					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P02					Dokumentum címe: **Irányítási szerepkörök és felelősségek 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**

Az alkalmazandó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	5.3 pont; A. melléklet 5. kontroll	
ISO/IEC 27002:2022	5. kontroll	
NIST SP 800-53 Rev. 5	PL-1–PL-4, PM-1–PM-13	
GDPR	5. cikk (1) bekezdés f) pont, 24. cikk, 37. cikk	
NIS2 irányelv	21. cikk (2) bekezdés a) pont	
DORA-rendelet	5. cikk	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Cél

1.1 Jelen szabályzat meghatározza az információbiztonság-irányítási rendszer (ISMS) hatékony működtetéséhez szükséges irányítási modellt, valamint a kapcsolódó szervezeti szerepköröket és felelősségeket.

1.2 A szabályzat egyértelmű elszámoltathatósági rendet, döntési hatásköröket és eszkalációs útvonalakat rögzít annak érdekében, hogy az információbiztonság a szervezet működésének minden szintjébe beépüljön, és összhangban álljon az üzleti-stratégiai célokkal.

1.3 A szabályzat végrehajtja az ISO/IEC 27001:2022 5.3 pontjában és A.5.2 kontrolljában meghatározott követelményeket, biztosítva, hogy a biztonsággal kapcsolatos tevékenységek felelőssége egyértelműen kijelölt, dokumentált, kommunikált és rendszeresen felülvizsgált legyen.

1.4 A szabályzat egyben alapot biztosít a más szakterületekkel — különösen a kockázatkezeléssel, a megfelelőséggel, az IT-üzemeltetéssel és a jogi területtel — megvalósuló integrált irányításhoz.

2. Hatály

2.1 Jelen szabályzat az ISMS hatályán belül alkalmazandó minden olyan személyre és szervezeti egységre, amely részt vesz az információbiztonság irányításában, működtetésében vagy felügyeletében. Ide tartoznak különösen:

2.1.1 a felső vezetés, a vezetők és az igazgatósági tagok;

2.1.2 az ISMS-vezetők, a CISO-k és a kontrollgazdák;

2.1.3 a folyamatgazdák és az eszközgazdák;

2.1.4 a kiszervezett partnerek és harmadik fél szolgáltatók, amelyekre biztonsági felelősséget ruháztak át.

2.2 A szabályzat egyaránt kiterjed a belső és külső forrásból biztosított funkciókra (pl. kiszervezett SOC, felhőplatform-adminisztrátorok), amennyiben az irányítási szerepkörök formálisan kijelöltek vagy szerződésben meghatározottak.

2.3 A szabályzat alkalmazandó azokra a szervezeti egységekre, részlegekre és projektcsapatokra is, amelyek biztonsági szempontból releváns eszközöket, rendszereket vagy szolgáltatásokat kezelnek, illetve azokra hatást gyakorolnak.

3. Célkitűzések

3.1 Annak biztosítása, hogy az információbiztonsági szerepkörök és felelősségek formálisan meghatározottak, kijelöltek, kommunikáltak és dokumentáltak legyenek.

3.2 Olyan irányítási modell fenntartása, amely biztosítja a feladatkörök szétválasztását, megszünteti az összeférhetetlenségeket, és lehetővé teszi a rendezetlen biztonsági kérdések eszkalációját.

3.3 Annak biztosítása, hogy a biztonsági döntésekhez kapcsolódó elszámoltathatóság és döntési hatáskör az üzleti hatásokkal és a szervezeti felépítéssel összhangban kerüljön meghatározásra.

3.4 Keretrendszer kialakítása a delegálások, a szerepkörváltozások és a kijelölt felelősségek felülvizsgálatának kezelésére.

3.5 Annak igazolása az érintettek — ideértve a szabályozó hatóságokat, auditorokat és ügyfeleket — számára, hogy az információbiztonság irányítása hatékonyan és az alkalmazandó szabványoknak megfelelően történik.

4. Szerepkörök és felelősségek

4.1 Felső vezetés

4.1.1 Stratégiai felügyeletet biztosít, erőforrásokat rendel az ISMS-hez, és gondoskodik arról, hogy az ISMS célkitűzései összhangban legyenek az üzleti célokkal.

4.1.2 Jóváhagyja az ISMS fő dokumentumait, beleértve az információbiztonsági szabályzatot, a kockázatkezelési terveket és az auditmegállapításokhoz kapcsolódó helyesbítő intézkedésekről szóló döntéseket.

4.1.3 Részt vesz az ISMS vezetőségi felülvizsgálataiban, és az igazgatósági szintű jóváhagyást igénylő döntéseket eszkalálja.

4.1.4 Előmozdítja a biztonságtudatos szervezeti kultúrát, és támogatja az irányítási elvek szervezeti szintű érvényesülését.

4.2 Információbiztonsági Irányító Bizottság (ISSC)

4.2.1 Az ISMS felügyeletét ellátó, több szakterületet átfogó irányítási testületként működik.

4.2.2 Felülvizsgálja a kockázati helyzetet, a kontrollok teljesítményét, az auditmegállapításokat és a stratégiai biztonsági kezdeményezéseket.

4.2.3 Elősegíti az együttműködést a szervezeti egységek között (pl. IT, jogi, HR, kockázatkezelés, megfelelőség, üzemeltetés).

4.2.4 Jóváhagyja az eszkalációs küszöbértékeket, a költségvetési allokációkat és azokat a szabályzatmódosításokat, amelyek felsővezetői döntést igényelnek.

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

9. Felülvizsgálati és aktualizálási követelmények

9.1 Felülvizsgálati ütemezés

9.1.1 Jelen szabályzatot legalább évente egyszer, továbbá az alábbi események bekövetkezésekor felül kell vizsgálni:

9.1.1.1 a szervezeti struktúra vagy a felsővezetői kör változása;

9.1.1.2 az ISMS hatályának bővítése vagy újradefiniálása;

9.1.1.3 a szerepkör-kijelölést vagy felügyeletet érintő szabályozási változások;

9.1.1.4 jelentős auditmegállapítások vagy az irányítási működés hibájával összefüggő incidensek.

9.2 Felülvizsgálati és jóváhagyási folyamat

9.2.1 Az ISMS-vezető kezdeményezi és vezeti a felülvizsgálati folyamatot, beleértve az érintetti visszajelzések és az auditokból származó észrevételek összegyűjtését is.

9.2.2 A javasolt módosításokat az ISSC felülvizsgálja, és azokat a felső vezetés formálisan jóváhagyja.

9.2.3 Minden verziót nyomon kell követni az ISMS dokumentumnyilvántartásában, amelynek az alábbi metaadatokat kell tartalmaznia:

9.2.3.1 a szabályzat azonosítója és címe;

9.2.3.2 verziószám és módosítási összefoglaló;

9.2.3.3 hatálybalépés dátuma és a következő felülvizsgálat időpontja;

9.2.3.4 a szabályzat gazdája és jóváhagyója;

9.2.3.5 a dokumentum besorolási szintje;

9.2.3.6 megőrzési és archiválási előzmények.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzatot az alábbi szabályzatokkal együtt kell értelmezni:

10.1.1 P1 – Információbiztonsági szabályzat: Meghatározza az átfogó biztonsági programot, és rögzíti a vezetői felelősségeket a szabályzat jóváhagyása és a stratégiai felügyelet tekintetében.

10.1.2 P5 – Változáskezelési szabályzat: Biztosítja, hogy az irányítási struktúrákat, szerepköröket vagy felelősségeket érintő változások dokumentált jóváhagyáshoz és kockázati felülvizsgálathoz kötöttek legyenek.

10.1.3 P6 – Kockázatkezelési szabályzat: Azonosítja és kezeli a szerepkörütközésekből, a kijelöletlen feladatokból vagy az eszkaláció hiányából eredő irányítási kockázatokat.

10.1.4 P7 – Beléptetési és kiléptetési szabályzat: Érvényesíti a kontrollok kijelölésére és visszavonására vonatkozó folyamatokat a személyi életciklus változásai során.

10.1.5 P33 – Audit- és megfelelőség-ellenőrzési szabályzat: Támogatja az irányítás eredményességének független felülvizsgálatát, és érvényesíti a nemmegfelelőséghez kapcsolódó helyesbítő intézkedéseket.

10.2 Ezek a szabályzatok együttesen egységes és alkalmazható ISMS-irányítási keretrendszert támogatnak.

11. Hivatkozott szabványok és keretrendszerek

11.1 Jelen szabályzat összhangban áll az információbiztonsági irányításra és a szerepkörökhöz kapcsolódó elszámoltathatóságra vonatkozó, nemzetközileg elismert szabványokkal és keretrendszerekkel. Biztosítja a szabályozási és tanúsítási követelményeknek való visszakövethetőséget, valamint támogatja a védhető ISMS-struktúrát.

11.2 ISO/IEC 27001

11.2.1 5.3 pont – Szervezeti szerepkörök, felelősségek és hatáskörök: Jelen szabályzat teljesíti azt a követelményt, hogy az információbiztonság szempontjából releváns szerepkörök egyértelműen kijelöltek, kommunikáltak és dokumentáltak legyenek.

11.2.2 9.3 pont – Vezetőségi felülvizsgálat: Jelen szabályzat negyedéves és éves felülvizsgálatok útján biztosítja az ISMS-szerepkörök és az irányítás felsővezetői felügyeletét.

11.2.3 A. melléklet 5.2 kontroll – Információbiztonsági szerepkörök és felelősségek: Meghatározza a technikai, operatív és stratégiai szinteken szükséges szerepköröket annak biztosítására, hogy megvalósuljon a feladatkörök szétválasztása, a kockázati felelősség és a visszakövethető elszámoltathatóság.

11.3 ISO/IEC 27002:2022 – 5. kontroll

11.3.1 Végrehajtási útmutatást ad az információbiztonsági felelősségek szervezeten belüli kijelöléséhez. Jelen szabályzat ezt az útmutatást alkalmazza a szerepkörtípusok, a delegálási szabályok, az eszkalációs eljárások és a felülvizsgálati mechanizmusok meghatározásával.

11.4 NIST SP 800-53 Rev. 5

11.4.1 PL-1–PL-4: Előírják a formális tervezési dokumentáció szükségességét, beleértve azokat a szabályzatokat is, amelyek meghatározzák az irányítást és kijelölik a biztonsági felelősségeket.

11.4.2 PM-1 (információbiztonsági programterv) és PM-2 (vezető információbiztonsági tisztségviselő): Jelen szabályzatban a CISO/ISMS-vezető kijelölésén és a formális irányítási szerepkörök meghatározásán keresztül jelennek meg.

11.4.3 PM-5–PM-13: Jelen szabályzat teljesíti a szerepkörök dokumentálására, a szervezeti szintű kockázati szerepkörökre, a konfigurációkezelés felügyeletére és az üzleti funkciókkal való integrációra vonatkozó követelményeket.

11.5 GDPR (2016/679)

11.5.1 5. cikk (1) bekezdés f) pont: Előírja a személyes adatok védelmét a jogosulatlan vagy jogellenes adatkezeléssel szemben. Jelen szabályzat biztosítja, hogy az adatvédelemért felelős személyek egyértelműen kijelöltek és felügyeltek legyenek.

11.5.2 24. cikk: Megfelelő szervezési intézkedések alkalmazását írja elő, beleértve az irányítási struktúrákat is.

11.5.3 37. cikk: Adatvédelmi tisztviselő (DPO) kijelölését írja elő, amelynek a szervezet irányítási keretrendszerében és szerepkör-nyilvántartásában is meg kell jelennie.

11.6 NIS2 irányelv (2022/2555)

11.6.1 21. cikk (2) bekezdés a) pont: Előírja, hogy a szervezetek kockázatelemzési és az információs rendszerek biztonságára vonatkozó szabályzatokat vezessenek be, ideértve a szerepkörspecifikus felelősségeket is. Jelen szabályzat meghatározza ezeket a szerepköröket és a hozzájuk kapcsolódó irányítási mechanizmusokat.

11.7 DORA-rendelet (2022/2554)

11.7.1 5. cikk – Irányítási és belső kontrollkeretrendszer: Előírja az IKT-kockázatkezelési felelősségek, döntési szerepkörök és jelentési csatornák formális kijelölését. Jelen szabályzat biztosítja a biztonsággal kapcsolatos szerepkörök irányításának alapját az IKT-környezetekben.

11.8 COBIT 2019

11.8.1 EDM01 – Irányítási keretrendszer kialakításának biztosítása: Jelen szabályzat biztosítja, hogy az ISMS világosan meghatározott, a szervezeti igényekhez igazodó irányítási struktúrával rendelkezzen.

11.8.2 EDM02 – Az előnyök megvalósulásának biztosítása: Összhangba hozza a szerepköralapú biztonsági tevékenységeket a stratégiai és operatív célokkal, biztosítva az elszámoltathatóságot és a mérhető eredményeket.

11.8.3 APO01 – I&T irányítási keretrendszer kezelése és APO12 – Kockázatkezelés: Jelen szabályzat támogatja az információbiztonsági szerepkörök strukturált kezelését a tágabb IT-irányítási és kockázatkezelési keretrendszerben.

11.8.4 MEA01 – Teljesítmény nyomon követése, értékelése és felmérése: Olyan felülvizsgálati mechanizmusokat épít be, amelyek ellenőrzik, hogy az irányítási szerepkörök eredményesek, naprakészek és alkalmazásban vannak-e.