3

Császári Közös Önkormányzati
Hivatal

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

(INFORMATIKAI KATASZTRÓFAVÉDELMI TERV)

2013.

I. Bevezetés

(1) Az információvédelemben és az informatikai rendszer megbízható működésében beállt katasztrófák olyan események, amelyek bekövetkezése az informatikai rendszer valamilyen mértékű leértékelődéséhez, károsodásához vezet. A kár értéke arányos az információ, illetve az informatikai rendszer vagy annak a káresemény által érintett része funkcionális, eszmei vagy anyagi értékével.

(2) A kár jellege lehet:

a) dologi károk, amelyeknek közvetlen vagy közvetett költségvonzatuk van

- károsodás az infrastruktúrában (épület, vízellátás, áramellátás, klímaberendezés stb.),
- károsodás az informatikai rendszerben (hardver, hálózat sérülése stb.),
- a dologi károk bekövetkezése utáni helyreállítás költségei;

b) károk a politika és a társadalom területén:

- állam- vagy szolgálati titok megsértése,
- személyiséghez fűződő jogok megsértése, személyek vagy csoportok jó hírének károsodása,
- bizalmas adatok nyilvánosságra hozatala,
- hamis adatok nyilvánosságra hozatala,
- közérdekű adatok titokban tartása,
- bizalomvesztés hatóságokkal, felügyeleti szervekkel szemben;

c) gazdasági károk

- pénzügyi károk,
- lopás károk,
- az intézmény vagy cég arculatának (image) romlása,
- rossz üzleti döntések hiányos vagy hamis információk alapján;

d) károk az informatikai személyzet, illetve a felhasználók személyi biztonsága területén, pl.: személyek megsérülése, megrokkanása (pl. áramütés következtében);

e) károk a hatályos jogszabályok és utasítások megsértéséből adódóan;

(3) Információvédelem

- az azonosítás és a hitelesítés folyamatának kialakítása,
- a hozzáférés rendszerének felépítése — jogosultság kiosztás (alanyok-eszközök meghatározása, attribútumok rögzítése, hozzárendelések — megengedő, illetve tiltó módszer a szigorodó követelményekre),
- a hozzáférés-ellenőrzés rendszerének megvalósítása — jogosultság ellenőrzés,
- a hitelesség garantálása
- a sértetlenség garantálásának kiépítése,

- a bizonyítékok rendszerének és folyamatának kialakítása.

(4) Megbízható működés

- a hibaáthidalás folyamatának kialakítása,
- az újraindítási képesség megvalósítása,
- a rendszer funkcionalitásának biztosítása.

(5) Ha egy informatikai rendszer esetleges kiesése kritikus folyamatokat érint, a következmények súlyosak lehetnek, jelentős veszteséget okozhatnak, megakadályozhatják a kívánt szolgáltatási szintek megvalósítását, kínos helyzetbe hozhatják a Polgármesteri Hivatalt. Az ennek következményeképpen fellépő károk azután sokkal szélesebb körű hatásokat gyakorolhatnak az ügyfelekre, adófizetőkre, a lakosságra és általában a társadalomra.

II. Az informatikával, illetve telekommunikációval előfordulható zavarok és az elhárítás folyamata

(1) Áramellátás kimaradása:

a) az áramszolgáltatás kimaradásának a valószínűsége – az elmúlt időszak tapasztalatait figyelembe véve - nagyon kicsi. Az áramszolgáltatást biztosító E.-ON Észak-dunántúli Zrt. megfelelő színvonalon, jelentősebb üzemzavarok nélkül biztosítja a Közös Hivatal villamos energiaellátását. Üzemzavar és az ebből adódó áramkimaradás esetén a telekommunikációs hálózat teljes kapacitással maximum 1 órán át képes üzemelni.

b) amennyiben az üzemszünet időtartama a 3 órát meghaladja, a titkárságnak értesítenie kell a jegyzőt. Ez a rendszabály nem vonatkozik azokra az esetekre, amikor az áramszolgáltató az áramkimaradásról előzetesen értesíti a Közös Hivatalt.

c) az áramellátás hosszabb kimaradása esetén a telekommunikációs hálózat működését kölcsön aggregátorral kell megoldani. Az aggregátor által termelt villamos energia azonban nem teszi lehetővé a Közös Hivatal számítógépes rendszerének üzemkészségét, így ebben az esetben a számítógépek teljes kiesésére kell felkészülni. A szerver maximum 5 perc múlva leáll.

d) a titkárságot az áramszolgáltatás kimaradásának időtartamára áramellátástól független telefonnal kell ellátni, amely a feladata.

Feladat	Határidő
Kölcsön aggregátor beszerzése	Áram kimaradástól max 8 nap
Analógvonal biztosítása a titkárságon	Áram kimaradástól max 2 óra
Számítógép hálózat lekapcsolása	Áram kimaradástól max 10 perc

(2) Telefonvonalak leállása

a) a telefonközpont – bármely okból történő - teljes leállása esetén, sem a külső, sem a belső telefonkapcsolatot felépíteni nem lehetséges. Az ilyen jellegű üzemzavar azonban csak a hangszolgáltatás megszűnését eredményezi, hanem az adatkapcsolat is megszűnik a külvilággal. A telekommunikációban bekövetkezett rendkívüli eseményt, a normál üzem visszaállításig alternatív módon mobiltelefonokkal kell megoldani és folyamatosan biztosítani.

b) a Közös Hivatal telefonközpontjának típusa: ..... alközpont. A telefonhálózat hangátviteli részének maximum 24 órás kimaradása esetén a Közös Hivatal működését – különös tekintettel a meghatározó beosztásban lévő munkatársakra és a vezetőkre - mobiltelefonok használatával kell biztosítani.

c) a Közös Hivatal zavartalan működését az internet-szolgáltatás 4 órán keresztül történő leállásából következő üzemzavar, tekintettel arra, hogy adott munkanapon belül azokat a feladatokat, amelyekhez az internet igénybevétele szükséges, átütemezve el lehet látni.

Feladat	Határidő
Szolgáltató értesítése	max..30 perc
Analógvonal biztosítása a titkárságon	max..2 óra
Javítás megkezdése	max. 2 óra

(3) Vagyonvédelmi rendszer meghibásodása, leállása

a) a Közös Hivatal vagyonvédelme technikai eszközökkel biztosított. A rendszer folyamatos és megbízható működtetése folyamatos karbantartás mellett biztosítható, amelyre a rendszer üzemeltetőjével folyamatos karbantartási szerződést kell kötni.

b) a rendszer meghibásodására a téves – indokolatlan – riasztások utalhatnak. Amennyiben a meghibásodás mértéke jelentős, a vagyonvédelmi rendszer teljes leállása, ezáltal a védelem teljes megszűnése is bekövetkezhet.

Feladat	Határidő	Felelős
A szolgáltató értesítése	max. 10 perc.	észlelő
Javítás megkezdése	max. 24 óra	Szolgáltató
Őrzés megszervezése	max 2 óra	Jegyző.

(4) Adatok és programok kezelése és védelme

a) a Közös Hivatal számítógépes adat-feldolgozási folyamatába kerülő információkat és programokat fokozott biztonsági szabályok szerint kell kezelni. A számítógépeken titkosnak minősített adatokat nem tárolnak, illetve a feldolgozás során keletkező adatok sem minősülnek titkosnak. Ettől eltérő esetben a titkos ügykezelés szabályai szerint kell eljárni.

b) a Közös Hivatalban működő számítógépeken csak előzetesen ellenőrzött programot szabad futtatni. Az ellenőrzésnek ki kell terjednie a vásárolt vagy átvett program

tesztelésére, esetleges működést akadályozó hibák felderítésére. A feltárt hiányosságokról jegyzőkönyvet kell felvenni, melyet a programot szállító szervhez haladéktalanul el kell juttatni. Hibás programot üzembe helyezni tilos.

c) tilos vírusellenőrzés nélkül adathordozót a számítógéphez csatlakoztatni, arról programot vagy adatot a rendszerbe tölteni!

d) vásárolt, vagy átvett adathordozókon tárolt program esetén minden esetben biztonsági másolatot kell készíteni, majd az eredeti lemezt írásvédetté kell tenni.

e) A programok felhasználói dokumentációját a felhasználás helyén kell elhelyezni.

f) számítástechnikai feldolgozásra csak tartalmilag és formailag ellenőrzött adatok kerülhetnek. Lehetőség szerint biztosítani kell, hogy az adatok a keletkezés helyén kerüljenek rögzítésre.

g) Az adatállományok módosítását kizárólag csak a feldolgozásra készült programmal lehet elvégezni.

h) Az adatfeldolgozás során számítógép- vagy programhibából adódó adatvesztés fordulhat elő. Ilyenkor az adatrögzítést azonnal be kell fejezni és a további adatvesztés elkerülésére az informatikai felelőst haladéktalanul értesíteni kell.

(5) Az adatok mentés

a) a számítógépeken tárolt információk biztonságos megőrzése céljából az adatokat szükséges rendszerességgel legalább két egyező példányban menteni kell.

b) naponta szükséges menteni az iktatási adatállományokat floppy lemezre és a hálózati rendszerbe is.

c) hetente mentést kell végezni a hálózati működést biztosító központi gépen történt adatváltozásokról.

d) egyedi gépek vagy programok esetén a mentés gyakoriságát az adott adatfeldolgozási tevékenységet felügyelő illetékes vezető határozza meg.

e) az egyedi gépekről a mentést az egyedi gép használója, a Hivatal központi szervergépéről a mentést a kijelölt számítástechnikai munkatárs végzi el.

(6) Másolás

a) A számítógépes programok a szerzői jog szerint védelmet élveznek, ezért másolásuk, harmadik fél számára történő továbbadásuk tilos.

(7) Törlés

a) Mágneses adathordozókon tárolt adatok és programok törlését csak a tevékenységet felügyelő illetékes vezető írásbeli engedélye alapján lehet elvégezni. Külön figyelmet kell fordítani az irattározási és selejtezési szabályok betartására.

III. Számítógépek, eszközök és dokumentációk védelme

1. Számítógépek védelme

a) a számítógépek és eszközök rendeltetésszerű használatáért a személyi leltár szerint a használatra kijelölt köztisztviselő felelős,

b) meghibásodás megelőzéséről folyamatos karbantartással kell gondoskodni, üzemzavar esetén a javítást csak arra kiképzett szakember végezheti,

c) fizikai sérülések megelőzésére (pl.: hálózati vezetékszakadás) a számítógépet telepítési helyéről elmozdítani, vagy áthelyezni nem szabad,

d) vagyonvédelmi megfontolásból azokat a szobákat, ahol számítógép üzemel, biztonsági felszereléssel kell ellátni. A köztisztviselő köteles a munkaidő végzetével a számítógépet kikapcsolni, az azok elhelyezésére szolgáló irodahelységet bezárni és a kulcsot az időpont dokumentálásával elzárt helyen letenni. A Közös Hivatalból javításra, vagy más célból elszállítani eszközöket csak bizonylatolás után lehet.

e) elektromos érintésvédelmi szempontból a számítástechnikai eszközöket csak védőföldeléses, minden számítógéphez leltár szerint tartozó biztonsági kapcsolóval ellátott dugaszoló aljzatba lehet csatlakoztatni. Annak sérülését minden esetben jelezni kell. A berendezéseket vízzel oltani vagy tisztítani tilos!

f) a tűz elleni védekezés rendjét és elhárítása érdekében szükséges intézkedéseket a Közös Hivatal Tűzvédelmi Szabályzata tartalmazza.

2. Mágneses adathordozók védelme

a) a mágneses adathordozók védelmére és azonosítására az adathordozókat azonosítóval (címkével) kell ellátni és azokról nyilvántartást kell vezetni.

b) a mentést tartalmazó adathordozók megőrzési idejét úgy kell meghatározni, hogy azokról az aktuális adatállomány sérülés esetén visszaállítható legyen.

c) vírust tartalmazó, nem mentesíthető adathordozót használatban tartani nem lehet.

d) az adathordozót óvni kell a szennyeződésektől és a fizikai sérüléstől, ezért használat közben óvakodni kell a mágnesezhető réteg megérintésétől, használat után pedig zárható dobozban, vagy a gyári csomagolásban elektromos erőterektől távol (monitor, televízió, hangszóró, ventilátor, telefon, rádió, stb.) kell tartani.

e) külső szervnek átadott adathordozókról bizonylatot (az átadás, átvétel időpontját, az átadás célját, az átadott adathordozó számát, tartalmát az átvevő szerv megnevezését és címét, az átadás idejét, (ideiglenesen vagy véglegesen) az átvevő szerv őrzéssel megbízott felelősének megnevezését, valamint az átadó és átvevő szerv erre feljogosított képviselőjének aláírását tartalmazó jegyzéket) kell készíteni.

IV. ZÁRÓ RENDELKEZÉS

(1) Ez a szabályzat a kiadásával egyidőben lép hatályba.

Császár, 2013. ...április 05....

.....

Dr. Pölös Géza
jegyző

CSÁSZÁRI KÖZÖS ÖNKORMÁNYZATI HIVATAL * JEGYZŐJE *