					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P01					Dokumentum címe: **Információbiztonsági 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**

1. Cél

1.1 Jelen szabályzat meghatározza a szervezet információbiztonság iránti átfogó elkötelezettségét egy formális információbiztonsági irányítási rendszer (IBIR) létrehozása révén.

1.2 Meghatározza a stratégiai irányt és azokat az alapvető követelményeket, amelyek szükségesek valamennyi információs vagyon bizalmasságának, sértetlenségének, rendelkezésre állásának és rezilienciájának védelméhez a fizikai, digitális és felhőalapú környezetekben.

1.3 A szabályzat az ISO/IEC 27001:2022 5.1 és 5.2 pontjával összhangban rögzíti a vezetői szándékot, a felső vezetés elkötelezettségét, valamint a biztonsági tevékenységek szervezeti célokkal való összhangját.

1.4 A szabályzat az IBIR hatálya alá tartozó valamennyi alárendelt szabályzat, szabvány és eljárás hiteles hivatkozási alapja, és alapvető fontosságú a kockázatalapú, megfelelésközpontú és folyamatosan fejlesztett biztonsági működés biztosításához.

2. Hatály

2.1 Jelen szabályzat az IBIR hatályán belül meghatározott valamennyi személyre, eszközre és folyamatra kiterjed, beleértve az alábbiakat:

2.1.1 Valamennyi üzleti egység, szervezeti egység, leányvállalat és telephely

2.1.2 Munkavállalók, vállalkozók, ideiglenes foglalkoztatottak, tanácsadók és harmadik fél szolgáltatók

2.1.3 Valamennyi adat, információs rendszer, alkalmazás, infrastruktúra és kommunikációs csatorna

2.1.4 Minden olyan fizikai, felhőalapú, távoli és hibrid környezet, ahol vállalati adat kezelése vagy elérése történik

2.2 A szabályzat minden olyan szervezeti szereplőre kötelező, aki szervezeti információt kezel, és az információ teljes életciklusára alkalmazandó a létrehozástól és továbbítástól a tárolásig és selejtezésig.

2.3 A hatály alóli bármely kizárást vagy korlátozást az IBIR hatálymeghatározó nyilatkozatában dokumentálni kell, és azt a felső vezetés formális jóváhagyásával kell alátámasztani.

3. Célkitűzések

3.1 Olyan, az ISO/IEC 27001:2022 követelményeivel összhangban álló IBIR kialakítása, amely támogatja a kockázatalapú döntéshozatalt a szervezet egészében.

3.2 Biztosítani, hogy a bizalmasság, sértetlenség és rendelkezésre állás biztonsági alapelvei beépüljenek minden szervezeti tevékenységbe, rendszerbe és együttműködésbe.

3.3 A szabályozói és szerződéses megfelelés biztosítása mérhető, szabályzatalapú biztonsági célok meghatározásával és azok üzleti működésbe történő integrálásával.

3.4 Az információbiztonsági incidensek bekövetkezési valószínűségének és hatásának csökkentése hatékony megelőző, felderítő és helyesbítő kontrollok alkalmazásával.

3.5 Az információbiztonsági érettség folyamatos fejlesztésének előmozdítása meghatározott teljesítménymutatók, auditeredmények és vezetőségi átvizsgálások alapján.

3.6 Az elszámoltathatóság, a tudatosság és a reziliencia kultúrájának erősítése annak érdekében, hogy a biztonsági felelősségi körök minden érintett számára egyértelműek legyenek, és azok végrehajtása megtörténjen.

4. Szerepkörök és felelősségek

4.1 Felső vezetés

4.1.1 Jóváhagyja és támogatja az Információbiztonsági szabályzatot és az IBIR keretrendszerét.

4.1.2 Biztosítja a biztonsági célok és az üzleti stratégia összhangját.

4.1.3 Példamutatóan jár el, és elősegíti az erős információbiztonsági kultúra kialakulását.

4.1.4 Felülvizsgálja és jóváhagyja az IBIR hatályát, a kockázatkezelést és az irányítási struktúrát érintő jelentős változásokat.

4.2 Információbiztonsági vezető (CISO) / IBIR-vezető

4.2.1 Felelős az IBIR működtetéséért, és gondoskodik jelen szabályzat ISO/IEC 27001 szerinti fenntartásáról.

4.2.2 Irányítja a kockázatértékelési, kontrollbevezetési és folyamatos fejlesztési folyamatokat.

4.2.3 Biztosítja a biztonsági tevékenységek szervezeti egységek közötti összehangolását, és felügyeli az alárendelt szabályzatokat.

4.2.4 Jelentést készít a felső vezetés részére az IBIR állapotáról, az incidensekről, az auditok eredményeiről és a mérőszámokról.

4.2.5 Biztosítja, hogy a szabályzat felülvizsgálata és aktualizálása a jelen dokumentum 9. szakaszával összhangban történjen.

[... 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 A felülvizsgálat gyakorisága

9.1.1 Jelen szabályzatot legalább évente egyszer, vagy az alábbi kiváltó események bármelyike esetén felül kell vizsgálni:

9.1.1.1 A jogi, szabályozói vagy szerződéses kötelezettségeket érintő jelentős változás

9.1.1.2 A szervezeti kockázati profil lényeges változása

9.1.1.3 Belső vagy külső auditok eredményei

9.1.1.4 Súlyos incidensek vagy kontrollhibák

9.2 A felülvizsgálat felelőse és folyamata

9.2.1 A felülvizsgálati folyamatot a CISO vagy a kijelölt IBIR-vezető irányítja.

9.2.2 A felülvizsgálat bemeneteinek ki kell terjedniük az alábbiakra:

9.2.2.1 Belső auditok eredményei

9.2.2.2 Kockázatértékelési trendek

9.2.2.3 Az üzleti folyamatokat és a technológiát érintő változások

9.2.2.4 A KPI-khez és kockázati küszöbértékekhez viszonyított teljesítmény

9.2.3 Minden aktualizálásnak meg kell felelnie az alábbiaknak:

9.2.3.1 Verziókövetetten és dokumentáltan kell történnie

9.2.3.2 A felső vezetésnek jóvá kell hagynia

9.2.3.3 Hivatalos kommunikációs csatornákon keresztül el kell juttatni minden érintett fél részére

9.2.3.4 Szükség esetén aktualizálni kell az alárendelt dokumentációt és a képzési anyagokat is

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen alapvető szabályzat közvetlen kapcsolatban áll az alábbi szervezeti biztonsági szabályzatokkal és keretrendszerekkel:

10.1.1 P2 – Irányítási szerepkörök és felelősségek szabályzata: Meghatározza a jelen dokumentumban hivatkozott irányítási struktúrát és jogosultsági hierarchiát.

10.1.2 P3 – Elfogadható használat szabályzata: Érvényesíti a magatartási megfelelést és az információs vagyonelemek elfogadható kezelését.

10.1.3 P4 – Hozzáférés-szabályozási szabályzat: Működési szintre fordítja a jelen átfogó szabályzatból levezetett hozzáféréskezelési kontrollokat.

10.1.4 P6 – Kockázatkezelési szabályzat: Biztosítja a kontrollok kiválasztásához és a fennmaradó kockázatok elfogadásához szükséges kockázatalapú keretet.

10.1.5 P33 – Audit- és megfelelőség-nyomonkövetési szabályzat: Részletezi, hogy a belső bizonyosságot nyújtó mechanizmusok miként ellenőrzik a szabályzat betartását.

10.2 Ezek az összefüggések biztosítják az IBIR-en belüli átfogó összhangot és nyomon követhetőséget, valamint támogatják az egységes kockázati és megfelelőségi irányítást.

11. Hivatkozott szabványok és keretrendszerek

11.1 Jelen Információbiztonsági szabályzat formálisan összhangban áll az alábbi szabványokkal és keretrendszerekkel a teljes megfelelés, az auditkészség és a szabályozói megfelelés igazolhatóságának biztosítása érdekében:

11.2 ISO/IEC 27001

11.2.1 5.1 pont – Vezetés és elkötelezettség: Jelen szabályzat igazolja a felső vezetés információbiztonság iránti elkötelezettségét, és meghatározza az IBIR-rel kapcsolatos felelősségeket és erőforrás-hozzárendeléseket.

11.2.2 5.2 pont – Információbiztonsági szabályzat: Jelen dokumentum a szervezet formális biztonsági szabályzataként szolgál, összhangban a meghatározott biztonsági célokkal, az üzleti stratégiával és az ISO/IEC 27001 követelményeivel.

11.2.3 6.1 pont – A kockázatok és lehetőségek kezelésére irányuló intézkedések: A jelen szabályzatban megjelenő kockázatalapú megközelítés biztosítja, hogy a biztonsági erőforrások a fenyegetésekkel arányosan kerüljenek alkalmazásra.

11.2.4 9.2 pont – Belső audit és 10. pont – Fejlesztés: Jelen szabályzat beépül a szervezet folyamatos fejlesztési ciklusába, és belső audit keretében ellenőrzésre kerül.

11.2.5 ISO/IEC 27002:2022 – 5.1 kontroll: Iránymutatást ad a biztonsági szabályzatok kialakításához és fenntartásához. Jelen szabályzat tükrözi az ISO/IEC 27002 ajánlásait a hierarchikus dokumentáció, a felülvizsgálati ciklusok és az alkalmazhatóság tekintetében.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Biztonságtervezési szabályzat és eljárások): Jelen szabályzat teljesíti a szervezetszintű, formális információbiztonsági szabályzat kidolgozására, közzétételére és felülvizsgálatára vonatkozó követelményt.

11.3.2 PM-1–PM-5: Kiterjed a programszintű irányításra, beleértve az információbiztonsági szerepköröket, az erőforrás-allokációt, a kockázati stratégiát és a biztonságtervezés vállalati működésbe történő integrációját.

11.4 GDPR (2016/679)

11.4.1 5. cikk (2): Érvényesíti az elszámoltathatóság elvét. Jelen szabályzat meghatározza a felelős szereplőket és a nyomon követhető végrehajtási intézkedéseket.

11.4.2 24. cikk: Előírja a technikai és szervezési intézkedések bevezetését, beleértve a kockázatokkal összhangban álló szabályzatokat is.

11.4.3 32. cikk: Támogatja a személyes adatok teljes életciklusa során megfelelő biztonsági intézkedések bevezetését.

11.5 NIS2 irányelv (2022/2555)

11.5.1 21. cikk (2) bekezdés a) pont: Előírja dokumentált biztonsági szabályzat bevezetését, amely kiterjed a kockázatkezelésre és az irányításra. Jelen szabályzat megfelel e követelménynek, és

támogatja a szélesebb körű kiberbiztonsági felkészültséget, valamint a kritikus infrastruktúra védelmét.

11.6 DORA-rendelet (2022/2554)

11.6.1 5. cikk (2) bekezdés: Dokumentált belső kontrollkeretrendszert ír elő az IKT-kockázatkezeléshez. Jelen szabályzat a DORA irányítási elvárásaival összhangban kijelölt szerepkörök, kontrollok és felügyeleti funkciók meghatározásával támogatja a pénzügyi szektorra vonatkozó megfelelést.

11.7 COBIT 2019

11.7.1 EDM01 – Irányítási keretrendszer meghatározása: Jelen szabályzat támogatja a vállalatirányítást az IBIR-szerepkörök, a vezetői elkötelezettség és a stratégiai célok meghatározásával.

11.7.2 APO01 – Irányítási keretrendszer: Támogatja a strukturált IBIR kialakítását és működtetését.

11.7.3 APO12 – Kockázatkezelés: Megteremti az információbiztonsági kockázatkezelés alapját.

11.7.4 MEA01/MEA03 – Nyomon követés, értékelés és felmérés: Megerősíti a teljesítmény folyamatos értékelését és a belső kontrollok nyomon követését a szabályzati megfelelés biztosításán keresztül.