BUDAPEST FŐVÁROS I. KERÜLET BUDAVÁRI POLGÁRMESTERI HIVATAL JEGYZŐJÉNEK
8/2024. (IV. 15.) SZÁMÚ UTASÍTÁSA

A BUDAPEST FŐVÁROS I. KERÜLET BUDAVÁRI POLGÁRMESTERI HIVATAL
ÜZLETMENET-FOLYTONOSSÁGI TERV SZABÁLYZATÁRÓL (BCP-v1)

BUDAVÁRI
POLGÁRMESTERI HIVATAL

Budapest 2024.

Dokumentum változáskövetés

Dátum	Verzió	A változás oka	A módosítást elvégezte
2023.06 hó	V1	2013. évi L. tv. és a 41/2015 BM rendelet miatti kialakítás	Ritek Zrt.
2024. 03-04. hó	V2	Egyeztetés a PH-val	Ritek Zrt.

Tartalom

I. Bevezetés

1. Budapest Főváros I. kerület Budavári Polgármesteri Hivatal (továbbiakban Hivatal) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban IBtv) valamint a végrehajtására kiadott, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló 41/2015. (VII.15.) BM rendelet (továbbiakban VHR), miatt létrehozza Budapest Főváros I. kerület Budavári Polgármesteri Hivatal **Üzletmenet-folytonossági Terv, Szabályzatát (BCP)** (továbbiakban: BCP Szabályzat), más szabályzatokkal összhangban.

2. A BCP Terv, Szabályzat célja a Hivatal által ellátott, kötelező, vagy önként vállalt önkormányzati, jegyző hatáskörébe utalt államigazgatási, valamint egyéb jogszabályokban meghatározott feladatok, ágazati jogszabályokban meghatározott kritikus időn belül történő ellátása, nem várt események vagy cselekmények esetén, helyettesítő eljárások alkalmazásával, az eredeti funkcionalitás helyreállításáig, a kritikus idők, a felelős személyek, tárgyak, eszközök, folyamatleírások biztosításával.

3. Ha a következő események (továbbiakban: **Katasztrófa)** valamelyike bekövetkezik és érinti a Hivatal működését, az szükségessé teszi a BCP Szabályzat Terv alkalmazását:

   a) **adatvédelmi incidens:** a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi; személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés;

   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) **fenyegetés:** olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;

   d) **incidens:** a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet szerint, „Internet biztonsági incidens minden olyan biztonsági esemény, amelynek célja az információs infrastruktúrák bizalmasságának, sértetlenségének vagy rendelkezésre állásának megsértése az interneten, mint nyílt információs infrastruktúrán keresztül."

   e) **rendkívüli esemény:** minden olyan esemény, amely Budapest Főváros I. kerület Budavári Polgármesteri Hivatal és intézményei tevékenységének folyamatosságát támogató informatikai rendszerek folyamatos, üzemzavar mentes működőképességét veszélyezteti, vagy akadályozza;

f) **részleges működőképesség:** az az állapot, amikor az informatikai architektúra valamely elemének meghibásodása miatt az informatikai rendszerek bizonyos funkciói, vagy egésze jelentős ideig működésképtelenné válnak. Ekkor a támogatott ügyviteli folyamatok egy részének informatikai támogatása még biztosított, más részük informatikai támogatásának helyreállítása jelentős időt vesz igénybe;

g) **teljes körű működésképtelenség:** az az állapot, amikor az informatikai architektúra valamely elemének meghibásodása miatt az informatikai rendszerek még a minimális, erősen korlátozott rendszer funkciókat sem tudják ellátni. A ügyviteli folyamatok többségének informatikai támogatása megszűnik, és ennek helyreállítása jelentős időt vesz igénybe;

h) **üzemzavar**: az az állapot, amikor az informatikai rendszerek működésében rövid idejű zavar keletkezik, s így a rendszer néhány funkciójának átmeneti meghibásodása következik be, a zavar elhárítását az Informatika Osztály a napi rutinja alapján a BCP életbe léptetésénél rövidebb idő alatt képes elvégezni.

4. A Hivatal jelen BCP Terv, Szabályzatban megfogalmazza, és az az alábbiakban részletezett követelmények szerint dokumentálja, valamint a Hivatalon belül kizárólag a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyek és szervezeti egységek számára kihirdeti az elektronikus információs rendszerekre vonatkozó üzletmenet-folytonossági tervet.

5. A BCP Terv, Szabályzat meghatározza az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket, a kapcsolódó Katasztrófa-elhárítási Kézikönyv Szabályzattal (DRP Terv, Szabályzat) összefüggésben rendelkezik a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről, valamint definiálja a szervezet által előzetesen meghatározott alapszolgáltatások fenntartásának menetét, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is.

6. A **jelen BCP Terv, Szabályzat része a Hivatal DRP Terv, Szabályzata**
Rendkívüli esemény bekövetkezése esetén életbe lépő alternatív, helyettesítő folyamatokat, a normál ügymenet visszaállításával kapcsolatos teendőket, valamint a megelőzéssel, felkészüléssel kapcsolatos feladatokat tartalmazó terv.

7. A BCP Terv, Szabályzatban meg kell határozni az elektronikus információs rendszer alapfunkcióit támogató kritikus rendszerelemeket is. A BCP Terv, Szabályzatban meg kell határozni, hogy az alapfunkciókat ellátó szervezetek az üzletmenet-folytonossági terv aktiválását követőn mennyi időn belül állíthatók fel.

8. A BCP Terv, Szabályzat meghatározza az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, biztosító infrastruktúra elemeket, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket, rendelkezik a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről.

II. Fogalmak a jelen BCP Szabályzat alkalmazásában

BCP (Business Continuity Plan = Üzletmenet Folytonossági Terv): Azon eljárások és forgatókönyvek kidolgozása, amelyekkel biztosítható, hogy a Hivatal működés szempontjából kritikus tevékenységei

minden körülmények között fenntarthatóak legyenek, illetve a meghatározott maximális kiesési időn belül helyreállíthatóak legyenek. Az üzletmenet folytonossági terv részét képezik az akciótervek, az általános feladatok meghatározása, valamint a felelősségi körök kialakítása.

DRP Terv Szabályzat gyakorlati tesztelése: Az informatikai katasztrófa-esemény bekövetkezésének szimulációs végrehajtási gyakorlata, a katasztrófa terv alkalmazásának részleges végrehajtása és dokumentálása;

katasztrófaterv (DRP): vészhelyzet vagy katasztrófa esetén megszakadt tevékenységek meghatározott időn belüli helyreállításához szükséges emberi, fizikai, műszaki és folyamat-erőforrások összessége

Minimális üzletmenet-folytonossági célkitűzés (MBCO): a hivatali szolgáltatásoknak az a minimális szintje, amely az üzletmenet-folytonosság megszakadása esetén elégséges a Hivatal alapfeladatainak és működésének ellátásához;

MTPD (Maximum Tolerable Period of Disruption): Maximálisan tolerálható megszakadási időtartam, az a legnagyobb idő intervallum, ameddig a szervezet tolerálni képes az általa nyújtandó szolgáltatás kiesését;

RPO (Recovery Point Objective): Helyreállítási pontérték, a maximálisan elfogadható adatvesztés vagy az a pont, amelyhez vissza kell állítani az információs rendszert, hogy az üzletmenetet folytatni lehessen;

RTO (Recovery Time Objective): helyreállítási idő célérték, az incidens bekövetkeztétől számított időpont, ameddig a szolgáltatást helyre kell állítani, az erőforrásokat vissza kell szerezni;

VKCS (Válságkezelő csoport): Azok, a Hivatal által delegált vezető kollégák, akiket a Jegyző a csoportba választ;

Hatóságok:

- a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 14. § (1) bekezdése szerinti hatóság,
- a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet GovCERT Kormányzati Eseménykezelő Központ,
- a Nemzeti Adatvédelmi és Információszabadság Hatóság

Fogalom	Jogforrás száma	Jogforrás neve
adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
adatállomány: az egy nyilvántartásban kezelt adatok összessége;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról

adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
adatfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel – az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
adatfeldolgozó: az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
adatfeldolgozó": az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
adatfelelős: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
adatgazda: annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
adatkezelés korlátozása: a tárolt adat zárolása az adat további kezelésének korlátozása céljából történő megjelölése útján;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
adatkezelés korlátozása": a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása,	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról

törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése		
adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
adatkezelés": a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
adatkezelő: az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
adatkezelő": az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet

és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;		
adatközlő: az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatot honlapon közzéteszi;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
adatmegsemmisítés: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
adatvédelmi incidens: az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
adatvédelmi incidens": a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
adminisztratív védelem: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
alapinfrastruktúra: az önkormányzati ASP rendszer működését biztosító adatközponti és hálózati informatikai infrastruktúra, valamint a szakrendszeri átjárhatóságot és a külső rendszerkapcsolatok kiépítésének lehetőségét biztosító integrációs platformszolgáltatás;	257/2016. (VIII. 31.) Korm. rendelet	önkormányzati ASP rendszerről
alapvető szolgáltatásokat nyújtó szolgáltató: a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról

2012. évi CLXVI. törvény 2/A. §-a alapján kijelölt szolgáltató		
alkalmazásüzemeltetés: az alkalmazások elérhetővé tétele és működtetése, jogosultságkezelés, hibakezelés; a rendszertámogatási szerződések megkötése;	257/2016. (VIII. 31.) Korm. rendelet	önkormányzati ASP rendszerről
álnevesítés: személyes adat olyan módon történő kezelése, amely - a személyes adattól elkülönítve tárolt - további információ felhasználása nélkül megállapíthatatlanná teszi, hogy a személyes adat mely érintettre vonatkozik, valamint műszaki és szervezési intézkedések megtételével biztosítja, hogy azt azonosított vagy azonosítható természetes személyhez ne lehessen kapcsolni;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
álnevesítés": a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
azonosítható természetes személy: az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
bejelentés-köteles szolgáltatás: az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 2. § j) pontjában meghatározott szolgáltatás	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
biometrikus adat: egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
biometrikus adat": egy természetes személy testi,	2016 / 679 Európai	Általános Adatvédelmi

fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat;	Parlament és a Tanács rendelete	Rendelet
bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
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;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
biztonsági osztályba sorolás: a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
biztonsági szint: a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
biztonsági szintbe sorolás: a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a	2011. évi CXII. törvény	az információs önrendelkezési jogról és az

büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;		információszabadságról
bűnüldözési célú adatkezelés: a jogszabályban meghatározott feladat- és hatáskörében a közrendet vagy a közbiztonságot fenyegető veszélyek megelőzésére vagy elhárítására, a bűnmegelőzésre, a bűnfelderítésre, a büntetőeljárás lefolytatására vagy ezen eljárásban való közreműködésre, a szabálysértések megelőzésére és felderítésére, valamint a szabálysértési eljárás lefolytatására vagy ezen eljárásban való közreműködésre, továbbá a büntetőeljárásban vagy szabálysértési eljárásban megállapított jogkövetkezmények végrehajtására irányuló tevékenységet folytató szerv vagy személy (a továbbiakban együtt: bűnüldözési adatkezelést folytató szerv) ezen tevékenység keretei között és céljából - ideértve az ezen tevékenységhez kapcsolódó személyes adatok levéltári, tudományos, statisztikai vagy történelmi célból történő kezelését is - (a továbbiakban együtt: bűnüldözési cél) végzett adatkezelése;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
címzett: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely részére személyes adatot az adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
címzett": az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
csatlakozás: a szolgáltatások tényleges használatának megkezdése;	257/2016. (VIII. 31.) Korm. rendelet	önkormányzati ASP rendszerről
egészségügyi adat: egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról

vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;		
egészségügyi adat": egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
EGT-állam: az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
EGT-állam: az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (a továbbiakban: Infotv.) meghatározott állam;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
elektronikus információs rendszer: a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat; b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
életciklus: az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
érintett hozzájárulása": az érintett akaratának	2016 / 679 Európai	Általános Adatvédelmi

önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;	Parlament és a Tanács rendelete	Rendelet
érintett: bármely információ alapján azonosított vagy azonosítható természetes személy	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
észlelés: a biztonsági esemény bekövetkezésének felismerése;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
felhasználó: egy adott elektronikus információs rendszert igénybe vevők köre;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
felügyeleti hatóság": egy tagállam által az 51. cikknek megfelelően létrehozott független közhatalmi szerv;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
genetikai adat": egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
globális kibertér: a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus

információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese;		információbiztonságáról
harmadik fél": az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
harmadik ország: minden olyan állam, amely nem EGT-állam;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
honvédelmi célú adatkezelés: a honvédségi adatkezelésről szóló törvény és a Magyarország területén szolgálati céllal tartózkodó külföldi fegyveres erők, valamint a Magyarország területén felállított nemzetközi katonai parancsnokságok és állományuk nyilvántartásáról szóló törvény hatálya alá tartozó adatkezelés;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
hozzájárulás: az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
információs társadalommal összefüggő szolgáltatás": az (EU) 2015/1535 európai parlamenti és tanácsi irányelv 1. cikke (1) bekezdésének b)	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet

pontja értelmében vett szolgáltatás;		
interfész: adatok automatizált módon, elektronikus úton történő átadását lehetővé tevő kapcsolódási felület;	257/2016. (VIII. 31.) Korm. rendelet	önkormányzati ASP rendszerről
IV.24. (1) Az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi.	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
képviselő": az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által a 27. cikk alapján írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez működtetéséhez;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
kibervédelem: a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
kockázatkezelés: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus

intézkedésrendszer kidolgozása;		információbiztonságáról
kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
korai figyelmeztetés: valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
közös adatkezelő: az az adatkezelő, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - az adatkezelés céljait és eszközeit egy vagy több másik adatkezelővel közösen határozza meg, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket egy vagy több másik adatkezelővel közösen hozza meg és hajtja végre vagy hajtatja végre az adatfeldolgozóval;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
központi szolgáltató: a NISZ Nemzeti Infokommunikációs Szolgáltató Zártkörűen Működő Részvénytársaság (a továbbiakban: NISZ Zrt.) és az IdomSoft Informatikai Zártkörűen Működő Részvénytársaság (a továbbiakban: IdomSoft Zrt.);	257/2016. (VIII. 31.) Korm. rendelet	önkormányzati ASP rendszerről
közvetett adattovábbítás: személyes adatnak valamely harmadik országban vagy nemzetközi	2011. évi CXII. törvény	az információs önrendelkezési jogról és az

szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére továbbítása útján valamely más harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére történő továbbítása;		információszabadságról
kritikus adat: az Infotv. szerinti személyes adat, különleges adat vagy valamely jogszabállyal védett adat	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
különleges adat: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok,	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
létfontosságú információs rendszerelem: az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
magyar kibertér: a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve Magyarország érintett benne;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
megelőzés: a fenyegetés hatása bekövetkezésének elkerülése;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
nemzetbiztonsági célú adatkezelés: a nemzetbiztonsági szolgálatok jogszabályban meghatározott feladat- és hatáskörében végzett adatkezelése, valamint a rendőrség terrorizmust elhárító szervének jogszabályban meghatározott	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról

feladat- és hatáskörében végzett, a nemzetbiztonsági szolgálatokról szóló törvény hatálya alá tartozó adatkezelése;		
nemzetközi szervezet: a nemzetközi közjog hatálya alá tartozó szervezet és annak alárendelt szervei, továbbá olyan egyéb szerv, amelyet két vagy több állam közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
nyilvántartási rendszer": a személyes adatok bármely módon - centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint - tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
önkormányzati ASP rendszer: a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény (a továbbiakban: Mötv.) 114. § (2) bekezdése szerinti, a helyi önkormányzatok feladatellátását támogató, számítástechnikai hálózaton keresztül távoli alkalmazásszolgáltatást (Application Service Provider, ASP) nyújtó elektronikus információs rendszer;	257/2016. (VIII. 31.) Korm. rendelet	önkormányzati ASP rendszerről
profilalkotás: személyes adat bármely olyan - automatizált módon történő - kezelése, amely az érintett személyes jellemzőinek, különösen a munkahelyi teljesítményéhez, gazdasági helyzetéhez, egészségi állapotához, személyes preferenciáihoz vagy érdeklődéséhez, megbízhatóságához, viselkedéséhez, tartózkodási helyéhez vagy mozgásához kapcsolódó jellemzőinek értékelésére, elemzésére vagy előrejelzésére irányul;	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
profilalkotás": személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
reagálás: a bekövetkezett biztonsági esemény	2013. évi L. törvény	az állami és önkormányzati

terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;		szervek elektronikus információbiztonságáról
releváns és megalapozott kifogás": a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy ezt a rendeletet megsértették-e, illetve hogy az adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a rendelettel; a kifogásban egyértelműen be kell mutatni a döntéstervezet által az érintettek alapvető jogaira és szabadságaira, valamint adott esetben a személyes adatok Unión belüli szabad áramlására jelentett kockázatok jelentőségét;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
rendszertámogatás: a fejlesztési időszakot követő hibajavítás, verziófrissítés, jogszabálykövetés;	257/2016. (VIII. 31.) Korm. rendelet	önkormányzati ASP rendszerről
sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
sérülékenység: az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
sérülékenységvizsgálat: az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
súlyos biztonsági esemény: olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben,	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról

alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek		
szakrendszer: az önkormányzati ASP rendszer által nyújtott, igazgatási feladatokat támogató szakalkalmazás;	257/2016. (VIII. 31.) Korm. rendelet	önkormányzati ASP rendszerről
számítógépes eseménykezelő központ: az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik [(európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)]	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
személyes adat: az érintettre vonatkozó bármely információ	2011. évi CXII. törvény	az információs önrendelkezési jogról és az információszabadságról
személyes adat": azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
személyes adatok határokon átnyúló adatkezelése": személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
szervezet: az adatkezelést végző, illetve az adatfeldolgozást végző vagy végeztető jogi személy vagy egyéni vállalkozó, valamint az üzemeltető	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról

teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
tevékenységi központ: a) az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő esetében az Unión belüli központi ügyvitelének helye, ha azonban a személyes adatok kezelésének céljaira és eszközeire vonatkozó döntéseket az adatkezelő egy Unión belüli másik tevékenységi helyén hozzák, és az utóbbi tevékenységi hely rendelkezik hatáskörrel az említett döntések végrehajtatására, az említett döntéseket meghozó tevékenységi helyet kell tevékenységi központnak tekinteni;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
ügyféltámogatás: a működéssel kapcsolatos felhasználói segítségkérelmek megválaszolása.	257/2016. (VIII. 31.) Korm. rendelet	önkormányzati ASP rendszerről
üzemeltető: az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
vállalkozás": gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
vállalkozáscsoport": az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások;	2016 / 679 Európai Parlament és a Tanács rendelete	Általános Adatvédelmi Rendelet
védelmi feladatok: megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
zárt célú elektronikus információs rendszer: a nemzetbiztonsági, honvédelmi, rendészeti, diplomáciai információs feladatok ellátását biztosító, rendeltetése szerint elkülönült elektronikus információs rendszer, amely kizárólagosan a speciális igények kielégítését, az e célra létrehozott szervezet és technika működését szolgálja;	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról
zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem.	2013. évi L. törvény	az állami és önkormányzati szervek elektronikus információbiztonságáról

III. A Szabályzat hatályai.

A Szabályzat személyi, tárgyi és területi hatálya megegyezik a Hivatal Informatikai Biztonsági Szabályzat hatályával.

IV. A Szabályzat felülvizsgálata

1. Jelen Szabályzatot felül kell vizsgálni:
   a) ha a Szabályzat tárgyi, területi vagy személyi hatályában változás történik,
   b) ha jogszabály vagy jogszabályváltozás előírja,
   c) ha a hivatali szervezetben, biztonsági besorolásban vagy a belső szabályozókban olyan változás történik, amely kihatással van a Szabályzat tartalmára,
   d) ha olyan technológia-változás történik, amely azt indokolja,
   e) ha a személyi hatályban érintettektől módosítási javaslat érkezik,
   f) a fentiektől függetlenül legalább évente

2. A Szabályzat frissítése, módosítása

a) Amennyiben a belső és / vagy külső felülvizsgálat indokolja, akkor a Szabályzatot módosítani vagy frissíteni kell.

b) A kockázatelemzést minden olyan esetben meg kell ismételni, amikor változás áll be az elektronikus információs rendszerben vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését), továbbá olyan körülmények esetén, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát, különösen: a védendő értékekben változás történik; a fenyegetettségben jelentős változás áll be; jogszabály vagy jogszabályváltozás előírja.

c) Jelen Szabályzat módosításával kapcsolatos javaslattételre jogosult minden érintett, aki jelen Szabályzat személyi hatálya alá tartozik. A javaslattételt írásban, indokolással kiegészítve a szervezeti egység vezetők teszik meg az Üzemeltetési és Informatikai Csoportvezetőnek, aki a javaslattételt megvizsgálja információbiztonsági, technikai kivitelezhetőségi, költségráfordítási (beleértve a humán erőforrás-ráfordítás tervezett költségét is) szempontból, és a javaslatot döntés-előkészítési javaslat formájában Jegyző elé tárja, aki dönt a Szabályzat módosításáról vagy annak elvetéséről.

d) A frissítéseket, módosításokat dokumentáltan, változáskövetéssel, vagy módosító Szabályzat esetén egységes szerkezetre alakítással kell elvégezni. A dokumentálásnak tartalmaznia kell a módosító személy nevét, a módosítás időpontját, a módosítás okát, a folytonosan növelt verziószámot.

e) A módosítás minden esetben tartalmazza a hatályba lépés időpontját.

V. A Szabályzat megismerése, kihirdetése

1. A Szabályzatot kizárólag azok a személyek ismerhetik meg, akiknek a körét a jegyző jóváhagyta.
2. Tilos a Szabályzatot publikus felületen közzétenni vagy harmadik személy által hozzáférhetővé tenni.

3. A Szabályzat Jegyző aláírásával és bélyegzőlenyomatával hitelesített papír alapú dokumentum képként történő beszkennelése során keletkező Portable Document Format (PDF vagy CPDF) formátumú és a módosítható állományt kizárólag az Üzemeltetési és Informatikai Csoportvezető tárolhatja olyan jogosultsággal, hogy módosítási joga a dokumentumon másnak nem lehet. A dokumentum digitális aláírással is hitelesíthető, melynek tárolása szintén az Üzemeltetési és Informatikai Csoportvezető feladata.
4. A Szabályzat végleges, legutolsó verziójú, módosítható szövegszerkesztő állományát adathordozón az Informatika páncélszekrényeiben is tárolni kell.
5. A Szabályzat tartalmának ismertetése – különösen a biztonság tudatos képzés és a feladat alapú biztonsági képzés – a Szabályzat alanyi hatálya alá tartozó természetes és jogi személyek képviselőinek számára az **Informatikai biztonsági képzési Eljárásrend** tárgyú utasítás szerint történik.

VI. Kapcsolódó jogszabályok, szabályzatok, eljárásrendek, dokumentumok

1. a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló az EU Parlament és Tanács 2016/679. számú Rendelete (GDPR),
2. a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló EU Parlament és a Tanács 910/2014/EU Rendelete,
3. az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infó tv.),
4. az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény,
5. az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény,
6. az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet ,
7. az elektronikus ügyintézés részletszabályairól szóló 451/2016 (XII.19.) Kormány rendelet,
8. a Kormányzati Adatközpont működéséről szóló 467/2017. (XII. 28.) Korm. rendelet,
9. az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról szóló 466/2017. (XII. 28.) Korm. rendelet

10. Budapest Főváros I. kerület Budavári Polgármesteri Hivatalnak:

    a) Informatikai Biztonsági Szabályzata,
    b) Informatikai Kockázatelemzési és -kezelési Szabályzata
    c) Informatikai Katasztrófa-elhárítási Terv, Szabályzata (DRP),
    d) Informatikai Felhasználói Szabályzat,
    e) Adatvédelmi és adatbiztonsági Szabályzata,
    f) Külsős vállalkozók és hatóságok Jegyzéke,
    g) Információátadási Szabályzata,
    h) Tűz- és munkavédelmi Szabályzata,
    i) Alkalmazáskatalógusa (meglévő alkalmazásokról, külső és belső üzemeltetésről),
    j) Infrastruktúra terve (hálózati leírás),

k) Képzési terve,

VII. Felkészülés katasztrófa helyzetekre és rendkívüli eseményekre.

1 **Releváns információk.**

A normális ügymenet folytatásakor alapvető felkészülést biztosít a Hivatal következő funkcionális al-szervezeteinek a folyamatos együttműködése, az üzletmenet-folytonosság és a lehetséges kockázatok szempontjából releváns információk al-szervezetek közötti megosztása.

2 **A folyamatosan együttműködő vezetők, al-szervezetek és vezetőik:**

a) A Jegyző;
b) A Hivatal szervezeti egységek vezetői;
c) Az Üzemeltetési és Informatikai Csoport dolgozói;
d) A Személyzeti dolgozók;
e) Az Informatikai biztonságért felelős személy;
f) A Közterület-felügyeleti Iroda vezetője, mint a portaszolgálat irányítója.

3 **A BCP Terv, Szabályzat funkcionális célja:**

A Hivatal egy rendkívüli esemény, katasztrófa, üzemzavar bekövetkeztekor megoldást találjon, mind a minimális szolgáltatás folyamatos biztosítására, mind a katasztrófa elhárítására.

4 **A Hivatal funkcionális együttműködésének szervezeti ábrázolása**

5 **A hivatali felkészülés**

Egy folyamatosan működő modell, amelyben a felelős személyek kötelesek:

a) a változó környezetben azonosítani a Hivatal ügyviteli, informatikai, emberi erőforrásai és tárgyi eszközeinek kritikus elemeit;
b) a tapasztalatokat kiértékelni;
c) indokolt esetben a szervezeti működésben, a szabályozó eljárásokban módosítást végrehajtani.

6 **A Hivatal kockázatelemzést folytat**

Az Informatikai Kockázatelemzési és -Kezelési Szabályzata szerint, hogy az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése megtörténjen.

7 **Kiemelt DRP kulcsfelhasználók**

A Hivatal vezetői kötelesek összeállítani a **Kiemelt DRP kulcsfelhasználók személyi** állományáról készített kimutatást és erről őket tájékoztatni. A Jegyző kötelezi a Hivatal szervezeti egységek vezetőit, hogy a saját és a Kiemelt DRP kulcsfelhasználók **távközlési elérhetőségekről** folyamatosan tájékoztassák őt és az Informatikai biztonságért felelős személyt. A vezetők és a Kiemelt DRP felhasználók személyi állományát Budapest Főváros I. kerület Budavári Polgármesteri Hivatal **ezen szabályzatának melléklete tartalmazza.**

8 **Riasztó-értesítő szolgálat**

A VKCS tagjai kötelesek kidolgozni a DRP Szabályzat végrehajtásában érintett **riasztó-értesítő szolgálat** leghatékonyabb módszerét és alkalmazási feltételeit. A vezetők és a Kiemelt DRP felhasználók személyi állományát Budapest Főváros I. kerület Budavári Polgármesteri Hivatal **ezen szabályzatának melléklete tartalmazza.**

9 **Áttelepülés**

A riasztó-értesítő szolgálaton keresztül vezetékes telefon, mobil telefon, elektronikus levél, személyes megkeresés módszerével a Hivatal szervezeti egységek egyes vezetői az Üzemeltetési és Informatikai Csoport vezetőjének szervezésében megkezdik és végrehajtják:

- a VKCS tagjainak,
- az informatikai üzemeltetőknek és
- a DRP Kiemelt felhasználók áttelepítésének megszervezését a tartalék oldalra.

10 **Irodaszerek**

Az Üzemeltetési és Informatikai Csoport vezetőjének gondoskodnia kell tartalék irodaszerekről, nyomtató papírról vagy azok ellátásának katasztrófa esetére való megszervezéséről.

11 **A kritikus jellegű elektronikus informatikai rendszerek meghatározása**

A belső audit és a folyamatos ellenőrzések tapasztalatai alapján, amelyet a Jegyző az Informatikai Kockázatelemzési és -kezelési Szabályzata elfogadott, a következők:

- Áramellátás
- Internet kapcsolat
- Külső és belső tűzfal rendszer
- Mentés
- Hálózati eszközök
- Szerverek
- Háttértárolók
- Adatbázisok és a kezelésükhöz szükséges szoftverek

12 **A tartalék eszközökre történő átállás**

A tartalék eszközökre történő átállás, valamint a normál, illetve a normál ügymenetre történő visszaállás elengedhetetlen feltétele a megfelelő, ellenőrzötten visszatölthető mentések rendelkezésre állása. Ezért különös figyelmet kell fordítani a kritikus folyamatokat minimális szinten támogató informatikai rendszereknek – az IBSZ mentési rendre vonatkozó fejezeteinek megfelelő módon és gyakorisággal történő – mentésére, valamint a mentések – szintén az IBSZ mentési rendre vonatkozó fejezeteiben szabályozott módon – megfelelő tárolására mind a normál ügymenet során, mind a katasztrófahelyzet alatt. Annak érdekében, hogy a kritikus folyamatok működtetése szempontjából kritikus rendszerek/alkalmazások minél előbb működésképes állapotba kerüljenek, a Hivatalnak szüksége van bizonyos tartalékokra. Az Informatikai biztonságért felelős személynek össze kell állíttatnia a szükséges **informatikai hideg**

tartalékok körét és a rendelkezésre állítását biztosítani kell.

13 **Tartalék helyszín**

A Hivatal az üzletmenet-folytonosság érdekében **tartalék helyszínnel rendelkezik katasztrófa helyzet esetére. A Hivatal tartalék feldolgozási helyszíne (DR-SITE):** a Hivatal eltérő címen lévő telephelye, ahol a szolgáltatások mindegyike – az NTG csatlakozási pont nem feltétlen biztosítása mellett - rendelkezésre állnak, nem feltétlenül ugyanakkora sebességgel, mint alap üzemmódban:

a) **a fő feldolgozási helyszín**: 1014 Budapest, Kapisztrán tér 1.
b) **a tartalék feldolgozási helyszín:** 1014 Budapest, Úri utca 58.

14 **A szoftver telepítő készletek**

A szoftver telepítő készletek és az ehhez szükséges dokumentációk rendelkezésre állásának előzetes biztosítása szükséges, továbbá:

a) A felhasználói alkalmazások és a futtatásukhoz szükséges rendszerkomponensek, licenc jogosultságok (operációs rendszerek, adatbázis kezelők, irodai alkalmazások) aktuális telepítő készleteit a fő és a tartalék helyszínek üzemeltetői helyiségeiben a rendszer dokumentációkkal együtt kell elhelyezni.

b) A kritikus felhasználói alkalmazások komponenseihez kapcsolódó fejlesztői-, üzemeltetői- és karbantartási dokumentációkat kinyomtatva mindkét oldalon az üzemeltetői szobában biztonságos helyen kell tárolni.

c) Minden szervezeti egységnek rendelkezni kell, illetve a tartalék munkavégzési helyszíneken is el kell helyezni egy iktatókönyvet, melyet az iktatórendszer rövidebb idejű kiesése esetén is használni kell.

15 **Harmadik féllel kötött szerződés**

A BCP Terv, Szabályzat **hatálya nem terjedhet ki** a nem a Hivatal üzemeltetésében lévő informatikai infrastruktúra katasztrófa elhárítására és rendkívüli események kezelésére, továbbá a külső support szolgáltatással kapcsolatos tevékenységére, az informatikai szolgáltatást végző **harmadik féllel kötött szerződésben** kell ezeket a feladatokat szabályozni.

16 **Képzések a felhasználók részére**

Önállóan az **Informatika az üzemeltetési tapasztalatok alapján rendszeres képzést** szervez meg valamely felhasználói alkalmazás vagy más informatikai területtel kapcsolatos használati vagy biztonsági ismeretek bővítésére, felfrissítésére, végül **biztonsági tudatosság fokozása érdekében.** Az oktatást a felhasználók részére az Informatikai Biztonsági Felelős tartja meg.

a) Informatikai biztonsági képzésen minden ügyintézőnek részt kell vennie **évente legalább egy alkalommal.**

b) Az újonnan belépett vagy tartós távollétből visszatérő felhasználók esetén soron kívüli képzést kell tartani.

c) Amennyiben olyan mértékű biztonsági kockázat vagy változás történik az információs rendszerekkel összefüggésben, hogy az indokol soron kívüli képzést, akkor az Informatikai

Csoport értesíti a képzésért felelős szervezeti egységet, aki megszervezi a felmerült biztonsági eseménnyel kapcsolatos képzést minden érintett ügyintéző számára.

17 DRP Terv Szabályzat gyakorlat

A jövőbeni katasztrófa helyzetekre és rendkívüli eseményekre történő felkészülés fontos eleme **DRP Terv Szabályzat gyakorlati rendszeres tesztelése:**

a) A DRP Szabályzatot legalább évente, de minden a szabályzat személyi vagy tárgyi hatályában, illetve a Hivatal feladatköreiben történő változások, vagy tényleges katasztrófa-esemény bekövetkezését követően felül kell vizsgálni és tesztelni kell.

b) A tesztelést követően az Informatikai biztonságért felelős személynek az üzemeltetők és a Hivatal vezetőinek jelentései alapján kiértékelést kell végezni.

c) A katasztrófa-elhárítási tervet a tartalék feldolgozási helyszínen is tesztelni kell, hogy a hivatali szervezet megismerje az adottságokat, és az elérhető erőforrásokat, valamint értékelje a tartalék feldolgozási helyszín képességeit a fő helyszín megsemmisülése vagy a helyreállítás tartós elhúzódásának, valamint az informatikai infrastruktúra végleges elköltöztetése esetére.

d) A felülvizsgálat vagy a tesztesetek eredménye alapján meghatározott változásokat változáskövetéssel, verziózással, dokumentáltan át kell vezetni.

e) Az elektronikus információs rendszer vagy a működtetési környezet változásainak, a katasztrófa-elhárítási terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálni, javítani kell a DRP Szabályzatot.

VIII. Munkafolyamatok Katasztrófa esetén és az üzletmenet-folytonosság biztosítása.

1 A cél megfogalmazása

Az üzletmenet-folytonosság biztosítása térben és időben változó bonyolult folyamat, amely hatékony működése esetén a változó eseményekre, kihívásokra minél gyorsabb szervezeti válaszokat képes adni.

2 Biztonsági mentések

A Hivatal **napi, heti és éves biztonsági mentéseket végez**, az elektronikus információs rendszer mentéseinek másodlatát az elsődleges helyszínnel azonos módon biztosítja a DR Site, tartalék oldalon (1014 Budapest, Úri utca 58.)

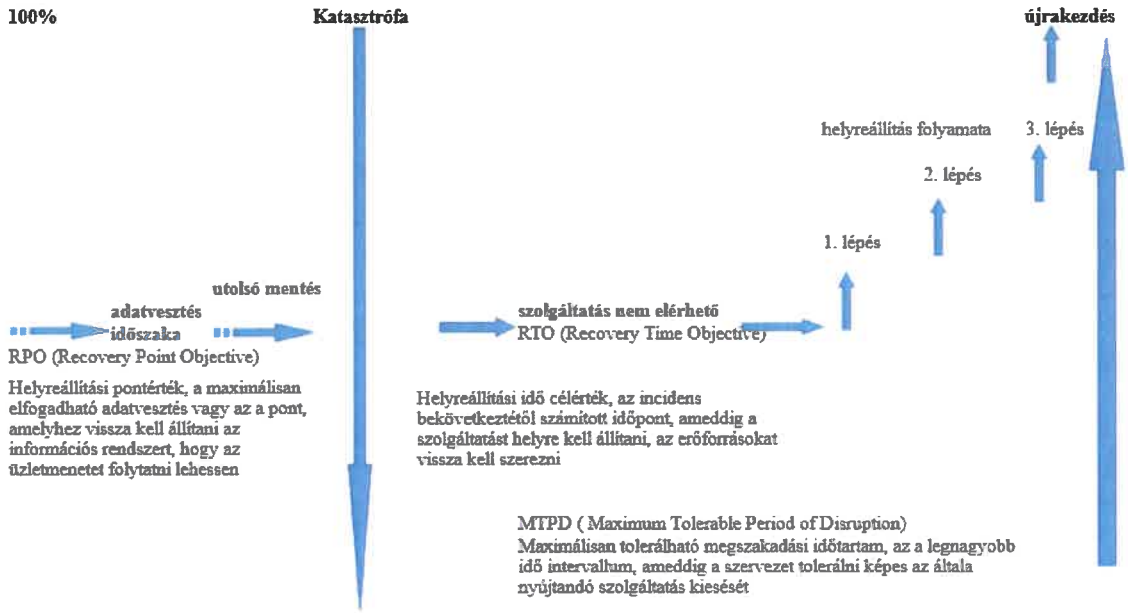
3 Folyamatok

A Katasztrófa esetén a következő folyamat szakaszokat kell betartani:

a) A Katasztrófa bejelentése;
b) A Katasztrófa és a válasz reakciók naplózása;
c) A Katasztrófa elemzése, a szükséges intézkedések meghozatala;
d) A Katasztrófa bekövetkezésével kapcsolatos kommunikáció;
e) Helyreállítás, a helyreállítási sorrend megállapítása;
f) A helyreállítás dokumentálása;
g) Kárfelmérés,

h) Események lezárása, kiértékelése.

4 A válságkezelés ábrázolása:



5 Ibf. Javaslat.

Ha az Informatikai biztonságért felelős személy a katasztrófa helyzetnek értékeli a bekövetkezett rendkívüli eseményt, akkor erre vonatkozó **döntési javaslatot** tesz a Jegyző számára.

6 Korai figyelmeztetés lehetősége

A Hivatal az Informatikai Kockázatelemzési és -Kezelési Szabályzat, továbbá a Elektronikus Információs Rendszerei és biztonsági kockázataik, fenyegetettségük és a biztonsági osztályba sorolásukról szóló Szabályzat tartalma, valamint a külső környezetben és / vagy a hivatali változások; azaz gondot okozó, figyelemre méltó jelenség (Issue) felismerése esetén az **Informatikai biztonságért felelős személy ún. Korai figyelmeztetés** kiadására jogosult, ha valamely fenyegetés várható bekövetkezésének bekövetkezése várható, a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni.

7 A Jegyző jogosultságai

a) **a katasztrófa helyzet kihirdetésére;**
b) jogosult elrendelni - az üzletmenet-folytonosság biztosítása érdekében - a tartalék feldolgozási helyszín és az ott telepített eszközök használatba vételét, a szervezeti feladatok területi ellátásának átszervezését (diszlokálás);
c) kijelöli a Hivatal szervezeti egységek azon vezetőit, akik a katasztrófa elhárítás megszervezésében az általa megbízott feladatokkal rendelkeznek, a probléma megoldásokra vonatkozó javaslat megtételére alkalmasak lehetnek, az üzletmenet folytonosság biztosításában kiemelt szervező feladatuk lehet,
d) kijelölheti a DRP Kiemelt felhasználókon kívüli munkavállalók feladatát,
e) kihirdetni a katasztrófa helyzet végét a sikeres helyreállítás és annak tesztjeit követően;
f) a Hivatal munkatársainak ezt követően a **DRP Terv Szabályzatban foglaltaknak megfelelően kell a munkájukat végezniük.**

8 **Minimális üzletmenet-folytonossági célkitűzés**

A Jegyző jogosult az Informatikai biztonságért felelős személy által ismertetett kárfelmérés eredményének megfelelően **meghatározni a Minimális üzletmenet-folytonossági célkitűzést**, tehát a még biztosítandó és elérhető szolgáltatások körét, amelyek a következők lehetnek:

a) Pénzügyi szolgáltatások, a banki rendszeren a megbízások felvitele és rögzítése, banki átutalások kezdeményezése, a bankszámlák feletti rendelkezési joggyakorlás, a készpénzforgalom pénztári biztosítása.

b) Az e-Szignó program használata, az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény és az Európai parlament és a Tanács 910/2014/EU rendelete (eIDAS-rendelet) által előírtaknak megfelelően.

c) Iktató és iratkezelő rendszer működtetése.

d) Szakirodai ügyfélszolgáltatások biztosítása.

e) PTR - Pénzbeli és Természetbeni Ellátások Rendszerének - elérhetősége és használata.

9 **Helyzetértékelés**

A VKCS meghatározza a helyzetértékelésnek megfelelően:

a) az átmenetileg alkalmazandó ügyviteli, informatikai módszereket,
b) a dokumentálási feladatokat,
c) a tartalék hardver és szoftver eszközök használatát,
d) a feladatok prioritását és ezeket egyezteti az érintettekkel.

10 **A VKCS szerepe a Minimális üzletmenet-folytonosságban**

A VKCS tagjainak biztosítania kell a Minimális üzletmenet-folytonosság érdekében, katasztrófa helyzet esetén az adott tartalék feldolgozási helyszínen:

a) a Hivatal pénztárának működését,
b) a külön ügyfélszolgálati helyiség, helyiségek működését,
c) a katasztrófa helyzet súlyának megfelelő és még biztosítható hivatali szolgáltatások elérhetőségét.

11 **A tartalék feldolgozási helyszín állapota**

A VKCS tagjainak előzetesen gondoskodnia kell, hogy a Hivatal működtetésével összhangban **a tartalék feldolgozási helyszín kialakításánál** az IBSZ-el összhangban, a következő szempontokat a Hivatal munkatársai vegyék figyelembe:

a) a tartalék feldolgozási helyszínre való belépés naplózható legyen (például a kulcsfelvételnél);
b) a statikai követelmények biztonságos teljesítése kötelező (várható maximális födémterhelés, eszközök száma, azok várható súlyának figyelembe vétele);
c) minden munkaállomás csatlakozzon a Hivatal elektromos hálózatára, legyen a számítógép(ek) üzemeltetéséhez megfelelő számú elektromos aljzat és az elektromos hálózat teherbírása haladja meg a számítógép(ek) teljesítményét;
d) a környezetből adódó rezgések, környezeti zavarok kizárása (pl. nagy-frekvenciás hálózat);
e) a szünetmentes tápellátást biztosítása kell;
f) törekedni kell arra, hogy a szerverterem ajtói rendelkezzenek legalább 30 perces (műszakilag bizonylatolt) tűzállósággal;

g) legyen a szerverteremben nem vizes tűzoltó berendezés;
h) törekedni kell arra, hogy a géptermen belül automatikus betörés- és tűzjelző rendszert kell telepíteni, ami mozgás-, nyitás-, füst-, üvegtörés és vízérzékelőkkel rendelkezzen; az érzékelők és a jeleket feldolgozó központ feleljen meg az MSZ 9785, valamint az EN 54 szabványsorozatok előírásainak, rendelkezzenek a hazai minősítő intézetek forgalombahozatali engedélyével;
i) törekedni kell a szerverteremben az ablakok elfalazásáról, de ha ablakok mégis megmaradnak, akkor azokon legyen belülről átlátszó fólia;
j) a szerverteremben a padlóburkolatok, berendezési tárgyak tűzálló és antisztatikus anyagból legyenek;
k) az épület villámvédelme elégítse ki a kommunális- és lakóépületekre vonatkozó előírásokat; az MSZ 274-5T:1993 szabvány szerint az LPZ 0B - LPZ 1 zónahatáron túlfeszültség elleni védelembe be kell vonni az árnyékolást megtestesítő, a helységhez tartozó összes fémszerkezetet (az elektromos hálózatot, víz, gáz, távfűtés, csatornahálózatokat, antenna bevezetéseket, adatátviteli és távbeszélő hálózatokat stb.);
l) legyen kialakítva külön szerver szoba és külön operátor szoba;
m) csatlakozzon a Hivatal telefon alközpontjához és legyen legalább egy telefon végpont;
n) legyen alternatív internet kapcsolat, melyet a Hivatal a DRP ideje alatt használni tud.

12 **A DRP Kiemelt kulcsfelhasználók feladata**

A **DRP Kiemelt kulcsfelhasználók** kötelesek minél rövidebb időn belül a tartalék oldalon megkezdeni a **hideg tartalék eszközök működésének ellenőrzését**, a használatra való alkalmasság egyszerű ellenőrzését, a belépési jogosultságuk érvényesíthetőségét.

13 **Külső és belső kommunikáció.**

a) A VKCS tagjai közé tartozó Kommunikációs vezető jogosult kizárólagosan az incidensek külső személyek, szervezetek felé történő kommunikálására, nyilatkozat tételére.
b) A nyilatkozatot a hivatali honlapon is meg kell jelentetni.
c) Amennyiben a rendkívüli esemény olyan horderejű, hogy a sajtó érdeklődésére számot tarthat, a Kommunikációs vezetőnek fel kell készülni a tájékoztatásra, továbbá az MTI felé történő kommunikációra.
d) A rendkívüli eseményekkel kapcsolatos közlemények elkészítését, a tájékoztatás szervezését a Kommunikációs vezető végzi, szükség szerint a nyilatkozatot összehangolva az érintett kormányzati szervvel.
e) A rendkívüli eseménnyel kapcsolatban, a média megkeresése esetén a Kommunikációs vezető nyilatkozik.
f) A Hivatal többi munkatársa a rendkívüli eseményekkel kapcsolatban nem nyilatkozhat, megkeresése estén a sajtót a Kommunikációs vezetőhöz irányítja.
g) Az informatikai rendszerben történő kár jellegétől függően a VKCS tagjai és az általuk megbízott személyek alternatív kommunikációs eszközöket használhatnak a felügyeleti hatóságok, az **egészségügyi, katasztrófa segélyhívások** és a Hivatal dolgozói közötti kommunikáció végrehajtására vonatkozóan.
h) A VKCS tagjainak értesíteni kell az informatikai rendszerben történő kár jellegétől függően az esetleges **külső üzemeltetőket, az informatikai eszköz szállítóit,** a külső support szolgáltatás szolgáltatóit.
i) Az Ibf-nek értesíteni kell az informatikai rendszerben történő kár jellegétől függően **az Ibtv. 14. § (1) bekezdése szerinti szervezeteket:**
   - **a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézetet**
   - **a Nemzeti Adatvédelmi és Információszabadság Hatóságot, valamint**

- **a Hivatallal szerződésben álló szervezeteket, amelyek érintettek a káreseményben.**

j) A GDPR Preambulum 86. bekezdése alapján a VKCS tagjainak értesíteni kell az érintettet az adatkezelő indokolatlan késedelem nélkül tájékoztatja, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, annak érdekében, hogy megtehesse a szükséges óvintézkedéseket. Az tájékoztatásnak tartalmaznia kell annak leírását, hogy milyen jellegű az adatvédelmi incidens, valamint az érintett a természetes személynek szóló, a lehetséges hátrányos hatások enyhítését célzó javaslatokat.

14 **Az üzletmenet-folytonosság helyreállítási lépései.**

Jelen Szabályzat szerint a helyreállítás sorrendje fő szabályként a következő:

a) IT alapinfrastruktúra,
b) Iratkezelő rendszer
c) Ügyviteli rendszer

15 **Pénzügyi források**

Amennyiben az üzletmenet-folytonosság biztosításához egyéb infrastruktúra szükséges, a Jegyző elrendeli az infrastruktúra kialakításához **szükséges forrás** felszabadítását, valamint az infrastruktúra biztosításáért (pl. áramellátás, épület, személyi védelem, stb.) felelős személyek rendkívüli munkavégzését.

16 **Dokumentálási kötelesség-**

A normál működés helyreállításához szükséges folyamat lépéseit is részletesen **dokumentálni kell**, hogy pontosan nyomon követhető legyen a rendszerek állapota.

17 **Az Informatikai üzemeltetők kötelességei:**

a) az Informatikai biztonságért felelős személy által kiadott Munkaállomás telepítési kézikönyv tartalmának megfelelően, a tartalék kliens számítógépek, munkaállomások működésének ellenőrzését elvégzik,
b) a katasztrófa helyzetnek megfelelően munkavégzésre kötelesek a normál üzemeltetés helyreállítása érdekében,
a) a Kiemelt DRP felhasználók felhasználói profiljának a külön-külön történő beállítását megcsinálják, a beállításokat ellenőrzik,
a) elvégzik a legfontosabb felhasználói típusú profil beállításokat, külső közös üzemeltetési eléréseket el kell végezni a hideg tartalékban levő gépeken,
c) ellátják a tartalék helyszínen a végpontok hálózatba való bekötését,
d) rendszeresen jelzik az Informatikai Csoport vezetőjének az általuk tapasztalt műszaki állapotot,
e) az Informatikai biztonságért felelős személy által meghatározott kiemelt prioritást élvező szoftverek telepítését elvégzik, munkájukat dokumentálják,
f) szükség esetén az alapbeállításra (BIOS; IP cím) a Kliens operációs rendszer, irodai szoftver csomag, a tartalék munkavégzéshez szükséges kliens web alkalmazás elérhetőségének a telepítését, valamint a vírusvédelemről való gondoskodnak,
g) a Kiemelt DRP kulcsfelhasználókkal történő aktív együttműködésre kötelesek.

18 **Kárfelmérés.**

Amennyiben a rendkívüli esemény bekövetkezéséből kár keletkezett, akkor – a további károk keletkezését megelőző akciók elvégzése után – a VKCS-nak meg kell határozni annak a mértékét, majd részletes tervezés után meg kell kezdeni a kárelhárítást.

19 A Katasztrófa VKCS általi kiértékelése

A Katasztrófa kezeléséről szóló jelentésnek tartalmaznia kell:

a) a rendkívüli esemény észlelőjének nevét;
b) a rendkívüli esemény fogadójának nevét és a fogadás idejét;
c) mentők és tűzoltók értesítésének idejét (ha szükséges volt);
d) azon információk felsorolását, amely alapján a Jegyző értesítve lett;
e) a Jegyző és az Informatikai biztonságért felelős személy értesítésének és megérkezésének időpontját;
f) az Informatikai biztonságért felelős személy, kárfelmérése során tapasztaltak felsorolását;
g) az Informatikai biztonságért felelős személy, további károk megakadályozására tett utasításokat, azok időpontját és a végrehajtóját;
h) a katasztrófa helyzet kihirdetésének időpontját;
i) a károk okainak megszüntetésének időpontját (fixált helyzet) és a helyreállítás megkezdésének időpontját;
j) a helyreállítás konkrét lépéseit és időpontjait;
k) a katasztrófa helyzet megszüntetésének időpontját;
l) a fennmaradó (BCP keretében kezelendő) rendszerhibák listáját és elhárításuk várható időpontját;
m) a helyreállítás anyagi vonzatait (beszerzések, vállalkozói költségek) tételesen felsorolva.

IX. A Szabályzat hatályba lépése.

Jelen BCP Terv, Szabályzat 2024. április 18. napján lép hatályba, ezzel egyidejűleg a Budapest Főváros I. Kerület Budavári Polgármesteri Hivatal Működés-folytonossági Szabályzatáról szóló 34/2022. (XII. 21.) jegyzői utasítás hatályát veszti.

Budapest, 2024. április 15.

Budapest Főváros I. ker. Budavári Polgármesteri Hivatal Jegyző

Czukkerné Dr. Pintér Erzsébet
jegyző

DRP ÉRTESÍTÉSI LISTA

Név	Beosztás	Elérhetőség