					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P06S					Dokumentum címe: **Kockázatkezelési 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**

Összhangban a vonatkozó szabványokkal és jogszabályokkal

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	6.1, 6.1. pont	
ISO/IEC 27002:2022	5.4, 5. pont	
NIST SP 800-53 Rev.5	RA-1–RA-7, PM-9	
EU NIS2	21. cikk (2) bekezdés a–d pont	
EU DORA	5. cikk	
COBIT 2019	APO12, MEA	

1. Cél

1.1 Jelen szabályzat meghatározza, hogy a szervezet hogyan azonosítja, értékeli és kezeli az információbiztonsággal, az üzemeltetéssel, a technológiával és a harmadik felek szolgáltatásaival kapcsolatos kockázatokat.

1.2 Biztosítja, hogy a kockázatkezelés a tervezés, a projektek végrehajtása, a beszállítók kiválasztása és az incidenskezelés szerves részét képezze, összhangban az ISO 27001, az ISO 31000 és a vonatkozó szabályozási követelmények előírásaival.

1.3 A szabályzat támogatja a megalapozott döntéshozatalt, az információs vagyonelemek védelmét és a kritikus üzleti működés ellenálló képességét.

2. Hatály

2.1 Jelen szabályzat hatálya kiterjed:

2.1.1 a szervezeten belüli valamennyi szervezeti egységre, rendszerre és felhasználóra,

2.1.2 valamennyi belső kezelésben lévő vagy harmadik felek által menedzselt információra, szolgáltatásra és eszközre,

2.1.3 a kockázatokkal kapcsolatos tevékenységekre, ideértve a projektfelülvizsgálatokat, a rendszerfrissítéseket, a kiszervezést és a jogszabályi megfelelést.

2.2 A szabályzat valamennyi kockázattípusra kiterjed, így különösen:

2.2.1 a kiberbiztonsági fenyegetésekre és a rendszersérülékenységekre,

2.2.2 az üzemeltetési zavarokra és szolgáltatáskiesésekre,

2.2.3 a jogi, megfelelőségi vagy reputációs kitettségekre,

2.2.4 a harmadik felekhez és az ellátási lánchoz kapcsolódó kockázatokra.

2.3 Valamennyi munkavállaló, szerződéses közreműködő és szolgáltató köteles e szabályzatot követni a kockázatok azonosítása és jelentése során.

3. Célkitűzések

3.1 Egyszerű és ismételhető kockázatértékelési eljárások beépítése a rendes üzletmenetbe.

3.2 Azon kockázatok azonosítása és priorizálása, amelyek hatással lehetnek a bizalmasság, sértetlenség, rendelkezésre állás vagy a jogszabályi megfelelés követelményeire.

3.3 Kockázattulajdonosi felelősség kijelölése és kezelési intézkedések meghatározása minden jelentős kockázatra.

3.4 Pontos és naprakész kockázati nyilvántartás fenntartása az auditkészültség és a kockázatok nyomon követhetősége érdekében.

3.5 A vezetőség bevonásának biztosítása a kockázattűrés és a jelentős kezelési tervek jóváhagyásába.

4. Szerepkörök és felelősségi körök

4.1 Ügyvezető

4.1.1 Meghatározza a szervezet kockázatvállalási hajlandóságát, és jóváhagyja a kockázatkezelési keretrendszert.

4.1.2 Jóváhagyja a jelentős kockázatkezelési döntéseket és az azokhoz szükséges erőforrásokat.

4.1.3 Negyedévente felülvizsgálja a legfontosabb kockázatokat a kockázatkoordinátorral.

4.2 Kockázatkoordinátor (vagy az ISMS tulajdonosa)

4.2.1 Támogatja a kockázatértékeléseket, és fenntartja a kockázati nyilvántartást.

4.2.2 Biztosítja a kockázati pontszámok, a kockázattulajdonosi felelősség és a kezelési intézkedések dokumentálását.

4.2.3 Évente legalább egy formális kockázati felülvizsgálatot szervez.

[... 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 Éves szabályzat-felülvizsgálat

9.1.1 Jelen szabályzatot évente legalább egyszer felül kell vizsgálnia az ügyvezetőnek és a kockázatkoordinátornak a relevancia és teljesség biztosítása érdekében.

9.2 Frissítési kiváltó okok

9.2.1 Soron kívüli felülvizsgálatot és frissítést kell végezni, ha:

9.2.1.1 egy jelentős incidens vagy auditmegállapítás kockázatkezelési hiányosságokat tár fel,

9.2.1.2 új üzleti egységek, technológiák vagy partnerségek kerülnek bevezetésre,

9.2.1.3 jogszabályi vagy szerződéses követelmény változik.

9.3 Verziókezelés

9.3.1 Jelen szabályzat minden frissítését verziószámmal kell ellátni az alábbi metaadatokkal:

9.3.1.1 verziószám és hatálybalépés dátuma,

9.3.1.2 a változások összefoglalása,

9.3.1.3 jóváhagyó (ügyvezető),

9.3.1.4 auditcélból archivált korábbi verziók.

9.4 Kommunikáció és tudatosság

9.4.1 A szabályzat frissített változatait és a jelentős kockázatkezelési terveket közölni kell az érintett munkatársakkal. Az éves ismétlő oktatásnak az alapvető kockázattudatossági elveket is tartalmaznia kell.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat több más szabályzattal összehangoltan működik az átfogó biztonsági irányítás biztosítása érdekében:

10.1.1 P2S – Irányítási szerepkörök és felelősségek szabályzat: meghatározza, hogy ki felel a kockázattulajdonosi felelősségért és a döntéshozatalért.

10.1.2 P5S – P05 Változáskezelési szabályzat: előírja a kockázatértékelést a technikai vagy folyamati változtatások végrehajtása előtt.

10.1.3 P17S – Adatvédelmi és személyesadat-védelmi szabályzat: a személyes adatok kezeléséhez kapcsolódó szabályozási kockázatokat kezeli.

10.1.4 P30S – Incidenskezelési szabályzat: biztosítja, hogy a kockázatkezelés a biztonsági incidensek során és azt követően is folytatódjon.

10.1.5 P33S – Üzletmenet-folytonossági szabályzat: azonosítja a maradék kockázatokat és a helyreállítási intézkedéseket a kritikus szolgáltatások esetében.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001:

11.1.1 6.1. pont – Előírja a formális kockázatkezelési folyamat és a kezelési tervezés kialakítását.

11.1.2 6.1.3 pont – Előírja a szervezetek számára a dokumentált kezelési tervek és jóváhagyások megőrzését.

11.2 ISO/IEC 27002:

11.2.1 5.4, 5.25 kontrollok – Bevezetési útmutatást adnak a kockázattulajdonosi felelősségre, a priorizálásra és az életciklus-kezelésre vonatkozóan.

11.3 NIST SP 800-53 Rev.:

11.3.1 RA-1–RA-7 – Meghatározzák a kockázatértékelés, a válaszstratégiák, a dokumentálás és a felülvizsgálati mechanizmusok követelményeit.

11.4 PM-9 – Előírja a szervezeti kockázatok következetes, vezetői szintű felügyeletét.

11.5 EU NIS2 irányelv

11.5.1 21. cikk (2) bekezdés a–d pont – Kötelező kockázatértékelési, kockázatcsökkentési és irányítási kontrollokat ír elő az alapvető és fontos szervezetek számára.

11.6 EU DORA

11.6.1 5. cikk – Előírja a szabályozott szervezetek számára az IKT-kockázatkezelési keretrendszerek meghatározását és működtetését, beleértve az azonosítást, az osztályozást és a reagálást.

11.7 COBIT 2019

11.7.1 APO12 – Kockázatkezelés: integrálja a kockázatkezelést a stratégiai és operatív tervezésbe.

11.7.2 MEA01 – Monitorozás, értékelés és felmérés: biztosítja a kockázati folyamatok és intézkedések eredményességét és megfelelőségét.