BUDAVÁRI
POLGÁRMESTERI HIVATAL

BUDAPEST FŐVÁROS I. KERÜLET BUDAVÁRI POLGÁRMESTERI HIVATAL JEGYZŐJE 40/2022. (XII.21.) NORMATÍV UTASÍTÁSA AZ INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERVRŐL

A jogalkotásról szóló 2010. évi CXXX. törvény 23. § (4) bekezdés j) pontjában biztosított jogkörömben eljárva a Budapest Főváros I. kerület Budavári Polgármesteri Hivatal Informatikai Katasztrófa-elhárítási terv tekintetében az az alábbi utasítást adom ki:

1. A Budapest Főváros I. kerület Budavári Polgármesteri Hivatal szabályos működése érdekében jelen utasítás mellékletében foglalt Informatikai Katasztrófa-elhárítási tervről szóló Szabályzatban meghatározott eljárásrendet kell alkalmazni.

2. Jelen utasítás 2022. december 22. napján lép hatályba.

3. Jelen Szabályzat hatályba lépésével egyidejűleg a Budapest Főváros I. kerület Budavári Polgármesteri Hivatalánál valamennyi, e tárgykörben korábban meghozott szabályzatot hatályon kívül helyezi.

4. Az Informatikai Katasztrófa-elhárítási tervről szóló Szabályzat elkészítéséért, aktualizálásáért és felülvizsgálatáért az Üzemeltetési és Informatikai Csoport a felelős.

5. Jelen szabályzat egy darab eredeti példánya az Jegyzői Irodán kerül elhelyezésre.

Budapest, 2022. december 21.

Budapest Főváros I. ker. Budavári Polgármesteri Hivatal Jegyző

dr. Németh Mónika
Jegyző

Budapest Főváros I. kerület Budavári Polgármesteri Hivatal

Informatikai katasztrófa-elhárítási terve

Hatályos: 2022. december 22.

1. A szabályzat célja

A Budapest Főváros I. kerület Budavári Polgármesteri Hivatal (továbbiakban Hivatal) feladatainak ellátáshoz elengedhetetlenül szükséges a megfelelően működő informatikai infrastruktúra, illetve információ-kezelő berendezések biztosítása és az információs rendszerek a lehető leghosszabb ideig történő hibamentesen működése.

A szabályzat az informatikai rendszert érintő nem kívánt eseményekre való felkészülést és a válasz fázist tartalmazza. Katasztrófa helyzetnek minősül minden olyan esemény, mely az adattovábbító-, tároló- és/vagy feldolgozó képesség elvesztését okozza.

2. Kockázat táblázat

Veszélyforrás	Valószínűség	Kár	Kockázat	Intézkedés
Tűzeset	1	5	5	3.1
Áramkimaradás	5	2	10	3.2
Csőtörés	1			3.3
Emberi erőforrás hiány	5	1	5	3.4
Hardver meghibásodás	3	2	6	3.5
Internet szolgáltatás meghibásodás	2	1	2	3.6
Vírus fertőzés	3	5	15	3.7
Klíma meghibásodás	2	1	2	3.8
Betörés	1	3	3	3.9
Számítógépes betörés	1	5	5	3.10

3. Lehetséges katasztrófa helyzetek

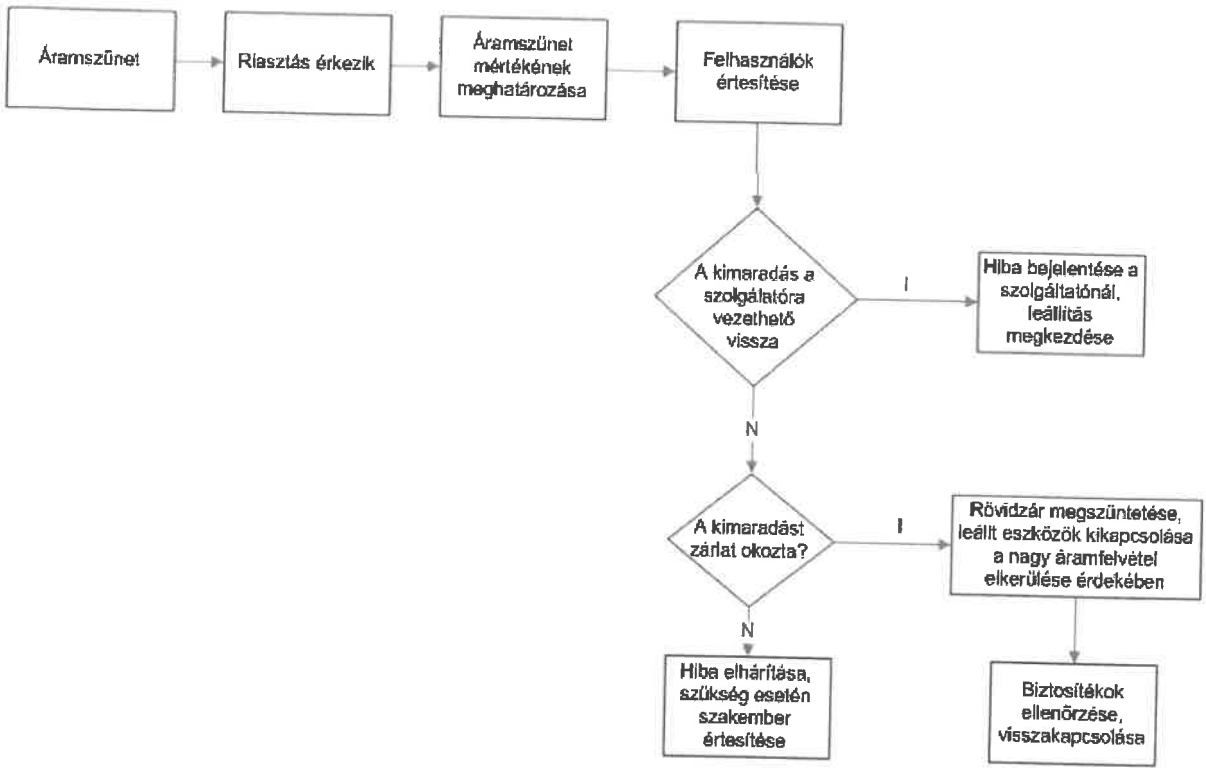
3.1. Tűzeset

Tűz esetén a Hivatal hatályos tűzvédelmi szabályzata szerint kell eljárni. Jelen fejezet, csak a legfontosabb irányelveket tartalmazza:

- Aki a tüzet vagy annak közvetlen veszélyét észleli, arról tudomást szerez, köteles a 112-ös segélyhívószámot késedelem nélkül értesíteni, illetve a portaszolgálat is. A tűzjelentésnek tartalmaznia kell:
- a tűzeset pontos helyét (kerület, utca, házszám, emelet stb.)
- mi az, ami ég és mi van veszélyeztetve,
- emberélet van-e veszélyben,
- a jelző nevét, a jelzésre használt telefon számát.

3.2. Áramkimaradás

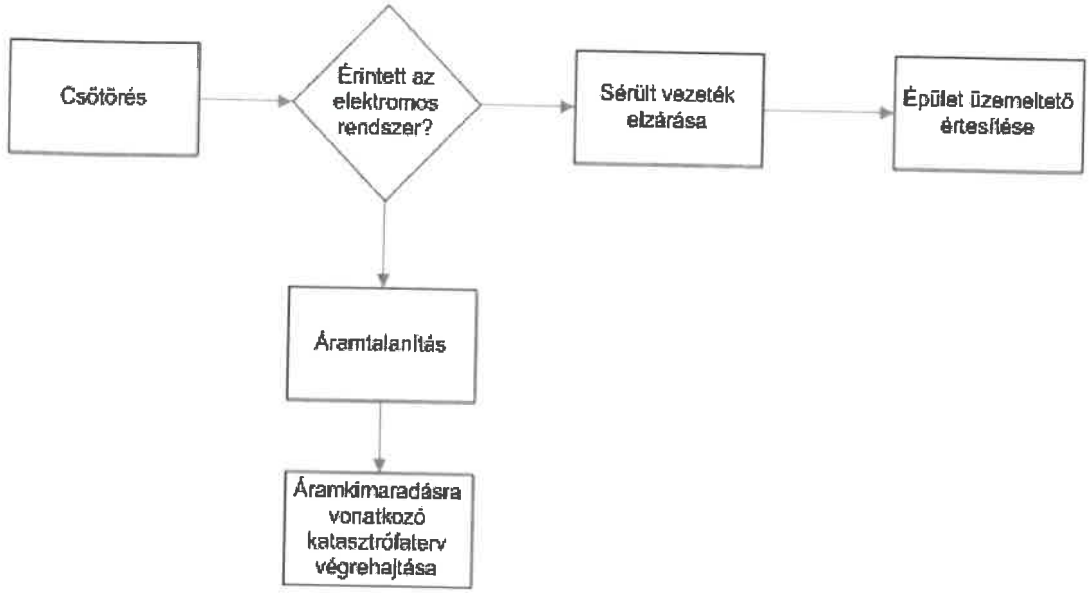
Az elektromos betáplálás megszűnése esetén a szünetmentes tápegységek csak korlátozott ideig képesek üzemeltetni a rendszert. Tartós áramkimaradás esetén teljes szolgáltatás kiesés fenyegeti a Hivatal informatikai rendszerét.



Fázis meghatározása	
Felkészülési fázis	Minden szerver és aktív eszköz szünetmentes tápegységen keresztül kapja az elektromos betáplálást, melynek kiesése esetén az informatikai rendszer működését a szünetmentes tápellátás biztosítja - korlátozott ideig.
Katasztrófa helyzet meghatározása	Az áramkimaradás abban az esetben tekinthető katasztrófának, ha a kimaradás érinti a szerverszobát is, és a hiba előreláthatólag nem hárítható el a szerverek automatikus leállása előtt.
Válaszfázis	Kimaradás okának meghatározása 2/a. Elektromos művek értesítése, kimaradás okának és időtartamának tisztázása. 2/b. Épület karbantartójának értesítése 3. A szerverek leállítását a szünetmentes tápegység automatikusan elvégzi. Tervezett leállítás esetén a leállítás sorrendjét a szerverek kritikussága alapján az üzemeltetést végző személyek határozták meg. A szerverek leállási sorrendjét a jelenlegi szabályzat 1.-es számú melléklete tartalmazza.
Helyreállítási fázis	Áramkimaradást követően a szerverek átgondolt és megfelelően megtervezett újraindítása kritikus jelentőségű. A visszakapcsolás sorrendjét a 2-es számú melléklet tartalmazza. A visszakapcsolást követően meg kell kezdeni a teljes rendszer ellenőrzését!

3.3. Csőtörés

A csőtörés esetén a legnagyobb veszélyforrás az, hogy a víz zárlatot okozhat, így áramkimaradáshoz vezethet

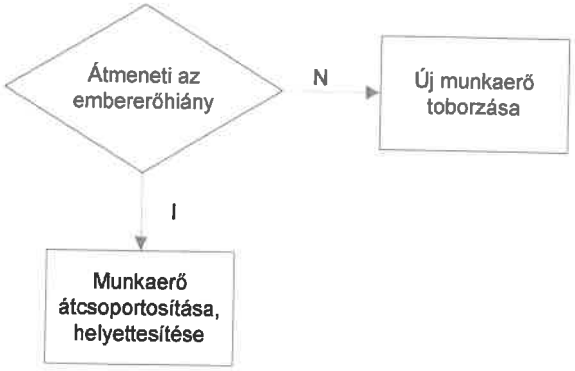


Fázis meghatározása	
Felkészülési fázis	A szerver szoba felett nincs mosdó és vízvezeték, így a szerverszobát elázás nem fenyegeti.
Katasztrófa helyzet meghatározása	Katasztrófa helyzetről csak abban az esetben beszélünk, ha az érinti az informatikai és/vagy az elektromos rendszert. Katasztrófa helyzetek: 1. eset: A szerverszoba az óvintézkedések ellenére egy csőtörés hatására beázik. 2. eset: A csőtörés következtében az épületet áramtalanítani kell.
Válaszfázis	1. esetben: a helyiséget azonnal áramtalanítani kell, vállalva a nem szabályos leállásból eredő kockázatokat. Az áramtalanítás során a szünetmentes tápegységeket is áramtalanítani kell! 2. esetben az áramkimaradásra vonatkozó terv az irányadó
Helyreállítási fázis	A szerverszoba beázását követően, az üzemeltetést csak a hibák felmérését a megfelelő környezet visszaállítását követőn szabad megkezdeni. Amennyiben az épületet áramtalanítani kellett az „áramkimaradás" fejezetben található lépések követendők.

3.4. Emberi erőforrás hiány

Az üzemeltető személyzet hiánya esetén előfordulhat, hogy az informatikai rendszerek rendelkezésre állása nem biztosítható. A kialakult hiány oka lehet például: rosszul szervezett szabadságolás, betegség, felmondás.

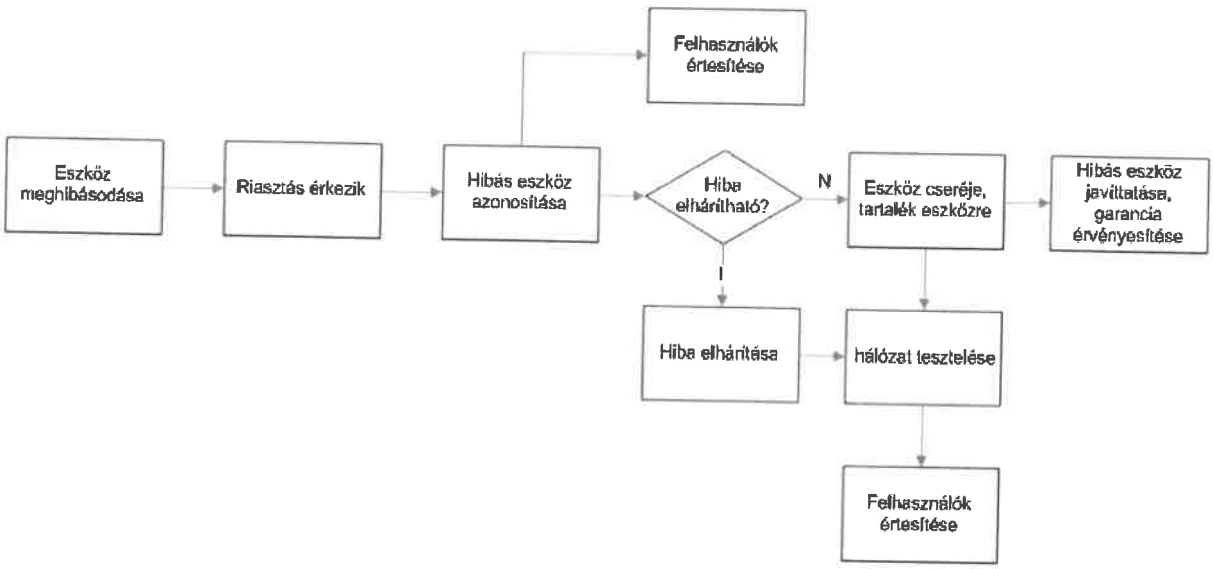
Átmeneti hiány esetén a munkarend átszervezésével, helyettesítéssel kell biztosítani a rendszer üzemelését. Amennyiben a hiány hosszabb, ideig fennáll, gondoskodni kell az új munkaerő felvételéről, kölcsönzéséről.



Fázis meghatározása	
Felkészülési fázis	A Hivatal Üzemeltetési és Informatikai Csoportjának vezetője több lépést is tesz annak érdekében, hogy egyetlen ember kiesése se okozza a munkamenet fennakadását. - Minden személynek van helyettese, aki képes ellátni a távollévő munkatárs feladatait. - A szabadságok megtervezésénél mindig ellenőrzik, hogy biztosított-e a szükséges munkaerő.
Katasztrófa helyzet meghatározása	Katasztrófa helyzetről abban az esetben beszélünk, ha a munkaerőhiány beavatkozás nélkül sokáig fennáll, illetve veszélyezteti a rendszer megfelelő üzemeltetését.
Válaszfázis	A helyettesítést az Üzemeltetési és Informatikai Csoportvezetőnek kell megoldania. Az új munkaerő felvételéről a humán erőforrásnak és az Üzemeltetési és Informatikai Csoportvezetőnek közösen kell gondoskodnia.
Helyreállítási fázis	A megfelelő számú munkaerő esetén vissza lehet állni a megszokott munkarendre.

3.5. Hardver meghibásodása

Amennyiben meghibásodik a Hivatal informatikai rendszerében található aktív eszközök valamelyike az eszköz elhelyezkedésétől függően elérhetetlenné válnak bizonyos szolgáltatások vagy szerverek, így egyszerre akár több funkció is kieshet.



Fázis meghatározása	
Felkészülési fázis	A szerver oldali eszközök redundánsan vannak bekötve. Az eszközök működését folyamatosan monitorozzák.
Katasztrófa helyzet meghatározása	Valamelyik kiemelt fontosságú rendszer elérhetetlenné válása.
Válaszfázis	Amennyiben a monitorozó alkalmazás az hibát jelez, vagy bejelentés nyomán az üzemeltetést végző személyek, az aktív eszköz hibáját állapítják meg, azonnal megkezdik a hiba okának feltárását, majd elhárítását. Amennyiben a hiba csak a javítással lehetséges a hibás eszköz javíttatását meg kell kezdeni, amennyiben az eszköz már nem garanciális, a javításról az illetékes vezető dönt a költségek figyelembe vételével.
Helyreállítási fázis	A hiba elhárítása után, vissza lehet állni a megszokott munkarendre.

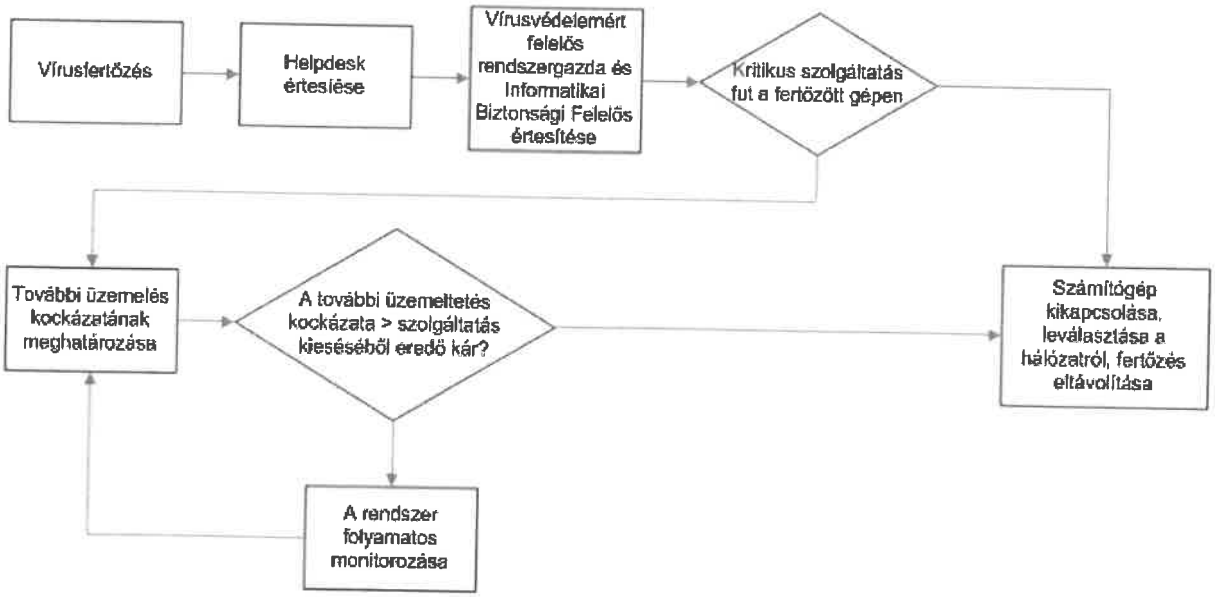
3.6. Internet szolgáltatás meghibásodása

A Hivatal több fontos szolgáltatása is aktív internetkapcsolatot igényel (web elérés, DMS, outlook levelezés, GovCenter, KIR, stb.). A internet kapcsolat kiesése esetén a munkatársak, nem férnek hozzá a ezekhez a szolgáltatásokat, így nem tudják munkájukat maradéktalanul elvégezni.

Fázis meghatározása	
Felkészülési fázis	A Hivatal redundáns internetkapcsolattal rendelkezik a tűzfal pedig a kapcsolatok monitorozásával és automatikus átállással igyekszik csökkenteni a vonalak kiesésének kockázatát.
Katasztrófa helyzet meghatározása	Mindkét internetszolgáltatás egyidejű elérhetetlenné válása.
Válaszfázis	Mivel a kapcsolatokat a Hivatal internetszolgáltatóktól veszi igénybe, a helyreállítást a szolgáltató szabályzatai tartalmazzák a Hivatal felelőssége a hiba észlelés utáni azonnali bejelentése.
Helyreállítási fázis	A szolgáltató rendelkezésre állásának mérése.

3.7. Vírus támadás

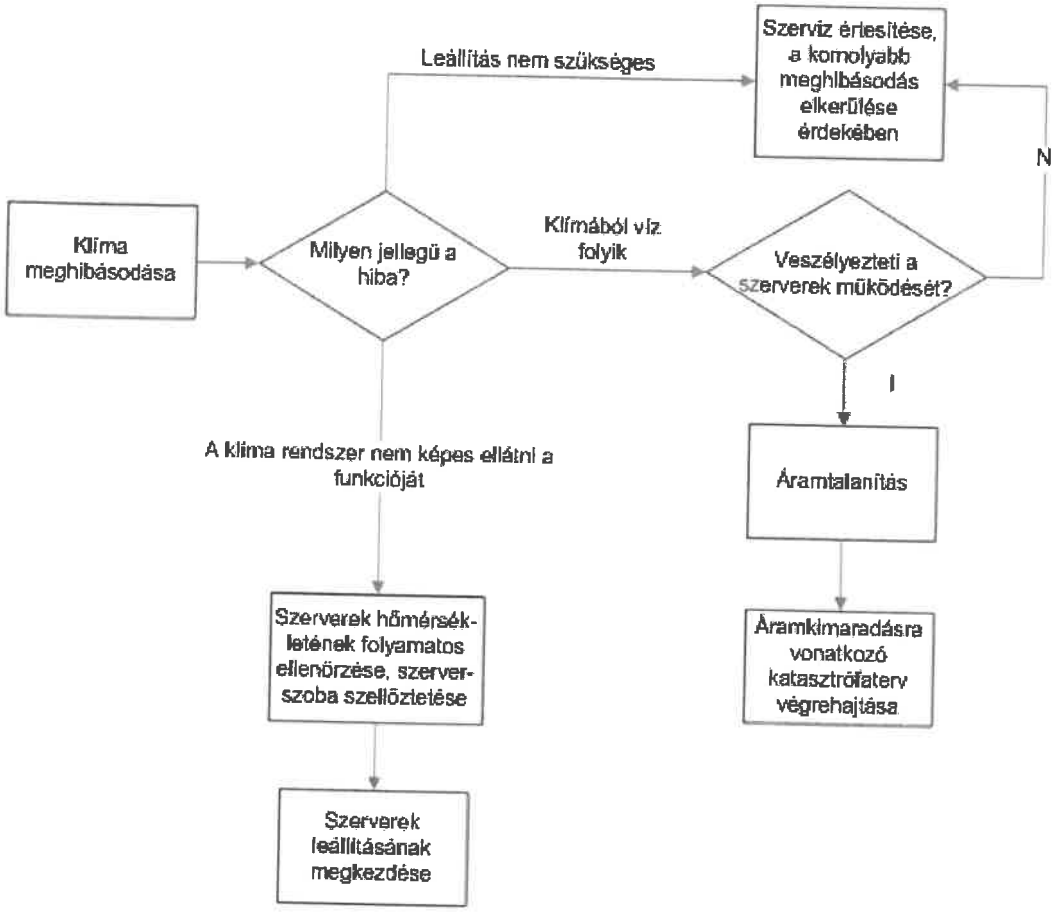
A PC-s hardveren futó alkalmazói rendszerek vírusfertőzés veszélyének vannak kitéve. Az esetleges vírusfertőzések fenyegetést jelentenek a PC-s rendszerek rendeltetésszerű működésére, a tárolt információk sértetlenségére, ezért a vírusvédelem kérdéseivel részletesebben is foglalkozni kell.



Fázis meghatározása	
Felkészülési fázis	A Hivatalnál működő szerver és kliens gépekre, vírusellenőrző programot kell telepíteni. A telepítések elvégzése az adott gépet telepítő rendszergazda feladata, a munka irányítását, felügyeletét és ellenőrzését pedig az Informatikai szolgáltatásmenedzsernek kell ellátnia. A rendszergazda az Üzemeltetési és Informatikai Csoport vezetője vagy az általa kijelölt személy. A vírusellenőrző program futását - a hibajavítás, illetve rendszerkarbantartás eseteit kivéve - megszakítani tilos. Amennyiben a Hivatal valamely munkatársa az általa használt munkaállomáson vírusfertőzöttséget vagy a vírusvédelmi rendszer rendellenes működését észleli, akkor azt jelenteni köteles az Informatikai Support-nak (e-mail: support@budavar.hu, a továbbiakban: Support).
Katasztrófa helyzet meghatározása	Több szervert érintő vírusfertőzés.
Válaszfázis	A szerverek vírusfertőzöttsége esetén az azt észlelő munkatárs azonnal értesíteni köteles az Informatikai Support-ot. A Support-nak tájékoztatási kötelezettséggel rendelkezik az Informatikai szolgáltatásmenedzser és az **Informatikai Biztonsági Felelős** felé. Szervergép vírusfertőzése esetén a vírusmentesítést a Support ellenőrzi. Szervergépek vírusfertőzése esetén az Informatikai szolgáltatásmenedzser ellenőrzést rendelhet el, és részletesen kivizsgáltathatja az esetet. A vírusfertőzés okainak feltárására vonatkozó vizsgálat eredményét jelentésbe kell foglalni. A szervergépek vírusfertőzését eredményező okok feltárásához a Hivatal szervezeti egységeinek vezetői és munkatársai kötelesek minden szükséges tájékoztatást megadni a vizsgálatot folytató Informatikai vezető részére.
Helyreállítási fázis	Felhasználók értesítése, a szolgáltató rendelkezésre állásának mérése.

3.8. Klíma rendszer meghibásodása

A szerverszoba hűtése fontos a szerverek megfelelő működéséhez. A klíma rendszer kikapcsolása esetén a szerverek nem képesek leadni a termelt hőt, a meghibásodás esetén a szerverszobát meg kell próbálni szellőztetéssel hűteni és folyamatosan figyelni a szerverek hőmérsékletét. A gyártói határérték átlépése előtt szabályosan le kell állítani a szervereket a leállítási sorrendnek megfelelően.



Fázis meghatározása	
Felkészülési fázis	Az Hivatal klímarendszer kiesésének esélyét a redundáns rendszer kialakításával és a folyamatos karbantartással igyekszik a lehető legkisebb értékre csökkenteni.
Katasztrófa helyzet meghatározása	Mindkét klímaberendezés egyidejű elérhetetlenné válása.
Válaszfázis	A klímát érintő bármely meghibásodás esetén a lépéseket a folyamat ábra tartalmazza.
Helyreállítási fázis	A klíma rendszer meghibásodása csak extrém esetben okozhat hibát a rendszerekben. A helyreállítás az érintett rendszerek működéséhez szükséges üzemi hőmérséklet elérése.

3.9. Betörés

Fázis meghatározása	
Felkészülési fázis	A Hivatal épületeiben portaszolgálat tevékenykedik, melynek feladata többek közt a Hivatal védett helyiségeibe történő ki- és belépés ellenőrzése és nyilvántartása A szerverszobába illetve az Informatika egyéb helyiségeibe csak az arra illetékesek léphetnek be és idegen személyek csak az ő kíséretükben – megfelelő indokkal - léphetnek be oda A belépés tényét és a bent-tartózkodás időtartamát a Belépési Naplóban rögzíteni kell
Katasztrófa helyzet meghatározása	Illetéktelen behatolás a szerverszobába, vagy védett adatot tartalmazó helyiségbe.
Válaszfázis	Az észlelő munkatárs azonnal értesíteni köteles a portaszolgálatot a behatolás tényéről. A portaszolgálat tájékoztatási kötelezettséggel rendelkezik az Informatikai szolgáltatásmenedzser és az Informatikai Biztonsági Felelős felé. Szükséges esetben a rendőrségi feljelentést kell tenni.
Helyreállítási fázis	Ellenőrizni kell, hogy a behatoló milyen adatokhoz férhetett hozzá.

3.10. Számítógépes betörés

Fázis meghatározása	
Felkészülési fázis	A Hivatal hálózatát tűzfal védi, amely különböző szabályokkal blokkolja az internet felől érkező rosszindulatú adatforgalmat.
Katasztrófa helyzet meghatározása	Illetéktelen behatolás a Hivatal hálózatába.
Válaszfázis	Az észlelő munkatárs azonnal értesíteni köteles a Support-ot a behatolás tényéről. A Support-ot tájékoztatási kötelezettséggel rendelkezik az Informatikai szolgáltatásmenedzser és az Informatikai Biztonsági Felelős felé. A hálózati rendszermérnöknek ki kell vizsgálnia az esetet, és jelentést írnia. Ezt a jelentést a Biztonsági felelős a GovCert-nek továbbítja. Szükséges esetben a rendőrségi feljelentést kell tenni.
Helyreállítási fázis	Ellenőrizni kell, hogy a behatoló milyen adatokhoz férhetett hozzá.

4. Intézkedési terv

4.1. Üzemzavar időtartama, és intézkedési kötelezettségek

4.1.1. Átmeneti üzemzavar

Átmeneti üzemzavarnak minősül az az üzemzavar, amely nem éri el az öt napot

- A hatóság az üzemzavar elhárítását követő huszonnégy órán belül az üzemzavar tényéről az ügyfelet elektronikus levélben tájékoztatni köteles.
- Az elektronikus levélben a hatóságnak az ügyféllel közölni kell az üzemzavar kezdő és megszűnési időpontját
- Ha a hatóság informatikai rendszerének tartós vagy átmeneti meghibásodása, illetve egyéb technikai ok miatt nem volt képes elektronikus dokumentumot fogadni, a hatóság az erről szóló tájékoztatással egyidejűleg az ügyfelet a szükséges eljárási cselekmény megismétlésére hívja fel.
- Az ügyintézés során felmerülő technikai problémákról a hatóság köteles tájékoztatni az ügyfelet, és az üzemzavar időtartamát figyelmen kívül kell hagynia a határidők számításánál

4.1.2. Tartós üzemzavar

Tartós üzemzavarnak minősül az az üzemzavar, amely legalább öt napon keresztül tart.

- a hatóság köteles legkésőbb az üzemzavar ötödik napját követő első munkanapon az ügyfelet az üzemzavar tényéről és kezdő időpontjáról könyvelt postai küldeményben értesíteni és tájékoztatni arról, hogy az ügyintézésre a hagyományos (írásbeli) eljárási módot lehet alkalmazni.
- A tartós üzemzavar esetén a hatóság köteles legkésőbb az üzemzavar ötödik napját követő első munkanapon az ügyfelet az üzemzavar tényéről és kezdő időpontjáról könyveit postai küldeményben értesíteni ás tájékoztatni arról, hogy az ügyintézésre a hagyományos (írásbeli) eljárási módot lehet alkalmazni.

4.2. Cselekvési terv

- Az üzemzavart észlelő haladéktalanul értesíti a rendszergazdát
- A rendszergazda értesíti azokat a további személyeket, akik részt vesznek a hiba elhárításában, vagy egyéb intézkedést kell hozniuk
- A rendszergazda felméri a kárt és megkezdi annak elhárítását
- Az üzemzavar elhárítását követően jegyzőkönyvet vesz fel az üzemzavar tényéről, az okozott kárról és az elhárítás módjáról és idejéről.

5. Melléklet

5.1. A szerverek leállítási sorrendje

Először a virtuális gépeket kell leállítani:

1. Alkalmazásszerverek (bv-app-2, bv-app-3, BV-SourceWeb, BV-WINSZOC)
2. Adatbázis szerverek (bv-db-1, bv-sourcedb)
3. Levelező szerverek (BV-EXCH-CAS16, BV-EXCH-CAS19)
4. Webszerverek (BV-WEBSERER-01, BV-INTRAWEB)
5. Fájlszerver (bv-fs-2016)
6. Egyéb virtuális szerverek (bv-app-4, bv-app-6, BV-CLOUD, BV-ECO-MAN, BV-ERA, BV-ICINGA, BV-NGINX-PROXY, BV-OVPN, BV-RDP, BV-SourceDev, IKER, PENZUGYC17)
7. Domén vezérlők (BV-INFRA-1, BV-INFRA-2)

Végül a fizikai gépeket kell leállítani:

Bv-clsn-1, Bv-clsn-2, bv-clsn-3, Bv-bck

5.2. A szerverek elindítási sorrendje

1. Fizikai szerverek Bv-clsn-2, bv-clsn-3, Bv-bck
2. Levelező szerverek (BV-EXCH-CAS16, BV-EXCH-CAS19)
3. Webszerverek (BV-WEBSERER-01, BV-INTRAWEB)
4. Adatbázis szerverek (bv-db-1, bv-sourcedb)
5. Fájlszerver (bv-fs-2016)
6. Alkalmazásszerverek (bv-app-2, bv-app-3, BV-SourceWeb, BV-WEBSERER-01, BV-INTRAWEB, BV-WINSZOC)
7. Egyéb virtuális szerverek (bv-app-4, bv-app-6, BV-INFRA-2 BV-CLOUD, BV-ECO-MAN, BV-ERA, BV-ICINGA, BV-NGINX-PROXY, BV-OVPN, BV-RDP, BV-SourceDev, IKER, PENZUGYC17)

MEGISMERÉSI ZÁRADÉK

Alulírott kijelentem, hogy a Budapest Főváros I. kerület Budavári Polgármesteri Hivatal Jegyzőjének a ...../2022. (.....) számú szabályzatát az Informatikai Katasztrófavédelmi tervről megismertem.

Tudomásul veszem, hogy az abban foglaltakat a munkám során köteles vagyok betartani.

Név	Beosztás	Dátum	Aláírás