					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P15S					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	8. pont	Az IBIR követelményeinek megfelelő biztonsági mentési kontrollok
ISO/IEC 27002:2022	5.29. kontroll, 8. fejezet	Iparági legjobb gyakorlatok a biztonsági mentéshez és az üzletmenet-folytonossággal való integrációhoz
NIST SP 800-53 Rev.5	CP-9, MP-6	Biztonsági mentés és adathordozó-védelem
EU NIS2	21. cikk (2) bekezdés c) pont	Reziliencia és üzletmenet-folytonosság biztonsági mentés révén
EU DORA	10. cikk (1) bekezdés	IKT-folytonosság – biztonsági mentés pénzügyi szervezetek számára
COBIT 2019	BAI04.05, DSS04	Biztonsági mentések dokumentálása és tesztelése, kontrollfolyamatok
EU GDPR	5. cikk (1) bekezdés f) pont, 32. cikk (1) bekezdés c) pont	Az adatok sértetlensége, rendelkezésre állása és időben történő helyreállíthatósága

1. Cél

1.1 Jelen szabályzat meghatározza, hogy a szervezet miként végzi és kezeli a biztonsági mentéseket az üzletmenet-folytonosság biztosítása, az adatvesztés megelőzése és az incidensekből történő időbeni helyreállítás érdekében.

1.2 A szabályzat kötelező érvényű előírásokat állapít meg arra vonatkozóan, hogy a rendszerekről és adatokról milyen módon kell biztonsági mentést készíteni, azokat tárolni és helyreállítani, különösen összetett IT-infrastruktúrával nem rendelkező KKV-k esetében.

1.3 Jelen szabályzat támogatja az auditkészültséget és az ISO/IEC 27001 tanúsítást azáltal, hogy biztosítja a lényeges biztonsági mentési kontrollok meglétét, következetes alkalmazását és rendszeres felülvizsgálatát.

1.4 A szervezet műszaki hibákból, véletlen törlésből vagy kiberincidensekből való helyreállítási képessége a jelen szabályzat szigorú betartásától függ.

2. Hatály

2.1 Jelen szabályzat valamennyi üzleti rendszerre és adatra kiterjed, ideértve különösen az alábbiakat:

2.1.1 pénzügyi nyilvántartások, ügyféladatok és HR-adatok;

2.1.2 az üzleti működés során használt asztali számítógépeket, laptopokat, szervereket és felhőalkalmazásokat;

2.1.3 biztonsági mentési adathordozókat, például USB-meghajtókat, külső tárolókat vagy felhőalapú biztonsági mentéseket.

2.2 A szabályzat vonatkozik továbbá minden olyan személyre, aki felelős a biztonsági mentési folyamatok végrehajtásáért vagy kezeléséért, beleértve:

2.2.1 az ügyvezetőt vagy más kijelölt felelős személyt;

2.2.2 a külső IT-támogatást nyújtó szolgáltatókat vagy tanácsadókat;

2.2.3 valamennyi munkavállalót, aki köteles az adatokat jóváhagyott helyekre menteni.

3. Célkitűzések

3.1 Biztosítani kell, hogy minden kritikus üzleti adatról és rendszerről a kockázatokkal és az üzleti igényekkel összhangban, megfelelő gyakorisággal készüljön biztonsági mentés.

3.2 Biztosítani kell, hogy az adatok üzemzavar esetén időben és teljes körűen helyreállíthatók legyenek.

3.3 Megfelelő tárolási kontrollokkal meg kell akadályozni a biztonsági mentési adatokhoz való jogosulatlan hozzáférést, azok módosítását vagy elvesztését.

3.4 Egyértelműen meg kell határozni és érvényesíteni kell a biztonsági mentési és helyreállítási eljárások végrehajtásához és teszteléséhez kapcsolódó szerepköröket és felelősségi köröket.

3.5 Strukturált és dokumentált biztonsági mentési gyakorlatokkal támogatni kell az ISO/IEC 27001, a GDPR és más szabályozási kötelezettségek teljesítését.

4. Szerepkörök és felelősségi körök

4.1 Ügyvezető

4.1.1 Jóváhagyja jelen szabályzatot, és biztosítja annak betartatását.

4.1.2 Erőforrásokat biztosít, valamint kijelöli a biztonsági mentési és helyreállítási tevékenységek felelőseit.

4.1.3 Felülvizsgálja a biztonsági mentési hibákat, incidenseket és szabályzattól való eltéréseket.

4.1.4 Irányítja az éves szabályzati felülvizsgálatot, és biztosítja az auditkészültséget.

4.2 Külső IT-szolgáltató (ha alkalmazandó)

4.2.1 Bevezeti és üzemelteti a biztonsági mentési megoldásokat (helyi vagy felhőalapú).

4.2.2 Nyomon követi a biztonsági mentések sikerességét, és ütemezi a helyreállítási teszteket.

4.2.3 A hibákat és incidenseket közvetlenül jelenti az ügyvezetőnek.

4.2.4 Biztosítja a titkosítást, a hozzáférés-korlátozást és a biztonsági mentési adathordozók megfelelő kezelését.

[... 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 ügyvezetőnek legalább évente egyszer felül kell vizsgálnia. Soron kívüli felülvizsgálatot különösen az alábbi események válthatnak ki:

9.1.1 jelentős változások a rendszerekben vagy a tárolási módszerekben;

9.1.2 új felhő- vagy IT-platformok bevezetése;

9.1.3 az adat-helyreállítást érintő jogi vagy szabályozási változások;

9.1.4 auditokból vagy incidensekből származó megállapítások.

9.2 Az ügyvezető felelős a felülvizsgálat kezdeményezéséért, a módosítások jóváhagyásáért és a változások kommunikálásáért.

9.3 A szabályzat verzióit nyomon kell követni és archiválni kell. A hatályon kívül helyezett verziókhoz való hozzáférést korlátozni kell annak érdekében, hogy audit vagy üzletmenet-helyreállítás során ne okozzanak félreértést.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat az alábbi KKV-szabályzatokkal áll összhangban, és azokhoz kapcsolódik:

10.1.1 P14S – Adatmegőrzési és selejtezési szabályzat: meghatározza, hogy a biztonsági mentési adatokat mennyi ideig kell megőrizni és biztonságosan törölni.

10.1.2 P13S – Adatosztályozási és jelölési szabályzat: támogatja annak meghatározását, hogy az osztályozási szintek alapján mely adatokról kell biztonsági mentést készíteni.

10.1.3 P30S – Incidenskezelési szabályzat: meghatározza a követendő eljárásokat, ha a biztonsági mentés sikertelen, vagy ha adatsértést vagy szolgáltatáskiesést követően adat-helyreállítás szükséges.

10.1.4 P2S – Irányítási szerepkörök és felelősségek szabályzata: egyértelmű döntési jogosultságot rendel a biztonsági mentések felügyeletéhez és a szabályzat betartatásához.

10.1.5 P17S – Adatvédelmi és magánszféra-védelmi szabályzat: biztosítja, hogy a személyes adatok biztonsági mentésekkel kapcsolatos kezelése összhangban álljon a jogi és adatvédelmi előírásokkal.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 8.1 pont: a biztonsági mentési rendszerek operatív tervezése és szabályozása az IBIR részeként.

11.2 ISO/IEC 27002

11.2.1 8.13 kontroll: meghatározza a biztonsági mentések ütemezésére, nyomon követésére és helyreállítására vonatkozó iparági legjobb gyakorlatokat.

11.2.2 5.29 kontroll: a biztonsági mentés integrációja az üzletmenet-folytonossággal és a helyreállítási felkészültséggel.

11.3 NIST SP 800-53 Rev.5

11.3.1 CP-9 (Vészhelyzeti tervezés): strukturált biztonsági mentési stratégiákat határoz meg az üzleti reziliencia érdekében.

11.3.2 MP-6 (Adathordozó-védelem): előírja a biztonsági mentési adathordozók biztonságos kezelését és megsemmisítését.

11.4 EU GDPR

11.4.1 5. cikk (1) bekezdés f) pont: előírja a személyes adatok sértetlenségét és rendelkezésre állását.

11.4.2 32. cikk (1) bekezdés c) pont: előírja annak képességét, hogy a személyes adatokhoz való hozzáférés időben helyreállítható legyen.

11.5 EU NIS2 irányelv

11.5.1 21. cikk (2) bekezdés c) pont: a reziliencia és a folytonossági tervezés részeként előírja a biztonsági mentést és a helyreállítást.

11.6 EU DORA

11.6.1 10. cikk (1) bekezdés: a pénzügyi szektor szervezeteinek biztosítaniuk kell a biztonsági mentést az IKT-folytonossági intézkedések részeként.

11.7 COBIT 2019

11.7.1 BAI04.05: dokumentált biztonsági mentési stratégiákat ír elő.

11.7.2 DSS04.07: hangsúlyozza a rendszeres tesztelést, valamint az adatmentési és helyreállítási folyamatok feletti kontrollt.