



**DUNAÚJVÁROSI EGYETEM**

**INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI KÉZIKÖNYV**

**Dunaújváros  
2016**



---

**Sz-40**  
**INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI KÉZIKÖNYV**

---

1. kiadás

2. módosítás

2 (24). oldal

---

**Dunaújvárosi Egyetem Szenátusa által 2-2016/2017. (2016.09.27.) számú határozatával elfogadva**

**Hatályos: 2016. szeptember 28. napjától**



## **Figyelmeztetés**

Minden informatikai katasztrófahelyzetben  
**elsődleges feladat a személyzet életének és testi épségének védelme!**

Minden egyéb feladat csak akkor kezdhető meg,  
ha a veszélyeztetett személyek biztonságba kerültek.

### **Katasztrófa esetén folytassa a kézikönyvet a 2. fejezetnél.**

A KATASZTRÓFA-ELHÁRÍTÁSI KÉZIKÖNYV rendelkezési az 1.5. fejezetben részletezett esetekben lépnek életbe.

*Az informatikai katasztrófa-elhárítási folyamat akkor ér véget, ha az DUNAÚJVÁROSI EGYETEM szolgáltatásai zavartalanná válnak, az információrendszer ismét normális módon működik*



## TARTALOMJEGYZÉK

<b>1</b>	<b>KATASZTRÓFA-ELHÁRÍTÁSI KÉZIKÖNYV ÁLTALÁNOS RÉSZ .....</b>	<b>6</b>
1.1	AZ INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV HASZNÁLATA .....	6
1.1.1	<i>Tipográfiai szabályok, értelmezések</i> .....	6
1.1.2	<i>Az informatikai katasztrófa-elhárítási kézikönyv szerkezete</i> .....	6
1.2	AZ INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV CÉLJA ÉS ÉRVÉNYSÉGI KÖRE.....	7
1.3	AZ INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV MELLÉKLETE .....	7
1.3.1	<i>Az informatikai katasztrófa-elhárítási terv mellékletének karbantartása</i> .....	7
1.4	AZ INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV MŰKÖDÉSÉNEK KÖVETELMÉNYEI.....	7
1.5	AZ INFORMATIKAI KATASZTRÓFA.....	8
1.5.1	<i>Az informatikai katasztrófa általános meghatározása</i> .....	8
1.5.2	<i>Az informatikai katasztrófa speciális meghatározása</i> .....	8
1.5.3	<i>Mit nem tekintünk informatikai katasztrófának</i> .....	8
1.6	AZ INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV KARBANTARTÁSA.....	9
1.7	A KORLÁTOZOTT ÜZEM MEGHATÁROZÁSA .....	9
1.8	A HELYREÁLLÍTÁSI SORRENDET MEGHATÁROZÓ KÖRÜLMÉNYEK.....	10
1.9	AZ INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁS SZEREPLŐI, FELADAT ÉS HATÁSKÖRŰK.....	10
1.9.1	<i>A katasztrófaelhárító szervezet</i> .....	10
1.9.2	<i>Katasztrófa menedzser</i> .....	10
1.9.3	<i>Katasztrófa menedzser team</i> .....	11
1.9.4	<i>Krízis központvezető</i> .....	11
1.9.5	<i>Krízis központ team</i> .....	11
1.9.6	<i>Szakértők</i> .....	11
1.9.7	<i>Közreműködők</i> .....	12
1.9.8	<i>Kulcsfelhasználók</i> .....	12
1.9.9	<i>Harmadik fél</i> .....	12
1.10	ÁLTALÁNOS RENDELKEZÉSEK .....	12
1.10.1	<i>Elsősegély</i> .....	13
1.10.2	<i>Biztonsági követelmények</i> .....	13
1.10.3	<i>Az informatikai katasztrófa események naplózása</i> .....	13
1.10.4	<i>Krízis központ</i> .....	13
1.10.5	<i>A szakértők és a harmadik fél számára figyelembeveendő irányelvek</i> .....	14
<b>2</b>	<b>TEENDŐK INFORMATIKAI KATASZTRÓFA ESETÉN .....</b>	<b>15</b>
2.1	AZ INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV AKTIVÁLÁSA, AZONNALI VÁLASZ.....	15
2.2	AZ ÁTFOGÓ AKCIÓTERV.....	15
2.3	AZ ESEMÉNYEK BEHATÁROLÁSA .....	16
2.3.1	<i>A feladat végrehajtója</i> .....	16
2.3.2	<i>Eszköz, erőforrás igény</i> .....	16
2.3.3	<i>Teendők</i> .....	16
2.4	ELHÁRÍTÁSI CSOPORT ÖSSZEHÍVÁSA, ÉRINTETT FELEK ÉRTESÍTÉSE.....	16
2.4.1	<i>A feladat végrehajtója</i> .....	16
2.4.2	<i>Eszköz, erőforrás igény</i> .....	16
2.4.3	<i>Teendők</i> .....	16
2.5	KULCSFELHASZNÁLÓK ÉS FELHASZNÁLÓK ÉRTESÍTÉSE.....	16
2.5.1	<i>A feladat végrehajtója</i> .....	16
2.5.2	<i>Eszköz, erőforrás igény</i> .....	16
2.5.3	<i>Teendők</i> .....	17
2.6	HARMADIK FÉL ÉRTESÍTÉSE.....	17
2.6.1	<i>A feladat végrehajtója</i> .....	17
2.6.2	<i>Eszköz, erőforrás igény</i> .....	17
2.6.3	<i>Teendők</i> .....	17
2.7	INFORMATIKAI SZOLGÁLTATÁSOK REKONSTRUKCIÓJA .....	17
2.8	ÁTTELEPÜLÉS A KÖZPONTI TARTALÉK MUNKAHELYEKRE .....	18
2.8.1	<i>A feladat végrehajtója</i> .....	18
2.8.2	<i>Eszköz, erőforrás igény</i> .....	18
2.8.3	<i>Teendők</i> .....	18



**Sz-40**  
**INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI KÉZIKÖNYV**

1. kiadás

2. módosítás

5 (24). oldal

2.9	KÉSZENLÉTI ÁLLAPOT .....	18
2.9.1	<i>A feladat végrehajtói .....</i>	<i>18</i>
2.9.2	<i>Eszköz, erőforrás igény .....</i>	<i>18</i>
2.9.3	<i>Teendők .....</i>	<i>19</i>
2.10	KIEGÉSZÍTŐ TERV .....	19
2.10.1	<i>A feladat végrehajtói .....</i>	<i>19</i>
2.10.2	<i>Eszköz, erőforrás igény .....</i>	<i>19</i>
2.10.3	<i>Teendők .....</i>	<i>19</i>
<b>3</b>	<b>OKTATÁSI TEMATIKA.....</b>	<b>21</b>
3.1.1	<i>Oktatási célok, követelmények.....</i>	<i>21</i>
3.1.2	<i>Szervezeti keretek, munkaformák, munkamódszerek, eszközök, tananyag időelosztása .....</i>	<i>21</i>
3.1.3	<i>Visszacsatolás.....</i>	<i>22</i>
<b>4</b>	<b>EGYÉB RENDELKEZÉSEK.....</b>	<b>23</b>



## 1 KATASZTRÓFA-ELHÁRÍTÁSI KÉZIKÖNYV ÁLTALÁNOS RÉSZ

### 1.1 Az informatikai katasztrófa-elhárítási terv használata

#### 1.1.1 Tipográfiai szabályok, értelmezések

Az informatikai katasztrófa-elhárítási terv használatához fontos, hogy az alkalmazott tipográfiai szokásokat minden felhasználó ismerje.

Az alább felsorolt jelek és formátumok speciális információkat jelölnek.

Formátum vagy jel	Az információ típusa
<i>Dőlt</i> szedés	Speciális fogalmak, vagy olyan általános helykitöltő szó, amely helyett konkrét szöveget kell begépelnünk (mondjuk egy fájl nevét). Például: <code>arj x archív_név</code> – be kell gépelni az „arj” betűket, majd egy szóközt, egy „x” karaktert, egy újabb szóközt, végül egy (az aktuális) archív nevét.
<b>Félkövér</b> szedés	Fontos információ, például:  Minden informatikai katasztrófa helyzetben <b>elsődleges feladat a személyzet életének és testi épségének védelme.</b>
▶ (felsorolásjelző karakter)	Lépésről lépésre bemutatott eljárás, például: <ul style="list-style-type: none"><li>▶ Az életet illetve vagyontárgyat fenyegető veszély esetén először a MENTŐKET, és/vagy a TŰZOLTÓKAT kell értesíteni és amennyiben szükséges az 1. 9. pontban (MINDEN KATASZTRÓFÁRA ÉRVÉNYES RENDELKEZÉSEK) leírtaknak megfelelően kell eljárni.</li><li>▶ A fenti teendők elvégzése után az ügyeletes KRÍZIS KÖZPONT VEZETŐT kell tájékoztatni az 1. 5. pontban leírtaknak megfelelő katasztrófa helyzet létrejöttéről.</li><li>▶ ...</li></ul>
Courier szedés	Példák a begépelendő utasításokra, illetve a fájlnevekre. Az utasításokat általában kisbetűvel kell begépelni, kivéve, ha a helyes működéshez nagybetűk használata szükséges, például: <ul style="list-style-type: none"><li>▪ <code>Help.doc</code></li><li>▪ <code>mount /dev/cdrom</code></li><li>▪ <code>tar [funkcióopció] [fájl_nev(ek)]</code></li></ul>
KIS KAPITÁLIS szedés	A hivatkozásként megemlített dokumentumok, helységek és informatikai katasztrófa-elhárítási szereplők (beosztása). Például: <ul style="list-style-type: none"><li>▪ E-601 ELJÁRÁSLEÍRÁS</li><li>▪ SZÁMÍTÓKÖZPONT</li><li>▪ SZAKÉRTŐ</li></ul>

#### 1.1.2 Az informatikai katasztrófa-elhárítási kézikönyv szerkezete

Az INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI KÉZIKÖNYV modulárisan felépített szerkezetű, három elkülöníthető részből áll.

Az **első rész** (az első fejezet) azokat az általános, az DUNAÚJVÁROSI EGYETEM bármely egyetemi (informatikai) alrendszerének katasztrófája során minden érintettre és minden informatikai katasztrófa helyzetre érvényes rendelkezéseket tartalmazza, amelyek a működés szempontjából statikusak, változásuk nem valószínű. Ezen rész tartalmát az INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV oktatása során mindenkinek meg kell ismernie.

A **második szerkezeti rész** (második fejezet) az informatikai katasztrófa-elhárítás forgatókönyveinek leírása. Az ebben a részben meghatározott intézkedéseket az INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI KÉZIKÖNYV által védett erőforrások nagymértékű változása vagy az INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI KÉZIKÖNYVVEL védett eszköz- és folyamat kör bővülése során kell módosítani.



A **harmadik szerkezeti rész** (melléklet) az informatikai katasztrófa-elhárítás során használatos naprakész adatok és részletező leírások. Az itt szereplő információk változása valószínű, tehát ennek a résznek a karbantartását havi rendszerességgel ellenőrizni, és változás esetén folyamatosan frissíteni kell.

## 1.2 Az informatikai katasztrófa-elhárítási terv célja és érvényességi köre

AZ INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV célja az DUNAÚJVÁROSI EGYETEM információrendszerében a kritikus szolgáltatások folyamatos működésének biztosítása az üzleti követelményeknek megfelelően,

- az informatikai katasztrófa bekövetkezése esetén fellépő kár csökkentése,
- a szükséges szolgáltatások elérhetővé tétele és folyamatosságának biztosítása,
- a rendeltetésszerű működés visszaállításának felgyorsítása egy rendszeresen karbantartható, strukturált informatikai katasztrófa-elhárítási terv alapján.

AZ INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV érvényességi köre informatikai katasztrófa bekövetkezése esetén az 1.8 fejezetben meghatározott egyetemi szolgáltatásokra, szereplőkre, illetve létesítményekre terjed ki.

## 1.3 Az informatikai katasztrófa-elhárítási terv melléklete

AZ INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV MELLÉKLETE az informatikai katasztrófa-elhárítás során használatos naprakész adatokat és részletező leírásokat tartalmazza. Az adatok érzékeny voltára való tekintettel, a melléklethez katasztrófa helyzetben kívül, csak az alábbi munkakörben dolgozók férhetnek hozzá:

- REKTOR
- KANCELLÁR (KATASZTRÓFA MENEDZSER)
- REKTORHELYETTESEK
- GAZDASÁGI ÉS ÜZEMELTETÉSI IGAZGATÓ
- HRSZK KÖZPONTVEZETŐ
- JOGI IRODA KÉPVISELŐJE (A KANCELLÁR ÁLTAL MEGHATALMAZOTT SZEMÉLY)
- ISZK KÖZPONTVEZETŐ (KRÍZIS KÖZPONT - KÖZPONTVEZETŐ)

Katasztrófa helyzetben az elhárításban résztvevők számára a melléklethez történő hozzáférést a KATASZTRÓFA MENEDZSER jóváhagyásával a KRÍZIS KÖZPONT VEZETŐ biztosítja.

A dokumentumból egy-egy nyomtatott példányt az alábbi helyeken kell elérhetővé tenni a fentebb megadott személyek számára:

- lezárt borítékban a HRSZK páncélszekrényében,
- az ISZK KÖZPONTVEZETŐ irodájában.

### 1.3.1 Az informatikai katasztrófa-elhárítási terv mellékletének karbantartása

A mellékletben szereplő információk változása valószínű, ezért a benne foglaltakat havi rendszerességgel ellenőrizni kell (lásd a 1.6. pont). Amennyiben módosítás válik szükségessé, úgy azt az alábbi lépések végrehajtásával lehet elvégezni:

- ▶ Az ISZK KÖZPONTVEZETŐ elvégzi a szükséges módosításokat a mellékletben.
- ▶ Az ISZK KÖZPONTVEZETŐ kezdeményezi a melléklet módosítását a KANCELLÁRNÁL.
- ▶ A KANCELLÁR jóváhagyja a módosításokat.

## 1.4 Az informatikai katasztrófa-elhárítási terv működésének követelményei

Ahhoz, hogy az INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV működőképes legyen, a következőket kell megvalósítani:

- Az INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV működését előkészítő tervszerű megelőző intézkedéseket (pl.: mentések, karbantartások megléte) maradéktalanul végre kell hajtani.



- Biztosítani kell, hogy a készenléti tartalék eszközök az előírt helyen és mennyiségben rendelkezésre álljanak.
- A mentési terveket, eljárásokat át kell vezetni az INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERVBE. A munka és a biztonsági mentések tárolási helyszíneit külön kell választani, és ki kell jelölni.
- A központi és tartalékszerverek, a diszk-alrendszerek és a szünetmentes tápegységek karbantartása tervszerű és rendszeres legyen. Az INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERVBE legyenek átvezetve a karbantartás eredményezte változtatások.
- Az INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERVET minden résztvevőnek (KATASZTRÓFAELHÁRÍTÓ, KULCSFELHASZNÁLÓ) megfelelően oktatni kell.
- Minden feladatra legalább két azonos képzettségű szakembernek kell rendelkezésre állnia az informatikai katasztrófa-elhárítási csoportban.
- Az INFORMATIKAI KATASZTRÓFA MENEDZSER TEAM számára rendelkezésre álljon olyan pénzkeret, amelyet szükség esetén utólagos elszámolás mellett, korlátozás nélkül felhasználhat.

## 1.5 Az informatikai katasztrófa

### 1.5.1 Az informatikai katasztrófa általános meghatározása

Katasztrófa az informatikai rendszerben minden olyan esemény, ami az DUNAÚJVÁROSI EGYETEM (DUE) üzleti tevékenységének folyamatosságát az informatikai rendszer kritikus szolgáltatásainak – sebezhetőségi ablakuk (működésképtelenség maximális időtartama) mértékét meghaladó – kiesésén keresztül sérti, vagy ezzel fenyeget.

Ilyen eseményt előidézhethet különösen, de nem kizárólagosan:

- a DUE épületeit sújtó tűzvész, robbanás vagy más külső behatás,
- az elektromos hálózat tartós kiesése,
- a telekommunikációs hálózat tartós kiesése,
- kritikus informatikai rendszerek súlyos üzemzavara.

Lényeges azonban, hogy az adott konkrét helyzetet sohasem a kiváltó ok, hanem mindig a kiváltott okozat alapján lehet és kell megítélni.

### 1.5.2 Az informatikai katasztrófa speciális meghatározása

Az informatikai rendszer kritikus szolgáltatásainak tekintendők azok a funkciók, alkalmazások, amelyek sebezhetőségi ablaka 8 óra.

Az egyes rendszerelem csoportokra nézve **teljes működésképtelenségként** értelmezünk minden olyan állapotot, amely az egyetemi rendszerben lehetetlenné teszi a korlátozott üzem szerinti minimális funkcionális szint biztosítását a védett szolgáltatások számára.

Az egyes rendszerelem csoportokra nézve **részleges működésképtelenségként** értelmezünk minden olyan állapotot, amelynek következtében a korlátozott üzem bevezetése szükséges, de az egyetemi rendszer egésze továbbra is alkalmas legalább a korlátozott üzem szerinti minimális funkcionális szint biztosítására a védett szolgáltatások számára.

A teljes és a részleges működésképtelenséget az DUNAÚJVÁROSI EGYETEM esetében a minimális szolgáltatási szintek 1.7 fejezet szerinti táblázata alapján, a sebezhetőségi ablak, illetve az adott szituáció további körülményeinek figyelembe vételével lehet megállapítani.

Minden egyéb működési zavar és/vagy hiányos funkcionalitás **üzemzavaros állapotnak** tekintendő. Az üzemzavaros állapot nem tartozik jelen kézikönyv hatálya alá.

### 1.5.3 Mit nem tekintünk informatikai katasztrófának

Nem tekintjük informatikai katasztrófának, ebből kifolyólag jelen kézikönyv nem terjed ki az alábbiakra:

- épületet érintő problémák (pl.: beázás, épület megrongálódása)
- áramellátást érintő problémák





- internetkapcsolatot érintő problémák (külső szolgáltató és kapcsolat hibái)
- külső vezetékes és mobil telefonhívásokat érintő problémák
- személyzetet érintő problémák (pl.: teljes üzemeltetés lebetegszik)

AZ INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV abból az állapotból indul ki, hogy az alábbiak rendelkezésünkre állnak:

- informatikai szolgáltatások nyújtására és igénybe vételére alkalmas épület,
- megfelelő áramellátás,
- működő internet kapcsolat,
- működő külső vezetékes és / vagy mobil telefonkapcsolat,
- megfelelő számú és szakértelmű személyzet.

Amíg a fentiek nem teljesülnek, addig az INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV nem hajtható végre.

## 1.6 Az informatikai katasztrófa-elhárítási terv karbantartása

Jelen tervben szereplő információk általános karbantartásáért az INFORMATIKAI SZOLGÁLTATÓ KÖZPONT vezetője felelős. A karbantartás több szinten valósul meg.

Havonta szűrőpróbaszerűen ellenőrizni kell a leltárak, címjegyzékek érvényességét, valamint legalább féléves gyakorisággal el kell végezni a terv egészének tartalmi felülvizsgálatát. Ezen felül az egyes szervezeti egységek vezetői kötelesek az alábbi változásokról értesíteni az INFORMATIKAI SZOLGÁLTATÓ KÖZPONTOT:

Változás	Kezdeményező
Új berendezés vásárlásakor, illetve operációsrendszer váltás alkalmával	ISZK KÖZPONTVEZETŐ
Új hibadetektáló rendszer és kontrol technológia üzembeállítás	ISZK KÖZPONTVEZETŐ
Új környezeti kontrol technológia bevezetése (például új tűzvédelmi rendszer)	MSZK KÖZPONTVEZETŐ
Személyzeti és szervezeti változások	HRSZK KÖZPONTVEZETŐ
A vállalkozók és szállítók változása	GO OSZTÁLYVEZETŐ ISZK KÖZPONTVEZETŐ
Címek és telefonszámok változása	HRSZK KÖZPONTVEZETŐ
Az üzemelési gyakorlat változása	ISZK KÖZPONTVEZETŐ
Jogsabályi változások	JOGI IRODA

Ezen túlmenően pedig az elvégzett tesztelések eredményei, tapasztalatai alapján is el kell végezni a szükséges módosításokat.

## 1.7 A korlátozott üzem meghatározása

Az DUNAÚJVÁROSI EGYETEM kritikus informatikai alkalmazásainak korlátozott üzemű működésével kapcsolatban az alábbi információkat kell megadni (szolgáltatásonként):

- Alkalmazás / Funkció megnevezése.
- Minimális szolgáltatási szint.  
(Mi az a minimális szolgáltatási szint, ami még elfogadható? pl.: adott számú felhasználó tudjon hozzá kapcsolódni, adott helyekről tudjanak hozzá kapcsolódni, stb...).



- Alternatív feldolgozás.  
(Ha a minimális szolgáltatási szint sem működik, akkor van-e lehetőség alternatív módon kiváltani a szolgáltatást? (pl.: intézményi levelezés helyett privát (pl.: GMAIL) levelező használata.))

A korlátozott üzem részletes leírását az „Informatikai katasztrófa-elhárítási kézikönyv” melléklete tartalmazza.

## 1.8 A helyreállítási sorrendet meghatározó körülmények

Az egyes informatikai katasztrófaeseményeket bekövetkezésük időpontjának az DUNAÚJVÁROSI EGYETEM üzleti folyamatainak ciklusában elfoglalt helye és várható fennállásuk időtartama alapján minősítettük.

Ez lehetővé teszi, hogy az elhárítás módja optimális legyen, azaz az DUNAÚJVÁROSI EGYETEM számára minimálisra csökkentse a kárt.

A helyreállítási sorrend részletes leírását az „Informatikai katasztrófa-elhárítási kézikönyv” melléklete tartalmazza.

## 1.9 Az informatikai katasztrófa-elhárítás szereplői, feladat és hatáskörük

### 1.9.1 A katasztrófaelhárító szervezet



### 1.9.2 Katasztrófa menedzser

A katasztrófa menedzser irányítja az informatikai katasztrófa Egyetemszintű elhárítását. Ennek keretében:

- a rendelkezésre álló információk alapján kinyilvánítja az informatikai katasztrófa állapotot,
- informatikai katasztrófa helyzetben dönt a szakértők és / vagy harmadik fél behívásáról,
- a rendelkezésre álló információk alapján dönt a normál üzemre való visszaállásról,
- kezdeményezheti az INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV kiegészítő terve végrehajtásának megkezdését.



### 1.9.3 Katasztrófa menedzser team

A katasztrófa menedzser team támogatja az informatikai katasztrófa menedzsért az informatikai katasztrófa Egyetemszintű elhárításának irányításában. Tagjai lehetnek (a katasztrófa jellegétől függően) az érintett üzleti folyamatok, szervezeti egységek legfelsőbb szintű vezetői, a Rektor, a Kancellár, a Rektorhelyettesek, a Gazdasági és Üzemeltetési Igazgató, a belső ellenőrzés vezetője, illetve az általuk delegált személyek, továbbá szükség esetén külső szakértők, tanácsadók.

A team feladata, hogy – tagjai esetleges egyéb elhárítási feladatain túl, – helyzetértékelésükkel, döntés-előkészítő tevékenységükkel segítsék az informatikai katasztrófa menedzser munkáját.

### 1.9.4 Krízis központvezető

A KRÍZIS KÖZPONT VEZETŐ az informatikai katasztrófa elhárításának operatív irányítója az informatikai területeken. Ennek keretében a KRÍZIS KÖZPONT VEZETŐ:

- az informatikai katasztrófa-elhárítási csoport vezetője,
- informatikai katasztrófa helyzetben javaslatot tesz a szükséges harmadik fél szakértőinek behívására,
- irányítja az informatikai katasztrófa-elhárítási munkálatokat, dönt a rendelkezésére álló emberi és anyagi erőforrások alkalmazásáról,
- a rendelkezésre álló információk alapján bármikor eltérhet az INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV által meghatározott forgatókönyvben leírtaktól,
- a forgatókönyvek egyes pontjaiban meghatározott egyetemi szereplőket az informatikai katasztrófa helyzet által igényelt számban és körben hívja be.

### 1.9.5 Krízis központ team

A KRÍZIS KÖZPONT TEAM tagjai a KRÍZIS KÖZPONT VEZETŐ irányításával végzik az informatikai katasztrófa elhárítását, azaz:

- saját területükön megszervezik a krízishelyzet kezeléséhez szükséges szakember háttér ügyeleti, elérhetőségi rendszerét, gondoskodnak a szükség szerinti helyettesítésükről,
- informatikai katasztrófa helyzetben az élet és vagyonbiztonságot közvetlenül fenyegető veszélyek elhárításában utasításra, vagy egyes esetekben öntevékenyen részt vesznek,
- képzettségének megfelelően közreműködnek a váratlan események következményeinek feltárásában, ellenőrzik a hozzájuk tartozó erőforrások épségét, tesztelik a berendezéseket, a rendszeresen tájékoztatják a KRÍZIS KÖZPONT VEZETŐJÉT,
- képzettségüknek megfelelően közreműködnek a szolgáltatások eredeti vagy csökkentett funkcióinak helyreállításában.

### 1.9.6 Szakértők

SZAKÉRTŐK (a KRÍZIS KÖZPONT TEAM tagjaiként) e terv érvényességi körén belül:

- ALKALMAZÁS RENDSZERGAZDA
- HÁLÓZATI RENDSZERMÉRNÖK
- HARDVER SZERVIZMÉRNÖK
- HELP DESK MUNKATÁRS
- ÜGYFÉLSZOLGÁLATI MUNKATÁRS
- SZOFTVER SZAKÉRTŐ
- TELEKOMMUNIKÁCIÓS SZAKEMBER
- ÜZEMELTETÉSI SZAKEMBER



A SZAKÉRTŐK:

- informatikai katasztrófa helyzetben az élet és vagyónbiztonságot közvetlenül fenyegető veszélyek elhárításában utasításra, vagy egyes esetekben öntevékenyen részt vesznek,
- képzettségüknek megfelelően közreműködnek a váratlan események következményeinek feltárásában, ellenőrzik a hozzájuk tartozó erőforrások épségét, tesztelik a berendezéseket, a rendszeresen tájékoztatják a KRÍZIS KÖZPONT VEZETŐJÉT,
- képzettségüknek megfelelően közreműködnek a szolgáltatások eredeti vagy csökkentett funkcióinak helyreállításában.

### 1.9.7 Közreműködők

A KÖZREMŰKÖDŐK e terv érvényességi körén belül:

- DISZPÉCSER (Információtovábbító és részfolyamat szervező)
- GÉPKOCSIVEZETŐ

Feladatuk, hogy az informatikai katasztrófa helyzetben az informatikai katasztrófa-elhárításban résztvevők munkájának eredményességét elősegítsék, így különösen segédkezzenek

- az informatikai katasztrófa-elhárítás dokumentálásában,
- adatok, információk továbbításában,
- a szükséges eszközök, személyek szállításában.

### 1.9.8 Kulcsfelhasználók

A KULCSFELHASZNÁLÓK e terv érvényességi körén belül az DUNAÚJVÁROSI EGYETEM információrendszerének a melléklet 4.3. pontjában meghatározott felhasználói, a szolgáltatások nyújtói vagy legfőbb igénybevevői,

- feladatkörüknek és képzettségüknek megfelelően közreműködnek a váratlan események következményeinek feltárásában, ellenőrzik a hozzájuk tartozó erőforrások épségét, tesztelik a berendezéseket, a rendszeresen tájékoztatják vezetőiken keresztül a KRÍZIS KÖZPONT VEZETŐJÉT,
- közreműködnek az általuk nyújtott egyetemi szolgáltatás csökkentett funkcióinak ellátásához szükséges tevékenységek elvégzésében,
- közreműködnek az általuk nyújtott egyetemi szolgáltatás eredeti funkcióinak helyreállításában, a korlátozott üzemben kézzel rögzített adatok bevitelében és ellenőrzésében.

### 1.9.9 Harmadik fél

HARMADIK FÉL e terv érvényességi körén belül a melléklet 4.4. pontjában meghatározott vállalkozók, szállítók, egyéb külső szolgáltatók, erőforrások.

Az DUNAÚJVÁROSI EGYETEM hiányzó erőforrásait kiegészítve informatikai katasztrófa helyzetben a veszélyek elhárításában a KRÍZIS KÖZPONT VEZETŐ javaslatára alapján a KATASZTRÓFA MENEDZSER felkérésére vesznek részt.

Az DUNAÚJVÁROSI EGYETEM hiányzó erőforrásait kiegészítve, vállalkozási és feladatkörükben közreműködnek a váratlan események következményeinek feltárásában, ellenőrzik a megbízásuk terjedelmébe eső erőforrások épségét, tesztelik a berendezéseket, a rendszeresen tájékoztatják képviselőjükön keresztül a KRÍZIS KÖZPONT VEZETŐJÉT.

Közreműködnek a megbízásuk terjedelmébe eső egyetemi alrendszer eredeti vagy csökkentett funkcióinak helyreállításában.

### 1.10 Általános rendelkezések

Amennyiben informatikai katasztrófa helyzet van, annak tényéről és körülményeiről **a sajtónak, egyéb médiumnak, illetve bármely más, az elhárításban közre nem működő külső félnek csak az DUNAÚJVÁROSI EGYETEM KOMMUNIKÁCIÓS KÖZPONTJA tehet nyilatkozatot, a katasztrófa-elhárításban résztvevők és családtagjaik NEM.** Az elhárításban közreműködő külső (harmadik) felek számára átadható információkat illetően a KRÍZIS KÖZPONT VEZETŐ, illetve az általa erre kijelölt személy az illetékes.



### 1.10.1 Elsősegély

Minden informatikai katasztrófa helyzetben **elsődleges feladat a személyzet életének és testi épségének védelme**. Minden egyéb feladat csak akkor kezdhető meg, ha a veszélyeztetett személyek biztonságba kerültek.

A legközelebbi orvosi rendelők címe, telefonszáma:

- Orvosi ügyelet éjszaka és munkaszüneti napokon (2400 Dunaujváros, Vasmű út 10.) (06 25) 410 600
- Mentők: 112

### 1.10.2 Biztonsági követelmények

Az informatikai katasztrófa helyzetben az egyetemi biztonság egészéért a KANCELLÁR a felelős.

Az informatikai katasztrófa helyzetben az informatikai rendszerek logikai hozzáférésére vonatkozó szabályzatok és függelékeik, vagyis

- Sz-02/15 – Informatikai és informatikai biztonsági szabályzat
- E6-01 eljárásleírás – Szoftverek és adatok felügyelete

hatályban maradnak. Az informatikai katasztrófa-elhárítás során ezek rendelkezéseit maradéktalanul be kell tartani.

Az egyetemi biztonsági intézkedések hatékonyságát nagymértékben ronthatja, ha a fenti dokumentumokban foglaltakat nem tartják be, így különösen a legalapvetőbb biztonsági követelményeket – a nyitás-zárásra, a zárt területek használatára, a pénz és érték tárolásra valamint a riasztók és támadásjelzők kipróbálására vonatkozó előírásokat kell maradéktalanul betartani.

Informatikai katasztrófa helyzet esetén, az elhárítási tevékenységek minden szakaszában, egészen a normális üzemre történő visszaállás sikeres befejezéséig, minden folyamatba épített és vezetői ellenőrzést fokozott figyelemmel kell végrehajtani.

Informatikai katasztrófa helyzet esetén az egyes informatikai rendszerek, alkalmazások által készített összes naplóállományokat, különös tekintettel az üzleti tranzakciókról, megbízásokról, illetve adathozzáférésekről készülő naplóállományokat, legalább 1 évig elektronikus formában is meg kell őrizni, a központi biztonsági mentésekre vonatkozó fizikai biztonsági követelményeknek megfelelő tárolás mellett.

Az informatikai katasztrófa helyzetben fellépő további áthidalhatatlan nehézségek esetén a kiegészítő terv az irányadó.

### 1.10.3 Az informatikai katasztrófa események naplózása

Az informatikai katasztrófa esemény kezdetétől a helyreállítás befejezéséig minden eseményről és intézkedésről időrendben naplót kell vezetni.

A KATASZTRÓFA NAPLÓ vezetése a mindenkori feladatok irányítójának (KRÍZIS KÖZPONT VEZETŐ) a felelőssége, az irányító vagy megbízottjának a kötelessége.

A KATASZTRÓFA NAPLÓ a vezetők, a résztvevők számára információforrásként szolgál, valamint az informatikai katasztrófa-helyzet utólagos analizálására, és az INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV felülvizsgálatára is lehetőséget nyújt.

A KRÍZIS KÖZPONT VEZETŐ rendszeresen tájékoztatja az DUNAÚJVÁROSI EGYETEM KATASZTRÓFA MENEDZSER TEAMET az informatikai katasztrófa-elhárítási tevékenység előrehaladásáról, a tartalék erőforrások használatbavételének módjáról, az áttéréshez szükséges időről, a rendszerkiesés következményeiről és a várható veszteségekről.

### 1.10.4 Krízis központ

Az informatikai katasztrófa-helyzet megszüntetéséig a KRÍZIS KÖZPONT VEZETŐ az elhárítást a KRÍZIS KÖZPONTBÓL irányítja. A krízis központot ott kell felállítani, ahol az informatikai rendszer központi funkcióinak helyreállítása történik.



### **1.10.5 A szakértők és a harmadik fél számára figyelembeveendő irányelvek**

1. Az eseményt és körülményeit minden érintett pontosan jegyezze fel. Ezzel megelőzhető az informatikai katasztrófa helyzetek hatását jelentősen súlyosbító kapkodás és dokumentálatlanság.
2. Az aktuális (sérült) állapotot mindenképpen rögzíteni kell. Ez lesz a kiinduló pont, ahová a helyreállítási tevékenység alatt mindig visszatérhet. Innen deríthető ki később a hiba pontos oka is.
3. Ne szégyelljen segítséget kérni, akkor sem, ha a hibát ön követte el. Ez még mindig jobb, mint egy porig rombolt rendszer. Katasztrófa helyzetben a legkisebb hiba akár teljes és visszavonhatatlan adatvesztést eredményez.
4. Minden módosítás előtt és után mentse le a rendszerelemeket, külön figyeljen a naplófájlok (log) mentésére.
5. A KRÍZIS KÖZPONT VEZETŐJÉT informálni kell minden új eseményről, illetve a feladatok státuszáról.



## 2 TEENDŐK INFORMATIKAI KATASZTRÓFA ESETÉN

### 2.1 Az informatikai katasztrófa-elhárítási terv aktiválása, azonnali válasz

Az aktiválási szakasz célja, hogy az élet és vagyonbiztonságot közvetlenül fenyegető veszélyek elhárítását elkezdjék, valamint, hogy a KRÍZIS KÖZPONT VEZETŐT tájékoztassák a kialakult helyzetről. Ezen szakaszban az DUNAÚJVÁROSI EGYETEM valamennyi dolgozójának kötelessége öntevékenyen részt venni.

- ▶ Az életet illetve vagyontárgyat fenyegető veszély esetén először a MENTŐKET és/vagy a TŰZOLTÓKAT (Tel: 112), illetve szükség esetén további vészelhárító szervezeteket kell értesíteni és amennyiben szükséges az 1.10. pontban (ÁLTALÁNOS RENDELKEZÉSEK) leírtaknak megfelelően kell eljárni.
- ▶ Amennyiben informatikai katasztrófa helyzet van, annak tényéről és körülményeiről **a sajtónak, egyéb médiumnak, illetve bármely más, az elhárításban közre nem működő külső félnek csak az DUNAÚJVÁROSI EGYETEM KOMMUNIKÁCIÓS KÖZPONT tehet nyilatkozatot, a katasztrófa-elhárításban résztvevők és családtagjaik NEM.** Az elhárításban közreműködő külső (harmadik) felek számára átadható információkat illetően a KRÍZIS KÖZPONT VEZETŐ, illetve az általa erre kijelölt személy az illetékes.
- ▶ A legrövidebb időn belül tájékoztatni kell a KRÍZIS KÖZPONT VEZETŐT, vagy el nem érhetősége esetén annak helyettesét az informatikai katasztrófa helyzet létrejöttéről vagy annak veszélyéről.
- ▶ A sikeres hívásokat és a sikertelen kísérleteket is KATASZTRÓFA NAPLÓBAN kell rögzíteni.
- ▶ Ha az első helyen megjelölt személy nem érhető el, akkor a bejelentőnek a helyettesként megjelölt személyt kell értesíteni. Ha mindkét próbálkozás eredménytelen, akkor a minden öt percben újra meg kell kísérelni a telefonos kapcsolatfelvételt.
- ▶ Amennyiben az ügyeletes (portaszolgálat, biztonsági szolgálat) a KRÍZIS KÖZPONT VEZETŐT (és a megjelölt helyettesét) az első kísérlettől számítva 15 percen belül nem tudja elérni, úgy az informatikai katasztrófa elhárítását a MŰSZAKI SZOLGÁLTATÓ KÖZPONT VEZETŐJE irányítja. (Ő lesz az ideiglenes KRÍZIS KÖZPONT VEZETŐ.)
- ▶ Ha az informatikai katasztrófa állapot elrendelésére jogosult (KATASZTRÓFA MENEDZSER) elrendeli az informatikai katasztrófa helyzetet, akkor össze kell hívni az adott szituáció elhárításában érintett csoport valamennyi tagját.
- ▶ **A fenti lépésekkel az INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV aktiválási szakasza lezárult, a további lépéseket a KRÍZIS KÖZPONT VEZETŐ utasításai szerint kell elvégezni.**

### 2.2 Az átfogó akcióterv

Az DUNAÚJVÁROSI EGYETEM informatikai katasztrófa elhárítását a KRÍZIS KÖZPONTBÓL a KRÍZIS KÖZPONT VEZETŐ irányítja.

A KRÍZIS KÖZPONT VEZETŐ és a SZAKÉRTŐK által jelentett információkat értékelve, szükség esetén egyéb SZAKÉRTŐK bevonásával deklarálja az informatikai katasztrófa tényét, a rendszerelem csoportok működésképtelenségének szintjét és a katasztrófa esemény bekövetkezésének időzónáját.

A KRÍZIS KÖZPONT VEZETŐ az esemény(ek) jellegének és következményeinek felmérése, az események behatárolása után meghatározza a megfelelő elhárítási forgatókönyvet. Ettől a végrehajtás során, amennyiben szükséges, a KRÍZIS KÖZPONT VEZETŐ utasítása alapján el lehet térni.

A megfelelő forgatókönyv kiválasztásánál a következő kérdésekre adott válaszokat kell első sorban figyelembe venni:

- Van-e áram a központban?
- A központi telephely(ek) lokális hálózata részben vagy egészben használható?
- A forró és meleg tartalékok rendelkezésre állnak-e?
- A tükrözött rendszerek valóban az aktuális állapotot mutatják?
- Az alkalmazások szerver oldali komponensei (adatbázis-kezelők, alkalmazásszerverek, stb.) működnek-e?
- Rendelkezésre állnak-e a mentések?
- Szükséges-e informatikai katasztrófa állapotot elrendelni, vagy „csak” üzemzavaros állapot van?
- Szükséges külső erőforrások, harmadik fél bevonása az elhárításba?





## **2.3 Az események behatárolása**

### **2.3.1 A feladat végrehajtója**

- KRÍZIS KÖZPONT VEZETŐ
- Rendelkezésre álló és esetlegesen behívott SZAKÉRTŐK
- DISZPÉCSER

### **2.3.2 Eszköz, erőforrás igény**

- Telefon, mobiltelefon, email, ezek hiányában gépkocsi, taxi, FUTÁR
- Diagnosztikai eszközök

### **2.3.3 Teendők**

- ▶ A KRÍZIS KÖZPONT VEZETŐJÉNEK felügyeletével az ALKALMAZÁS RENDSZERGAZDÁK és a HÁLÓZATI RENDSZERMÉRNÖKÖK felmérlik az általuk üzemeltetett informatikai szolgáltatások működőképességét.
- ▶ Probléma esetén meghatározzák a váratlan esemény jellegét, a jelenlegi és / vagy várható következményeit.
- ▶ A következmények felmérését a KRÍZIS KÖZPONT VEZETŐ irányítja, szükség esetén meghatározza azokat a szakértői csoportokat, akik meghatározott rendszerelem csoportokat ellenőriznek.
- ▶ A SZAKÉRTŐK az érintett rendszerelemek tesztelésének eredményéről, felhasználási lehetőségeiről a lehető legrövidebb idő alatt jelentést tesznek a KRÍZIS KÖZPONT VEZETŐJÉNEK, aki szükség esetén további tesztek, ellenőrzéseket rendelhet el.

## **2.4 Elhárítási csoport összehívása, érintett felek értesítése**

### **2.4.1 A feladat végrehajtója**

- DISZPÉCSER (annak megérkezéséig a KRÍZIS KÖZPONT VEZETŐ)

### **2.4.2 Eszköz, erőforrás igény**

- Telefon, mobiltelefon, email, ezek hiányában gépkocsi, taxi, FUTÁR

### **2.4.3 Teendők**

- ▶ Az informatikai katasztrófa helyzetnek megfelelő szakembereket a Katasztrófaelhárítói lista (a melléklet 4.2. pontja) alapján be kell hívni.
- ▶ A listából munkaidőn túl KÉSZENLÉTES SZAKÉRTŐKET kell elsősorban kiválasztani és behívni. Amennyiben a KÉSZENLÉTES SZAKÉRTŐ nem érhető el, a listán utána következő azonos szakterületi SZAKÉRTŐT kell behívni. Munkaidőben a bent lévő munkatársak közül a KRÍZIS KÖZPONT VEZETŐ jelöli ki a megfelelő szakértőt.

## **2.5 Kulcsfelhasználók és felhasználók értesítése**

### **2.5.1 A feladat végrehajtója**

- DISZPÉCSER
- Érintett rendszerek/területek vezetői

### **2.5.2 Eszköz, erőforrás igény**

- Telefon, mobiltelefon, email, ezek hiányában gépkocsi, taxi, FUTÁR





### 2.5.3 Teendők

► Az DISZPÉCSER a KRÍZIS KÖZPONT VEZETŐ által meghatározott sorrendben, a rendelkezésre álló leggyorsabb kommunikációs csatorna segítségével értesíti az érintett rendszerek/területek vezetőit és a következő információkat adja meg az érintetteknek:

a) Katasztrófa helyzetben:

- Katasztrófa állapot és annak vázlatos ismertetése, megadva a katasztrófa által érintett főbb területeket (egyetemi vagy informatikai jellegű-e a katasztrófa).
- Az informatikai katasztrófa elhárításának várható, becsült időszükséglete.
- A korlátozott üzem indulásának várható ideje
- Szükség-e az adott szervezeti egység központi tartalék munkahelyekre való áttelepülése.
- A kézi üzemhez szükséges információk.
- Kapcsolattartó neve, beosztása, elérhetősége.

b) A normál üzemre visszaállásakor:

- Az informatikai katasztrófa helyzetnek vége van.
- A kézi adatfeldolgozás eredményeinek visszaállításához szükséges információk.

► Az érintett rendszerek/területek vezetői belátásuk szerinti sorrendben telefonon vagy szóban értesítik a beosztottaikat. Az értesítés során a fent meghatározott információkat adják tovább.

## 2.6 Harmadik fél értesítése

### 2.6.1 A feladat végrehajtója

- DISZPÉCSER
- KRÍZIS KÖZPONT VEZETŐ

### 2.6.2 Eszköz, erőforrás igény

- Telefon, mobiltelefon, email, ezek hiányában gépkocsi, taxi, FUTÁR

### 2.6.3 Teendők

► A KRÍZIS KÖZPONT VEZETŐ utasítása alapján, az DISZPÉCSER telefonon megkeresi a katasztrófa elhárításához igénybe venni kívánt harmadik felek képviselőit.

► Az értesítés során a következő információkat kell megadni az érintetteknek:

- Az igényelt szolgáltatások, erőforrások.
- A teljesítéshez rendelkezésre álló idő.
- A szerződésben meghatározott esetleges egyedi adatok.
- Kapcsolattartó neve, beosztása, elérhetősége.

Amennyiben szükséges gépkocsit, FUTÁRT vagy taxit kell elküldeni a szállítóhoz, szolgáltatóhoz az igényelt eszközökért, szakértőkért.

## 2.7 Informatikai szolgáltatások rekonstrukciója

Az 1.8 fejezet szerinti rendszerek, szolgáltatások helyreállításának menetét (rendszerenként) az alábbi tartalommal kell megadni:

- Előfeltételek (épület, áram, eszköz, szolgáltatás, mentés, stb.), amelyeknek teljesülni kell a visszaállítás megkezdéséhez.
- A visszaállítás menete (lépésről lépésre a szükséges műveletek leírása).



Az informatikai szolgáltatások rekonstrukciójának részletes leírását az „Informatikai katasztrófa-elhárítási kézikönyv” melléklete tartalmazza.

## 2.8 Áttelepülés a központi tartalék munkahelyekre

Amennyiben az egyes alkalmazások a számukra előírt minimális szolgáltatási szint szerinti működést sem képesek nyújtani felhasználók eredeti munkahelyén, vagy a felhasználók vannak akadályozva abban, hogy ezen szolgáltatásokat eredeti munkahelyükön használják, úgy szükségessé válhat egyes alkalmazások, illetve egyes szervezeti egységek felhasználói munkahelyeinek áttelepítésére.

### 2.8.1 A feladat végrehajtója

- DISZPÉCSER
- TELEKOMMUNIKÁCIÓS SZAKEMBEREK
- ÜZEMELTETÉSI SZAKEMBEREK

### 2.8.2 Eszköz, erőforrás igény

- Számítógépek, kommunikációs eszközök a készenléti leltár szerint
- Telefon, mobiltelefon, ezek hiányában gépkocsi, taxi, FUTÁR
- Ha a felhasználók szállításához szükséges: gépkocsi, taxi, FUTÁR

### 2.8.3 Teendők

- ▶ A KRÍZIS KÖZPONT VEZETŐ utasítása alapján az DISZPÉCSER értesíti az érintett alkalmazás KULCSFELHASZNÁLÓIT, illetve az érintett szervezeti egység vezetőit az áttelepülés szükségességéről. (Ezt a pontot csak akkor kell végrehajtani, ha a 2.5 fejezet végrehajtásakor ez nem történt meg.)
- ▶ Amennyiben szükséges, az DISZPÉCSER gépkocsit, FUTÁRT vagy taxit küld a felhasználók szállításához.
- ▶ Az DISZPÉCSER ugyancsak értesíti azon szervezeti egységek vezetőit, amelyeknek jelenleg használatában vannak a készenléti leltárban szereplő eszközök.
- ▶ A KRÍZIS KÖZPONT VEZETŐ az adott helyzet ismeretében, de az érintett szervezeti egységek vezetőivel konzultálva dönt arról, hogy az áttelepülés során a számítógépes munkahelyek jelenlegi helyükön maradhatnak, vagy azokat a kijelölt tartalék helyiségekbe kell vinni.
- ▶ A szakértők (miután szükség esetén az eszközöket az eredeti munkahelyekről a tartalékként kijelölt helyiségbe viszik) meggyőződnek arról, hogy az kijelölt számítógépes munkaállomáson rendelkezésre állnak az előírt informatikai szolgáltatások, futtathatók az alkalmazások.

## 2.9 Készenléti állapot

Készenléti állapot akkor lép életbe, ha

- Az információrendszer üzemel, de tűzriadó, bombariadó vagy egyéb más veszély fenyegetése miatt a SZÁMÍTÓKÖZPONTOT ki kell üríteni
- Katasztrófa helyzet áll fenn, de a tartalékszerverek már valamelyik tartalék helyszínen korlátozottan átvették a központi szerverek funkcióit és kielégítik a KULCSFELHASZNÁLÓK informatikai igényét.

A készenléti állapot során a tükrözött rendszerek, a forró és meleg tartalékszerverek üzemeltetésére, karbantartására, illetve rendelkezésre állásuk ellenőrzésére kiemelt figyelmet kell fordítani.

### 2.9.1 A feladat végrehajtói

- A KATASZTRÓFA MENEDZSER TEAM tagjai

### 2.9.2 Eszköz, erőforrás igény

- Telefon, mobiltelefon, fax, email
- Informatikai rendszerek dokumentációi



### 2.9.3 Teendők

- Minden belső specialistából egy főnek állandóan elérhetőnek kell lennie (intenzív ügyelet).
- Minden felhasználói rendszerért felelős vezetőnek vagy helyettesének állandóan elérhetőnek kell lennie (intenzív ügyelet).
- Az ügyeletes gépkocsit csak korlátozottan, a KATASZTRÓFA MENEDZSER engedélyével lehet használni.
- Értesíteni kell a felhasználókat arról, hogy a KÖZPONTI SZÁMÍTÓGÉPTEREM veszélyeztetettségéből adódó adatkiesés csökkentése, valamint a kisebb kapacitás miatt a halasztható feladatokat hagyják függőben és készüljenek fel az informatikai katasztrófa helyzet kihirdetésére (ha az még nem történt meg).
- A napi karbantartási rendnél gyakoribb hardver és szoftver ellenőrzés és karbantartás.
- Amennyiben a katasztrófa helyzet jellege miatt feltételezhető, hogy a tartalékszerverek fizikai biztonsága fokozottabban veszélyeztetett (például bombariadó esetén) akkor erősített őrzést kell szervezni a tartalékszerverek és a TARTALÉK SZÁMÍTÓGÉPTEREM védelmére.

### 2.10 Kiegészítő terv

A kiegészítő terv akkor lép életbe, ha

- Az informatikai katasztrófa elhárítása során újabb katasztrófa lép fel,
- A mentések, a tartalék eszközök, vagy a személyzet lényeges szereplői nem elérhetők,
- Olyan helyzet áll elő, amelyre nézve az informatikai katasztrófa-elhárítási kézikönyv semmilyen iránymutatással sem szolgál.

Erre az esetben nem fogalmazhatók meg előre egyértelmű feladatok. Az elhárítás pontos menetét ilyenkor az általános elvek figyelembevételével, a pillanatnyi állapot ismeretében, a menedzserek és a szakértők részvételével tartott operatív értekezleten lehet meghatározni.

#### 2.10.1 A feladat végrehajtói

- DUNAÚJVÁROSI EGYETEM KATASZTRÓFA MENEDZSER
- A KATASZTRÓFA MENEDZSER TEAM tagjai
- KRÍZIS KÖZPONT VEZETŐ
- Meghívott Szakértők

#### 2.10.2 Eszköz, erőforrás igény

- Pénz (eszköz és munkaköltségre)
- Telefon, mobiltelefon
- FUTÁR, gépkocsi, taxi
- Minden, az informatikai rendszerrel kapcsolatos dokumentáció

#### 2.10.3 Teendők

- ▶ A KATASZTRÓFA MENEDZSER utasítására az DISZPÉCSERNEK értesíteni kell az DUNAÚJVÁROSI EGYETEM KATASZTRÓFA MENEDZSER TEAM tagjait, az érintett rendszerek fő felhasználóinak a vezetőit, a rendszergazdáit.
- ▶ Operatív értekezlet.
  - Az operatív értekezletet a KRÍZIS KÖZPONT VEZETŐJE vagy valamelyik felettese kezdeményezheti.
  - Az operatív értekezlet témája az informatikai katasztrófa helyzet során fellépett nem várt esemény.
  - Az értekezletet a KATASZTRÓFA MENEDZSER (vagy akadályoztatása esetén megbízott helyettese) vezeti. A KATASZTRÓFA MENEDZSER és a KRÍZIS KÖZPONT VEZETŐ tájékoztatja a résztvevőket a kialakult helyzetről, az informatikai katasztrófa által okozott károkról, a megtett intézkedésekről, a rendelkezésre álló erőforrásokról.



- A SZAKÉRTŐK a KRÍZIS KÖZPONT VEZETŐ vezetésével fontossági sorrendben meghatározzák a szakterületükön kialakult helyzet megoldásához szükséges teendőket, a megoldáshoz szükséges erőforrásokat (elsősorban: ember, eszköz, pénz).
- A felhasználókat képviselő vezetőknek ezek után nyilatkozniuk kell arról, hogy az általuk képviselt (igénybevett vagy nyújtott) szolgáltatásoknak ebben a kritikus esetben mekkorára növelhető a sebezhetőségi ablaka (a leállási idő), milyen megoldásokat lehet alkalmazni az információrendszer vagy egyetemi szolgáltatás kiesésének ellensúlyozására.
- Az operatív értekezlet vezetője összefoglalja a feladat megoldásának menetét, biztosítja a szükséges erőforrásokat és meghatározza a részterületek képviselőinek speciális feladatát.

Olyan esetben, amikor a normális üzemre visszaállásnak kicsiny a lehetősége, nem lehet pontos forgatókönyvet készíteni, csak alapelveket ismertetünk. Ezek a következők:

- Hagyni kell a szakembereket dolgozni, az elhárításban résztvevőkkel kapcsolatos kérdéseket, feladatokat a KRÍZIS KÖZPONT VEZETŐN keresztül kell eljuttatni az érintettekhez.
- Amennyiben a probléma nem triviális, kérjék fel a gyártó vagy szállító cég, esetleg egyéb harmadik fél speciális szakértőjét a feladat megoldásában való közreműködésre. Egy speciális szakértő díja még mindig olcsóbb, mint egy maximális veszteséget okozó informatikai katasztrófa költsége.
- Konzisztenciára kell törekedni, a hiányzó adatokat inkább kézzel vigyék be újra a felhasználók, mintsem, hogy esetleg különböző mentésekből inkonzisztens állapotot állítsanak vissza.
- Mindent dokumentálni kell a későbbi rekonstruáláshoz.
- A 4 szem elvét kell betartani a kritikus folyamatoknál, vagyis biztosítani kell, hogy a kritikus feladatok elvégzésénél legalább két szakértő legyen jelen, akik egymás munkáját ellenőrzik, kiegészítik.
- Minden elektronikus naplót (log), ami a helyreállítás során keletkezik, el kell menteni a további analízishez.
- Az informatikai rendszerben működő automatikus folyamatokat le kell állítani. (Például az automatikus futó mentések).
- Pontos analízist kell készíteni a katasztrófát kiváltó helyzetről és az azokkal interferáló egyéb tényezőkről, többszöröződésekről.
- A jogosultságokat rendszeresen felül kell vizsgálni.
- A mentések helyreállíthatóságát még informatikai katasztrófa helyzetben is tesztelni kell.
- Minden résztvevő az elhárítási tevékenységben gyakorlott szakember legyen (A legalább egy informatikai katasztrófa-elhárítási gyakorlaton keresztülment személyek azok, akikre egy hávária helyzetben számítani lehet).



### 3 OKTATÁSI TEMATIKA

#### 3.1.1 Oktatási célok, követelmények

Az általános oktatási célok a katasztrófa-elhárításban résztvevő számára azonosak, csak az ismeret mértékében és a feldolgozás, rendszerezés, elmélyítés módjában és ezzel párhuzamosan ezek alkalmazásának módjában térhetnek el.

Az informatikai katasztrófában résztvevők gyorsan, biztosan, szakszerűen, az DUNAÚJVÁROSI EGYETEM szabályainak és elveinek megfelelően lássák el az elhárítás során számukra meghatározott feladatokat.

Az oktatásba bevont személyek ismerjék az INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI KÉZIKÖNYVBEN meghatározott jelenségeket, eszközöket, fogalmakat, a szerepkörökre meghatározott feladataikat gyakorolják be a szakterületüknek megfelelő szinten.

A katasztrófaelhárító csoport számára nélkülözhetetlen az ismeretek megértése, feldolgozása, rendszerezése, elmélyítése, elsajátítása és ezzel párhuzamosan azok alkalmazása. Mindezzel, az ebbe a csoportba tartozó szereplőknek az ismeretek eredményes alkalmazását lehetővé tevő jártasságait, rutinszerűen, automatizáltan működő készségeit, az elhárítási tevékenységek széles körében érvényesíthető képességeit, azok fejlődését, fejlesztését kell megalapozni.

A katasztrófaelhárító csoport tagjainak a részletes oktatási céljai:

- Üzemeltetés és balesetvédelem.
- Tudatos magatartás, a biztonsági követelmények és szabályzatok teljes körű ismerete.
- Az azonnali válasz tevékenységeinek önálló alkalmazása.
- A katasztrófa-elhárítási kézikönyv fogalmainak, konvencióinak, szabályainak alkalmazása ismert és váratlan szituációkban.
- A katasztrófa-elhárítás során alkalmazható alapelvek, elméletek és rendszerek alkalmazása ismert és váratlan szituációkban.
- A különböző területeken az elhárítás során eredményes, hatékony döntések, tevékenységek, teljesítmények biztosítása.
- A katasztrófa-elhárításban a meghatározott részterületen gyors, biztos, szakszerű tevékenység folytatása.

#### 3.1.2 Szervezeti keretek, munkaformák, munkamódszerek, eszközök, tananyag időelosztása

A katasztrófaelhárító csoport óraterve:

Téma/óra	Szervezeti keretek / Munka formák	Munkamódszerek	Eszközök
Általános katasztrófa ismeretek 1 óra	Csoport munka	Előadás, megbeszélés	írásvetítő, előadói PC, tábla
A DUNAÚJVÁROSI EGYETEM INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI KÉZIKÖNYVÉNEK bemutatása 3 óra	Frontális csoportmunka	Előadás, megbeszélés	írásvetítő, előadói PC, tábla, INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI KÉZIKÖNYV
Feltételezett katasztrófa gyakorlat 2 óra	Csoportmunka	Megbeszélés, véleménycsere, problémamegoldó kommunikációs tréning	írásvetítő, PC, tábla



Téma/óra	Szervezeti keretek / Munka formák	Munkamódszerek	Eszközök
Katasztrófa gyakorlat értékelése  2 óra	Csoportmunka	Megbeszélés	írásvetítő, előadói PC, tábla

### 3.1.3 Visszacsatolás

A katasztrófa-elhárítási tevékenység fontossága és komplexitása miatt kétféle visszajelzési technikát kell alkalmazni. Ezek a következők:

- azonnali hallgatói reagálás – ennek megfelelő forma a megbeszélés és a csoportmunka,
- esszé jellegű kérdések – ezek lehetőséget nyújtanak arra, hogy az oktatásban résztvevők rendszerezék az ismereteiket, illetve kritikai észrevételeikkel hozzájáruljanak az INFORMATIKAI KATASZTRÓFA-ELHÁRÍTÁSI TERV javításához.



#### 4 EGYÉB RENDELKEZÉSEK

A Kézikönyvet mellékleteivel együtt a Szenátus 2016. szeptember 27. napján tartott ülésén a 2-2016/2017.(2016.09.27.) sz. határozatával fogadta el, hatályba lép 2016. szeptember 28. napján, ezzel egyidejűleg minden, a jelen szabállyal ellentétes rendelkezés hatályát veszti.

Dr. habil András István  
rektor  
Szenátus elnöke



