Iktatószám: 220-42/2020

INFORMATIKAI
KATASZTRÓFA-ELHÁRÍTÁSI TERV

Hatályos: 2020. janár 1-jétől

Jóváhagyta:

Zsigmond Anikó
jegyző

Bokod Község jegyzője

INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV

Bokodi Polgármesteri Hivatalának (a továbbiakban: Hivatal) Informatikai katasztrófa-elhárítási tervét (a továbbiakban: Szabályzat)

- az információs önrendelkezési jogról és az információszabadságról szóló a 2011. évi CXII. törvény, valamint
- a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény

előírásai alapján a következők szerint határozom meg.

1. A Szabályzat célja

Napjainkban egyre nagyobb jelentőséggel bír a számítástechnikai eszközök használatából, ezek szolgáltatásaiból, valamint az általuk létrehozott adatoktól, dokumentumoktól stb. való függőség. Egyre fontosabb, hogy ezek a szolgáltatások, információk, mindig egy előre meghatározott minőségben álljanak rendelkezésre. Abban az esetben, ha ezeknek a szolgáltatásoknak a minősége csökken, a felhasználók nem tudják elvégezni mindennapi munkájukat, a szervezet hatékonysága csökken. Alapvetően fontos, hogy az információtechnológiai szolgáltatásokban bekövetkező kieséseket minimalizáljuk - mivel rendszerkiesések a tapasztalatok szerint előfordulnak -, valamint minél hamarabb helyre tudjuk állítani az eredeti szolgáltatások színvonalát.
Ehhez nyújt segítséget a katasztrófa-elhárítási terv.

2. Veszélyforrások, prioritások, megelőzés

2.1. Legáltalánosabb veszélyforrások

Hardverhiba: A számítógép részegységeinek meghibásodás, ezen belül kiemelt veszélyességgel a merevlemez fizikai károsodása.

Szoftverhiba: Felhasználói programok, alkalmazások hibái, az operációs rendszer összeomlása, rosszindulatú számítógépes vírusok, egyéb kódok által okozott károk.

Természeti katasztrófák: A számítógép elemeiben (és a rajta tárolt adatokban) a természeti csapások - tűz, víz, áramkimaradás - által okozott károk.

Emberi hiba: Nem megfelelő számítástechnikai ismeretek hiánya, figyelmetlenség, biztonsági szabályok be nem tartásából következő károk.

2.2. Veszélyforrások bekövetkezésének valószínűsége

A felsorolt veszélyforrások közül - az eddigi tapasztalatokat is figyelembe véve - első helyre a kliens oldali számítógépek operációs rendszerének megsérülése helyezendő. Második helyre tehető a hardver eszközök meghibásodása, mivel ezek az eszközök mozgó, kopó alkatrészeket tartalmaznak. Ennek függvényében a veszélyforrások bekövetkezésének a valószínűsége az alábbi:

- Szoftverhiba: ezen belül is az operációs rendszer megsérülése.
- Hardverhiba.
- Vírusok, egyéb kártékony kódok által okozott károk.
- Emberi hiba.
- Célalkalmazások hibái.
- Természeti katasztrófák.

3. Veszélyeztetett eszközök

3.1. Hálózati infrastruktúra

A Hivatalban kialakított számítástechnikai hálózat. A hivatal hálózati kiépítettsége 100%, a telepítésre kerülő számítógépek mindegyike alkalmas e hálózatra való kapcsolódásra, valamint a központi szerveren futó alkalmazások elérésére.

3.2. Szerver
A Hivatal informatikai infrastruktúrájából adódóan a legveszélyeztetettebb eszköz a szerver, valamint az azokon futó szoftverek, és ezek adatállományai. Az IT struktúra tervezése és megvalósítása során törekedtünk arra, hogy a felhasználók központi szerveren futó alkalmazásokat használjanak, valamint a kliens oldali szoftverek - célalkalmazások, irodai programcsomagok stb. - által létrehozott dokumentumokat, adatokat a központi szerveren számukra biztosított tárhelyen helyezzék el.

3.3. Kliens oldali számítógépek
A hivatalban elhelyezet számítógépek (munkaállomások).

3.4. Szoftverek
Szoftveren belül értjük a dobozos gyári szoftvereket (operációs rendszer, irodai programcsomag), valamint a célalkalmazásokat (iktatás, adóügy stb.).

4. Prioritások meghatározása

A prioritás-meghatározás esetén két lehetséges módszert alkalmazhatunk.
Az első esetben azt kell megvizsgálnunk, hogy a katasztrófa vagy meghibásodás esetén mely eszközök, állományok pótolhatóak a legkevésbé. Ennek függvényében a veszélyeztetett eszközök közül legmagasabb prioritással a nehezen pótolható hardver eszközöket és célszoftver adatállományokat értjük. Ezek az alábbiak:

- Célalkalmazások adatállományai.
- Szerver.
- Felhasználói célalkalmazások.
- Egyedi készítésű dokumentumok (Word, Excel stb.).
- Hálózati infrastruktúra.
- Kliens oldali számítógépek (munkaállomások).

A felsorolás egyben prioritást is jelent a védelem szempontjából, így esetleges katasztrófa vagy veszély kialakulása esetén a fentiekben felsorolt ütemben kell a mentéseket és/vagy a helyreállításokat elvégezni.
Második esetben a kritikusságot időbeni prioritás alapján osztályozhatjuk. Ennek alapján a prioritási sorrend az alábbiakban alakul:

- Szerver.
- Felhasználói célalkalmazások.
- Célalkalmazások adatállományai.
- Hálózati infrastruktúra.
- Kliens oldali számítógépek (munkaállomások).
- Egyedi készítésű dokumentumok (Word, Excel stb.).

Egyes esetekben az alkalmazások képesek arra, hogy nem csak hálózatos környezetben, hanem egyedi gépes környezetben is fussanak. Ezekben az esetekben biztosítani kell a lehetőség arra, hogy az üzemzavar elhárítása alatt legalább információs célzattal ezek az alkalmazások működjenek.

5. Katasztrófa-megelőzési eljárások, módszerek

5.1. Mentés
A katasztrófa és veszélyhelyzetek kiküszöbölése, valamint a helyreállítás szempontjából a legalapvetőbb védelmi forma, az alkalmazások, alkalmazások adatállományainak, valamint maguknak a számítógépek operációs rendszerének a mentése.
A Hivatalban az alábbi mentési rendet kell alkalmazni:
A szerver esetében folyamatosan tükrözéssel tárolódnak az adatok. Ezen felül (lehetőség szerint automatizáltan) mindennap mentést kell elvégezni az erre a célra kijelölt háttértárolóra az alkalmazások adatállományairól, illetve a szerver operációs rendszeréről is.

A kliens oldali számítógépeken futó alkalmazások, illetve a helyileg létrehozott dokumentumok mentésére biztosítani kell a felhasználónak számára a szerveren tárhelyet, igény esetén automatizálni kell a napi mentését.

5.2. Jogosultságok
Az alkalmazások hozzáféréseit a rendszergazdai feladatokat ellátó informatikus szigorú jogosultsági rendszeren keresztül a Jegyző javaslata alapján határozza meg, illetve osztja ki.

5.3. Tűzjelző és tűzoltó eljárás
Olyan tűzvédelmi eszközt kell tárolni, igény esetén alkalmazni, mely használata esetén nem okoz kárt (zárlat) a számítástechnikai eszközökben.

5.4. Áramkimaradás elleni védelem
A Hivatal számítástechnikai eszközeit lehetőség szerint szünetmentes áramforrással kell ellátni úgy, hogy áramkimaradás esetén igény esetén a szerverek távolról is könnyen leállíthatóak legyenek.

5.5. Adat- és szoftvervédelmi eljárások
Adat- és szoftvervédelmi eljárások közé soroljuk azokat az alkalmazásokat is, melyek segítségével biztosítjuk a kliens és szerver oldali vírus és egyéb kártékony kódok elleni védelmet. Ezen eljárások során minden esetben a kliens, a szerver valamint az Internet kapcsolaton folyamatos vírus- és betörésvédelem alkalmazandó. Az internet kijárón tűzfalvédelem, a belső számítástechnikai infrastruktúrában pedig kliens oldali vírusvédelem van aktiválva. Emellett egyéb ingyenes eszközökkel további spyware, adware, trojanware stb. védelmet kell igény szerint aktiválni.
A kliens oldali operációs rendszereken minden esetben biztosítani kell a rendszergazda, illetve az informatikai karbantartást végző(k) számára a rendszergazdai jogosultságot, hogy igény esetén védelem és az esetleges károk elhárítása során az eszközhöz hozzáférjen.

5.6. Tartalmi és személyi feltételek
A katasztrófa-elhárítási terv szempontjából létfontosságú, hogy annak tartalmát a végrehajtásban résztvevők ismerjék, a terv tartalmazza a közvetlen számítástechnikai feladatot ellátó személyek elérhetőségét, valamint maga a terv folyamatosan elérhető legyen a hivatal dolgozói számára. Ennek függvényében a katasztrófa-elhárítási tervnek:

- Folyamatosan elérhetőnek kell lennie a belső informatikai hálózaton.
- Egy példányát, mellékelve az informatikai feladatot ellátó munkatársak elérhetőségével a telefonközpont-kezelőnél kell elhelyezni
- Tartalmát negyedévente a Jegyzőnek felül kell vizsgálni, és amennyiben szükséges, módosítani kell.
- A tervben szereplő eszközöket (mentésre kijelölt számítógépek stb.) havonta rendszeresen felül kell vizsgálni, meghibásodás esetén a javíttatásáról, vagy cseréjéről haladéktalanul és soron kívül gondoskodni kell.

5.7. Egyéb szerződések
A megelőzés szempontjából lényeges, hogy az eszközök karbantartása, meghibásodás esetén a cseréje folyamatosan megoldott legyen. Ennek érdekében a hivatalnak folyamatos szerződéssel kell rendelkezni karbantartásra és átalánydíjas javításra, illetve a hálózati infrastruktúra felügyeletére.

5.8. Oktatás, képzés
Az emberi hiba kiküszöbölése szempontjából a megelőzés, a dolgozók oktatása, képzése az elsődleges. A tudatos emberi visszaélések megelőzése érdekében a rendszergazdának, valamint a számítástechnikai karbantartást végző személyeknek folyamatosan ellenőrizni kell a jogosultsági rendszereket.

6. Katasztrófa esetén követendő eljárások

6.1. Adminisztráció
a) Terv módosítása

- A katasztrófa-elhárítási terv utolsó módosítója: Zsigmond Anikó jegyző.
- Dátum: 2013. március 1.

b) Eseménynapló
Eseménynaplót kell vezetni minden, a katasztrófa elhárítási tervet érintő történésről. Az eseménynaplónak tartalmaznia kell, hogy mikor mi történt, és azt milyen intézkedés követte. Az eseménynapló tartalmi formáját az 1. számú melléklet tartalmazza.

c) A katasztrófa-elhárításában résztvevők és értesítendők listája:
- Zsigmond Anikó jegyző: 06-20/448-06-99
- informatikai rendszergazda: Cybernet Kft. – Helgert József
- Polgári védelmi erők igénybevétele esetén: -

6.2. Életbeléptetés
A katasztrófa-elhárítási tervet minden olyan esetben életbe kell léptetni, amikor olyan veszélyforrás van kialakulóban, vagy alakult ki, amely a számítástechnikai infrastruktúrát, annak használatát, az azon tárolt állományokat, adatokat, vagy az azokkal való munkavégzést akadályozza meg, valamint maradandó adatvesztés, vagy anyagi kár keletkezhet. Az életbeléptetés a katasztrófa elhárításában résztvevők valamelyikének értesítésével léptethető életbe.

6.3. A terv egy példánya megtalálható:
- Belső informatikai hálózat (Intranet);
- Titkárság;
- Irattár.

6.4. Informatikai infrastruktúra
A polgármesteri hivatal nem rendelkezik tartalék szerverrel, így veszély esetén a szerver áttelepítése az elsődleges. A szervert veszély esetén a hivatal más, nem veszélyeztetett helyiségébe kell áthelyezni. A használatukhoz szükséges hálózati eszközök beszerzéséről haladéktalanul és soron kívül kell intézkedni.

6.5. A Hivatal épületét fenyegető katasztrófa és veszély fellépése esetén a követendő eljárás az alábbi:
- Szerveren a bejelentkezés letiltása.
- A bejelentkezett felhasználók kiléptetése a rendszerből.
- Szerver leállítása.
- Szerver áttelepítése (lehetőség szerint) a hivatal más helyiségeibe.
- Amennyiben szükséges (és lehetséges), a szerver hálózatra kapcsolása és beindítása.
- Az adatállományok integritásának ellenőrzése.

A helyreállítás során minimális erőforrásszintet kell elérni, mely az alábbiakat jelenti:
- Szerver működőképes.
- A szerveren tárolt szoftverek és adatállományok elérhetők.
- Ezek sérülésmentesek.
- Szükség esetén elvégezhető a mentés.
- A szerver szükség esetén hálózatba kapcsolható.

Az ideiglenes helyen üzemelő szerverek esetében fokozottabban kell figyelemmel kísérni a folyamatokat, a mentések számát gyakoribbá kell tenni.

6.6. Biztonság
Áramkimaradás esetén azonnal értesíteni kell a Jegyzőt vagy a gondnoki feladatokkal megbízott munkatársat. Amennyiben az áramszünet 15 percnél tovább tart, meg kell kezdeni a szerver lekapcsolását. Követendő eljárás:
- Szerveren a bejelentkezés letiltása.
- A bejelentkezett felhasználók kiléptetése a rendszerből.
- Amennyiben az áramszünet ideje eléri a 15 percet, a szerver leállítása.

6.7. Tűzriadó
Tűzriadó esetén a szervert, valamint a munkaállomásokat a hivatal valamelyik nem veszélyeztetett irodahelyiségébe vagy a hivatal épületén kívülre kell menekíteni.

Amennyiben erre nincs mód, a Jegyző vagy a rendszergazda által tárolt, mentéseket tartalmazó adathordozókat (CD és DVD lemezeket) kell lehetőség szerint a hivatal munkatársainak magukhoz venni, és biztonságos helyre menekíteni.

6.8. Bombariadó

Bombariadó esetén a kijelölt menekülési útvonalak mentén kell elhagyni az épületet, úgy, hogy a mentéseket tartalmazó adathordozókat (CD, DVD lemezeket) a Jegyzőnek (távolléte esetén a helyettesítőjének) magához kell venni, és biztonságos helyre menekíteni.

6.9. Értesítendő szervezetek

Veszély és katasztrófa esetén értelemszerűen az alábbi szervezeteket kell értesíteni:

- **Mentők: 104**
- **Rendőrség: 107**
- **Tűzoltóság: 105**
- **Segélyhívó: 112**

valamint a Jegyzőt (06-20/448-06-99). Egyéb szervezetek (gázművek, villamos művek, vízművek stb.) értesítéséről a Jegyző, illetve a gondnoki feladatok ellátásával megbízott munkatárs gondoskodik.

6.10. Tartalék telephely:

- a 2855 Bokod, Dadi u. 3/a.

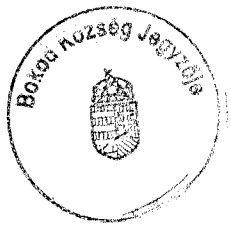
7. Záró rendelkezések

7.1. A Szabályzat 2020. január 1. napján lép hatályba.

7.2. A Szabályzat rendelkezéseit minden érintettel meg kell ismertetni.

7.3. A 2013. március 01. napjától hatályos informatikai katasztrófa-elhárítási terv 2019. december 31. napján hatályát veszti.

Bokod, 2020. február 26.



Zsigmond Anikó
jegyző

1. sz. melléklet

Eseménynapló

Esemény	Dátum	Intézkedés	Aláírás

Megismerési nyilatkozat

A Bokodi Polgármesteri Hivatal 2020. január 1-jétől hatályos Informatikai katasztrófa-elhárítási tervét megismertem. Tudomásul veszem, hogy az abban leírtakat a munkám során köteles vagyok betartani.

Név	Beosztás	Dátum	Aláírás
Tóthné Szám Tünde Katalin	általános igazgatási főmunkatárs	2020 FEBR 27.	
Gerencsér Judit	adóügyi főmunkatárs	2020 FEBR 27.	
Baloghné Vajay Adrienn	pénzügyi főelőadó	2020 FEBR 27.	
Kolumbán Magdolna	gazdálkodási főelőadó	2020 FEBR 27.	
Lázár Erika	általános igazgatási előadó	2020 FEBR 27.	
Baumann Péter	pályázati pénzügyi előadó	2020 FEBR 27.	