					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P08					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	7.3 pont, A melléklet 6.3. kontroll	Meghatározza a jelen szabályzatban kezelt tudatossági és képzési követelményeket
ISO/IEC 27002:2022	6. kontroll	Támogatja a munkakörhöz igazított, megfelelő tudatossági képzés kialakítását
NIST SP 800-53 Rev.5	AT-1–AT-5	Összhangban áll a szabályzatokkal és eljárásokkal, a tudatossági képzéssel, a szerepköralapú képzéssel, a képzési nyilvántartásokkal és a biztonsági csoporttal való kapcsolattartással
EU GDPR	32., 39. cikk; (78) preambulumbekezdés	Képzést ír elő a személyes adatokat kezelő munkatársak számára, valamint általános munkavállalói tudatosságot követel meg
EU NIS2	21. cikk (2) bekezdés a), b); 21. cikk (3) bekezdés	Kockázatkezelési és biztonsági képzési szabályzatokat, valamint tudatosságnövelő kezdeményezéseket követel meg
EU DORA	5., 8., 13. cikk	Előírja az IKT-kockázatokkal kapcsolatos tudatosságot és képzést mint a rezilienciakontrollok részét
COBIT 2019	APO07, DSS05, MEA	Megerősíti a munkavállalói tudatosság, a felhasználói oktatás és a megfelelés nyomon követésének követelményét

1. Cél

1.1 Jelen szabályzat meghatározza azt a formális keretrendszert, amely biztosítja, hogy valamennyi munkatárs tisztában legyen információbiztonsági felelősségi köreivel, és megkapja az információs vagyon bizalmasságának, sértetlenségének és rendelkezésre állásának védelméhez szükséges képzést.

1.2 A szabályzat támogatja az ISO/IEC 27001 7.3 pontját és az A melléklet 6.3. kontrollját azáltal, hogy előírja egy strukturált, kockázatalapú tudatossági és képzési program működtetését, amely a szervezeti szerepkörökhöz és a változó fenyegetésekhez igazodik.

1.3 A szabályzat hozzájárul az emberi tényezőből eredő sérülékenységek csökkentéséhez, a biztonságtudatos magatartás előmozdításához, valamint a biztonságos gyakorlatok folyamatos megerősítéséhez a szabályozási és szerződéses követelményekkel összhangban.

2. Hatály

2.1 Jelen szabályzat hatálya kiterjed minden olyan belső és külső személyre, aki hozzáfér a szervezet információs rendszereihez, adataihoz vagy létesítményeihez, ideértve az alábbiakat:

2.1.1 munkavállalók (teljes munkaidős, részmunkaidős, ideiglenes)

2.1.2 szerződéses közreműködők, tanácsadók, beszállítók és gyakornokok

2.1.3 szolgáltatási megállapodás alapján logikai vagy fizikai hozzáféréssel rendelkező harmadik felek

2.2 A hatály az alábbiakra terjed ki:

2.2.1 kezdeti beléptetési biztonságtudatossági képzés

2.2.2 szerepkörspecifikus képzés (pl. fejlesztők, pénzügyi munkatársak, emelt jogosultságú hozzáféréssel rendelkező felhasználók)

2.2.3 időszakos ismétlő képzés és tudatosságnövelő kampányok

2.2.4 incidensekre vagy új fenyegetésekre reagáló eseti képzés

2.3 A jelen szabályzat hatálya alá tartozó képzésszervezési és -lebonyolítási mechanizmusok közé tartozik az e-learning, a személyes eligazítás, a szimulációk, a tudástesztek, a plakátok, a hírlevelek és a kötelező visszaigazolások.

3. Célkitűzések

3.1 Annak biztosítása, hogy valamennyi munkatárs megértse a szervezeti vagyonelemek védelmével és a biztonsági szabályzatok betartásával kapcsolatos felelősségét.

3.2 Folyamatos, mérhető tudatossági képzés biztosítása a szerepköralapú kockázati kitettséghez igazítva.

3.3 A biztonságos magatartás beépítése a napi működésbe olyan gyakorlatok megerősítésével, mint a jelszavak biztonságos használata, az incidensjelentés és az adathalászattal szembeni ellenálló képesség.

3.4 A jogszabályi megfelelés és az auditkészültség biztosítása az információbiztonsági képzési követelmények tekintetében valamennyi érintett iparágban és joghatóság alatt.

3.5 A gondatlanságból, a tudatosság hiányából vagy hibás döntésből eredő biztonsági incidensek csökkentése viselkedésformálással és folyamatos megerősítéssel.

4. Szerepkörök és felelősségi körök

4.1 Felső vezetés

4.1.1 Jóváhagyja a szervezet információbiztonsági képzési stratégiáját, biztosítja a szükséges erőforrásokat, valamint azt, hogy a stratégia beépüljön a vállalati prioritások közé.

4.1.2 Vezetői szinten nyomon követi a megfelelést, és biztosítja a szabályzatok betartását a szervezeti egységekben.

4.2 Információbiztonsági vezető / IBIR-vezető

4.2.1 Felelős a jelen szabályzatért, és meghatározza a tudatossági és képzési keretrendszert a kockázatokkal, a megfeleléssel és az üzleti igényekkel összhangban.

4.2.2 Felügyeli valamennyi biztonsági képzési kezdeményezés tervezését, végrehajtását, nyomon követését és felülvizsgálatát.

4.2.3 Biztosítja, hogy a képzések időszakosan frissítésre kerüljenek, és tükrözzék a változó fenyegetéseket, valamint a megjelenő technológiákat.

[... 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 Felülvizsgálati gyakoriság

9.1.1 Jelen szabályzatot és a kapcsolódó képzési programot az alábbi esetekben kell felülvizsgálni:

9.1.1.1 évente, vagy

9.1.1.2 jelentős, emberi hibával vagy belső fenyegetéssel összefüggő incidenseket követően

9.1.1.3 jelentős új technológiák vagy fenyegetések bevezetésekor

9.1.1.4 jogi, szerződéses vagy tanúsítási kötelezettségek változása esetén

9.2 Felülvizsgálati folyamat

9.2.1 A felülvizsgálatot az információbiztonsági vezető vezeti az alábbiakkal együttműködésben:

9.2.1.1 HR- és képzési szervezeti egységek

9.2.1.2 jogi terület és adatvédelmi tisztviselők

9.2.1.3 IT-biztonsági és operatív kockázatkezelési funkciók

9.2.2 Minden frissítést az alábbi követelmények szerint kell kezelni:

9.2.2.1 azokat az IBIR irányító bizottságnak jóvá kell hagynia

9.2.2.2 verziókezelés alá kell vonni, és azokat az IBIR dokumentumkontroll-nyilvántartásban dokumentálni kell

9.2.2.3 a felhasználókat tájékoztatni kell, ha az érdemi változások érintik a képzés hatályát vagy a felelősségi köröket

9.3 Tartalomfrissítési irányítás

9.3.1 A képzési modulokat és tudatossági anyagokat 12 havonta felül kell vizsgálni annak biztosítása érdekében, hogy:

9.3.1.1 relevánsak maradjanak a fenyegetettségi környezet szempontjából

9.3.1.2 szabályozási szempontból pontosak legyenek

9.3.1.3 formátumuk kompatibilis legyen (pl. akadálymentesség, lokalizáció)

9.3.2 Az elavult vagy félrevezető tartalmat haladéktalanul vissza kell vonni, és jóváhagyott alternatívával kell helyettesíteni.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzatot az alábbi szabályzatok támogatják, és azok alkalmazását is támogatja:

10.1.1 P01 – Információbiztonsági szabályzat: a biztonságtudatosságot a szervezet IBIR-ének alapvető kontrolljaként határozza meg.

10.1.2 P03 – Elfogadható használati szabályzat: előírja a felhasználói tudomásulvételt a képzés során, és egyértelművé teszi a napi technológiahasználathoz kapcsolódó felelősségeket.

10.1.3 P07 – Beléptetési és kiléptetési szabályzat: biztosítja, hogy a képzés a belépéskor beépüljön a folyamatokba, és a foglalkoztatás teljes időtartama alatt nyomon követhető legyen.

10.1.4 P06 – Kockázatkezelési szabályzat: összekapcsolja az emberi tényezőre fókuszáló képzést a fenyegetésmodellezéssel és a maradványkockázat-csökkentési stratégiákkal.

10.1.5 P33 – Audit- és megfelelésmonitorozási szabályzat: igazolja, hogy a tudatossági kontrollok az auditok során működnek, mérhetők és hatékonyak.

10.2 Ezek a szabályzatok együttesen olyan átfogó magatartási kontrollkeretrendszert alkotnak, amely integrálja a tudatosságot, az elszámoltathatóságot és a szervezeti kultúra megerősítését.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 7.3 pont – Tudatosság: előírja, hogy a szervezetek biztosítsák, hogy a munkavállalók tisztában legyenek az információbiztonsági szabályzatokkal és saját felelősségi köreikkel. Jelen

szabályzat ezt a követelményt strukturált beléptetéssel, időszakos képzéssel és mérhető kampányrészvétellel ülteti át a gyakorlatba.

11.1.2 A melléklet 6.3. kontroll – Információbiztonsági tudatosság, oktatás és képzés: teljes körűen lefedett a kezdeti, szerepköralapú és folyamatos képzési programok által, a felhasználói kockázati profilokhoz igazítva.

11.2 ISO/IEC 27002:2022 – 6. kontroll

11.2.1 Támogatja a munkaköröknek megfelelő tudatossági képzés kialakítását és megvalósítását, hangsúlyozva a biztonságos magatartás megerősítését és a fenyegetési információk, valamint az audit-visszajelzések alapján végrehajtott időszakos frissítéseket.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1–AT-5 (Awareness and Training Family): Jelen szabályzat összhangban áll az AT-1 (szabályzat és eljárások), AT-2 (tudatossági képzés), AT-3 (szerepköralapú képzés), AT-4 (biztonsági képzési nyilvántartások) és AT-5 (kapcsolattartás biztonsági csoportokkal) kontrollokkal.

11.3.2 IA-5, AC-2: megerősíti a felhasználók felelősségét a biztonságos hitelesítés és az elfogadható használat terén, amelyek a tudatossági programok magatartási eredményeinek alapvető elemei.

11.3.3 IR-1–IR-8: az incidenskezelési felkészültséget célzott tudatosságnövelő kampányok és szimulációk erősítik.

11.4 EU GDPR (2016/679)

11.4.1 32. cikk – Az adatkezelés biztonsága: előírja, hogy a személyes adatokat kezelő munkatársakat fel kell készíteni a személyes adatokkal kapcsolatos kockázatok felismerésére, megelőzésére és jelentésére. Jelen szabályzat biztosítja, hogy a személyes adatokat kezelő munkatársak és minden releváns szerepkör ennek megfelelő képzésben részesüljön.

11.4.2 39. cikk – Az adatvédelmi tisztviselő feladatai: magában foglalja az adatkezelési műveletekben részt vevő munkatársak tudatosságának növelését és képzését.

11.4.3 (78) preambulumbekezdés: ösztönzi a megfelelő tudatossági intézkedések alkalmazását a robusztus biztonsági gyakorlatok és a szabályzatok betartásának biztosítása érdekében.

11.5 EU NIS2 irányelv (2022/2555)

11.5.1 21. cikk (2) bekezdés a), b): előírja, hogy a szervezetek valamennyi releváns munkatársra kiterjedő kockázatelemzési és biztonsági képzési szabályzatokat fogadjanak el. Jelen szabályzat e követelménynek folyamatos, szerepkörérzékeny képzési folyamatok kialakításával felel meg.

11.5.2 21. cikk (3) bekezdés: ösztönzi a vezetés és a munkatársak kiberbiztonsági kockázatokkal kapcsolatos tudatosságának növelését tudatossági kezdeményezésekkel és szimulációkkal.

11.6 EU DORA (2022/2554)

11.6.1 13. cikk – Digitális működési reziliencia stratégia: előírja, hogy az IKT-kockázatokkal kapcsolatos tudatosság és képzés az irányítási modell részét képezze. Jelen szabályzat biztosítja, hogy az emberi kockázatok kezelése folyamatos oktatás és fenyegetési szimuláció útján megvalósuljon.

11.6.2 5. és 8. cikk: hangsúlyozza a belső kontrollkeretrendszerek fontosságát, amelyeknek az IKT-reziliencia és a kiberhigiénia szempontjából alapvető eleme a tudatosság és a képzés.

11.7 COBIT 2019

11.7.1 APO07 – Managed Human Resources: megerősíti a biztonsági felelősségi körökkel kapcsolatos tudatosság fejlesztésének szükségességét és ennek a munkaerő-kezelésbe való beépítését.

11.7.2 DSS05 – Biztonsági szolgáltatások kezelése: meghatározza a felhasználói oktatásra és az incidensjelentésre vonatkozó kontrollokat, amelyek jelen szabályzat szerves részét képezik.

11.7.3 MEA03 – Monitor, Evaluate, and Assess Compliance: előírja a felhasználói magatartás és a szabályzatok betartásának hatékonysági felülvizsgálatát, amelyet jelen szabályzat adathalászati tesztekkel, tudásteszteket és tudatosságnövelő kampánymutatókkal valósít meg.