RÉPCELAK VÁROS ÖNKORMÁNYZATÁNAK INFORMATIKAI KATASZTRÓFA ELHÁRÍTÁSI TERVE
(IKET)

Bevezetés

Ahogy az információtechnológia használatától való függőség egyre nő a kormányzati, közszolgálati szektorban is, egyre fontosabb, hogy a szolgáltatásokat egy előre meghatározott, megállapodott minőségben nyújtsák. Minden esetben, amikor a szolgáltatás színvonala csökken, vagy éppenséggel nem áll rendelkezésre, a felhasználók nem tudják elvégezni mindennapi munkájukat. Az informatikától való függőség trendje várhatóan megmarad, és egyre növekvő mértékben fogja befolyásolni a felhasználókat és a vezetést. Ezért alapvetően fontos, hogy a szolgáltatásokat zökkenőmentesen tudjuk nyújtani.

Rendszerkiesések a tapasztalatok szerint előfordulhatnak, ezért kell felkészülnünk arra, hogy az igényeknek megfelelő határokon belül helyre tudjuk állítani az eredeti szolgáltatási színvonalat. A katasztrófa elhárítási terv létéből származó legnagyobb haszon tehát az informatikai szolgáltatásokkal kapcsolatos kockázati szint csökkenése.

A szabályzat által:

- az informatikai rendszerek ellenőrzött helyreállítása könnyebben végrehajtható,
- csökken a kieső idő, ezáltal a felhasználók számára a szolgáltatások folytonossága biztosított,
- könnyebben beláthatóak a hiányosságok, így a szervezet hatékonyabban tudja az erőforrásait a rendszer működéséhez biztosítani.

A kormányzati közszolgálati szervek függősége az informatikai rendszerektől egyre nagyobb. Az alaptevékenységek ellátásának színvonalát nem lehet veszélyeztetni, tehát védeni kell az informatikai rendszereket.

Mivel önkormányzatunk rendszere jóval egyszerűbb, szerényebb rendszerrel, illetve informatikai rendszerrel működik, mint egy-egy komolyabb vállalat, így a katasztrófa lehetőségek és annak elhárítási lehetőségei is nyilván mérsékeltebb számban jelentkeznek azokénál. Ez a katasztrófa-elhárítási tervezet kiélezett informatikai katasztrófára, így nem foglalkozik az olyan eseményekkel, közműkiesésekkel, melyek nem érintik közvetlenül az informatikai rendszert (pl.: vízvezeték-hálózat, stb.)

Elsősorban mindenképpen fel kell becsülni az informatikai szolgáltatások elvesztésének hatását. Meg kell határozni a kritikus szolgáltatásokat, illetve informatikai szolgáltatásokat és alkalmazásokat, amelyeknek üzemelniük kell.

Az Informatikai szolgáltatások elvesztése felbecsülhetetlen károkat képes okozni egy-egy részegységnél. A kiesés néhol semmi komoly leállást, következményt, vagy jogi következményt nem von maga után, ám vannak kritikus informatikai alkalmazások, illetve szolgáltatások, melyek egyszerűen nem állhatnak le hosszabb távon.

A rendszer kulcsfontosságú elemei, részegységeink:

1. Környezeti infrastruktúra

A környezeti infrastruktúra részei: az

- épület,
- áramellátás,
- világítás,
- telefon és telekommunikációs eszközök,
- adatátviteli vezetékek stb.

Fenyegető tényezők:

- a tűz, víz vagy természeti csapás által okozott károk,
- személy által kifejtett rombolás vagy eltulajdonítás,
- rendszer szoftver, hardver, áram vagy egyéb környezeti kiesés.

Az elmúlt időszakot és a rendszer működését figyelembe véve megállapítható, hogy a környezeti infrastruktúra kiesése az egyik leggyakoribb katasztrófa kiváltó ok. A tűz, víz, vihar vagy természeti csapás okozta kárra tulajdonképpen tökéletesen felkészülni, megelőzni szinte lehetetlen. Az elhárításra viszont több intézkedés is létezik, melyeket alkalmazunk. Ezek:

- tűzvédelmi oktatás
- a tűzvédelmi előírásoknak megfelelő helyen és számban az épületen belül poroltókészülékek vannak elhelyezve, melyek használatára minden dolgozót felkészítettek a tűzvédelmi oktatás során
- az épület villámhárítóval van felszerelve
- a tetőszerkezet és az ép csatornarendszer meggátolja az épület beázását
- az eltulajdonítás munkaidőben szinte lehetetlen, egyéb időszakokban pedig mozgásérzékelővel ellátott, a rendőrségnek is jelző riasztórendszer, betörésvédelem védi az épületet
- a legfontosabb iratok széfekben vannak tárolva a különböző irodákban, melyek ha a nagyon-nagy hőtöl nem is, de az eltulajdonítástól többnyire védelmet nyújtanak
- egy-egy munkafolyamatot több munkaállomáson is lehet végezni, így a szoftver, vagy hardverkiesés általában megoldható

- a kulcsfontosságú munkaállomásokat szünetmentes tápegységekkel, illetve túlfeszültség-védelemmel láttuk el, így sem a hálózatot ért villámkár, sem az áramkimaradás nem jelent ezeken a helyeken problémát

Az épületet érő elemi kár esetén hatalmas probléma lép fel. Ha az elemi kár az épületet és a gépparkot is érinti, akkor egyetlen megoldás, a gépek újravásárlása lehet.

Ilyen esetben a visszaállítás és az adatok visszatöltése is nagy kiesést és hatalmas problémát okozna. Ez az eset olyan anyagi ráfordítással jár, melyet az önkormányzat képtelen volna önerőből megfinanszírozni és mindenképpen külső segítséget kellene igénybe venni. Amennyiben az épületben a további munka nem lehetséges, a munkát másik épületben kell folytatni. Erre lehetőség van az önkormányzat intézményeiben. A biztonsági mentéseket is célszerű mindkét épületben 2 példányban tárolni, mivel pl.: tűzkár esetén komplett visszaállítás lehetséges.

Tapasztalatok szerint a leggyakoribb hibaok az épületen belüli áramkimaradás, illetve áramingadozás. E problémát sajnálatos módon képtelen az önkormányzat elhárítani, mivel a hiba szolgáltató oldali, és gyakorlatilag minden héten bekövetkezik legalább egy-egy pillanatnyi áramkimaradás. E miatt, az összes kulcsfontosságú gép és szerver szünetmentes tápegységgel van ellátva. Elképzelhető azonban olyan idejű kimaradás, hogy a tápegységek nem tudják adott ideig táplálni az eszközöket. Ez az időintervallum 30 perc és 120 perc között ingadozik, a tápegységek méretétől és a rá kötött eszközök energiafogyasztásától függően. Az eszközök többségénél lehetőség van az energiatakarékosságra, mint pl.: server esetén a monitor kikapcsolására, így még tovább bírják a szünetmentes tápegységek. Amennyiben előreláthatólag úgy tűnik, hogy hosszabb ideig tart az áramkimaradás, mint amit a tápegységek ki bírnának szolgálni, az eszközöket még ennek bekövetkezte előtt le kell állítani. Az áramszolgáltató a hosszabb kimaradásokat, melyek többnyire karbantartás miatt következnek be, előre be szokta jelenteni, így csak a hétvégi kimaradások okozhatnak problémát. Ebben az esetben, a serverek leállítását a pénteki munkanap végén el kell végezni. Olyan esetben pedig, amikor a szolgáltató a kimaradás bejelentési kötelezettségének nem tesz eleget szintén gondoskodni kell a gépek leállításáról a bekövetkezéskor. Ha az eszközök mégis kikapcsolnának a tápok ellenére, gondoskodni kell a visszakapcsolásról.

Ha a server tápegységét bármilyen probléma éri célszerű azonnal kicserélni, átmeneti megoldásként bármelyik munkaállomás tápegységére. Az átmeneti megoldást 72 órán belül orvosolni kell végleges megoldással, mely a tápegység javítása, illetve cseréje lehet.

Ha a telefonhálózatot éri probléma, az önkormányzat külső segítséget, telekommunikációs szakemberek segítségét veszi igénybe. Az Internet elérésünk nem telefonon keresztüli így a kommunikáció többnyire csak bejövő irányba szakad meg. A mobiltelefonok elterjedésének köszönhetően, gyakorlatilag átmeneti megoldásként semmiképp sem szűnik meg a kommunikáció, így a karbantartás nem azonnali végrehajtása sem okoz jelentős kiesést.

Az adatátviteli vezetékek meghibásodása esetén az adott szolgáltató szakemberei azonnali értesítésre kerülnek. A telefonkábelek a falban lévő csatornában helyezkednek el, a riasztórendszer és a helyi hálózat kábelei pedig felszerelt csatornákban futnak, melyek egyrészt megfelelő sérülésvédelmet nyújtanak, másrészt meghibásodás esetén könnyűvé teszik a cserét. A hibás kábel megtalálása sem jelent gondot a rendszerben, mivel a kábelek jelölésekkel vannak ellátva.

2. Hardver

Ezek alatt értjük:

- a felhasználói számítógépeket,
- nyomtatókat,
- a nagykapacitású fénymásolót,
- a telefonközpontot,
- a központi szervert.

Fenyegető tényezők:

- műszaki meghibásodás,
- elöregedés,
- környezeti hatás miatti meghibásodás,
- szoftver által kiváltott hibák,
- személyek által okozott hibák.

A technológia milyenségéből fakadóan ezek azok a problémák, melyek elkerülését nem lehet elérni. Tudatos magatartással viszont mérsékelni lehet bekövetkezésük valószínűségét. A személyek által okozott károk gyakorlatilag nem következnek be, amennyiben a gépeket, eszközöket használó személyek követik az Informatikai Szabályzat ide vonatkozó irányelveit. Amennyiben bekövetkezik a probléma, máris hardver vagy szoftver meghibásodásként kell kezelni.

Az önkormányzat az informatikai feladatok ellátását a Sárvári Kistérség alkalmazásában álló személlyel oldja meg.. A hiba észlelése után az esetet neki kell jelenteni, aki megfelelő vizsgálat után orvosolja a problémát, és amennyiben a probléma javítása anyagi ráfordítást igényel, a beszerzés megkezdése előtt azt közli a jegyzővel. A műszaki hiba elhárítására néhány egyszerűbb esetekben rendelkezünk tartalék alkatrészekkel, így a tesztelési fázisban többnyire kiderül a probléma oka.

A számítógépek meghibásodását túlnyomórészt hivatalon belül ki tudjuk váltani másik gép átmeneti beállításával, ám a zökkenőmentes ügyintézés érdekében a hibát célszerű 72 órán belül elhárítani.

Biztonságosabbá tehető a rendszer, ha:

- megbízható szállítótól, megbízható termékeket vásárolunk,
- ügyelünk a garanciális feltételekre,
- ügyelünk a javítási szerződésekre,
- rendszeresen megelőző karbantartást végzünk,
- megismertetjük és betartatjuk az Informatikai Szabályzatot.

Ezek mindegyikére nagy figyelmet fordítunk. Az elmúlt időszakokat vizsgálva 1-2 eset kivételével nem találkoztunk garanciális problémával.

Ez a megbízható hardver jelenlétének alapvető bizonyítéka, de a garanciális ügyintézés során sem ütköztünk problémába.

A nagykapacitású fénymásolóink bármilyen meghibásodása esetén telefonon jelezni szoktuk a ZRox Kft. irányába a 06-70-3841-737 -es számon, és az ..... irányába a 06-30-9560-987 számon. Szerelőik 72 órán belül, de a gyakorlat azt mutatja, hogy általában még a bejelentés napján, vagy a rá következő munkanapon el is hárítják a problémáinkat.

Az elöregedés problémája nem igazán érint kiesést, mivel nem azonnal, hirtelen, váratlanul következik be, hanem évek során, lassan zajlik le. Természetesen ilyen esetben a komplett csere a megoldás, melyet hivatalunkban folyamatosan végzünk, és figyelemmel kísérjük a géppark állapotát, az Informatikai Stratégiánkkal szinkronban.

A megelőzés hardver meghibásodás ellen abban nyilvánulhat meg, hogy a gépeket nem tesszük ki szélsőséges viszontagságoknak, így kerüljük a hideget, meleget, áramszünetet, mozgatást. A gépek szervizelésekor minden esetben nagynyomású levegővel való portalanításra is sor kerül, melynek megelőző szerepe nem elhanyagolható.

3. Szoftver

Részei:

- rendszerszoftverek
- alkalmazói szoftverek

Önkormányzatunknál a server kivételével mindegyik kliensen Microsoft Windows operációs rendszer fut. Ezeknek a konfigurációjuk túlnyomórészt azonos, egy-két kivétellel. Az alkalmazói szoftverek ellátásában már nagyobb a különbség. Minden szoftver telepítő-anyagával rendelkezünk, amennyiben a szoftver gyártója a rendelkezésünkre bocsájtotta azt. Ezeknek a programoknak a feltelepítése a felhasználó kézikönyvükben leírtak szerint történik. Léteznek olyan komplett rendszerek, mint pl. az iktatás vagy a szociális ügyintézést felügyelő rendszerünk, mely telepítését a gyártó végzi. Ezen szoftverek gyártóinak elérhetőségét a szoftverek Súgó menüpontja, illetve a felhasználó kézikönyv tartalmazza.

Fenyegető tényezők:

- szoftverhiba,
- vírusveszély,
- jogosulatlan bejutás,
- kezelési hiba,
- szoftver sérülés vagy használhatatlanná válása hardverhiba miatt,
- szándékos rongálás, törlés.

A szoftverek meghibásodási problémáinak nagy része, hasonlóan a hardverhez, helyben elvégezhetőek. A hibákat mégis jobb elkerülni. Az elkerülés érdekében követendő:

- csak legális, vagy ingyenes szoftver használata,
- elfogadott szoftver használata,
- ellenőrzött, akkreditált szoftver használata,
- szoftverek rendszeres karbantartása, vizsgálata,
- idegen szoftverek használatának tilalma,
- hozzáférési rendszerek, jelszavak használata,
- megfelelő vírus és behatolás-védelem.

Ezeknek a kritériumoknak a lehetőségekhez mérten eleget teszünk. A felhasználói programjainkat gondosan szoktuk megválasztani, mindig figyelemmel kísérve a hozzá nyújtott támogatást (support).

Hivatalunknál a vírusvédelmet a nod32 rendszer biztosítja.

4. Adathordozók, adatok, dokumentációk

Részei:

- szoftvert tartalmazó adathordozók
- biztonsági másolatok, archív adatok
- tárolt adatok
- mindenféle dokumentum, irat, amely papíron van és informatikai rendszerrel kapcsolatos

Fenyegető tényezők:

- külső esemény okozta károsodás

- elöregedés, lemágneseződés
- fizikailag hibás adathordozó
- lopás, szándékos megkárosítás
- adathoz jutás kiselejtezett adathordozóról
- hibás adatbevitel
- futó program megszakítása
- vírus, jogosulatlan másolás
- adatsérülés feldolgozás, tárolás, kiadás során
- elvesztett, olvashatatlanná vált dokumentumok
- nem aktualizált dokumentumok

Helyzetelemzés:

Az adatokat minden esetben védeni kell, hiszen sok közülük pótolhatatlan, vagy csupán nagyon-nagy ráfordításokkal és csak rengeteg munkával pótolható. Sok adatbiztonsággal foglalkozó vállalat állítja, hogy olyan, hogy tökéletes adatbiztonság nem létezik, azonban mégis a lehetőségekhez mérten törekedni kell a tudatos, adatmentő, adatmegóvó magatartásra. A hivatalban 2 olyan számítógép található melyeken gyakorlatilag adat nem, vagy alig található. Ezek olyan gépek, melyek többnyire egy-egy adatszerverre csatlakozva működnek, így megóvni való adat nem található rajtuk.

A fontos adatokat napi rendszerességgel menteni szoktuk. A mentést több módszerrel végezzük. 2 számítógépen az önkormányzati testületi ülések hanganyagának feldolgozását végzik. Ezeket a hanganyagokat rendszeresen CD lemezekre mentik. Ezen kívül a felhasználók az adott programba beépített mentés menüpont segítségével külső adathordozóra (lemez, pendrájv) manuálisan végzik a mentést, illetve minden gépen naponta előre meghatározott időközönként Cobian Backup program segítségével inkrementáló mentés történik automatikusan a szerverre. A szerveren így összegyűjtött adatokat a Blue System Kft. nevű adatmentéssel foglalkozó cég Interneten keresztül 128 bites titkosítással, automatizált megoldással egy szombathelyi és egy budapesti szerverre menti le. Ezekről a külső szerverekről bármely adat bármikor visszatölthető. Ebből is látható, hogy adataink ennél nagyobb biztonságban nem lehetnének.

Az Internet felé tűzfallal és vírusvédelemmel vagyunk biztosítva így a vírusok nem jelentenek gondot, a jogosulatlan másolás pedig csak intézményen belülről valósulhat meg.

Néhányan jelszavakkal védik dokumentumaikat, vagy megosztásukat, így gátolva meg a jogosulatlanok hozzáférését. Természetesen nem tarthatunk figyelemmel, minden kimenő személyt, vagy kiküldött e-mail, de tapasztalataink szerint ez eddig nem

jelentett potenciális veszélyforrást. Az irodákban többnyire többen dolgoznak együtt, ráadásul általában közös vagy hasonló feladatkörben, így a dokumentumokat szándékosan megosztják egymással.

Hivatalunkra jellemzőek a szoftverek által előállított dokumentumok és az adatbázisszerverek, így egy-egy kijuttatott dokumentum az adatbázis szerver nélkül jóformán használhatatlan. Ezeket a szoftvereket pedig jelszavakkal védjük.

Sok adatunk nyilvános, melyeket Répcelak város honlapján ( ) is publikálni kell, így ezek az adatok gyakorlatilag a webserveren, távol, elszeparáltan a hivataltól biztonságban vannak.

Az írásos formában tárolt dokumentumok 2 fajtája a jellemző. Az általunk elkészített dokumentumok, és a hardverek, szoftverek dokumentációi.

Az általunk készített dokumentációkból minden esetben megőrizzük a digitális változatot, amennyiben valamilyen oknál fogva nem kerül elő, a dokumentum újrascannelése a megoldás.

A hardverek dokumentációit általában a szoftverekkel együtt megőrizzük, elévülésük vagy elvesztésük sem jelent gondot, mivel minden gépünk Internetkapcsolattal rendelkezik, így könnyen bármi a rendelkezésünkre áll.

Biztonsági intézkedések:

- másodpéldányok más helyen tartása
- környezeti körülmények ellenőrzése
- öreg vagy nem preferált adathordozók átmásolása
- az előállított adathordozók azonnali visszaolvasása, ellenőrzés végett
- privát adathordozók tiltása (kivétel usb mehajtók) keveredés elkerülésére
- selejtezett adathordozók törlése, megsemmisítése
- hardver beszerzésekor dokumentáció követelése
- legális szoftverhasználat.

5. személyzet, felhasználók

Részei:

- személyek akikre közvetve vagy közvetlenül szükség van az informatikai rendszer használatához

Fenyegető tényezők:

- munkából való kiesés (betegség, szabadság stb.)

- nem szándékos hibás viselkedés
- szándékos hibás viselkedés
- belső ismeretek továbbadása harmadik személynek, gyanútlanul
- belső ismeretek továbbadása harmadik személynek, szándékosan

A dolgozók szerves részei, felhasználói az informatikai rendszernek, így mindenképpen fontos, hogy azt szakszerűen, minél hiba mentesebben és biztonságosabban tudják kezelni. Az új dolgozókkal meg kell ismertetni a munka- és tűzvédelmi szabályzatot, valamint az informatikai szabályzatot is, a rendszer és önmaga megóvása érdekében. Az informatikai szabályzatban sok alapelv le van fektetve, így elvileg a megismerésével a dolgozó elkerülheti a hibás viselkedést. Az információk továbbadását titoktartási nyilatkozattal és azzal érjük el, hogy az eltávozó dolgozók jelszavait, hozzáféréseit megváltoztatjuk, illetve töröljük. Ahogy azt a stratégiánk is tartalmazza, támogatunk minden irányú informatikai alap- illetve továbbképzést a dolgozóink érdekében.

Biztonsági intézkedések:

- nyugodt, stresszmentes munkakörnyezet biztosítása
- távozó dolgozók jelszavainak törlése
- távozó dolgozók utódjainak betanítása a távozás előtt
- informatikai alapkiképzés
- szakmai továbbképzés
- oktatás az érvényes szabályozásokról
- biztonságtudat kialakítása és megtartása

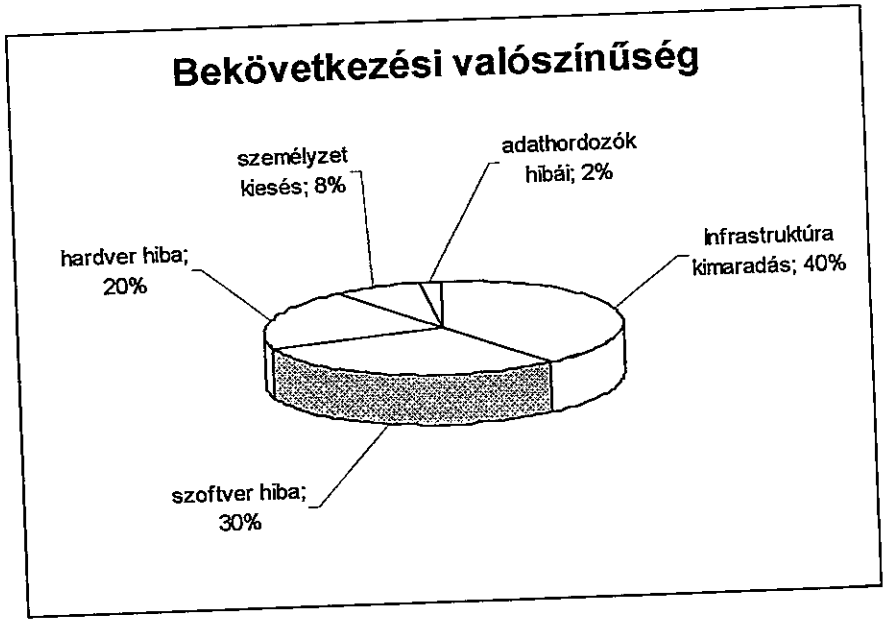
Szolgáltatások kieséseinek hatáselemzése:

A kiesések egyike sem tartható fenn hosszú távon, így mindig törekedni kell a minél hamarabbi helyreállításra. A rendszer teljes elvésztesének bekövetkeztekor önállóan képtelenek vagyunk visszaállítani a munkát, de összességében elmondható, hogy az egyéb problémákat 72 órán belül el lehet hárítani.

A felmért kockázati tényezők, veszélyforrások bekövetkezésének valószínűsége nyilván csak becslés alapján történhet, mivel sok veszélyforrás nem következett még be, így csak valószínűsíteni tudjuk annak bekövetkezésének esélyét.

Tapasztalataink szerint a legnagyobb problémát az áramkiesés okozza, ezt követik az operációs rendszereket, esetleg vírusokat, spameket érintő szoftveres problémák. Bekövetkezési valószínűség szerinti sorrendben ezek után a hardver meghibásodások állnak, ez főleg a nagyon igénybevett fénymásolónak köszönhető, de egyre gyakoribbak a spontán meghibásodások is. A sort a személyzet betegsége, hiányzása, majd az adathordozókból fakadó hibák zárják.

A többi felmért kockázati tényező 1% alatti bekövetkezési valószínűséggel bír, így azokat ábrázolni sem célszerű.



Az esetek nagy részében a hibát költségmentesen el lehet hárítani, ez alól kivételt képez a hardverhiba. Így ilyen probléma esetén a beavatkozás általában több időt vesz igénybe. A prioritások természetesen itt mindig beleszólnak a munkamenetbe. És a vezetői döntések szerint a helyreállítás időintervalluma is módosulhat.

A helyreállítás módja:

A helyreállításra szinte mindig van alternatíva. A megoldás folyamata lehet azonnali, de többlépcsős, helyettesítő eljárás is. Kiválasztása mindig az adott eseménytől függ. Az alábbi lehetőségek állnak rendelkezésünkre:

- semmit nem teszünk: mely egy veszélyekkel terhes változat, hiszen ha úgy gondoljuk, hogy tovább tudunk működni bizonyos informatikai szolgáltatások nélkül, akkor fel kell tennie azt a kérdést, hogy minek használjuk őket egyáltalán. A semmit sem teszünk kockázata az, hogy bármi bekövetkezhet.
- kézi helyettesítő eljárásokat alakítunk ki: ez a változat gyakran nem megfelelő, minthogy nem áll rendelkezésre elégséges számú és képzettségű személyzet, akik működtetni tudnának egy helyettesítő rendszert, éppen az informatikai szolgáltatásoktól való függőség miatt, mégis gyakran van használva, átmeneti megoldásként.
- kölcsönösségi egyezményt kötünk: ebben a változatban két, kompatibilis eszközöket használó szervezet megegyezik, hogy bármelyik a másik számára

szükség esetén pótolja kieső szolgáltatást. Ez a megközelítés nem túl jó megoldás számunkra, mert adott esetben ez a saját működésünk rovására menne. A tesztelés is jelentős gondokat okoz. Valamint alternatívaként csupán valamelyik intézményünk jöhet szóba.

- a lehetséges kockázatokat a minimálisra csökkentjük az informatikai szolgáltatások folyamatos elérhetősége érdekében. E változatban nincs alternatív telephely, viszont jelentős összegeket kell költeni az eredeti telephely biztonságosabbá tételére, a berendezések többszörözése által, környezeti felügyeleti és fizikai biztonsági intézkedések foganatosítása által. Részben segítenek a riasztórendszerek, poroltók stb.

- egy üres számítógép termet tartunk fenn, mely rendelkezik a szükséges áram és egyéb környezeti feltételekkel, telekommunikációs lehetőségekkel. Anyagilag nem tartjuk indokoltnak.

- a telephely szállítható, ami szintén nem járható út egy komplett intézmény esetén hatalmas ráfordításokat igényelne.

Fontos, hogy folyamatosan figyelemmel kísérjük a bekövetkezett katasztrófa-helyzeteket és a lehetőségekhez mérten rendszeresen, ennek megfelelően karbantartsuk a katasztrófa-elhárítási tervet.

Répcelak, 2011. március 28.

Dr. Németh Kálmán
polgármester

Répcelak Város Önkormányzata
Répcelak

Dr. Kiss Julianna
jegyző