					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P01S					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**

Az alkalmazandó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	5.1, 5.2, 5.3, 6.1, 6.2, 8. pont	Meghatározza a vezetői elkötelezettségre, a szabályzati követelményekre, a szerepkörök kijelölésére, a kockázatértékelésre és az operatív kontrollokra vonatkozó követelményeket
ISO/IEC 27002:2022	5.1–5.5 kontrollok	Meghatározza a dokumentált információbiztonsági szabályzatok kialakítására, a szerepkörök kijelölésére, a feladatkörök szétválasztására és a vezetői felelősségekre vonatkozó előírásokat
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Követelményeket ír elő a biztonsági programtervre, a tervezési szabályzatra, az értékelésre és engedélyezésre, valamint a hozzáférés-szabályozásra vonatkozóan
GDPR (2016/679)	5. cikk (2) bekezdés, 32. cikk	Az elszámoltathatóság elve és az adatkezelés biztonságát szolgáló intézkedések, különös tekintettel a dokumentált szerepkörökre
az EU NIS2 irányelve (2022/2555)	21. cikk (2) bekezdés a) pont	Előírja a kiberkockázatok kezeléséhez szükséges kockázatkezelési intézkedéseket, szerepköröket és felelősségeket
az EU DORA-rendelete (2022/2554)	9. cikk, 10. cikk	Előírja az IKT-kockázatkezeléshez és az üzletmenet-folytonossághoz kapcsolódó szerepkörök kijelölését
COBIT 2019	EDM03, APO13, DSS05	Egyértelmű szerepkör-kijelöléssel támogatja a kockázatok optimalizálását, a biztonság irányítását és a biztonsági szolgáltatások irányítását

1. Cél

1.1 Jelen szabályzat rögzíti szervezetünk elkötelezettségét az ügyfél- és üzleti információk védelme iránt azáltal, hogy egyértelműen meghatározza a felelősségi köröket és a gyakorlati biztonsági intézkedéseket, különös tekintettel a dedikált IT-csapattal nem rendelkező szervezetekre.

1.2 Biztosítja, hogy minden munkavállaló, szerződéses közreműködő és szolgáltató kötelező érvényű szabályok szerint járjon el, lehetővé téve az ISO/IEC 27001 tanúsítási követelményeinek teljes körű teljesítését.

1.3 Jelen szabályzat lehetővé teszi, hogy szervezetünk erősítse az ügyfelek bizalmát azáltal, hogy egyértelműen bemutatja, miként védi információikat meghatározott felelősségi körökkel, szabályozott folyamatokkal és egyértelmű elszámoltathatósággal.

2. Hatály

2.1 Jelen szabályzat hatálya kiterjed minden olyan személyre, aki hozzáfér a szervezet adataihoz és rendszereihez, vagy azokat kezeli, ideértve az alábbiakat:

2.1.1 üzlettulajdonosok és ügyvezetők

2.1.2 munkavállalók, szerződéses közreműködők, gyakornokok

2.1.3 külső IT-szolgáltatók vagy tanácsadók

2.2 A szabályzat az információk, rendszerek és szolgáltatások valamennyi típusára kiterjed, beleértve:

2.2.1 üzleti nyilvántartásokat, ügyféladatokat, jelszavakat és e-maileket

2.2.2 IT-eszközöket, például laptopokat és mobiltelefonokat

2.2.3 fájltárolásra, kommunikációra vagy pénzügyi működésre használt felhőszolgáltatásokat

2.2.4 irodai helyszíneken tárolt papíralapú dokumentumokat

2.3 A szabályzat valamennyi munkakörnyezetre alkalmazandó — irodai, távoli és felhőalapú működésre egyaránt —, és kiterjed minden olyan eszközre és szoftverre, amelyet üzleti információk kezelésére vagy tárolására használnak.

3. Célkitűzések

3.1 Egyértelmű felelősségi körök kijelölése: Biztosítani kell, hogy az információbiztonságért mindig egyértelműen kijelölt felelős személy feleljen. Ez jellemzően az ügyvezető vagy az általa hivatalosan kijelölt személy.

3.2 Ügyfél- és üzleti információk védelme: Megbízható és következetes védelmi intézkedéseket kell alkalmazni az érzékeny adatok — ideértve az ügyfél- és pénzügyi nyilvántartásokat is — jogosulatlan felhasználásának, elvesztésének vagy eltulajdonításának megelőzésére.

3.3 Az ISO/IEC 27001 tanúsítás támogatása: Lehetővé kell tenni, hogy a szervezet igazolja az ISO/IEC 27001 követelményeinek teljes körű megfelelését, biztosítva az auditra való felkészültséget és a tanúsíthatóságot összetett infrastruktúra nélkül is.

3.4 A biztonság beépítése az üzleti működésbe: Az információbiztonságot be kell építeni a szervezet napi feladataiba és döntéseibe.

3.5 A biztonságtudatosság és a biztonsági kultúra erősítése: El kell érni, hogy minden munkavállaló megértse és betartsa a biztonsági gyakorlatokat, például az erős jelszavak használatát és a gyanús tevékenységek jelentését.

4. Szerepkörök és felelősségek

4.1 Ügyvezető vagy üzlettulajdonos

4.1.1 Teljes körű felelősséggel tartozik az információbiztonságért.

4.1.2 Jóváhagyja és karbantartja jelen szabályzatot.

4.1.3 Biztosítja, hogy minden lényeges biztonsági feladatot közvetlenül ellásson, vagy azokat írásban delegálja.

4.1.4 Ellenőrzi, hogy a delegált biztonsági feladatokat — például a hozzáférések kezelését vagy az incidenskezelést — eredményesen végrehajtják.

4.1.5 Alapértelmezett kapcsolattartóként jár el minden belső és külső biztonsági ügyben, beleértve az auditokat és az ügyfélmegkereséseket is.

4.1.6 Az éves felülvizsgálat során nyomon követi az e célkitűzések teljesülése terén elért előrehaladást. A célkitűzéseknek lehetőség szerint mérhetőknek kell lenniük (pl. képzésben

részesült munkatársak aránya, jelentett incidensek száma), és azokat a biztonsági megállapítások, valamint a kockázatok változásai alapján felül kell vizsgálni.

4.2 Kijelölt munkavállaló (ha alkalmazandó)

4.2.1 Támogathatja az ügyvezetőt a napi feladatok ellátásában, például felhasználói fiókok létrehozásában, a kilépő munkatársak hozzáférésének megszüntetésében vagy az IT-szolgáltatóval történő egyeztetésben.

4.2.2 Hivatalosan kell kijelölni, és rendelkeznie kell a feladatok ellátásához szükséges jogosultságokkal és eszközökkel.

4.2.3 Minden problémát jelent az ügyvezetőnek.

[... 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 felülvizsgálat

9.1.1 Jelen szabályzatot az ügyvezetőnek évente legalább egyszer felül kell vizsgálnia annak biztosítására, hogy az továbbra is megfeleljen az ISO/IEC 27001 tanúsítási követelményeinek, a szabályozási változásoknak (például a GDPR, a NIS2 és a DORA előírásainak), valamint a változó üzleti igényeknek.

9.2 Rendkívüli felülvizsgálatok

9.2.1 További felülvizsgálatot kell lefolytatni minden jelentős változás esetén, például:

9.2.1.1 súlyos biztonsági incidensek vagy adatvédelmi, illetve szabályozási szempontból jelentős sérülések esetén

9.2.1.2 új üzleti folyamatok vagy technológiák bevezetésekor (pl. új szoftver, távmunka-platform vagy felhőszolgáltatás)

9.2.1.3 az információkezelést érintő jogi vagy szabályozási követelmények változásakor

9.3 A változások dokumentálása

9.3.1 Minden szabályzat-felülvizsgálatot és módosítást hivatalosan dokumentálni kell, egyértelműen feltüntetve a dátumot, a módosítás jellegét és az ügyvezető jóváhagyását.

9.3.2 A szabályzatverziók előzményeit biztonságosan meg kell őrizni annak igazolására, hogy a szabályzat miként fejlődött, és hogy az auditok során a megfelelés igazolható legyen.

9.4 A módosítások közlése

9.4.1 Jelen szabályzat minden módosításáról haladéktalanul tájékoztatni kell az összes munkavállalót, szerződéses közreműködőt és érintett külső felet.

9.4.2 A szabályzat frissített változatainak minden érintett személy számára könnyen hozzáférhetőnek kell lenniük (pl. elektronikus megosztással vagy a munkahelyen történő fizikai kifüggesztéssel).

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat szorosan kapcsolódik a szervezet SME szabályzatcsomagjának további szabályzataihoz, különösen az alábbiakhoz:

10.1.1 P2S – Irányítási szerepkörök és felelősségek szabályzat: Egyértelműsíti a biztonsági feladatok és felelősségek kijelölését.

10.1.2 P4S – Hozzáférés-szabályozási szabályzat: Meghatározza a szervezeti információkhoz való hozzáférés biztonságos kezelését.

10.1.3 P8S – Információbiztonsági tudatossági és képzési szabályzat: A munkatársak képzéséhez és tudatosságához szükséges alapvető iránymutatásokat tartalmazza.

10.1.4 P17S – Adatvédelmi és személyes adatok védelmére vonatkozó szabályzat: Biztosítja a GDPR és más adatvédelmi jogszabályoknak való megfelelést.

10.1.5 P30S – Incidenskezelési szabályzat: Leírja a biztonsági incidensekre adott válasz során szükséges részletes intézkedéseket.

10.2 E kapcsolódó szabályzatok egyértelmű operatív útmutatást adnak, és azokat együttesen kell alkalmazni az ISO/IEC 27001 tanúsítási követelményeinek teljes körű teljesítéséhez.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 5.1 pont – Vezetői szerepvállalás és elkötelezettség: Előírja a felső vezetés elkötelezettségét és elszámoltathatóságát az információbiztonság szervezeten belüli eredményességéért.

11.1.2 5.2 pont – Információbiztonsági szabályzat: Előírja az egyértelmű, dokumentált, a szervezeti stratégiával és megfelelőségi követelményekkel összhangban álló szabályzatokat.

11.1.3 5.3 pont – Szervezeti szerepkörök és felelősségek: Meghatározza az információbiztonsági felelősségek egyértelmű kijelölését a szervezet egészében, ami elengedhetetlen a hatékony irányításhoz és az auditmegfeleléshez.

11.1.4 6.1 pont – A kockázatok és lehetőségek kezelésére szolgáló intézkedések: Biztosítja, hogy az információbiztonsági kockázatokat rendszerszerűen azonosítsák, értékeljék és kezeljék.

11.1.5 8.1 pont – Operatív tervezés és kontroll: Előírja, hogy a szervezet megtervezze és végrehajtsa az információbiztonsági célok eléréséhez és a kapcsolódó kockázatok eredményes kezeléséhez szükséges folyamatokat.

11.2 ISO/IEC 27002:2022 5.1–5.5 kontrollok

11.2.1 Az 5.1 kontroll – Információbiztonsági szabályzatok: Meghatározza a dokumentált információbiztonsági szabályzatok kialakítását és kommunikációját.

11.2.2 Az 5.2 kontroll – Információbiztonsági szerepkörök: Egyértelműsíti és hivatalosan kijelöli az információbiztonsági szerepköröket és felelősségeket az érintett felek számára.

11.2.3 Az 5.3 kontroll – Feladatkörök szétválasztása: Előírja a feladatkörök egyértelmű szétválasztását az összeférhetetlenség és a csalási kockázatok csökkentése érdekében az érzékeny információk kezelése során.

11.2.4 Az 5.4 kontroll – Vezetői felelősségek: Előírja, hogy a vezetés aktív felügyelettel és erőforrások biztosításával igazolja az információbiztonság iránti elkötelezettségét.

11.2.5 Megerősíti az egyértelműen dokumentált információbiztonsági szabályzatok, szerepkörök, felelősségek és irányítási struktúrák szükségességét, biztosítva a következetes irányítást és az auditálhatóságot a szervezet egészében.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Információbiztonsági programterv: Előírja a dokumentált információbiztonsági irányítási stratégiákat és szabályzatokat, keretet adva a következetes alkalmazáshoz és irányításhoz.

11.3.2 PL-1 – Biztonsági tervezési szabályzat: Előírja a szervezet egészére kiterjedő biztonsági tervezési szabályzatot az információbiztonsági tevékenységek biztonságos működésének és stratégiai összhangjának biztosítására.

11.3.3 CA-1 – Biztonsági értékelési és engedélyezési szabályzat: Előírja az egyértelműen meghatározott értékelési és engedélyezési szerepköröket az információbiztonsági követelmények folyamatos eredményességének és megfelelésének biztosítása érdekében.

11.3.4 AC-1 – Hozzáférés-szabályozási szabályzat: Előírja, hogy a szervezetek egyértelműen határozzák meg, dokumentálják és alkalmazzák a hozzáféréskezelési gyakorlatokat és felelősségeket.

11.4 GDPR (2016/679)

11.4.1 5. cikk (2) bekezdés – Elszámoltathatóság elve: Előírja, hogy a szervezetek igazolják az adatvédelmi elveknek való megfelelést, ideértve az adatvédelmi felelősségekre vonatkozó dokumentált szerepköröket és szabályzatokat is.

11.4.2 32. cikk – Az adatkezelés biztonsága: Előírja a megfelelő technikai és szervezési intézkedések bevezetését, beleértve az egyértelmű biztonsági felelősségeket is, a személyes adatok sérülésekkel és jogosulatlan hozzáféréssel szembeni védelme érdekében.

11.5 az EU NIS2 irányelve (2022/2555)

11.5.1 21. cikk (2) bekezdés a) pont – Kockázatkezelési intézkedések: Előírja az egyértelmű irányítási rendet, beleértve az információbiztonsághoz kapcsolódó meghatározott szerepköröket és felelősségeket, amelyek alapvetők a kiberkockázatok eredményes kezeléséhez.

11.6 az EU DORA-rendelete (2022/2554)

11.6.1 9. cikk – IKT-kockázatkezelés: Előírja, hogy a szervezetek egyértelműen jelöljék ki az IKT-kockázatkezeléssel kapcsolatos szerepköröket és felelősségeket, erősítve az ellenálló képességet és az üzletmenet-folytonossági felkészültséget.

11.6.2 10. cikk – IKT-üzletmenet-folytonosság: Előírja az IKT-ellenálló képesség és a folytonosság fenntartásához szükséges egyértelmű elszámoltathatóságot és szabályozott szerepköröket, biztosítva, hogy a szervezetek megbízhatóan tudjanak reagálni a zavarokra.

11.7 COBIT 2019

11.7.1 EDM03 – A kockázatok optimalizálásának biztosítása: Hangsúlyozza a szervezeti kockázatok kezeléséhez szükséges egyértelműen meghatározott elszámoltathatóságot és szerepköröket, erős irányítást és hatékony felügyeletet biztosítva az információbiztonsági kockázatok felett.

11.7.2 APO13 – A biztonság irányítása: Előírja, hogy a szervezetek egyértelműen alakítsák ki és kommunikálják a biztonságirányítási felelősségeket, biztosítva az üzleti célokkal és a szabályozási követelményekkel való összhangot.

11.7.3 DSS05 – A biztonsági szolgáltatások irányítása: Szabályozott szerepköröket és egyértelmű felelősségeket ír elő a biztonsági szolgáltatások irányításához, lehetővé téve a következetes végrehajtást és a megfelelés ellenőrzését.