BUDAPESTI CORVINUS EGYETEM	**VEZETŐI BIZOTTSÁGI RENDELKEZÉS**	**1/2024.** Verziószám: **00.**

INFORMATIKAI MŰKÖDÉSFOLYTONOSSÁGI ÉS KATASZTRÓFAELHÁRÍTÁSI TERV

Szakmai felelős:	**Sopronyi Tibor**	IT vezető
Szakmai ellenőrző:	**Locsmándi Balázs**	adatvédelmi felelős
Jogi ellenőrző:	**Borbás Zsuzsanna**	gazdasági jogi, beszerzési, munkajogi vezető
Döntéshozó:	**Vezetői Bizottság**	
Szerkesztésért és közzétételért felelős:	**Erős Anikó**	felsőoktatási szakértő

Verziószám	**Közzététel dátuma**	**Hatálybalépés dátuma**	**Verziókövetés**
00.	2024. 10. 01.	2024. 10. 01.	**Közzététel** VB-8/2024. (IX. 30.). sz. határozat

Tartalomjegyzék

A rendelkezés célja 3
A rendelkezés hatálya 3
Fogalmak 3
A rendelkezés tartalma 4
Kapcsolódó szabályzatok, dokumentumok 4
A rendelkezés karbantartása 4
A rendelkezés tesztelése 5
A kommunikáció útvonala 5
Informatikai rendszerek osztályozása 5
Az IT szolgáltatásfolytonosságot biztosító alapvető elemek 7
Incidens esetén alkalmazandó intézkedések 8
Záró rendelkezések 9

A rendelkezés célja

1. §

(1) Az IT szolgáltatás folytonossági terv célja, hogy definiálja az esetleges informatikai jellegű katasztrófahelyzetet okozó kockázatokat, azok kezelésének elemeit és lépéseit, annak érdekében, hogy biztosítva legyen a Budapesti Corvinus Egyetem (továbbiakban: Egyetem) informatikai/információs rendszereinek folyamatos rendelkezésre állása.

(2) Az Egyetem folyamatos ügymenetének szempontjából alapvető cél, hogy a meghatározó jelentőségű informatikai erőforrások/funkciók kiesése – úgynevezett informatikai katasztrófa helyzet (továbbiakban: informatikai katasztrófa helyzet vagy incidens) – esetén az IT szolgáltatások mielőbbi helyreállítása megtörténjen, akár megkerülő megoldások igénybevételével, de mindenképpen az egyes szakterületi adat- és folyamatgazdák által elvárt időn belül.

(3) A rendelkezés meghatározza egyrészről a normál működési rend során elvégzendő felkészülési feladatokat, azokat a felmérési, tervezési, ellenőrzési és javítási feladatokat, melyek biztosítják, hogy egy esetleges katasztrófa helyzetet követően a normál működés mielőbb helyreálljon. Másrészről meghatározza a helyreállítás személyi és tárgyi feltételeit.

(4) A dokumentum segítségével az informatikai katasztrófa helyzet bekövetkezése esetén az Informatika:

- képes a gyors és koordinált reagálásra, a károk felmérésére,
- képes a működésben bekövetkező kiesését és ennek hatásait a minimálisra csökkenteni,
- képes az informatikai szolgáltatások mielőbbi helyreállítására.

A rendelkezés hatálya

2. §

(1) Személyi hatály: kiterjed minden személyre, aki az Egyetem informatikai vagy azzal összefüggő rendszerét, szolgáltatásait, informatikai infrastruktúráját üzemelteti. Ide kell érteni az informatikai szolgáltatások zavartalan működéséét biztosító rendszerek üzemeltetéséért felelős területeket is, valamint a rendszereket üzleti oldalról üzemeltető szakértőket is.

(2) Tárgyi hatálya: kiterjed az Egyetem működése szempontjából kiemelt fontosságú informatikai rendszerekre, amelyek tárolják, kezelik, feldolgozzák, felügyelik, ellenőrzik és/vagy továbbítják az Egyetem kezelésében/tulajdonában álló adatokat, információkat.

Fogalmak

3. §

(1) *Informatikai katasztrófa helyzet*: Incidens (informatikai): váratlan esemény. Az informatikai rendszer használatában bekövetkező rendellenes működés, kisebb-nagyobb zavarok, pl.: betörés v. betörési kísérlet, adatvesztés, adatok kitudódása, illetéktelen hozzáférés, vírusfertőzés, a rendelkezésre állás sérülése.

(2) *Informatikai Működésfolytonossági Terv*: terv, a váratlan események kezelésére annak érdekében, hogy biztosítsuk az ügymeneti folyamatoknak a kívánt időn belüli helyreállíthatóságát.

(3) *Informatikai rendszer*: a hardverek és szoftverek olyan kombinációjából álló rendszer, amit az adat-, illetve információfeldolgozás különböző feladatainak teljesítésére alkalmazunk.

(4) *Információs rendszer*: azon eljárások, tevékenységek összessége, amelyek a szervezet működéséhez és irányításához szükséges információkat tárolják, előállítják, szétosztják.

(5) *Rendelkezésre állás*: az a tényleges állapot, amikor az információk vagy adatok elérhetősége és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva.

A rendelkezés tartalma

4. §

(1) Az terv azon intézkedésekre terjed ki, melyeket az Egyetem Informatika szervezeti egységénél kell végrehajtani.

(2) A tervben nem szerepelnek

- a rövid időn belül pótolható, helyettesíthető elemek,
- az informatikai üzemzavar esetei, amelyek az 1 munkanapos sebezhetőségi ablakon belül megoldhatók

(3) Az IT szolgáltatás folytonossági terv csak az elektronikus információs rendszerekre vagy az azokat kiszolgáló rendszerekre terjed ki, nem foglalkozik a humán erőforrás biztosításával, esetleges mentésével, illetve más (nem informatikai biztonsági szolgáltatást nyújtó) vagyontárgyak kezelésével kapcsolatos katasztrófa helyzetek esetén szükséges intézkedésekkel, beavatkozásokkal.

Kapcsolódó szabályzatok, dokumentumok

5. §

(1) Jelen rendelkezésben foglaltakat a mindekor hatályos Informatikai Biztonsági Szabályzat rendelkezéseivel összhangban kell alkalmazni.

A rendelkezés karbantartása

6. §

(1) Az Egyetem IT szolgáltatásainak informatikai katasztrófa helyzet esetén felmerülő folyamatos biztosítására létrehozott tervet annak megfelelősége, hatékonysága érdekében rendszeresen, évente, illetve a lent felsorolt esetek előfordulása esetén egyedi jelleggel felül kell vizsgálni:

- a folyamatok változásakor,
- az Egyetem működési feltételei, körülményei (fizikai, gazdasági, jogi, együttműködési, stb.) megváltozásakor,
- a működést támogató meghatározó informatikai eszközök, hardverek vagy szoftverek cseréjekor.

(2) A felülvizsgálatot, karbantartást az Informatika koordinálja.

(3) Az IT szolgáltatás folytonossági terv a végrehajtásban érintettek számára hozzáférhető helyen, nyomtatott formában kerül tárolásra annak érdekében, hogy az elektronikus változat sérülésekor is bármikor hozzáférhető legyen.

A rendelkezés tesztelése

7. §

(1) A terv alkalmasságának tesztelését 3 éves ciklusban teljeskörűen el kell végezni. A bekövetkezett eseményekre történő reagálást is az adott esemény tesztjének minősül, s ennek megfelelően kerül dokumentálásra, a tapasztalatait fel kell használni.

(2) A tesztelés a belső auditok keretében, a tesztelési tervnek megfelelően kerül elvégzésre, dokumentálása belső auditoknak megfelelően történik. Amennyiben a teszt eredménye nem kielégítő, az IT vezető helyesbítő intézkedést kezdeményez. Az intézkedés akkor tekinthető lezártnak, ha a tesztet megismételve meggyőződtünk az intézkedés eredményességéről, valamint a módosításokat rögzítettük és véglegesítettük az üzletmenet folytonossági tervben.

A kommunikáció útvonala

8. §

(1) Amennyiben előfordul olyan szolgáltatás kiesés, amely a teljes egyetemi munkavállalói és/vagy hallgatói kört érinti, akkor a következő kommunikációs folyamatot kell betartani:

- Az incidenst észlelő szakértő haladéktalanul jelzi a felettesének írásban (emailen) is a kiesés tényét, megnevezve a rendszert, a kiesés okát, annak pontos idejét.
- A bekövetkező incidensről azonnal írásban (emailen) tájékoztatni kell az IT vezetőt.
- A felettes vezető (ez lehet az Informatika bármelyik operatív vezetője) értesíti a Kommunikációt. Az értesítésnek tartalmaznia kell:
  - Az incidens rövid leírását
  - Annak hatását, az érintettek felhasználók és rendszerek körét
  - Az incidens bekövetkezett időpontját és a becsült elhárítás időpontját
  - A publikálás javasolt helyét (intranet vagy honlap)
  - A javasolt kerülő megoldást (amennyiben van ilyen)
  - A szükséges teendőket (ha meghatározható pl. áramtalanítsa az eszközt, indítsa újra, törölje a meghatározott üzenetet stb.)
  - Személy megjelölése, hogy kihez kell fordulni technikai probléma esetén
- Ezek alapján az IT és a Kommunikáció munkatársai közösen eldöntik, hogy mely platformokon kell értesíteni a munkatársakat és/vagy a hallgatókat a bekövetkezett szolgáltatás kiesésről (intranet, weblap, e-mail).

Informatikai rendszerek osztályozása

9. §

(1) Az Egyetem kiszolgáló rendszerei hatás és fontosság szerint osztályozva négy biztonsági osztályba sorolhatók. Azokat a rendszereket tekintjük magasabb biztonsági osztályba soroltnak, amelyek az alaptevékenység kiszolgálása szempontjából kritikusnak tekinthetők.

a) Kritikus rendszerek:

Egyrészről az Egyetem alaptevékenységeinek ellátása szempontjából kritikus rendszerek.

Másrészről az adatvédelmi szempontból kiemelt védelmet igénylő rendszerek, és az Egyetem működése és/vagy kommunikációja szempontjából kiemelt fontosságú rendszerek.

Ide tartoznak az alábbiak:

- Központi infrastruktúra (szerverek (szerver és hypervisor), SAN switch, storage)
- Központi hálózati eszközök
- DNS szerverek
- Központi bejelentkeztető szerver (Active Directory)
- DB szerverek (Oracle)
- Hallgatói tanulmányi rendszer, továbbá az ehhez kapcsolódó hallgatói szolgáltató rendszerek: Neptun
- Moodle
- Egyetemi honlap (uni-corvinus portál)

b) Kiemelt rendszerek:

Az Egyetem egyes fontos tevékenységének ellátása szempontjából kiemelt fontosságú rendszerek, amelyek elsősorban technikai jellegűek, a rajtuk tárolt adatok elsősorban nem személyes jellegűek.

- DHCP szerverek
- Radius authentikációs rendszer
- Teljes vezetékes hálózat (aktív és passzív eszközök)
- KIM
- Központi felhasználókezelő rendszer (Cusman/AD360)
- Központi számítógépkezelő rendszer (SCCM)
- M365 szinkronizációs szerver (EntraID Sync)
- Központi iktatórendszer, Poszeidon
- Teljes körű Ügyviteli, Szolgáltató és Bérügyviteli Rendszer: SAP

c) Normál rendszerek:

Az Egyetem egészének napi működése szempontjából nem kiemelt fontosságú rendszerek, ill. a nyújtott szolgáltatások felhasználói köre az Egyetem egyes intézményeire, csoportjaira korlátozódik. Védendő, akár személyes adatokat is tartalmazhatnak.

- Wi-Fi hálózat
- VPN szerverek
- Informatikai támogató szerverek (Licenc, víruskereső, samba)
- Telefonközpontok (IP és hagyományos)
- Hallgatói számítógépes laborok
- MyCorvinus és hozzá kapcsolódó rendszerek

d) Egyéb rendszerek:

Működésük az Egyetem egészére nincs kihatással. Szűkebb csoportok vagy személyek oktatási, tanulmányi vagy kutatási munkáját segítik. Ide tartozik minden más, fenti kategóriákba be nem sorolt rendszer. Érzékeny, incidensektől védendő adatokat tartalmazhatnak. Mennyiségüket tekintve kiemelendőek.

- Az Egyetem hálózatára kapcsolódó oktatói, kutatói számítógépes munkaállomások
- Az Egyetem hálózatára kapcsolódó nyomtatók
- Hallgatói szabad felhasználású számítógépes munkaállomások

(2) A Kritikus és Kiemelt fontosságú rendszerek kiesése és meghibásodása esetén jelen rendelkezésben rögzített kommunikációs protokoll lép életbe, illetve végre kell hajtani az incidens esetén szükséges intézkedéseket.

Az IT szolgáltatásfolytonosságot biztosító alapvető elemek

10. §

(1) A kritikus jelentőségű infrastruktúra a Sóházban, a szerverszobában található. Itt vannak a kiszolgálók (szerverek) és a központi hálózati eszközök is, amelyek a nem a földi telepítésű rendszerek elérésének lehetőségét biztosítják. Ezeknek a zavartalan működése nélkül nem lehetséges a szolgáltatások biztosítása, valamint sem a Kritikus, sem pedig a Kiemelt osztályba sorolt rendszerek nem érhetők el.

A kritikus jelentőségű adatközpontok elhelyezkedése:

- Adatközpont 1. és 2.
  - 1093 Budapest Fővám tér 13-15., Sóház, I. emelet 108
  - 1093 Budapest Közraktár utca 4., C épület, 14. szoba
- A bérelt vonali internet szolgáltatás átadási pontja:
  - 1093 Budapest Fővám tér 13-15., Sóház, I. emelet 108
- Telefonközpont
  - 1093 Budapest Fővám tér 8., E épület 343

(2) **Az adatközpontok fizikai biztonsága**

Az adatközpont bejáratát hitelesítéssel (kártyával, illetve ujjlenyomat azonosítással) rendelkező beléptető rendszer biztosítja.
Az adatközpontok fizikai biztonságát a Campus szolgáltatások szervezeti egysége a belső szabályoknak megfelelően garantálja.

(3) **Az adatközpontok szünetmentes áramellátása**

Az 1. és 2. számú Fővám campuson található adatközpontot ellátó szünetmentes áramforrások paraméterei:

- Típus: Eaton 9355-30-N-0 teljesítmény: 30 kVA Adatközpont 1.
  - Feladata: Adatközpont szünetmentes hálózatának tápellátása
  - Áthidalási idő: 29 perc
- Típus: APC Smart-UPS 3000 teljesítmény 3 kVA Adatközpont 2.
  - Feladata: Mentési infrastruktúra szünetmentes tápellátása

- Áthidalási idő: 12 perc

A szünetmentes áramforrások évente 1 alkalommal kerülnek átvizsgálásra.

(4) **Dízel aggregátoros betáplálás**

Az E épület alagsorában lévő aggregátor indítása áramszünet esetén automatikus.

Az aggregátor bekapcsolás után 1 percen belül kezdi meg a Sóház Adatközpont 1. szünetmentes áramforrás táplálását.

Incidens esetén alkalmazandó intézkedések

11. §

(1) Tennivalók **az adatközpontokat érintő katasztrófahelyzet vagy működés folytonosságot érintő incidens** esetén:

A szolgáltatás folytonossági intézkedéseket haladéktalanul meg kell kezdeni, amennyiben:

- A kritikus IT infrastruktúra rendszer bármelyik eleme fizikailag meghibásodik (szerverek, adattárolók, hálózati gerinc elemek)
- A kritikus IT üzemeltető felület bármelyike nem használható (eszköz konzolok, AD alapú szolgáltatások, virtualizáció).
- A rendszerekbe nem lehetséges a bejelentkezés
- Nem érhetőek el az alkalmazások

(2) Az üzletmenet folytonossági intézkedések megkezdését kezdeményezheti az adott szervezeti egység munkáltatói jogkört gyakorló vezetője, vagy ügyeletese.

(3) Intézkedések és sorrendjük

„T” = a katasztrófa, vagy a kritikus incidens bekövetkezési időpontja

Sorszám	INTÉZKEDÉS	FELELŐS	Határidő
1	Értesíteni kell az IT Ügyfélszolgálatot (lehetőleg telefonon) és az IT vezetőt.	Észlelő	T+15 perc
2	Feladatok pontos meghatározása és eszkalálása az operatív vezetőknek.	IT vezető	T+20 perc
3	Károk felmérése	Észlelő, IT operatív vezetők, támogatók	T+45 perc
4	Amennyiben a 11.§ (1) bekezdésben felsoroltak egyike fennáll, akkor el kell rendelni a szolgáltatás folytonossági intézkedések végrehajtását	IT vezető, IT operatív vezetők	Max T+ 2óra
5.	A JISZ vezető, valamint az adatvédelmi tisztviselő tájékoztatása az Adatkezelés rendjéről szóló 13/2023. ET rendelkezés szerint	IT vezető, IT operatív vezetők	Max T+ 2óra

(4) Károk felmérése

A károk felmérése – amennyiben lehetséges - az érintett adatközpont vagy kommunikációs csillagpont bejárásával, az eszközök állapotának felmérésével kezdődik.

Amennyiben lehetséges ellenőrizni kell az eszközök státusz jelzéseit.

Amennyiben lehetséges meg kell kísérelni a kritikus IT infrastruktúra elemek és az azokon futó IT szolgáltatások adminisztrátori felületeinek elérését.

Részleges, egy-egy egységet érintő meghibásodás esetén elemezni kell az összefüggéseket, a kapcsolódó IT szolgáltatásokat.

A területenként értesítendő Informatikai vezetők és területek:

Minden esetben értesítendő:

- Sopronyi Tibor IT vezető (tibor.sopronyi@uni-corvinus.hu) +36 30 137 9483
- Kohán Réka IT operatív vezető (reka.kohan@uni-corvinus.hu)
- IT Ügyfélszolgálat (ithelpdesk@uni-corvinus.hu) +36 1 482 7500

Adatközponti és kritikus rendszerek meghibásodása esetén:

- Mák Tamás IT központi szolgáltatások csoportvezető (tamas.mak@uni-corvinus.hu)
- Dinnyés Gergely Vezető hálózatüzemeltetési szakértő (gergely.dinnyes@uni-corvinus.hu)

Záró rendelkezések

12. §

(1) Jelen rendelkezés 2024. október 1. napján lép hatályba.

(2) Jelen rendelkezés a mindenkor hatályos Informatikai biztonsági szabályzat rendelkezéseivel összhangban értelmezendő.