Székesfehérvári Városfejlesztési Közhasznú Nonprofit Kft.

Katasztrófa Elhárítási Terv

Informatikai biztonsági incidensek kezelése

Hatályos: 2018. május 25-től visszavonásig

TARTALOM

1 ÁLTALÁNOS RENDELKEZÉSEK

1.1 A SZABÁLYZAT CÉLJA ÉS TERÜLETI ÉRVÉNYESSÉGE

A biztonságot érintő események negatív hatásai jelentősen csökkenthetők, ha sikerül az incidensekről időben tudomást szerezni és a szervezet képes hatékony intézkedéseket hozni a problémák elhárítására, illetve a további károk megelőzésére. Az informatikai működés folytonosságának helyreállítása leggyorsabban akkor lehetséges, ha erre tervezett módon felkészülünk, az érintett munkatársak tudják feladataikat és a helyreállításhoz szükséges eszközök és tervek rendelkezésre állnak. Az informatikai üzemzavarok legsúlyosabb formáját informatikai katasztrófahelyzetnek nevezzük.

A Katasztrófa Elhárítási Terv (a továbbiakban: KET) célja, hogy pontosan megfogalmazza a cég adatainak megőrzésével kapcsolatos elveket, feladatokat és meghatározza az ebből eredő felelősségi köröket és kötelességeket.

1.2 A SZABÁLYZAT ALKALMAZÁSI TERÜLETE

A KET hatálya kiterjed a **Székesfehérvári Városfejlesztési Közhasznú Nonprofit Kft.**-vel (a továbbiakban, mint Városfejlesztési Kft.) munkaviszonyban és munkaviszonyra irányuló egyéb jogviszonyban álló dolgozók, szervezeti egységek, illetve szervezetek közül mindazokra, akik a Városfejlesztési Kft. informatikai rendszerével és/vagy adataival valamilyen módon kapcsolatba kerülnek.

1.3 AZ INFORMATIKAI SZOLGÁLTATÓ

A Városfejlesztési Kft. részére az informatikai szolgáltatásokat az Önkormányzati Informatikai Központ (ÖIK) nyújtja. Az együttműködés feltételeit Szolgáltatási szerződésben kerültek rögzítésre. A dokumentumban alkalmazott „*Informatika*” hivatkozás minden esetben az ÖIK által nyújtott szolgáltatásokra vonatkozik.

1.4 DEFINÍCIÓK

A szabályzatban alkalmazott fogalmak magyarázatát az alábbiakban adjuk meg.

a) *alternatív megoldás*: a zavar áthidalását célzó (egyik) lehetőség;

b) *biztonsági esemény:* nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

c) *egyszerű informatikai incidens*: egyedi, kis jelentőségű meghibásodások. Az informatikai rendszer működése lényegében folyamatos. Tipikus esetek: elfelejtett jelszó, felhasználói gép meghibásodása.

d) *elsődleges informatikai szolgáltatások*: azok az informatikai szolgáltatások, amelyekkel az szakmai felhasználók közvetlenül találkoznak.

e) *incidens, esem*ény: egymás szinonimájaként használt kifejezések, amely alatt az információbiztonság (bizalmasság, sértetlenség és rendelkezésre állás) sérülését értjük. Általánosan használt kifejezések, amelyek a legkisebb jelentőségű eseménytől (pl. jelszó elfelejtése) a katasztrófa helyzetig terjed.

f) *informatikai katasztrófa:* informatikai katasztrófák esetén az informatikai szolgáltatások jelentős része nem elérhető. Helyreállítás nem lehetséges a sebezhetőségi ablakon belül. Tipikus esetek: tűz, természeti katasztrófa, rendszer elleni vírus vagy hacker támadás.

g) *informatikai üzemzavar*: egy-két szerver vagy hálózati aktív eszköz meghibásodása. Az informatikai szolgáltatások egy része nem elérhető.

h) *káresemény*: a káresemény az információbiztonság (bizalmasság, sértetlenség és rendelkezésre állás) sérülése. Az esemény, incidens kifejezések szinonimája azokban az esetekben, amikor az esemény valóban információbiztonsági kárral jár.

i) *Katasztrófa Helyreállítási Team:* több működési terület szakmai képviselőiből, továbbá informatikai támogató szervezetekből álló munkacsoport, amely a fellépő katasztrófa helyzetek megoldásban döntési jogkörrel rendelkezik;

j) *katasztrófa*: A szakmai folyamatok, és/vagy az azokat kiszolgáló háttérrendszerek folyamatos és zavarmentes működését veszélyeztető, átmenetileg, vagy végleg lehetetlenné tevő rendkívüli esemény. Katasztrófaforrások lehetnek pl.: informatikai rendszerelemek hibái, egyéb kiszolgáló infrastruktúra hibái és/vagy hiányosságai, természeti katasztrófák és egyéb külső tényezők, külső, vagy belső rosszakaratú károkozás, belső nem rosszakaratú károkozás, stb.;

k) *sebezhetőségi ablak:* A sebezhetőségi ablak az a maximális időtartam, ameddig az szervezet feladatainak ellátása lényegében fenntartható egyes informatikai erőforrások kiesése esetén. A sebezhetőségi ablak időtartamánál nem hosszabb szolgáltatás kiesés legfeljebb alacsony szakmai hatást (veszteséget) okozhat.

2 BEVEZETÉS

2.1 INFORMATIKAI BIZTONSÁGI INCIDENSEK JELENTÉSE

Az adatok és információ feldolgozó eszközök biztonságát érintő eseményeket, és az informatikai rendszer működésének zavarait haladéktalanul jelenteni kell:

- az informatikának és a
- a közvetlen munkahelyi vezetőnek.

2.2 INFORMATIKAI BIZTONSÁGI INCIDENSEK BESOROLÁSA

Az informatikai biztonsági incidenseket a következő kategóriákba soroljuk természetük szerint

- bizalmassági (biztonsági sértés)
- rendelkezésre állási incidens

2.2.1 Incidensek

A rendelkezésre állási incidensek súlyosságuk szerint:

- Meghibásodás

- Üzemzavar
- Informatikai vészhelyzet (katasztrófa helyzet)

2.2.2 Biztonsági sértés

Biztonsági sértésről akkor beszélünk, amikor bizalmas adatok illetéktelen tudomására jutnak, vagy ennek a gyanúja felmerül, illetve amikor a Városfejlesztési Kft. adatainak megszerzésére vagy az informatikai rendszer megkárosítására irányuló cselekményt észlelünk.

Biztonsági sértés lehet például:

- Az informatikai eszközök elvesztése
- A fizikai vagy logikai hozzáférések megsértése
- A biztonsági szabályzatok vagy utasítások megszegése

Biztonsági sértések az esemény észlelője köteles azonnal jelenteni azt munkahelyi vezetőjének. Az ellenintézkedések megtétele és az esemény kivizsgálása az ügyvezető igazgató felelőssége, melynek során a tevékenységbe bevonja az informatikai szolgáltatót is.

Az esemény súlyossága indokolhatja külső szervezetek, hatóságok bevonását a vizsgálatba. Külső felek bevonása csak az ügyvezető igazgató engedélyével történhet.

2.3 MEGHIBÁSODÁS ÉS ÜZEMZAVAR

Meghibásodásnak tekintünk minden olyan felhasználói számítógépet érintő hibát vagy a hálózati eszközök, illetve szerver rövid idejű leállását, amely nem zavarja számottevően a normális munkavégzést és a napi üzemeltetési feladatok sorában gyorsan kijavítható.

A meghibásodások elhárítása az Informatika feladata.

A meghibásodásról az elhárítás közben kiderülhet, hogy komolyabb problémáról van szó, azaz a meghibásodások nagyobb számú felhasználót érintenek, több eszköz súlyosan meghibásodott, illetve nyilvánvalóvá válik, hogy a normál működési állapot nem állítható vissza az üzemeltetési eljárásokban meghatározott időtartamon belül. Ebben az esetben üzemzavarral állunk szemben.

2.4 INFORMATIKAI VÉSZHELYZET – INFORMATIKAI KATASZTRÓFA HELYZET

Informatikai vészhelyzetről akkor beszélünk, ha az informatikai üzemzavart nem sikerült az elvárt visszaállítási időn belül megszüntetni vagy nyilvánvalóan katasztrófa helyzet alakult ki (tűz, robbanás stb.). Informatikai vészhelyzet esetén értesíteni kell az ügyvezetőt.

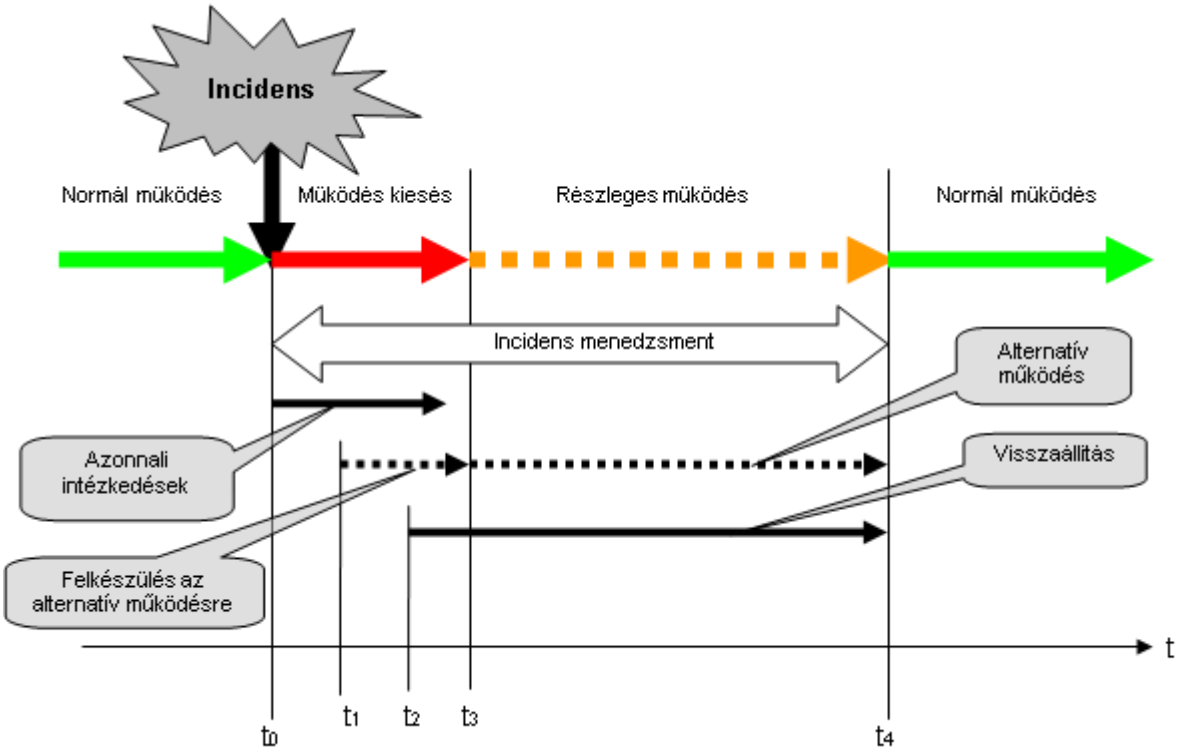
Informatikai katasztrófa szakmai folyamatok, és/vagy az azokat kiszolgáló háttérrendszerek folyamatos és zavarmentes működését veszélyeztető, átmenetileg, vagy végleg lehetetlenné tevő rendkívüli esemény. Katasztrófaforrások lehetnek pl.: informatikai rendszerelemek hibái, egyéb kiszolgáló infrastruktúra hibái és/vagy hiányosságai, természeti katasztrófák és egyéb külső tényezők, külső, vagy belső rosszakaratú károkozás (vírus vagy hackertámadás) , belső nem rosszakaratú károkozás, stb..

3 INFORMATIKAI BIZTONSÁGI INCIDENSEK KEZELÉSE

3.1 AZ INCIDENSTŐL A NORMÁL MŰKÖDÉSRE VALÓ VISSZAÁLLÁSIG

Az incidens (a káresemény) bekövetkeztével egyes informatikai szolgáltatások nem elérhetőek. Az incidens bekövetkeztétől biztosítani kell az események folyamatos kézben tartását, menedzselését. Az azonnali tevékenységek keretében elsősorban kárelhárító, kárfelmérő tevékenységet kell végezni. Amennyiben az adott szolgáltatás kiesésekhez létezik alternatív működési eljárás, ezek elindításáról az ÖIK informatikai vezető dönt. Hasonlóképpen Ő dönt a visszaállítási tervek elindításáról, amikor a helyzet ezt lehetővé teszi. A folyamat a normál működésre való visszaállással ér véget.

A folyamatot a következő ábra szemlélteti:



Amennyiben nem létezik helyettesítő (alternatív) szolgáltatás a t1és a t3 időpontok nem értelmezhetők.

A visszaállítási eljárás kezdete lehet t1 előtt vagy t3 után is, attól függően, hogy a körülmények és az erőforrások rendelkezésre állása hogyan alakul. A tervek lehívása, elindítása az Informatika feladata és felelőssége.

3.2 INCIDENS MENEDZSMENT

Incidens menedzsment az a tevékenység, amely az incidens kezdetétől a normál állapotba történő visszaállásig irányítja a teendőket. Az informatikai incidens menedzsment tevékenységet az Informatika látja el.

1. **FÁZIS**

Az incidenseket az Informatikának jelentik be a felhasználók. Az incidens menedzsment ettől a pillanattól kezdődik és ennek megfelelően az incidens menedzser az informatikus (rendszergazda), aki a bejelentést fogadja.

Az incidens menedzser (a rendszergazda) értékeli a helyzetet és eldönti:

1) képes-e saját hatáskörben megoldani a problémát vagy
2) nem képes saját hatáskörben megoldani a problémát.

Az első esetben az incidens besorolása: meghibásodás

A második esetben az incidens besorolása: üzemzavar, és ekkor a rendszergazda értesíti az ÖIK informatikai vezetőt, távollétében a kijelölt helyettesét. Ettől kezdve az informatikai vezető az incidens menedzser, aki egy személyben látja el ezt a feladatot.

2. FÁZIS

Az incidens menedzser (az informatikai vezető) értékeli a helyzetet és eldönti:

1) képes-e a Informatika megoldani a problémát az elvárt idő alatt vagy
2) az Informatikán kívül további erőforrások bevonása szükséges.

Az első esetben az incidens besorolása: üzemzavar. Üzemzavar esetén az informatikai vezető irányításával a következő lépések történnek:

- Azonnali intézkedések
- Visszaállítási tervek lehívása

Az második esetben az incidens besorolása: informatikai vészhelyzet és ekkor a informatikai vezető értesíti az ügyvezetőt és javasolja a Katasztrófa Helyreállítási Team összehívását. Az ügyvezető igazgató összehívja a Katasztrófa Helyreállítási Team. Ettől kezdve az ügyvezető igazgató az incidens menedzser, aki a Katasztrófa Helyreállítási Team élén látja el ezt a feladatot.

3. FÁZIS

A Katasztrófa Helyreállítási Team felépítése:

A team vezetője:

- az ügyvezető

A team tagjai:

- az ügyvezető által az elhárításhoz kijelölt vezetők
- az informatikai vezető

A team feladata, hogy operatív döntéseket hozzon és irányítsa a vészhelyzeti állapot megszüntetését biztosító tevékenységeket.

A BIZOTTSÁG FELADATA A VÉSZHELYZETI ÁLLAPOT FENNÁLLÁSA ALATT:

1) Az informatikai helyreállítási feladatok közvetlen és folyamatos irányítása, a helyreállításhoz szükséges további erőforrások biztosítása

2) A vállalati területek egyedi vészhelyzeti feladatainak meghatározása

3) A partnerek tájékoztatása a szükséges és kívánatos módon

4) Külső szervek, hatóságok bevonása, ha szükséges

4.3 Azonnali intézkedések

Azonnali intézkedések alatt értjük azokat az eljárásokat és tevékenységeket, amelyeket az informatikai üzemzavar (vagy vészhelyzeti állapot) bekövetkeztének pillanatától (t0 időponttól) kell végezni, annak érdekében, hogy a Városfejlesztési Kft. hatékonyan és érdemben tudjon reagálni az eseményekre. Ezek a következők:

- azonnali kárelhárítás,
- tevékenységek, szolgáltatások leállítása,
- bizonyítékok gyűjtése és megvédése,
- értesítések.

Az azonnali intézkedések megtételéért az incidens menedzser a felelős.

3.2.1 Azonnali kárelhárítás

Magába foglal minden olyan tevékenységet, ami az incidens továbbterjedését, súlyosabbá válását megakadályozhatja. Például: emberek kimenekítése, tűzoltás, vízbefolyás megszüntetése, illetéktelenek eltávolítása stb.

TEVÉKENYSÉGEK, SZOLGÁLTATÁSOK LEÁLLÍTÁSA

Szükség esetén ki kell kapcsolni az áramszolgáltatást, a gázellátást (robbanásveszély), számítógépeket, vagy informatikai szolgáltatásokat kell lekapcsolni (pl. veszélyes vírustámadás, vagy behatolás)

Bizonyítékok gyűjtése és megvédése

Az incidenseket okozhatja szándékos cselekmény (bűntény), ezért a bizonyítékok megvédésére és összegyűjtésére tekintettel kell lenni.

ÉRTESÍTÉSEK

Az érdekelt feleket értesíteni kell az incidensről, az alábbi sorrendben.

1. Külső, katasztrófa elhárítással foglalkozó szervezetek: mentők, tűzoltók, rendőrség, katasztrófa védelem (ha szükséges)

2. az incidens elhárításában résztvevők

3. az érintett felhasználók

4. vállalati vezetők

5. média (ha szükséges) – a média bevonásához az ügyvezető igazgató engedélye szükséges.

Az értesítéseket az adminisztrációs szekció végzi az incidens menedzser utasításai alapján.

3.3 VISSZAÁLLÍTÁSI TERVEK LEHÍVÁSA

A visszaállítási tervek célja az üzemzavarok elhárítása, az elvárt időn belül (sebezhetőségi ablak), vagy a lehető legrövidebb időn belül. A visszaállási terv része lehet a tartalék erőforrások biztosítása, továbbá az alternatív működési eljárások elrendelése.

3.3.1 Alternatív működési eljárás

Súlyosabb, várhatóan hosszabb ideig tartó szolgáltatás kiesés esetén az informatikának meg kell vizsgálnia, hogy a normál működés visszaállításáig valamilyen helyettesítő (alternatív) szolgáltatást nyújtható-e a felhasználóknak. Az alternatív működés általában alacsonyabb szolgáltatási szintet jelent, mint a normál működés, de lehetővé teszi a Vállalati folyamatok bizonyos szintű működtetését. Kisebb szolgáltatás kiesések esetében is érdemes helyettesítő folyamatot alkalmazni, ha az viszonylag egyszerű, kézenfekvő. Meg kell fontolni, hogy az alternatív működés költsége arányban áll-e az általa biztosított előnnyel.

3.3.2 Tartalék erőforrások biztosítása

A működésfolytonossági tevékenység kapcsán szükséges azokat a tartalék erőforrásokat meghatározni és rendelkezésen tartani, amelyek képesek pótolni az incidensek következtében megsérült vagy nem elérhető erőforrásokat.

3.4 AZ INCIDENSKEZELÉSI TEVÉKENYSÉG DOKUMENTÁLÁSA ÉS ELEMZÉSE

Az információbiztonsági eseményekről (bizalmassági, meghibásodás, üzemzavar, vészhelyzet) feljegyzést készítaz Ö.I.K. Kft üzemeltetési felelőse.

A feljegyzés tartalmazza a következőket: a bejelentő (neve, üzleti terület), a bejelentés időpontja, az esemény rövid leírása, az elhárítási intézkedés, a normál üzemállapot visszaállásának időpontja vagy a magasabb fokozatú esemény deklarálásának időpontja.

A bizalmassági, az üzemzavar és a vészhelyzeti esemény esetén a feljegyzést elemzéssel kell kiegészíteni. Az elemzés tartalmazza az esemény kiváltó okait, és a lehetséges intézkedéseket, amelyek csökkenthetik az esemény ismételt bekövetkezésének valószínűségét. Az elemzés mélysége legyen arányban az esemény súlyosságával. (A meghibásodásokat csak regisztrálni kell, elemzés nem szükséges.)

3.4.1 Elemzés üzemzavar esetén

Az üzemzavar minősítésű incidenseket a Informatika által végzett alap feljegyzéseken túl részletesen dokumentálni szükséges. A megfelelő dokumentálás az Informatika feladata és az informatikai vezető felelőssége.

Az üzemzavar dokumentálása két részből áll:

1. Feljegyzés üzemzavarról, amely az incidens kezelés során meghozott döntéseket és a történéseket tartalmazza.
2. Üzemzavar elemzése

Az üzemzavar elemzése a következőket tartalmazza:

- az üzemzavar bekövetkezésének körülményeit,
- az üzemzavar közvetlen és közvetett kiváltó okait
- a lehetséges intézkedéseket, amelyek csökkenthetik az üzemzavar ismételt bekövetkezésének valószínűségét.
- elemzést az üzemzavar során tett intézkedések hatékonyságáról, és szükség esetén javaslatokat a visszaállítási tervek javítására

Az elemzés mélysége legyen arányban az esemény súlyosságával.

3.4.2 Elemzés informatikai vészhelyzet esetén

Az informatikai vészhelyzet minősítésű incidensekre a dokumentálás szempontjából ugyanaz vonatkozik, mint az üzemzavarra, azzal az eltéréssel, hogy a felelős: az ügyvezető igazgató.

4 VISSZAÁLLÍTÁSI TERVEK

A visszaállítási eljárások kialakítása során figyelembe kell venni az architektúra sajátosságait:

- a központi szolgáltatásokat az ÖIK gépterme biztosítja
- nem áll rendelkezésre redundáns központi infrastruktúra
- a szolgáltatások igénybe vételéhez szükséges az adatátviteli vonal működőképessége (üvegszál)

A szerverszoba üzemzavara esetén nincs lehetőség a kritikus rendszerek átterhelésére, másik helyszínre, tartalék eszközre, ugyanígy az adatátviteli vonal szakadása is az informatikai szolgáltatások gyakorlatilag teljes kiesését eredményezi.

A működésfolytonosság tervezése során olyan megoldásokat kell alkalmazni, amelyek a fenti hátrányos adottság mellett is lehetővé teszik reális időn belül legalább a kritikus rendszerek főbb funkcióinak helyreállítását.

A visszaállítást segítő lehetőségek:

- A rendszermentések és a napi mentések biztonságos tárolása.
- Szerver virtualizálás: elősegíti a különféle szerverek egységes kezelését és lehetővé teszi a rendszerek függetlenítését a hardverektől.
- Hideg tartalék eszközök beszerzése és raktározása, a szerverszobától távol eső helyen, másik épületben vagy legalább másik tűzszakaszban. Mivel az üzemeltetett rendszerek nem kívánnak speciális eszközöket, célszerű tartalékolás helyett vészhelyzet esetén az azonnali beszerzés mellett dönteni.
- Ki kell jelölni egy olyan helyiséget a Városfejlesztési Kft. területén belül, ahol rendelkezésre áll az elektromos tápellátás és a belső informatikai hálózat

kiépítése, vagy ideiglenes informatikai hálózat létrehozási lehetősége, hogy a szerverszoba használhatatlanná válása vagy tartós elérhetetlensége esetén ott lehessen ideiglenesen beüzemelni a tartalék szervereket.

4.1 AZ INFORMATIKAI RENDSZER ERŐFORRÁSAI

4.1.1 Hardver

Azon hardverelemek, melyekkel a Katasztrófa Elhárítási Terv foglalkozik, három csoportra oszthatók:

- Kiszolgálók
- Hálózati aktív és passzív eszközök
- Munkaállomások és egyéb eszközök

Helyreállító eszközök

Egy katasztrófa bekövetkezése után a szerverek újra működőképessé tételéhez alapvetően szükségesek a mentések, a mentő eszköz, illetve a szerver, aminek visszaállításra sor kerül. A mentés körülményeit a Mentési és Archiválási Szabályzat határozza meg.

Hálózati eszköz konfigurációk és környezeti beállítások mentése

A hálózati eszközök konfigurációs állományait, továbbá a szerver környezetek mentését telepítéskor, illetve minden lényeges változás után végre kell hajtani.

4.1.2 Alkalmazások

Az egyes szerverek alkalmazásait sérülés esetén mentésből kell visszaállítani a mentési rendnek megfelelően. Ezért az alkalmazások aktuális installációját a használt paraméterekkel együtt szintén menteni kell, melyet minden változtatás estén újra meg kell tenni.

4.2 DOKUMENTUMOK BIZTOSÍTÁSA

A katasztrófa helyzet menedzselésére kijelölt helyiségekben, valamint a mentések tárolására használt helyiségben (ÖIK), zárható helyen, értesítési listákat kell elhelyezni, melyek tartalmazzák az elhárításban részt vevő team tagok nevét, valamint a katasztrófahelyzet esetén értesítendő felső vezetők és hatóságok listáját.

(1) Szállítók listája: a Városfejlesztési Kft. beszállítóinak, illetve az informatikai támogatást biztosító cégeknek (rendszer támogatók, telefon-, internetszolgáltató stb.) az elérhetőségi adatait tartalmazza (cég, kontaktszemély, elérhetőség, szerződés azonosító adatai), akik szerződésben rögzített feltételek mellett segítik a belső munkatársakat a visszaállításban, helyreállításban.

(2) Felsővezetők és hatóságok: azon felsővezetők, hatóságok, és felügyeleti szervek elérhetőségi adatait tartalmazza, melyeket feltétlenül értesíteni kell egy katasztrófa bekövetkezése esetén.

(3) Munkatársak listája: a Városfejlesztési Kft. egyes felhasználói rendszereinek kulcs-felhasználói munkatársainak listája (szervezeti egység, név, munkakör,

elérhetőség). A felsorolásba azok a munkatársak kerülnek, akik az egyes rendszerek helyreállításában közreműködhetnek.

(4) Egyéb dokumentumok: el kell helyezni a következő dokumentumokat is a kijelölt helyiségekben:
   a) Hardver leltár és dokumentációk
   b) Rendszerszoftverek felsorolása
   c) Alkalmazói szoftverek felsorolása és dokumentációi
   d) Mentési dokumentumok

A dokumentumok aktualizálása is a katasztrófa terv karbantartására vonatkozó előírásainak megfelelően időközönként ellenőrizni, illetve változás esetén aktualizálni kell.

4.3 A KATASZTRÓFA ELHÁRÍTÁSI TERV TESZTELÉSE

A Informatikai vezető felel a Katasztrófa Elhárítási Terv rendszeres teszteléséért. Bármilyen tesztelés csak a Informatikai vezető előzetes jóváhagyásával és engedélyével lehetséges.

(1) Tesztelés gyakorisága: évente egy alkalommal a Katasztrófa Elhárítási Terv-t tesztelni kell. Amennyiben a Városfejlesztési Kft. működésében olyan alapvető változás, átszervezés, eszközbeszerzés stb. következik be, amely a Katasztrófa Elhárítási Terv azonnali tesztelését igényli, az informatikai vezető dönt a tesztelés elrendeléséről, és kijelöli:

- A tesztelés végrehajtásának időpontját és helyszínét,
- A teszt módszerét (Szóbeli, vagy Helyzet-szimuláció) és alkalmazott módszertanát.
- A tesztben résztvevők körét.

(2) Tesztelési módszer, szóbeli tesztelés: az informatikai biztonság felelős a résztvevőkkel előzetesen egyeztetve tűzi ki a szóbeli teszt időpontját és helyszínét, valamint a résztvevők körét. Egy fiktív katasztrófa helyzetet szimulálva a résztvevők szóban kifejtik feladatukat a következő szempontok figyelembe vételével:

Feladatszegmensek

- Input / output adatok, dokumentumok
- Értesítési utak, módok, kontaktszemélyek,
- Adattárolás, adatrögzítés, iktatás

4.3.1 A tesztelések lebonyolítása

A tesztelések időzítésénél figyelemmel kell lenni a tesztelés hosszára, amit előre meg kell tervezni a lebonyolításért felelős személynek. A Katasztrófa Elhárítási Terv teszteléséről jegyzőkönyvet kell vezetni.

A tesztelés lebonyolítása során arra kell törekedni, hogy nem maradhatnak homályos, nem kellőképpen tisztázott részek. A tesztelés lebonyolítója futtassa végig ismételten a kérdéses folyamatot, ha tisztázatlan szerepeket, vagy feladatokat tapasztal teszt lefolyása során.

A teszt befejeztével a résztvevők megbeszélik a teszt lefolyását, össze kell gyűjteni a javaslatokat és véleményeket. A lebonyolító és a tesztelés felelőse a funkcionális vezetőkkel

közösen ez alapján feljegyzést készít a tapasztalatokról a következő szempontok figyelembevételével:

- A katasztrófa elhárítására tett intézkedések a meghatározott időn belül megtörténtek-e
- A visszaállítás és a helyreállítás garantálja-e az előre meghatározott funkcionalitást az előre meghatározott időn belül
- Mennyire folyamatos a visszaállítási és helyreállítási tevékenység, vannak-e szakadási pontok
- Az információáramlás, feladatdelegálás megfelelően zajlik-e
- Vannak-e a katasztrófa tervben olyan pontok, amelyek megfogalmazása, ennek következtében az ellátandó feladat nem egyértelmű.

Minden teszt eredményéről, tapasztalatairól írásos feljegyzést kell készíteni, amelynek tapasztalatait Katasztrófa Elhárítási Terv esedékes évi karbantartásakor be kell építeni a következő oktatási programba.

4.4 OKTATÁS

A Katasztrófa Elhárítási Tervben definiált folyamatokkal kapcsolatba kerülő munkatársakat oktatni kell. A Katasztrófa Elhárítási Terv oktatását a „szükséges tudás” figyelembe vételével kell megvalósítani. A Katasztrófa Elhárítási Terv oktatását az informatikai vezető irányítja. Ő delegálhatja az „oktatás megszervezése”, valamint „oktatás megtartása” feladatokat a személyügyi terület felé.

Tapasztalatok levonása

Katasztrófa bekövetkezése esetén a helyreállítást követően a Team tagjai és az elhárításban részt vevők összeülnek, és kiértékelik a team munkáját. Az értékelés eredményét dokumentálják, és bedolgozzák a következő oktatási anyagba.

4.5 A KATASZTRÓFA ELHÁRÍTÁSI TERV KARBANTARTÁSA

RENDSZERES KARBANTARTÁS

Évente egy alkalommal az informatikai vezető gondoskodik a Katasztrófa Elhárítási Terv karbantartásáról. A karbantartás az alábbi feladatok végrehajtását jelenti:

- Az informatikai munkatársak értesítési listáinak, a team tagjainak, és a szállítói értesítési listának frissítése,
- A hardver és szoftverleltárak, a hálózati topológia áttekintése, a változások átvezetése az ÖIK bevonásával,
- A katasztrófa menedzselésére kijelölt helyiségekben elhelyezett dokumentumok érvényességének ellenőrzése, szükség esetén frissítése,
- Az utolsó karbantartás óta végrehajtott Katasztrófatesztek tapasztalatainak feldolgozása és integrálása a Katasztrófa Elhárítási Terv-be
- A Katasztrófa Elhárítási Terv új változatának véglegesítése, az érvényes verzió jelölése, és a korábbi verzió visszavonása.

ESETI FRISSÍTÉS

A Katasztrófa Elhárítási Terv évi rendszeres karbantartásán túl frissítése az alábbi esetekben valósulhat meg:

- Katasztrófát követően a helyreállítási feladatok elvégzése után,
- Informatikai beruházások kivitelezése után,
- Szervezeti változások után.

A Katasztrófa Elhárítási Terv eseti karbantartását a Katasztrófa team bármely tagja, illetve az egyes területek vezetői is kezdeményezhetik, amennyiben a felelősségi körükbe tartozó területen végbement változások ezt szükségessé teszik. Az eseti karbantartás végrehajtásáról a Informatikai vezető gondoskodik.

5 A KATASZTRÓFA ELHÁRÍTÁSI TERV MELLÉKLETEI

5.1 ÉRTESÍTÉSI LISTÁK

Székesfehérvári Városfejlesztési Közhasznú Nonprofit Kft.

- Székhely: 8000 Székesfehérvár, Városház tér 1.
- Telephely, levelezési cím: 8000 Székesfehérvár, Honvéd u. 1.
- Guti Péter ügyvezető
  telefon: 70/33-18-415
  e-mail: guti.peter@proalbaregia.hu

Önkormányzati Informatikai Központ Nonprofit Kft.

- Székhely: 8000 Székesfehérvár, Városház tér 1.
- Telephely, levelezési cím: 8000 Székesfehérvár, Honvéd u. 1.
- Barabás Tibor ügyvezető
  telefon: 70/321-62-26
  e-mail: barabas.tibor@szekesfehervar.hu