					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P06					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**

Jogi nyilatkozat (szerzői jog és felhasználási korlátozások)

(C) 2025 Clarysec LLC. All rights reserved.

Ez a dokumentum a Clarysec LLC szellemi tulajdona. A dokumentum semmilyen része nem másolható, nem használható fel újra, nem terjeszthető és nem módosítható kereskedelmi vagy bevezetési célból előzetes, kifejezett írásbeli engedély nélkül.

A jogosulatlan felhasználás szigorúan tilos, és jogi eljárást vonhat maga után.

Licenceléssel kapcsolatban keresse: info@clarysec.com

A vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	6.1., 8.32. és 10. pont	A kockázatok azonosításának és kezelésének alapja, integráció a változáskezelésbe, folyamatos fejlesztés
ISO/IEC 27005:2024	A teljes kockázatkezelési életciklus módszertana	A szabványnak megfelelő teljes kockázatkezelési folyamat
ISO 31000:2018	Kockázatkezelési alapelvek és keretrendszer	A keretrendszerben alkalmazott kockázatkezelési alapelvek
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Iránymutatás és struktúra a kockázatértékelésekhez, többszintű kockázatirányítás
GDPR	24., 25. és 32. cikk	Adatvédelmi kockázatkezelési folyamatok és kontrollok
NIS2 irányelv	21. cikk (2) bekezdés a)–d) pont	Kockázatértékelési és biztonsági értékelési kötelezettségek
DORA-rendelet	5. és 6. cikk	IKT-kockázatkezelés és operatív reziliencia
COBIT 2019	APO12, MEA	Kockázatkezelési struktúra és felügyelet

1. Cél

1.1 Jelen szabályzat egységes és formalizált keretrendszert határoz meg az információbiztonsági kockázatok szervezetszintű azonosítására, elemzésére, értékelésére, kezelésére, nyomon követésére és felülvizsgálatára.

1.2 Biztosítja a kockázatalapú elvek következetes alkalmazását az információs vagyonelemek bizalmasságának, sértetlenségének és rendelkezésre állásának védelme érdekében, összhangban az ISO/IEC 27001:2022 6.1. pontjával és az ISO 31000:2018 szabvánnyal.

1.3 A szabályzat beépíti az információbiztonsági kockázatkezelést a szervezeti döntéshozatali folyamatokba a belső stratégiai célok és a külső szabályozási követelmények teljesítése érdekében.

2. Hatály

2.1 Jelen szabályzat kiterjed minden szervezeti egységre, üzleti folyamatra, rendszerre, munkatársra és harmadik féllel fennálló együttműködésre, amely információs vagyonelemek kezelésében, fejlesztésében, tárolásában vagy irányításában érintett.

2.2 A hatály kiterjed a fizikai, digitális és felhőalapú vagyonelemekre, ideértve a strukturált és strukturálatlan adatokat, az alkalmazásokat, az infrastruktúrát, a hálózatokat és a szolgáltatásokat.

2.3 A szabályzat a stratégiai, operatív, projekt- és technikai szintű információbiztonsági kockázatokra terjed ki, és kötelező valamennyi munkavállaló, szerződéses közreműködő és szolgáltató számára, akik az információbiztonsági irányítási rendszer tevékenységeiben részt vesznek.

2.4 Kockázatkezelést kell alkalmazni az alábbi esetekben:

2.4.1 Új projekt vagy rendszer bevezetése esetén

2.4.1.1 Jelentős változások esetén (pl. architektúra, tulajdonosi felelősség, folyamatok)

2.4.1.2 Beszállítók beléptetése és harmadik féllel kötött megállapodások esetén

2.4.1.3 Incidenskezelés és incidens utáni felülvizsgálatok (PIR) esetén

2.4.1.4 Időszakos szervezeti kockázati felülvizsgálatok vagy auditok során

3. Célkitűzések

3.1 Az ISO/IEC 27005 és az ISO 31000 módszertanára épülő, ismételhető, a teljes szervezetre kiterjedő kockázatkezelési folyamat kialakítása és működtetése.

3.2 Annak biztosítása, hogy a kockázatok azonosítása, elemzése, értékelése és kezelése strukturált és visszakövethető módszerekkel történjen, beleértve a kockázattulajdonosi felelősség kijelölését és a kontrollkapcsolatok rögzítését.

3.3 Központi, verziókezelt kockázati nyilvántartás és kockázatkezelési terv fenntartása, amely tükrözi az aktuális kockázati állapotot, a kontrolllefedettséget és a kockázatcsökkentés előrehaladását.

3.4 A kockázati döntések összehangolása a dokumentált kockázatvállalási hajlandósággal és tűréshatárokkal, valamint megalapozott irányítási döntések támogatása a kockázat elfogadása, csökkentése, átruházása vagy elkerülése tekintetében.

3.5 A kockázati trendek folyamatos nyomon követése és a kockázatkezelési intézkedések eredményességének biztosítása, továbbá a fenyegetési környezet vagy az üzleti működés változása alapján szükséges proaktív módosítások lehetővé tétele.

4. Szerepkörök és felelősségek

4.1 Felső vezetés / Igazgatóság

4.1.1 Jóváhagyja a kockázatkezelési keretrendszert, és meghatározza az elfogadható kockázatvállalási hajlandóságot és kockázattűrési küszöbértékeket.

4.1.2 Jóváhagyja a tűréshatárt meghaladó maradványkockázatok kezelésére vonatkozó stratégiákat.

4.1.3 Erőforrásokat és felügyeletet biztosít a kockázatkezelési program eredményes működéséhez.

4.2 IBIR-vezető / kockázatkezelési felelős

4.2.1 Jelen szabályzat gazdája, és biztosítja annak összhangját az ISO/IEC 27001 és 27005 szabványokkal.

4.2.2 Irányítja a szervezeti kockázatértékelési folyamatot, valamint fenntartja a kockázati nyilvántartást és a kockázatkezelési tervet.

4.2.3 Biztosítja a kulcsfontosságú kockázatok rendszeres felülvizsgálatát és eszkalációját a felső vezetés vagy az IBIR irányító bizottság felé.

[... 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 és a kapcsolódó keretrendszert évente felül kell vizsgálni, illetve soron kívül is felül kell vizsgálni:

9.1.1 Jelentős kockázati esemény vagy biztonsági incidens után

9.1.2 Jelentős szervezeti vagy technikai változást követően

9.1.3 Auditmegállapítások vagy új szabályozási követelmények hatására

9.2 Az IBIR-vezető, a kockázatkezelési felelős és a megfelelőségi csapat együttesen felelősek az alábbiakért:

9.2.1 A felülvizsgálati ciklus kezdeményezése

9.2.2 Az üzleti egységektől származó inputok összegyűjtése

9.2.3 Az eljárások és küszöbértékek szükség szerinti módosítása

9.3 Valamennyi módosítást:

9.3.1 Verziókezeléssel kell ellátni, és naplózni kell

9.3.2 A felső vezetésnek jóvá kell hagynia

9.3.3 Az érintett felekkel közölni kell

9.3.4 Legalább 5 évig meg kell őrizni az auditarchívumban

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat az alábbi információbiztonsági szabályzatokkal áll kölcsönös összefüggésben:

10.1.1 P1 – Információbiztonsági politika: Meghatározza azt az átfogó biztonságirányítási modellt, amelynek keretében jelen kockázatkezelési szabályzat működik.

10.1.2 P2 – Irányítási szerepkörök és felelősségek szabályzat: Meghatározza a felelős tulajdonosokat és azokat az irányítási szinteket, amelyekre a kockázati eszkalációs mátrix hivatkozik.

10.1.3 P5 – Változáskezelési szabályzat: Kiváltja a kockázatok újraértékelését az infrastruktúrát és a szervezetet érintő változások esetén.

10.1.4 P13 – Adatosztályozási és címkézési szabályzat: Támogatja a hatásértékelést a kockázatazonosítás során.

10.1.5 P33 – Audit- és megfelelőségmonitorozási szabályzat: Ellenőrzi a szabályzatok betartását, beleértve a kockázati nyilvántartás teljességét és a kockázatkezelési intézkedések bizonyítékait.

11. Hivatkozott szabványok és keretrendszerek

11.1 Jelen szabályzat kifejezetten az alábbi szabványokkal és keretrendszerekkel áll összhangban annak biztosítása érdekében, hogy megfeleljen az információbiztonsági kockázatkezelésre vonatkozó nemzetközi legjobb gyakorlatoknak és szabályozói elvárásoknak.

11.2 ISO/IEC 27001:

11.2.1 6.1. pont: Meghatározza a kockázatok és lehetőségek azonosítására vonatkozó követelményeket, beleértve az információbiztonsági kockázatértékelések és kockázatkezelési intézkedések teljes életciklusát. Jelen szabályzat a 6.1.2. és 6.1.3. pont követelményeit strukturált keretrendszer útján ülteti át a gyakorlatba, amely előírja a dokumentált kockázatazonosítást, elemzést, értékelést, kezelést és a maradványkockázat elfogadására vonatkozó eljárásokat.

11.2.2 8.32. pont: A kockázatalapú szemlélet változáskezelési folyamatokba történő integrálása biztosítja, hogy minden jelentős szervezeti változás formális kockázat-újraértékelést váltson ki.

11.2.3 10. pont: A folyamatos fejlesztés a rendszeres szabályzat-felülvizsgálatokon, a kockázati trendelemzésen és a kockázati megállapítások által vezérelt SoA-frissítéseken keresztül valósul meg.

11.3 ISO/IEC 27005:

11.3.1 Részletes és szakterületi útmutatást nyújt az információbiztonsági kockázatkezeléshez. Jelen szabályzat az ISO/IEC 27005 teljes kockázatkezelési folyamatmodelljét alkalmazza: a kontextus meghatározása, a kockázatok azonosítása, a kockázatelemzés, a kockázatértékelés, a kockázatkezelés, a kockázat elfogadása, a kockázatkommunikáció, valamint a kockázatok nyomon követése és felülvizsgálata.

11.4 ISO 31000:

11.4.1 Jelen szabályzat integrálja az ISO 31000 alapelveit, így különösen a vezetői elkötelezettséget, a döntéshozatalba történő beépítést és a folyamatos fejlesztést. Biztosítja, hogy a kockázatkezelés a szervezeti kultúra és működés részét képezze.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Összhangban áll a NIST kockázatértékelési útmutatójával, beleértve a fenyegetések azonosítását, a sérülékenységelemzést, a valószínűség becslését és a hatás meghatározását. Jelen szabályzat felépítése tükrözi a NIST által meghatározott kockázatértékelési lépéseket, és azokat technikai és üzleti folyamatokra egyaránt alkalmazza.

11.6 NIST SP 800-39:

11.6.1 Támogatja a szervezeti szintű kockázatirányítást, hangsúlyozva a többszintű kockázatkezelést szervezeti, küldetés-/üzletifolyamat- és információsrendszer-szinten. A szabályzat biztosítja, hogy a kockázattulajdonosi felelősség minden szinten egyértelműen meghatározott legyen, és szervezeti szintű kezelési stratégiákat is tartalmazzon.

11.7 GDPR:

11.7.1 24. cikk: Előírja a megfelelő technikai és szervezeti intézkedések végrehajtását annak biztosítására, hogy az adatvédelmi kockázatok megfelelően legyenek kezelve; ezt jelen szabályzat strukturált kockázatkezelési folyamata biztosítja.

11.7.2 25. cikk: Az „alapértelmezett és beépített adatvédelem” elve összhangban áll a kockázatkezelési intézkedések rendszerek és folyamatok tervezésébe történő beépítésével.

11.7.3 32. cikk: Kockázatalapú megközelítést ír elő a biztonsági intézkedések meghatározásához; ezt a hatásalapú kockázatértékelések és a kontrollkiválasztás biztosítják.

11.8 NIS2 irányelv:

11.8.1 21. cikk (2) bekezdés a)–d) pont: Előírja, hogy a szervezetek kockázatértékeléseket végezzenek, a kockázatelemzésre vonatkozó szabályzatokat vezessenek be, és arányos biztonsági intézkedéseket alkalmazzanak. Jelen szabályzat a folyamatos kockázatkezelési életciklus alkalmazása és a dokumentált irányítás révén teljesíti ezeket a kötelezettségeket.

11.9 DORA-rendelet:

11.9.1 5. cikk: Dokumentált IKT-kockázatkezelési keretrendszert ír elő; ezt jelen szabályzat teljes körűen lefedi, beleértve az SoA-leképezést és a KRI-k alkalmazását.

11.9.2 6. cikk: Megköveteli a kockázatkezelés integrálását az operatív reziliencia stratégiáiba, amelyet az eszkalációs mátrixok és a kritikus vagyonelemek nyomon követése biztosít.

11.10 COBIT 2019:

11.10.1 APO12 – Kockázatkezelés: Közvetlenül megfeleltethető a szervezet strukturált kockázatkezelési megközelítésének kialakításával, a szerepkörök kijelölésével, a kezelések nyomon követésével és az igazgatósági szintű elszámoltathatóság biztosításával.

11.10.2 MEA01 – Teljesítmény és megfelelőség monitorozása, értékelése és felmérése: Tükröződik a szabályzat trendelemzésre, a KRI-k nyomon követésére és az audit-visszacsatolások folyamatos fejlesztési ciklusokba történő integrálására helyezett hangsúlyában.