					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P13					Dokumentum címe: **Adatosztályozási és címkézési 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 információs vagyonának érzékenység, kockázati kitettség és szabályozási kötelezettségek szerinti osztályozására és címkézésére szolgáló formális keretrendszert.

1.2 Biztosítja, hogy valamennyi információ – függetlenül a tárolás, továbbítás vagy kezelés formájától – egyértelműen kategorizált és címkézett legyen, oly módon, hogy az jelezze a szükséges védelmi és kezelési szintet.

1.3 A szabályzat a szervezet kockázatkezelési gyakorlatával összhangban álló, strukturált osztályozást ír elő, támogatva a bizalmasság, sértetlenség és rendelkezésre állás célkitűzéseit mind a digitális, mind a fizikai adattípusok esetében.

1.4 Ez a kontroll elengedhetetlen a szerepköralapú hozzáférés-szabályozás, az auditkészség, a megfelelő adatmegosztás, valamint az olyan technikai védelmi intézkedések hatékony alkalmazásának biztosításához, mint a titkosítás, a biztonsági mentés és a nyomon követhetőség.

2. Hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 Valamennyi szervezeti információs vagyonra, beleértve a dokumentumokat, adatbázisokat, nyilvántartásokat és kommunikációt

2.1.2 Valamennyi adatformátumra, beleértve a digitális, nyomtatott, írott és szóbeli formát

2.1.3 Valamennyi környezetre: helyszíni, távoli, mobil és felhőalapú környezetekre

2.1.4 Valamennyi munkavállalóra, vállalkozóra, szolgáltatóra és adatfeldolgozó harmadik félre, akik szervezeti információt hoznak létre, kezelnek vagy tárolnak

2.2 A hatály kiterjed a belső fejlesztésű tartalmakra, a külső forrásból származó adatokra, az adatvédelmi jogszabályok hatálya alá tartozó személyes adatokra (pl. GDPR), valamint az ügyfelekkel, partnerekkel és szabályozó hatóságokkal megosztott információkra.

2.3 A szabályzat minden olyan rendszerre alkalmazandó, amelyet adatok tárolására vagy továbbítására használnak, beleértve a vállalati alkalmazásokat, fájlszervereket, e-mail-rendszereket, felhőplatformokat és biztonsági mentési tárhelyeket.

3. Célkitűzések

3.1 A szervezet egészére kiterjedő, szabványosított osztályozási séma kialakítása az adatok nyilvánosságra kerülésének vagy kompromittálódásának hatása alapján.

3.2 Annak biztosítása, hogy valamennyi információ látható és tartós címkézéssel rendelkezzen, amely tükrözi az osztályozási szintet és a kezelési követelményeket.

3.3 Az osztályozáshoz igazodó adatkezelési és hozzáférés-szabályozási kontrollok érvényesítése, beleértve a titkosítást, a naplózást, az adattovábbítás védelmét és a megőrzési ütemezést.

3.4 A nemzetközi szabványoknak (ISO/IEC 27001, 27002), jogi keretrendszereknek (GDPR, NIS2, DORA) és a belső kockázatkezelési szabályzatoknak való megfelelés támogatása.

3.5 Annak biztosítása, hogy valamennyi felhasználó tisztában legyen az adatok védelmével, a címkék alkalmazásával és az osztályozott információk megfelelő kezelésével kapcsolatos felelősségével.

3.6 Az osztályozási állapot, a kapcsolódó kontrollok és a szervezet eszköznyilvántartása közötti visszakövethetőség fenntartása audit- és megfelelőségi célokból.

4. Szerepkörök és felelősségi körök

4.1 Információbiztonsági vezető

4.1.1 Felelős az információosztályozási és címkézési szabályzatért, valamint biztosítja annak összhangját a szabályozási, szerződéses és működési követelményekkel.

4.1.2 Jóváhagyja az osztályozási szinteket, a címkézési szabványokat és a szabályzat módosításait.

4.1.3 Auditok, mérőszámok és kivételfelülvizsgálatok útján felügyeli a szabályzatnak való megfelelést.

4.1.4 Koordinálja a területek közötti irányítást a jogi, adatvédelmi és kockázatkezelési csapatokkal.

4.2 Az információs vagyon tulajdonosai

4.2.1 Felelősek az irányításuk alá tartozó információs vagyon szervezeti osztályozási séma szerinti besorolásáért.

4.2.2 Az osztályozási címkéket létrehozáskor, módosításkor vagy átvételkor alkalmazzák.

4.2.3 Időszakosan felülvizsgálják a vagyonelemek osztályozását, különösen az érzékenység, a szabályozási hatály vagy az üzleti érték változása esetén.

4.2.4 Biztosítják, hogy az érzékeny adatok teljes életciklusuk során megfelelően legyenek kezelve és címkézve.

[... 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 Jelen szabályzatot legalább évente felül kell vizsgálni annak biztosítására, hogy összhangban maradjon az alábbiakkal:

9.1.1 a változó szabályozási követelményekkel (pl. GDPR, NIS2, DORA),

9.1.2 az ISO/IEC 27001 vagy 27002 osztályozásra vonatkozó iránymutatásainak frissítéseivel,

9.1.3 az adatérzékenységet vagy tulajdonosi felelősséget érintő szervezeti változásokkal,

9.1.4 a technológiai változásokkal, beleértve az új dokumentum- vagy adatkezelési platformokat.

9.2 Az információbiztonsági vezető köteles kezdeményezni a felülvizsgálatot az Információbiztonsági Bizottsággal, a jogi területtel és az érintett üzleti egységekkel együttműködésben.

9.3 A felülvizsgálatnak ki kell terjednie:

9.3.1 az osztályozás érvényesítésének hatékonyságára és a felhasználói megfelelésre,

9.3.2 a hibás osztályozáshoz kapcsolódó incidensek vagy kivételek elemzésére,

9.3.3 a felhasználói visszajelzésekre a címkézési eszközökkel vagy iránymutatásokkal kapcsolatban,

9.3.4 az iparági osztályozási szabványokkal való összevetésre.

9.4 A szabályzat frissítéseit verziókezelés alatt kell tartani, dokumentálni kell az IBIR adattárában, és valamennyi érintett munkatárssal közölni kell, különös tekintettel az új felelősségi körökre vagy az eszközváltozásokra.

9.5 Az új belépőket a beléptetés során meg kell ismertetni a szabályzat aktuális változatával. Valamennyi munkavállaló köteles ismétlő képzést teljesíteni jelentős szabályzatmódosításokat követően.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzatot közvetlenül támogatják az alábbi kapcsolódó szabályzatok, és azokban meghatározott kontrollokat érvényesíti:

10.1.1 P4 - Hozzáférés-szabályozási szabályzat: Az információkhoz való hozzáférést az osztályozási szintek szabályozzák; az érzékenyebb adatok szigorúbb hozzáférés-szabályozást és jóváhagyási mechanizmusokat igényelnek.

10.1.2 P11 - Felhasználói fiók- és jogosultságkezelési szabályzat: megerősíti a szükséges ismeret elve alapján történő jogosultságkiosztást, amelyet az osztályozási szintek határoznak meg.

10.1.3 P12 - Eszközkezelési szabályzat: biztosítja, hogy a nyilvántartásban szereplő minden vagyonelem tartalmazza az osztályozását és címkéjét, támogatva a visszakövethetőséget és az elszámoltathatóságot.

10.1.4 P14 - Adatmegőrzési és selejtezési szabályzat: a selejtezési és megőrzési szabályokat az adatok osztályozási szintje és a szabályozói megőrzési követelmények határozzák meg.

10.1.5 P18 - Kriptográfiai kontrollok szabályzata: az információs vagyonelemek osztályozása alapján megfelelő titkosítási szabványokat alkalmaz.

10.1.6 P22 - Naplózási és felügyeleti szabályzat: lehetővé teszi az osztályozott információkhoz való hozzáférés és azok mozgásának nyomon követését, biztosítva az auditálhatóságot, valamint a hibás címkézés vagy a visszaélés észlelését.

10.2 Minden kapcsolódás biztosítja az információk következetes védelmét a teljes életciklusuk során, a létrehozástól és osztályozástól kezdve a biztonságos kezelésen, tároláson és továbbításon át a végleges megsemmisítésig.

11. Hivatkozott szabványok és keretrendszerek

11.1 Jelen szabályzat összhangban áll az érzékeny információk osztályozását és címkézését szabályozó, nemzetközileg elismert szabványokkal és szabályozási keretrendszerekkel.

11.2 ISO/IEC 27001

11.2.1 4.2. pont - Az érdekelt felek igényeinek és elvárásainak megértése. Az osztályozási követelmények gyakran az érdekelt felek által előírt jogi, szabályozási vagy szerződéses kötelezettségekből erednek (pl. GDPR, ügyféllel kötött titoktartási megállapodások), amelyeket a szabályzatban tükrözni kell.

11.2.2 6.1.3. pont - Információbiztonsági kockázatkezelés. Az osztályozás közvetlenül befolyásolja a kockázatkezelési kontrollok kiválasztását, beleértve a hozzáférés-szabályozást, a titkosítást és a megőrzést, az adatok érzékenysége alapján.

11.2.3 7.2. pont - Alkalmasság. A szabályzat előírja, hogy az osztályozásért és címkézésért felelős személyzet megfelelő képzésben részesüljön, ami az alkalmassági követelmények körébe tartozik.

11.2.4 7.3. pont - Tudatosság. A szabályzat előírja, hogy valamennyi felhasználó legyen tisztában az osztályozási szintekkel és az információkezeléssel kapcsolatos felelősségével, összhangban a biztonságtudatossági kötelezettségekkel.

11.2.5 7.5. pont - Dokumentált információ. Maga az osztályozási szabályzat is szabályozott dokumentum, továbbá az eljárások, a képzési nyilvántartások és az osztályozási címkék is a dokumentált információ részét képezik.

11.2.6 8.1. pont - Működéstervezés és működési szabályozás. Az osztályozás és a címkézés az adat-életciklus-kezelésbe beépített működési folyamatok, és ez a pont biztosítja, hogy az ilyen tevékenységek tervezetten, végrehajtottan és szabályozottan működjenek.

11.2.7 9.1. pont - Megfigyelés, mérés, elemzés és értékelés. A szabályzat rendelkezéseket tartalmaz az osztályozásnak való megfelelés, az incidensminták és a címkézési séma hatékonyságának nyomon követésére.

11.2.8 10.1. pont - Nemmegfelelőség és helyesbítő intézkedés. A szabályzat meghatározza a hibás osztályozásra adott válaszokat, beleértve az olyan helyesbítő intézkedéseket, mint az ismételt képzés, a frissítések és a kivételkezelés.

11.3 ISO/IEC 27002:2022

11.3.1 5.12. kontroll - Információk osztályozása. Ez a kontroll biztosítja, hogy az információ osztályozása az érzékenység, az érték és a kritikusság alapján történjen – pontosan ezt formalizálja jelen szabályzat.

11.3.2 5.13. kontroll - Információk címkézése. Ez a kontroll előírja az információ megfelelő címkézését az osztályozási szintnek megfelelően, amelyet a szabályzat teljes körűen kezel.

11.3.3 5.10. kontroll - Az információk és egyéb kapcsolódó vagyonelemek elfogadható használata. A szabályzat előírja, hogyan kell a felhasználóknak az osztályozott adatokat kezelniük, közvetlenül támogatva az elfogadható használatot és megelőzve a visszaéléseket.

11.3.4 5.11. kontroll - Vagyonelemek visszaszolgáltatása. Az osztályozás segít biztosítani, hogy az érzékeny adatok azonosíthatók legyenek, és munkavállaló vagy beszállító távozásakor biztonságosan visszaszolgáltassák vagy megtisztítsák azokat.

11.3.5 5.9. kontroll - Információk és egyéb kapcsolódó vagyonelemek nyilvántartása. Az osztályozás gyakran az eszköznyilvántartáshoz kapcsolódik, amelynek tükröznie kell minden tétel osztályozási szintjét a megfelelő kontrollkiosztás támogatása érdekében.

11.3.6 5.14. kontroll - Információtovábbítás. Az osztályozási szintek befolyásolják a belső és külső adattovábbításokra vonatkozó kontrollokat (pl. titkosítás, jóváhagyás, hozzáférési korlátozások).

11.3.7 8.12. kontroll - Adatszivárgás megelőzése. Az osztályozás és a címkézés érvényesítése támogatja a jogosulatlan nyilvánosságra hozatal és az adatvesztés megelőzését.

11.3.8 8.11. kontroll - Adatmaszkolás. Bizonyos osztályozási szintek (pl. Bizalmas, Korlátozott) előírhatják a maszkolást, amikor az adatokat tesztelési, fejlesztési vagy elemzési célra használják.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - Rendszer- és kommunikációvédelmi szabályzat és eljárások: támogatja az osztályozási szabályzatokat mint az átfogó adatvédelem részét.

11.4.2 AC-16 - Biztonsági attribútumok: a hozzáférés érvényesítését osztályozási metaadatok és felhasználói jogosultságok alapján valósítja meg.

11.4.3 MP-3 / MP-5 - Adathordozók jelölése és szállításvédelme: előírja az adatok címkézését és védelmét tárolás és továbbítás során az osztályozás alapján.

11.5 GDPR (2016/679)

11.5.1 5. cikk - Az adatkezelés alapelvei: előírja, hogy a személyes adatok kezelése biztonságosan, az adatok érzékenységével arányosan történjen.

11.5.2 32. cikk - Az adatkezelés biztonsága: megerősíti az osztályozást mint a kockázatalapú adatvédelem és a megfelelő technikai intézkedések egyik eszközét.

11.6 NIS2 irányelv (2022/2555)

11.6.1 21. cikk (2) bekezdés a) pont: előírja az információbiztonsági kockázatkezelésre vonatkozó szabályzatokat, beleértve az eszköz- és adatosztályozási kontrollokat.

11.6.2 21. cikk (3) bekezdés: ösztönzi a megfelelő adatkezelés érvényesítését szolgáló intézkedések alkalmazását, amelyet az osztályozásalapú címkézés támogat.

11.7 DORA-rendelet (2022/2554)

11.7.1 5. cikk - Irányítás és kontroll: előírja azokat az irányítási keretrendszereket, amelyek az adatvagyonelemeket IKT-kockázatkezelési célból osztályozzák.

11.7.2 9. cikk - IKT-kockázatkezelés: technikai és szervezeti intézkedéseket ír elő a kritikus IKT-vagyonelemekre, beleértve az osztályozást és címkézést.

11.8 COBIT 2019

11.8.1 DSS05.02 - Biztonsági szolgáltatások kezelése: előírja az információbiztonsági osztályozások alkalmazását a vállalati adatok védelmének biztosítása érdekében.

11.8.2 MEA03 - A megfelelés nyomon követése, értékelése és felmérése: támogatja az osztályozási gyakorlat rendszeres auditját és felülvizsgálatát a szabályzatok betartásának és az érettség biztosítása érdekében.