére a szerepkör szerinti hozzáférés elvét kell alkalmazni, valamint a biztonsági adminisztrátori szerepkört elkülönítetten kell létrehozni.

c) A rendszernek alkalmasnak kell lennie a hozzáférési jogok egyedi vagy csoport szinten való megkülönböztetésére és szabályozására. A hasonló szerepű személyek csoportjai munkájának támogatására hozzáférési jogosultsági csoportokat kell kialakítani.

d) **[40]** Jogosultság igénylést, módosítást és visszavonást – az NVSZ Adatvédelmi Szabályzatának „A hozzáférési jogosultságok” fejezetével összhangban – csak jogosultság

---

[38] Módosította: 16/2018. NVSZ főigazgatói utasítás 11. pontja. Hatályos: 2018.06.05-től.

[39] Beiktatta: 26/2014. (VIII. 15.) NVSZ főigazgatói utasítás 9. pontja. Hatályos: 2014.08.16-tól.

[40] Megállapította: 2/2016. (I. 11.) NVSZ főigazgatói utasítás 3. pontja. Hatályos: 2016.01.12-től.

igénylő nyomtatványon, pontos könyvtárnév és jogosultság típus megadásával, a nyilvántartási szám teljes feltüntetésével, a jogosult vezető sajátkezű aláírásával és szervezeti elem körbélyegző-lenyomatával ellátva lehet kérni, a másolati példány elektronikus úton vagy kézbesítő általi továbbításával az IO felé. A jogosultság kérelem eredeti példánya az igénylő szervezeti elemnél kerül iratkezelésre.

21/A.[41] Az NVSZ-től történő leszerelés esetén az IO által beállított jogosultságok visszavonására automatikusan – külön szolgálati jegy nélkül – intézkedés történik a Humánigazgatási Főosztály átirata alapján. [42]Informatikai jogosultságot is keletkeztető szerződés lejárta esetén, az IO által beállított jogosultságok visszavonását az NVSZ részéről az IO végzi a teljesítést igazoló személy - legkésőbb a szerződés lejártának napjáig megküldött - átirata alapján. Az átiratnak tartalmaznia kell a szerződés alapján létrejött jogviszony megszűnésének konkrét időpontját.

21/B.[43] A jogosultságokat 60 naponta felül kell vizsgálniuk az igénylő vezetőknek.

22. A felhasználói jelszavak kezelése

a) [44] Az informatikai rendszerekben a felhasználók hitelesítésének alapvető módja a felhasználónév és jelszó páros megadása.

b) A belépéskor kapott, illetve - pl. ha a felhasználó elfelejtette a jelszavát - az ideiglenes jelszó átadása csak biztonságos csatornán történhet kérelme alapján, a felhasználó előzetes - pl. személyes - azonosítása után. Az ideiglenes jelszavak megváltoztatása kötelező az első belépést követően.

c) Automatikus bejelentkezési eljárások (pl.: batch-fájlok vagy funkcióbillentyűhöz rendelt makrók) nem tartalmazhatnak felhasználói jelszót.

d) Biztosítani kell, hogy a felhasználók tényleges hozzáférési jogosultsága munkakörüknek megfelelő legyen.

e) [45]

23. A felhasználó feladatai

a) [46] Meg kell akadályozni az illetéktelen felhasználói hozzáférést az általa használt informatikai rendszer erőforrásaihoz. Az informatikai biztonság hatékonyságához nélkülözhetetlen az engedéllyel rendelkező felhasználók együttműködése. A szolgáltatások felhasználója teljes felelősséggel tartozik az adott szolgáltatások, erőforrások pazarlása miatt az üzemeltetésben keletkező többletköltségekért.

b) A jelszavakat nem szabad papíron tárolni. Amennyiben ez elkerülhetetlen (pl. a kezdeti jelszó), akkor gondoskodni kell a jelszó zárt borítékban történő, biztonságos tárolásáról. Amennyiben a felhasználó azt gyanítja, hogy jelszavát valaki megismerte, azonnal

---

41 Megállapította: 2/2016. (I. 11.) NVSZ főigazgatói utasítás 4. pontja. Hatályos: 2016.01.12-től.

42 Beiktatta a 16/2017. (IV. 20.) NVSZ főigazgatói utasítás 11. pontja. Hatályos: 2017. 04. 21-től.

43 Megállapította: 2/2016. (I. 11.) NVSZ főigazgatói utasítás 4. pontja. Hatályos: 2016.01.12-től.

44 Megállapította: 26/2014. (VIII. 15.) NVSZ főigazgatói utasítás 10. pontja. Hatályos: 2014.08.16-tól.

45 Hatályon kívül helyezte: 26/2014. (VIII. 15.) NVSZ főigazgatói utasítás 17. pontja. Hatálytalan: 2014.08.16-tól.

46 Kiegészítette: 26/2014. (VIII. 15.) NVSZ főigazgatói utasítás 13. pontja. Hatályos: 2014.08.16-tól.

módosítania szükséges.

c) A jelszó kívülálló számára ne legyen egyszerűen kitalálható, ne tartalmazzon a felhasználó személyére utaló információkat (pl. neveket, telefonszámokat, születési dátumokat).

d) Amennyiben a munkaállomásokon a hitelesítési folyamatban a beírt jelszó olvasható (az alkalmazás nem rejti el megfelelően a jelszót), az alkalmazás üzemeltetőjének figyelmeztetése alapján, a felhasználó köteles gondoskodni arról, hogy más illetéktelen személy ne láthassa meg az általa beírt jelszót.

e) A felhasználó azonosítójával és jelszavával az informatikai rendszerben végrehajtott műveletekért személyesen felel.

f) [47] A felhasználóknak gondoskodniuk kell a felügyelet nélkül hagyott eszközök megbízható védelméről úgy, hogy az NVSZ által előírt védelmi rendszereket (riasztó, zár stb.), alkalmazza. A számítógépet ideiglenesen elhagyva, az azon lévő adatokhoz történő illetéktelen hozzáférés érdekében, a munkaállomást zárolni kell (pl: a ⊞ + „L" billentyű lenyomásával) Munkaállomásokon felhasználóváltás esetén a korábbi felhasználónak ki kell jelentkeznie és az új felhasználónak saját felhasználó nevével és jelszavával be kell jelentkeznie.

g) A felhasználó törekedjen arra, hogy a monitort úgy helyezze el, hogy az azon megjelenő adatokat illetéktelen személy ne láthassa.

h) A napi munkavégzés befejezését követően a munkaállomások kikapcsolása kötelező, kivéve, ha olyan alkalmazás fut, amely a szolgálati feladatok elvégzése szempontjából elengedhetetlenül szükséges.

i) A számítógépek használata során fokozott figyelmet kell fordítani a tűz-, érintés- és munkavédelmi szabályok betartására. Ennek megfelelően a számítógépek szellőzőnyílásait nem szabad letakarni, az elektromos csatlakozási lehetőségeknél pedig kiemelt figyelmet kell fordítani az áramütés veszélyére.

j) Az eszközök tisztaságáért a felhasználó a felelős. Kerülni kell az eszközök közelében az étel és ital fogyasztását, és olyan tevékenységet, amellyel az eszköz bepiszkolódhat. Különös tekintettel óvni kell az optikai alkatrészt is tartalmazó eszközt /pl.: CD, DVD-olvasó/.

k) Számítástechnikai berendezések közelében nedves, vizes tárgyakat, eszközöket (pl.: virág, szökőkút stb.) tartani és üzemeltetni tilos.

1) Elektromos meghibásodás, pl. zárlat gyanúja esetén az eszközt áramtalanítani kell.

m) A kiosztott informatikai eszközöket köteles az eszköz használója, több felhasználó esetén a szervezeti egység vezetője által kijelölt személy átadás-átvételi bizonylaton átvenni és a tőle elvárható gondossággal kezelni.

n) Tilos az IO írásos értesítése nélkül az informatikai eszközöket átszállítani egy másik helyiségbe. Az informatikai eszközök áthelyezése esetén jegyzőkönyvet kell készíteni, amelyből 1 példányt el kell juttatni az IO-ra. A jegyzőkönyv elkészítéséért az a szervezeti egység vezetője a felelős, akinél az áthelyezés előtt volt az eszköz, kivéve, ha az informatikai raktárból illetve raktárba történik az áthelyezés, ebben az esetben az IO készíti el a jegyzőkönyvet.

o)[48] Törekedni kell, hogy a munkaállomások számítógépháza, lehetőség szerint az asztalon kerüljön elhelyezésre.

p)[49] Leszerelés és áthelyezés esetén, a munkatársnak tájékoztatást kell kérnie a GHI GFO

---

47 Kiegészítette: 26/2014. (VIII. 15.) NVSZ főigazgatói utasítás 14. pontja. Hatályos: 2014.08.16-tól.

48 Beiktatta: 26/2014. (VIII. 15.) NVSZ főigazgatói utasítás 15. pontja. Hatályos: 2014.08.16-tól.

49 Beiktatta: 15/2014. (V. 13.) NVSZ főigazgatói utasítás 15. pontja. Hatályos: 2014.05.14-től.

KGO-tól, hogy milyen eszközök vannak a nevére terhelve. Amennyiben ezek az eszközök régi szolgálati helyén maradnak, akkor azokról átadás-átvételi jegyzőkönyvet kell készíteni minimum 3 példányban (1 pld IO; 1 pld KGO; 1 pld leszerelő), melyen az eszközt dokumentáltan átadja egy a szervezeti egységnél maradó kollégának, aki azt nevére veszi, melyet aláírással megerősít. Az IO példányát, leszerelő-lap aláírásakor, magával kell hoznia és az IO-nak átadni köteles. Az átadás-átvételi jegyzőkönyv nélkül, az eszközökkel történő elszámolás nem végrehajtható.

q)[50] Tilos a munkaállomásokon mappákat megosztani.

24.[51] Az NVSZ informatikai rendszereinek, hálózatainak elektronikus naplózási rendjét az IBSZ függeléke tartalmazza.

25.[52] Hálózati nyomtatás használata

a) Az NVSZ Informatikai rendszerébe kötött multifunkciós hálózati nyomtatókra történő nyomtatás esetén a felhasználóknak különösen körültekintően kell eljárniuk. Olyan adatokat nyomtatni, amelyek minősített adatokat tartalmaznak, kizárólag olyan módon lehet (amennyiben az eszköz lehetővé teszi), hogy a tényleges nyomtatás az aktuálisan kiválasztott nyomtatón történő felhasználói azonosítás és jelszó megadása után valósuljon meg. Lehetőség szerint ugyanilyen módon kell történnie a személyes és szolgálati adatokat tartalmazó dokumentumok nyomtatásának is, illetve ha ez mégsem így valósul meg, az ilyen jellegű adatok nyomtatóra küldése után, az elkészült nyomatokért haladéktalanul el kell menni a nyomtatást kezdeményező felhasználónak.

b) Körültekintően kell eljárni a kinyomtatott dokumentumot a nyomtató lapgyűjtőjéből elvevő személyeknek is az alábbi alapszabályok betartásával:

ba) Kinyomtatott oldalak átforgatásával meg kell győződni, hogy a nyomat minden lapja a saját nyomtatásához tartozik; amennyiben nem, vissza kell helyezni a lapgyűjtőre az idegen oldalakat rendezett módon (oldalak „ összeütve ” a nyomtatás irányának megfelelően). Ha az idegen oldalak a későbbiek során kerülnek észlelésre, azokat haladéktalanul vissza kell vinni a nyomtatóhoz és a lapgyűjtőre kell helyezni rendezett módon.

bb) Amennyiben a lapgyűjtőn az aktuális munkát megakadályozó vagy zavaró „gazdátlan" nyomatok találhatók, úgy azokat ideiglenesen el kell onnan venni, majd az aktuális nyomtatás befejeztével rendezett módon ugyanoda vissza kell tenni.

bc) Nyomtatás után huzamosabb ideig (több mint fél óra) a lapgyűjtőben található dokumentumokat, amennyiben a nyomtatás tulajdonosa nem azonosítható - így értesítése lehetetlen - a nyomtatóhoz legközelebbi titkárságon le kell adni és a munkanap végén meg kell semmisíteni.

bd) A multifunkcionális nyomtatók fénymásoláshoz / szkenneléshez / faxoláshoz használható lapadagolójában, illetve tárgyüvegén található, ottfelejtett dokumentumokat amennyiben tulajdonosuk nem azonosítható be / le kell adni a nyomtatóhoz legközelebbi titkárságon. A dokumentum tulajdonosának azonosításához az elvégezett fénymásolási / szkennelési / faxolási munkák esetén, a hozzávetőleges

---

50 Megállapította: 2/2016. (I. 11.) NVSZ főigazgatói utasítás 5. pontja. Hatályos: 2016.01.12-től.

51 Beiktatta: 15/2014. (V. 13.) NVSZ főigazgatói utasítás 1. pontja. Hatályos: 2014.05.14-től.

52 Beiktatta: 15/2014. (V. 13.) NVSZ főigazgatói utasítás 16. pontja. Hatályos: 2014.05.14-től.

időpont megadásával, a napló állományok tárolási idejére tekintettel az IO munkatársai tudnak segítséget nyújtani.

be) Az NVSZ épületeiben elhelyezett nagyteljesítményű multifunkciós berendezések 12 óra időtartamra őrzik a rájuk küldött nyomtatási munkákat, melyek a 12 óra leteltével törlődnek.

26.[53] Az ellenőrzés rendje:

a) Az IBSZ-ben foglalt szabályok betartását rendszeresen ellenőrizni kell mind a felhasználói oldal, mind a hálózatmenedzsment és adminisztráció szempontjából.

b) A felhasználói oldal tekintetében különösen a mindennapi munkavégzés során betartandó alapvető magatartási szabályok tudatosítása szükséges, a magasabb informatikai és személyi biztonság elősegítése érdekében a közvetlen vezető által folyamatos jelleggel, illetve az Ellenőrzési Osztály által ad hoc módon ellenőrizni kell az IBSZ Alapelveiben (5. – 9. pontok), valamint a felhasználó feladatai (23. pont) között felsorolt szabályok maradéktalan betartását, kiemelt figyelmet fordítva a használatban nem lévő munkaállomások lezártságára és az NVSZ tulajdonú/engedélyezett USB eszközök használatának kizárólagosságára.

c) A hálózatmenedzsment és adminisztráció tekintetében kiemelt jelentőségű a jogosultságok naprakészségének ellenőrzése, különös tekintettel a személyzeti változások következtében felmerülő jogosultság visszavonások prioritására a GHI Tájékozató kiadását követő 15 nap elteltével az NVSZ rendszerbiztonsági felügyelője által az érintett szervezeti elemnél, illetve az Ellenőrzési Osztály által ad hoc jelleggel.

[54]Informatikai tudatosság és képzés

27) Biztonság-tudatossági képzés eljárásrendje

a) Az informatikai biztonság-tudatossági képzés célja elősegíteni, hogy a dolgozók felismerjék azokat a veszélyhelyzeteket, amelyek az NVSZ-nek károkat okozhatnak (pl. vírusok terjedése, adatvesztés, jogosulatlan szoftver/hardver használat).

b) A megelőzés érdekében a dolgozók az informatikai biztonság tudatosság követelményeit kötelesek ismerni és ezt a jártasságot legalább évente egyszer, illetőleg az információs rendszerek változásaihoz és egyéb igényekhez igazodva, vagy informatikai incidenst követően soron kívül megújítani.

c) A szervezetbe újonnan belépők az informatikai jogosultságok kiadását követő 1 hónapon belül kötelesek az informatikai biztonság tudatosság szabályait elsajátítani. A képzés önképzés útján valósul meg, amelyhez az IBF az NVSZ belső intranetes honlapján a „Tudatosság” pont alatt elérhető szakanyagokat biztosít, amelynek feltöltéséről az IO gondoskodik.

d) Az informatikai biztonság tudatosság szabályainak megismeréséről és azok maradéktalan betartásáról az NVSZ munkatársa egy nyilatkozatot köteles tenni (amelynek mintáját a 2.

---

[53] Megállapította: 2/2016. (I. 11.) NVSZ főigazgatói utasítás 6. pontja. Hatályos: 2016.01.12-től. (Az egységes szerkezetbe foglalt norma pontjainak folyamatos számozására tekintettel e pont számozása helyesen: 26.)

[54] A fejezetet beiktatta a 23/2017. (VII. 14.) NVSZ főigazgatói utasítás 6. pontja. Hatályos: 2017. 07. 15-től.

függelék tartalmazza). A nyilatkozat célja tudatosítani, hogy munkájuk során a lehető legnagyobb gondossággal járjanak el az elektronikus információs rendszerekben tárolt információk használatakor annak érdekében, hogy az adatok bizalmassága, sértetlensége és rendelkezésre állása a dolgozó szándékos, vagy gondatlan magatartásából ne sérüljön, illetve a felelősségük számon kérhető legyen. A nyilatkozat kitöltő közvetlen vezetője az általa ellenjegyzett nyilatkozat elektronikus példányát az IBF részére küldi meg, a papír alapú példányt a szervezeti elemnél kell tárolni.

Az elektronikus információs rendszerek nyilvántartása, rendszerelem leltár

28) Az NVSZ az elektronikus információs rendszereiről, valamennyi hardver- és szoftverelemről nyilvántartást vezet. A nyilvántartást az üzemeltető elektronikus formában vezeti, és rendszeres felülvizsgálatokkal gondoskodik, hogy a nyilvántartás mindig naprakész legyen, pontosan tükrözze az elektronikus információs rendszer aktuális állapotát.

29) A nyilvántartásnak minden rendszerre nézve tartalmaznia kell annak alapfeladatait, a rendszerek által biztosítandó szolgáltatásokat, az érintett rendszerekhez tartozó licenc számot (amennyiben azok az NVSZ kezelésében vannak), a rendszer felett felügyeletet gyakorló személy adatait, a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezeteknek a rendszer tekintetében illetékes kapcsolattartó személyeinek elérhetőségi adatait.

30) A különböző adatokat nem szükségszerűen egy nyilvántartásban kell tárolni, hanem logikus módon szétválaszthatóak. Minden rendszereszközt a beszerzéssel egyidejűleg fel kell venni a nyilvántartásba. A nyilvántartásból rendszereszközt kivenni csak annak selejtezésekor lehet.”