					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P32					Dokumentum címe: **Üzletmenet-folytonossági és katasztrófa utáni helyreállítási szabályzat**							
Verzió: 1.0		Hatálybalépés dátuma: 01.01.2025			A dokumentum tulajdonosa:							
X	Szabályzat		Szabvány		Eljárás		Űrlap		Nyilvántartás		Egyéb	

Felülvizsgálati előzmények				
Felülvizsgálat száma	**Felülvizsgálat dátuma**	**Változások**	**Felülvizsgálta**	**A folyamat tulajdonosa**

Jóváhagyások			
Név	**Beosztás**	**Dátum**	**Aláírás**

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	8. fejezet	
ISO/IEC 27002:2022	5.29, 5.30 kontroll	
NIST SP 800-53 Rev.5	CP-1–CP-11	
NIST SP 800-34 Rev.1	Vészhelyzeti tervezés	Keretrendszer
ISO 22301:2019		Az üzletmenet-folytonossági irányítási rendszer követelményei
GDPR	32. cikk	
NIS2 irányelv	21. cikk (2) bekezdés f) pont	
DORA-rendelet	10. cikk	
COBIT 2019	DSS	

1. Cél

1.1. Jelen szabályzat meghatározza azokat a kötelező kontrollokat és felelősségi köröket, amelyek biztosítják, hogy a szervezet a működést zavaró incidens során és azt követően képes legyen a kritikus üzleti működés és az azt támogató IKT-szolgáltatások fenntartására vagy helyreállítására.

1.2. A szabályzat célja az emberi élet védelme, a működési stabilitás biztosítása, a jogszabályi kötelezettségek és ügyfélvállalások teljesítése, valamint a szervezet jó hírnevének megőrzése proaktív tervezés, ellenőrzött helyreállítási képességek és a reziliencia beépítése révén.

1.3. Jelen szabályzat alapot biztosít a szervezet üzletmenet-folytonossági és katasztrófa utáni helyreállítási keretrendszeréhez, és biztosítja a vonatkozó szabályozási, szerződéses és iparági követelményeknek való megfelelést.

2. Hatály

2.1. Jelen szabályzat kiterjed valamennyi olyan szervezeti egységre, információs rendszerre, üzleti folyamatra, munkatársra és harmadik fél által nyújtott szolgáltatásra, amely az üzleti hatásvizsgálat (BIA) eredménye alapján kritikusnak vagy lényegesnek minősül.

2.2. A szabályzat az alábbiakra terjed ki:

2.2.1. természetes eredetű és ember által okozott működéskiesésekre, ideértve a kibertámadásokat, infrastruktúrahibákat, adatközpont-kieséseket, pandémiákat és a beszállítói szolgáltatáskieséseket;

2.2.2. üzletmenet-folytonossági és katasztrófa utáni helyreállítási tervek (BCP/DRP) tervezésére, tesztelésére és folyamatos fejlesztésére;

2.2.3. szerepkörökre és felelősségekre a vészhelyzeti reagálás, a helyreállítás koordinálása és az incidenseszkaláció terén.

2.3. Jelen szabályzat rendelkezései kötelezőek minden olyan munkatársra, ideértve az IT-területet, az üzleti területek tulajdonosait, a válságkezelésben részt vevő személyeket és a beszállítókat is, akik folytonossági vagy helyreállítási feladatot látnak el.

3. Célkitűzések

3.1. Az üzleti működés és a szolgáltatások folytonosságának biztosítása előre meghatározott és tesztelt eljárásokkal, a működési, reputációs és jogi hatások minimalizálása mellett.

3.2. Az IKT-szolgáltatások helyreállítása a meghatározott helyreállítási időcélok (RTO) és helyreállítási pont célértékek (RPO) szerint, az üzleti kockázattűrési szintekkel összhangban.

3.3. Az üzletmenet-folytonossági és katasztrófa utáni helyreállítási tervezés, végrehajtás és irányítás tulajdonosi felelősségének egyértelmű kijelölése a teljes szervezetre kiterjedően.

3.4. Annak biztosítása, hogy a folytonossági képességeket rendszeresen teszteljék, karbantartsák, és valósághű forgatókönyvek, valamint auditmegállapítások alapján fejlesszék.

3.5. Az ISO-, NIST-, GDPR-, DORA- és NIS2-követelmények teljesítése, támogatva a kellő gondosság igazolását az operatív reziliencia és a rendelkezésre állás terén.

4. Szerepkörök és felelősségek

4.1. Felső vezetés

4.1.1. Jóváhagyja az üzletmenet-folytonossági és katasztrófa utáni helyreállítási szabályzatot, és biztosítja annak stratégiai összhangját.

4.1.2. Költségvetést és erőforrásokat biztosít az üzletmenet-folytonosság, a vészhelyzeti reagálás és a helyreállítási gyakorlatok támogatásához.

4.2. Üzletmenet-folytonossági vezető

4.2.1. Felelős a szervezetszintű üzletmenet-folytonossági tervek kidolgozásáért és karbantartásáért, valamint a folytonossági tesztek koordinálásáért.

4.2.2. Fenntartja a BIA ütemtervét, támogatja a képzéseket, és biztosítja, hogy a dokumentáció megfeleljen a megfelelőségi követelményeknek.

[... A 4.3–8. szakaszok nem szerepelnek ebben az előnézetben. A teljes tartalom eléréséhez vásárolja meg a teljes dokumentumot. ...]

9. Felülvizsgálati és frissítési követelmények

9.1. Jelen szabályzatot az üzletmenet-folytonossági vezetőnek és az információbiztonsági vezetőnek évente felül kell vizsgálnia az alábbiakkal való összhang biztosítása érdekében:

9.1.1. az üzleti működésben, a kritikus rendszerekben vagy az infrastruktúrában bekövetkezett változások;

9.1.2. incidensekből, auditokból, asztali gyakorlatokból vagy DR-tesztekből származó tanulságok;

9.1.3. frissített szabályozási vagy szerződéses kötelezettségek (pl. DORA, GDPR, ügyféloldali RTO/RPO-követelmények);

9.1.4. a szervezet kockázatvállalási hajlandóságának vagy folytonossági stratégiájának változásai.

9.2. A felülvizsgálatoknak tartalmazniuk kell:

9.2.1. a tervek relevanciájának és a kapcsolattartási adatoknak az ellenőrzését;

9.2.2. az RTO-k, az RPO-k és a helyreállítási szintek újraértékelését;

9.2.3. a biztonsági mentési és helyreállítási szolgáltatási kapacitás értékelését;

9.2.4. azon érintett felek visszajelzéseit, akik a közelmúltban helyreállítási terveket vagy teszteket hajtottak végre.

9.3. Minden szabályzatmódosítást:

9.3.1. verziókezelés alatt, dokumentált indoklással és az érintettek jóváhagyásával kell kezelni;

9.3.2. közölni kell a kulcsszereplőkkel és az érintett csapatokkal a frissített felelősségi körökkel együtt;

9.3.3. meg kell jeleníteni a frissített képzésekben, tudatosságnövelő anyagokban és működési eljárásokban.

9.4. Sürgősségi, soron kívüli frissítést kell kiadni, ha jelentős szervezeti változás, jogi előírás vagy kritikus megállapítás miatt a jelenlegi tervek vagy a szabályzat már nem alkalmazhatók.

10. Kapcsolódó szabályzatok és összefüggések

10.1. Jelen szabályzat az alábbi kulcsfontosságú dokumentumokkal összehangoltan működik:

10.1.1. P1 – Információbiztonsági szabályzat: meghatározza a kockázatalapú, reziliens működés követelményét minden körülmények között.

10.1.2. P5 – Változáskezelési szabályzat: biztosítja, hogy minden helyreállítással összefüggő konfiguráció- vagy infrastruktúraváltozás dokumentált és jóváhagyott munkafolyamat szerint történjen.

10.1.3. P14 – Adatmegőrzési és megsemmisítési szabályzat: szabályozza a folytonossági működés során használt biztonsági mentési adathordozók és helyreállított adatok életciklusát.

10.1.4. P15 – Biztonsági mentési és helyreállítási szabályzat: előírja a biztonsági mentési gyakoriságra, a védelemre és a helyreállítás ellenőrzésére vonatkozó kontrollokat.

10.1.5. P18 – Kriptográfiai kontrollok szabályzata: biztosítja, hogy a helyreállítási folyamatok megfeleljenek a titkosítási és bizalmassági követelményeknek.

10.1.6. P22 – Naplózási és felügyeleti szabályzat: támogatja a folytonosságot érintő események észlelését és eszkalációját.

10.1.7. P30 – Incidenskezelési szabályzat: meghatározza a folytonossági kiváltó eseményekhez igazított elszigetelési, eszkalációs és gyökérokelemzési folyamatokat.

10.1.8. P33 – Audit- és megfelelőségfelügyeleti szabályzat: ellenőrzi a folytonossági és helyreállítási gyakorlatok sértetlenségét és hatékonyságát a rendszerek és folyamatok teljes körében.

11. Hivatkozott szabványok és keretrendszerek

11.1. Jelen szabályzat összhangban áll a nemzetközileg elfogadott üzletmenet-folytonossági és katasztrófa utáni helyreállítási szabványokkal, támogatva az auditálhatóságot, a rezilienciát és a jogi megfelelést.

11.2. ISO/IEC 27002

11.2.1. Az 5.29. kontroll – Információbiztonság működést zavaró események alatt: előírja a biztonsági kontrollok folytonosságát kedvezőtlen körülmények között.

11.2.2. Az 5.30. kontroll – IKT-felkészültség az üzletmenet-folytonosságra: előírja az IKT-helyreállítási képességek előkészítését, tesztelését és ellenőrzését.

11.3. ISO 22301:2019 – Üzletmenet-folytonossági irányítási rendszerek

11.3.1. Keretet biztosít az üzletmenet-folytonossági gyakorlatok kialakításához, bevezetéséhez és fenntartásához a szervezeti célokkal és kockázati küszöbértékekkel összhangban.

11.4. NIST SP 800-34 Rev.1 – Vészhelyzeti tervezési útmutató

11.4.1. Bemutatja az IT-rendszerek vészhelyzeti terveire vonatkozó legjobb gyakorlatokat, beleértve a folytonossági stratégia kialakítását, a hatáselemzést és a tervek tesztelését.

11.5. GDPR (2016/679)

11.5.1. 32. cikk – Az adatkezelés biztonsága: előírja az adatkezelő rendszerek rezilienciáját, valamint a rendelkezésre állás és a személyes adatokhoz való hozzáférés időben történő helyreállítását incidens esetén.

11.6. NIS2 irányelv (2022/2555)

11.6.1. 21. cikk (2) bekezdés f) pont: előírja az üzletmenet-folytonossági és válságkezelési intézkedéseket a hálózati és információs rendszerek biztonságának támogatása érdekében.

11.7. DORA-rendelet (2022/2554)

11.7.1. 10. cikk – IKT-üzletmenet-folytonosság: előírja, hogy a pénzügyi szervezetek kockázatalapú RTO/RPO-értékeket és átkapcsolási képességeket is magában foglaló IKT-folytonossági terveket dolgozzanak ki és teszteljenek.

11.8. COBIT 2019

11.8.1. DSS04 – Folytonosság kezelése: lefedi a folytonossági tervezés valamennyi elemét, beleértve a fenyegetések azonosítását, a hatáselemzést, a helyreállítási stratégiát és a rendszeres tesztelést.