					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P08S					Dokumentum címe: **Információbiztonsági tudatossági és képzési 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	7. pont	
ISO/IEC 27002:2022	6. kontroll	
NIST SP 800-53 Rev.5	AT-2, AT-4	
EU NIS2	21. cikk (2) bekezdés i) pont	
EU DORA	13. cikk	
COBIT 2019	BAI08, DSS05	
EU GDPR	32. cikk, 39. cikk	

1. Cél

1.1. Jelen szabályzat biztosítja, hogy valamennyi munkavállaló és vállalkozó tisztában legyen az információbiztonsággal kapcsolatos felelősségi köreivel.

1.2. Célja az emberi hibák valószínűségének csökkentése, az incidensek észlelésének és jelentésének javítása, valamint a biztonságtudatos szervezeti kultúra erősítése.

1.3. A szabályzat támogatja az ISO/IEC 27001, a NIS2, a GDPR és a DORA követelményeinek való megfelelést azáltal, hogy a biztonságtudatosságot a mindennapi munkavégzés és a szerepköralapú elvárások részévé teszi.

2. Hatály

2.1. Jelen szabályzat minden munkavállalóra, vállalkozóra, gyakornokra és külső félre vonatkozik, aki hozzáfér a vállalati rendszerekhez vagy adatokhoz.

2.2. A szabályzat kiterjed az alábbiakra:

2.2.1. a beléptetéshez kapcsolódó induló képzés az újonnan belépő munkatársak számára

2.2.2. az éves ismétlő biztonságtudatossági képzés

2.2.3. az eseti tudatosságnövelő tevékenységek (pl. incidenshez kapcsolódó tájékoztatások, plakátok vagy figyelemfelhívó üzenetek)

2.3. A szabályzat minden munkakörre, szervezeti egységre és munkavégzési helyre kiterjed.

3. Célkitűzések

3.1. Biztosítani kell, hogy valamennyi munkatárs időben, érthető és releváns biztonságtudatossági képzésben részesüljön.

3.2. Biztosítani kell, hogy a munkavállalók képesek legyenek azonosítani és elkerülni a gyakori fenyegetéseket, így különösen az adathalászatot, a kártékony kódokat és az adatszivárgást.

3.3. A jogi, szerződéses és auditkövetelményeknek való megfelelés igazolása érdekében biztosítani kell a képzések teljesítésének dokumentálását.

3.4. Fenn kell tartani a naprakész képzési tartalmat, amely tükrözi a szervezet szabályzatait, a fenyegetéseket és az alkalmazandó jogszabályi követelményeket.

3.5. Erősíteni kell a munkatársak proaktív szemléletét annak érdekében, hogy a biztonság a napi felelősségvállalás részévé váljon.

4. Szerepkörök és felelősségek

4.1. Ügyvezető

4.1.1. Jóváhagyja a képzési követelményeket, és biztosítja a szükséges erőforrások rendelkezésre állását.

4.1.2. Felülvizsgálja a teljesítési jelentéseket, és szükség esetén eszkalálja a meg nem felelés eseteit.

4.2. Irodavezető / HR

4.2.1. Koordinálja az új belépők képzéseit és az éves ismétlő képzéseket.

4.2.2. Vezeti a képzési nyilvántartásokat és teljesítési naplókat.

4.2.3. Biztosítja, hogy a munkatársak tudomásul vegyék az alapvető biztonsági szabályzatokat és a titoktartási megállapodásokat.

[... 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 és a HR-nek évente felül kell vizsgálnia annak biztosítása érdekében, hogy az tükrözze az aktuális kockázatokat, jogszabályi követelményeket és a szervezet munkaerő-állományával kapcsolatos igényeit.

9.2. Soron kívüli frissítések

9.2.1. A szabályzatot és a képzési tartalmat az alábbi esetekben is felül kell vizsgálni, és szükség szerint módosítani kell:

9.2.1.1. jelentős biztonsági incidens

9.2.1.2. jogi vagy szerződéses változás

9.2.1.3. szervezeti átalakítás vagy rendszermigráció

9.3. Verziókezelés és terjesztés

9.3.1. Minden frissítésnek tartalmaznia kell:

9.3.1.1. a verziószámot és a hatálybalépés dátumát

9.3.1.2. a változások összefoglalását

9.3.1.3. az ügyvezető jóváhagyását

9.3.1.4. valamennyi korábbi verzió archívumát, legalább hároméves megőrzési idővel

9.4. Munkavállalói kommunikáció

9.4.1. A szabályzat frissítéseiről minden munkatársat tájékoztatni kell, és lényeges módosítás esetén be kell szerezni a tudomásulvételt.

10. Kapcsolódó szabályzatok és összefüggések

10.1. Jelen szabályzat az alábbiakat támogatja:

10.1.1. P2S – Irányítási szerepkörök és felelősségek szabályzat: kijelöli a képzési koordináció és felügyelet felelősségi köreit

10.1.2. P3S – Elfogadható használati szabályzat: megerősíti a képzésben tárgyalt magatartási elvárásokat

10.1.3. P4S – Hozzáférés-szabályozási szabályzat: biztosítja, hogy a felhasználók megértsék a hozzáférésbiztonság jelentőségét

10.1.4. P7S – Beléptetési és kiléptetési szabályzat: beépíti a képzést a belépési folyamatba

10.1.5. P30S – Incidenskezelési szabályzat: biztosítja, hogy a munkatársak tudják, hogyan kell az incidenseket haladéktalanul és megfelelően jelenteni

11. Hivatkozott szabványok és keretrendszerek

11.1. ISO/IEC 27001

11.1.1. 7.3. pont – előírja, hogy a szervezetek biztosítsák a munkatársak tudatosságát a felelősségi köreikkel és a biztonsági hatásokkal kapcsolatban

11.2. ISO/IEC 27002

11.2.1. 6.3. kontroll – részletezi a biztonsági képzés hatályára és lebonyolítására vonatkozó elvárásokat

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – előírja a rendszerekhez hozzáféréssel rendelkező felhasználók tudatossági képzését

11.3.2. AT-4 – kiterjed a szerepköralapú képzésre és a meg nem felelés következményeire

11.4. EU GDPR

11.4.1. 32. cikk – előírja a személyes adatok védelmét szolgáló biztonsági intézkedéseket, beleértve a munkatársak képzését is

11.4.2. 39. cikk – alkalmazandó esetben előírja, hogy az adatvédelmi tisztviselő felügyelje a tudatosságnövelést és a képzést

11.5. EU NIS2 irányelv

11.5.1. 21. cikk (2) bekezdés i) pont – folyamatos kiberbiztonsági tudatossági és képzési programokat ír elő

11.6. EU DORA

11.6.1. 13. cikk – előírja, hogy a pénzügyi szervezetek oktatást és képzést valósítsanak meg minden olyan munkatárs számára, aki IKT-val kapcsolatos felelősségi körrel rendelkezik

11.7. COBIT 2019

11.7.1. BAI08 – Tudásmenedzsment: biztosítja, hogy a munkatársak megfelelő kompetenciával rendelkezzenek és képzésben részesüljenek

11.7.2. DSS05 – Biztonsági szolgáltatások kezelése: kiemeli a tudatosságot mint kulcsfontosságú védelmi kontrollt