					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P15					Dokumentum címe: **Biztonsági mentési és 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	6.1.3., 8. pont	Kockázatkezelési, tervezési és operatív biztonsági mentési kontrollok
ISO/IEC 27002:2022	8.13., 5.28., 5. kontroll	Biztonsági mentések kezelése, biztonságos megsemmisítés
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	Rendszermentési, helyreállítási és adathordozó-tisztítási követelmények
GDPR	32. cikk, 49. preambulumbekezdés	A személyes adatok helyreállítása és rendelkezésre állása, üzletmenet-folytonosság
NIS2 irányelv	21. cikk (2) bekezdés c–e pont	A rezilienciát támogató biztonsági mentési és folytonossági kontrollok
DORA-rendelet	10., 11. cikk	A pénzügyi szektor biztonsági mentési, helyreállítási és tesztelési követelményei
COBIT 2019	DSS01, DSS04, MEA	Biztonsági mentési műveletek, folytonosság és a megfelelés nyomon követése

1. Cél

1.1 Jelen szabályzat célja az adatok, rendszerek és alkalmazások biztonsági mentésére és helyreállítására vonatkozó kötelező követelmények meghatározása az operatív reziliencia, az adatintegritás és az üzletmenet-folytonosság támogatása érdekében.

1.2 A szabályzat egységes keretrendszert határoz meg az alábbiakra:

1.2.1 A szervezeti adatok védelme a törlésből, adatsérülésből, meghibásodásból vagy kibertámadásokból eredő adatvesztéssel szemben

1.2.2 A helyreállítási elvárások meghatározása egyértelmű RTO (Recovery Time Objective) és RPO (Recovery Point Objective) paraméterek útján

1.2.3 A biztonsági mentési műveletek integrálása a tágabb IBIR-be, valamint az üzletmenet-folytonossági tervekbe (BCP/DRP)

1.2.4 A rendelkezésre állásra és helyreállíthatóságra vonatkozó alkalmazandó jogszabályoknak és ágazati előírásoknak való megfelelés biztosítása

1.3 A szabályzat érvényesíti az ISO/IEC 27001:2022 szabvány biztonságos adatmegsemmisítéssel (5.28), rezilienciával (5.29) és információk biztonsági mentésével (8.13) kapcsolatos kontrolljait, továbbá illeszkedik az ISO/IEC 27002:2022, a NIST SP 800-53 Rev.5, a GDPR, a DORA-rendelet és a NIS2 irányelv bevált gyakorlataihoz.

2. Hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 Az IBIR hatálya alá tartozó valamennyi üzletmenet-kritikus és operatív rendszerre

2.1.2 Valamennyi strukturált és strukturálatlan üzleti adatra, ideértve az adatbázisokat, fájlokat, e-maileket és konfigurációkat

2.1.3 Minden környezetre — helyszíni, felhőalapú, hibrid, valamint távoli/telephelyen kívüli tárolásra

2.1.4 Valamennyi munkatársra, aki a biztonsági mentési folyamatok kezeléséért, végrehajtásáért, ellenőrzéséért vagy a helyreállításért felelős

2.2 A szabályzat az alábbiakra is alkalmazandó:

2.2.1 A biztonsági mentési adathordozókra és infrastruktúrára, beleértve a fizikai szalagokat, virtuális készülékeket, lemezképeket és felhőalapú biztonsági mentési megoldásokat

2.2.2 Azokra a harmadik fél szolgáltatókra, amelyekkel a szervezet szerződést kötött a biztonsági mentések üzemeltetésére, kezelésére vagy feldolgozására

2.2.3 A naplók, konfigurációk, auditnyomok és az üzletmenet-folytonosság szempontjából kritikus operatív dokumentáció biztonsági mentésére

2.3 Azokat a rendszereket, amelyek kifejezetten kizártak a biztonsági mentésből, dokumentálni kell, kockázatértékelés alá kell vetni, és kizárásukat az információbiztonsági vezetőnek és a rendszergazdának formálisan jóvá kell hagynia.

3. Célkitűzések

3.1 Biztosítani kell, hogy minden kritikus rendszer és adat megbízhatóan, megfelelő gyakorisággal, redundanciával és biztonsági kontrollok mellett kerüljön mentésre.

3.2 Olyan helyreállítási mechanizmusokat kell biztosítani, amelyek az üzleti hatásvizsgálatokkal összhangban teljesítik a meghatározott RTO- és RPO-követelményeket.

3.3 Fenn kell tartani a biztonsági mentési eljárásokra, megőrzési ütemezésekre, szerepkörökre és technológiákra vonatkozó teljes körű dokumentációt.

3.4 A biztonsági mentési műveletek eredményességét rendszeres helyreállítási teszteléssel, a hibák naplózásával és a helyesbítő intézkedések nyomon követésével kell ellenőrizni.

3.5 A biztonsági mentési adatokat teljes életciklusuk során védeni kell a jogosulatlan hozzáféréstől, módosítástól vagy megsemmisítéstől.

3.6 Biztosítani kell a megfelelést az alábbiaknak:

3.6.1 Az ISO/IEC 27001 operatív és folytonossági kontrollkövetelményeinek

3.6.2 A NIST SP 800-53 CP és MP kontrollcsaládjainak a biztonsági mentés és az adathordozó-tisztítás területén

3.6.3 A GDPR 32. cikkének és 49. preambulumbekezdésének a személyes adatokhoz való hozzáférés helyreállítására vonatkozó követelményeinek

3.6.4 A DORA-rendelet 10. cikkének és a NIS2 irányelv 21. cikkének az IKT-folytonosság és reziliencia vonatkozásában

3.7 Biztosítani kell, hogy a harmadik fél által nyújtott biztonsági mentési szolgáltatások megfeleljenek a szerződéses és jogszabályi biztonsági kötelezettségeknek, beleértve a titkosítást, a megsemmisítést és az értesítési protokollokat.

4. Szerepkörök és felelősségi körök

4.1 Felső vezetés

4.1.1 Jóváhagyja ezt a szabályzatot, és biztosítja, hogy az üzletmenet-kritikus rendszerek védelmét jóváhagyott biztonsági mentési és helyreállítási gyakorlatok támasszák alá.

4.1.2 Felelős azért, hogy a biztonsági mentési műveletek megfelelő erőforrásokkal rendelkezzenek, és jogszabályi megfelelőségi szempontból rendszeres felülvizsgálat alá kerüljenek.

4.2 Információbiztonsági vezető

4.2.1 A szabályzat gazdája, és biztosítja annak összhangját a tágabb információbiztonsági, kockázatkezelési és folytonossági keretrendszerekkel.

4.2.2 Felügyeli a biztonsági mentési eljárások integrálását a BCP/DRP-be, az incidenskezelésbe és a rezilienciatervezésbe.

4.2.3 Felülvizsgálja a biztonsági mentési kivételeket, és értékeli a kritikus rendszerek kizárására vonatkozó kockázatelfogadási javaslatokat.

[... 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 legalább évente egyszer felül kell vizsgálni, vagy ennél korábban, ha azt az alábbiak indokolják:

9.1.1 Az üzletmenet-folytonossági vagy katasztrófa-helyreállítási stratégia változásai

9.1.2 Új jogszabályi vagy egyéb jogi kötelezettségek, amelyek a biztonsági mentés gyakoriságát vagy az adatmegőrzést érintik

9.1.3 A rendszerarchitektúra, a biztonsági mentési eszközök vagy a szolgáltatók változásai

9.1.4 Jelentős incidensek vagy auditmegállapítások adatvesztéssel vagy helyreállítási hibákkal kapcsolatban

9.2 A felülvizsgálatot az információbiztonsági vezető koordinálja az alábbiakkal együttműködésben:

9.2.1 IT-infrastruktúra és üzemeltetés

9.2.2 Belső audit

9.2.3 Adatvédelmi tisztviselő (DPO)

9.2.4 Üzletmenet-folytonossági és katasztrófa-helyreállítási csapatok

9.3 A biztonsági mentési ütemezéseket, a rendszerbeválasztási listákat, a helyreállítási dokumentációt és a kivételnyilvántartásokat párhuzamosan felül kell vizsgálni annak biztosítása érdekében, hogy:

9.3.1 A biztonsági mentési lefedettség valamennyi kritikus vagyonelemre pontos legyen

9.3.2 Teljesüljenek az RTO/RPO- és megőrzési követelmények

9.3.3 A tesztelési naplók és incidensjelentések teljes körűek legyenek

9.3.4 A korábban azonosított kontrollhiányosságok javítása megtörténjen

9.4 Minden frissítésnek:

9.4.1 Verziókezelés alatt kell állnia, és az IBIR dokumentációs tárában meg kell őrizni

9.4.2 Tartalmaznia kell a változások összefoglalását és azok indoklását

9.4.3 A felső vezetés jóváhagyásával kell rendelkeznie

9.4.4 Az érintett műszaki és üzleti munkatársak felé kommunikálni kell

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat közvetlenül támogatja és kapcsolódik az alábbi dokumentumokhoz:

10.1.1 P6 - Kockázatkezelési szabályzat: Meghatározza a rendszerek és szolgáltatások biztonsági mentési védelmének kockázatalapú priorizálását.

10.1.2 P12 - Eszközkezelési szabályzat: Biztosítja, hogy a biztonsági mentésre kijelölt rendszerek szerepeljenek az eszköznyilvántartásban, és kapcsolódjanak az életciklus-követéshez és az osztályozáshoz.

10.1.3 P13 - Adatosztályozási és címkézési szabályzat: Meghatározza, mely adatkategóriák igényelnek biztonsági mentést, beleértve a prioritáskezelést támogató címkézési metaadatokat.

10.1.4 P14 - Adatmegőrzési és megsemmisítési szabályzat: Összehangolja a biztonsági mentések megőrzését a jogszabályi megőrzési korlátokkal és a lejárt adathordozók megfelelő megsemmisítésével.

10.1.5 P16 - Adatmaszkolási és álnevesítési szabályzat: Támogatja az adattakarékosságot az érzékeny adatkészletek biztonsági mentése során.

10.1.6 P30 - Incidenskezelési szabályzat: Aktiválódik biztonsági mentési hibák, helyreállítási problémák vagy a biztonsági mentési adattárak kompromittálódása esetén.

10.2 Ezek az egymáshoz kapcsolódó szabályzatok egységes keretrendszert alkotnak, amely biztosítja, hogy a biztonsági mentések irányítása beépüljön a szervezet tágabb IBIR-ébe és operatív rezilienciastratégiájába.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001:

11.1.1 6.1.3. pont - Kockázatkezelési terv: Támogatja a kockázatalapú biztonsági mentési priorizálást és helyreállítási tervezést.

11.1.2 8.1. pont - Operatív tervezés és szabályozás: A helyreállítási és folytonossági kontrollokat az operatív védelmi intézkedések részeként integrálja.

11.1.3 A melléklet 5.28. kontroll - Berendezések biztonságos megsemmisítése vagy újrahasználata: Szabályozza a biztonsági mentési adathordozók biztonságos törlését.

11.1.4 A melléklet 5.29. kontroll - Információbiztonság zavarhelyzet idején: Biztosítja a helyreállítási képességeket incidensek vagy katasztrófahelyzetek során.

11.1.5 A melléklet 8.13. kontroll - Információk biztonsági mentése: Közvetlenül lefedett az ütemezett, tesztelt és biztonságos biztonsági mentési műveletek révén.

11.2 ISO/IEC 27002:2022 - 8.13., 5.28., 5. kontroll: Ezek a kontrollok megerősítik a rendszeres biztonsági mentések, a sértetlenség ellenőrzése és a helyreállítási tervezés követelményét valamennyi IT-környezetben.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - Rendszermentés: Átfogó biztonsági mentési eljárásokat határoz meg, beleértve a telephelyen kívüli tárolást és a helyreállítási tesztelést.

11.3.2 CP-10 - Rendszer-helyreállítás és visszaállítás: Olyan ellenőrzött eljárásokat ír elő a teljes vagy részleges helyreállításhoz, amelyek összhangban állnak a helyreállítási célokkal.

11.3.3 MP-6 - Adathordozók tisztítása: Biztosítja az elavult biztonsági mentési adathordozók biztonságos kezelését.

11.3.4 SI-12 - Információkezelési eljárások: Megerősíti az érzékeny adatokhoz kapcsolódó biztonsági mentési és helyreállítási felelősségeket.

11.4 GDPR (2016/679):

11.4.1 32. cikk - Az adatkezelés biztonsága: Előírja a helyreállítási képességeket és az adatok rendelkezésre állását biztosító védelmi intézkedéseket, különösen a személyes adatok esetében.

11.4.2 49. preambulumbekezdés: Támogatja az üzletmenet-folytonossági és katasztrófa-helyreállítási intézkedéseket, beleértve a biztonságos biztonsági mentést a szervezeti reziliencia részeként.

11.5 NIS2 irányelv (2022/2555):

11.5.1 21. cikk (2) bekezdés c–e pont: Előírja azokat a technikai és szervezeti intézkedéseket, köztük a biztonsági mentési és folytonossági kontrollokat, amelyek a szolgáltatások rezilienciáját biztosítják.

11.6 DORA-rendelet (2022/2554):

11.6.1 10. cikk - IKT-üzletmenet-folytonosság: Előírja, hogy a pénzügyi szervezetek teljes körű adatmentési, helyreállítási és folytonossági tervezéssel rendelkezzenek.

11.6.2 11. cikk - Az IKT-üzletmenet-folytonossági tervek tesztelése: Hangsúlyozza a helyreállítási képességek rendszeres tesztelés útján történő ellenőrzését.

11.7 COBIT 2019:

11.7.1 DSS01 - Menedzselt üzemeltetés: Támogatja a szolgáltatások megbízható nyújtását a védett adatok rendelkezésre állása révén.

11.7.2 DSS04 - Menedzselt folytonosság: Meghatározza a stratégiai és operatív folytonossági kontrollokat, beleértve az ellenőrzött biztonsági mentéseket.

11.7.3 MEA03 - Megfelelés monitorozása, értékelése és felmérése: Előírja a folytonossági intézkedések, köztük a biztonsági mentési kontrollok eredményességének időszakos felülvizsgálatát.