					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P13S					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**

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	5.3, 8. pont	
ISO/IEC 27002:2022	5.12, 5. kontroll	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
EU NIS2	21. cikk (2) bekezdés a) pont	
EU DORA	5. cikk (8) bekezdés	
COBIT 2019	BAI03.05, DSS05	
EU GDPR	5., 32. cikk	

1. Cél

1.1 Jelen szabályzat meghatározza, hogy a szervezet által kezelt valamennyi információt hogyan kell osztályozni és jelölni annak érdekében, hogy a bizalmasság, sértetlenség és rendelkezésre állás az információ teljes életciklusa során biztosított legyen.

1.2 A szabályzat az adatok egységes kezelését azáltal biztosítja, hogy az információkhoz azok érzékenysége, üzleti hatása vagy jogi kötelezettségei alapján megfelelő védelmi szinteket rendel.

1.3 Az osztályozás és jelölés hozzájárul az érzékeny adatok véletlen nyilvánosságra hozatalából, jogosulatlan hozzáféréséből vagy nem megfelelő kezeléséből eredő kockázatok csökkentéséhez, különösen olyan kis- és középvállalkozások esetében, amelyek egyszerűbb rendszerekre és kevésbé formalizált kontrollokra támaszkodhatnak.

1.4 Jelen szabályzat kiemelten fontos az ISO/IEC 27001 szerinti tanúsításhoz és a jogszabályi megfeleléshez, különösen az olyan adatvédelmi jogszabályok tekintetében, mint a GDPR, valamint az olyan kiberbiztonsági keretrendszerek esetében, mint a NIS2 és a DORA.

2. Hatály

2.1 Jelen szabályzat a szervezeti adatok teljes körére alkalmazandó, formátumtól és tárolási helytől függetlenül, ideértve különösen az alábbiakat:

2.1.1 elektronikus dokumentumok, táblázatok, e-mailek, űrlapok, képek és beolvasott fájlok;

2.1.2 fizikai dokumentumok, például nyomtatott nyilvántartások, jelentések, számlák és jegyzetek;

2.1.3 felhőszolgáltatásokban, helyszíni szervereken, cserélhető adathordozókon vagy üzleti célra használt saját tulajdonú eszközökön tárolt vagy kezelt adatok;

2.1.4 az üzleti működés során keletkező ideiglenes vagy átmeneti adatok, például naplók, gyorsítótárfájlok és e-mailek.

2.2 Jelen szabályzat betartása kötelező valamennyi munkavállaló, vállalkozó, ideiglenes munkavállaló és a szervezeti adatokhoz hozzáférő külső szolgáltató számára.

2.3 A szabályzat az adatok teljes életciklusára kiterjed, a létrehozástól és tárolástól a hozzáférésen és továbbításon át az archiválásig vagy törlésig.

3. Célkitűzések

3.1 Egyszerű, kikényszeríthető osztályozási rendszer meghatározása, amely a szervezet egészében könnyen érthető és alkalmazható.

3.2 Annak előírása, hogy minden adatvagyont az érzékenységének megfelelően kell osztályozni, és ennek megfelelően kell jelölni a helyes kezelés, tárolás és hozzáférés biztosítása érdekében.

3.3 Annak biztosítása, hogy az adatok jelölési gyakorlata beépüljön az üzleti folyamatokba, például a beléptetésbe, a projektindításba és a rendszerbevezetésbe.

3.4 Az adatvédelmi incidensek kockázatának csökkentése az osztályozási szinthez igazított kezelési kontrollok, például titkosítás és hozzáférés-korlátozás alkalmazásával.

3.5 A magánszféra-védelmi és információbiztonsági jogszabályoknak való megfelelés biztosítása annak igazolásával, hogy az érzékeny adatok, például a személyes, pénzügyi vagy tulajdonosi jellegű adatok, megfelelően jelöltek és kezeltek.

3.6 Az osztályozási döntésekhez kapcsolódó elszámoltathatóság meghatározása, valamint az időszakos felülvizsgálatok és frissítések biztosítása a változó üzleti és jogi követelmények alapján.

4. Szerepkörök és felelősségi körök

4.1 Ügyvezető

4.1.1 Jelen szabályzat tulajdonosa, és jóváhagyja az osztályozási rendszert.

4.1.2 Biztosítja a felügyeletet annak érdekében, hogy az osztályozással kapcsolatos felelősségi körök kijelölése és érvényesítése megtörténjen.

4.1.3 Felülvizsgálja és jóváhagyja az osztályozási vagy jelölési követelmények alóli valamennyi kivételt.

4.1.4 Biztosítja, hogy az adatkezelési gyakorlatok megfeleljenek az olyan jogszabályok követelményeinek, mint a GDPR és a DORA.

4.2 Információtulajdonos / adatkezelési felelős

4.2.1 Minden új adatállományhoz vagy információvagyon-elemhez kezdeti osztályozást rendel a létrehozás vagy beszerzés időpontjában.

4.2.2 Biztosítja, hogy ahol ez alkalmazható, jól látható jelölések kerüljenek alkalmazásra, például fájlfejlécekben, láblécekben, vízjelekben vagy mappanevekben.

4.2.3 Az osztályozást időszakosan felülvizsgálja annak ellenőrzése érdekében, hogy az továbbra is releváns és pontos-e, valamint szükséges-e annak módosítása, például minősítés megszüntetése vagy közzététel után.

4.2.4 Az informatikai vezetővel együttműködve biztosítja az osztályozásnak megfelelő technikai védelmi intézkedések alkalmazását, például a hozzáférési jogosultságok és a titkosítás tekintetében.

[... 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 az ügyvezetőnek és az adatkezelési felelősnek évente felül kell vizsgálnia annak biztosítása érdekében, hogy az tükrözze:

9.1.1 az üzleti működés vagy az adattípusok változásait;

9.1.2 az új szabályozási követelményeket, például az adatvédelem vagy a pénzügyi felügyelet területén;

9.1.3 a jelölési vagy osztályozási képességeket érintő technológiai változásokat.

9.2 A felülvizsgálatnak ki kell terjednie az osztályozási kategóriák, a jelölési eszközök vagy gyakorlatok, valamint a tudatosságnövelő és képzési tartalmak frissítésére.

9.3 A szabályzat módosításait az ügyvezetőnek jóvá kell hagynia, és azokat valamennyi munkatárssal közölni kell. A verziómódosítások nyilvántartását auditcélból meg kell őrizni.

10. Kapcsolódó szabályzatok és összefüggések

10.1 P2S – Irányítási szerepkörök és felelősségek szabályzata: meghatározza a szabályzat tulajdonlásával és érvényesítésével kapcsolatos elszámoltathatóságot.

10.2 P4S – Hozzáférés-szabályozási szabályzat: biztosítja az összhangot a rendszerhozzáférés és az adatosztályozási szintek között.

10.3 P12S – Eszközkezelési szabályzat: nyomon követi az osztályozott adatokat tároló fizikai és digitális vagyonelemeket.

10.4 P17S – Adatvédelmi és magánszféra-védelmi szabályzat: szabályozza a személyes adatok védelmét, amelyek jelentős része Bizalmas besorolású.

10.5 P30S – Incidenskezelési szabályzat: meghatározza az eszkalációs útvonalakat és reagálási eljárásokat osztályozási szabálysértés vagy adatkitettség esetén.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 5.3. pont: előírja az adatkezeléshez és adatvédelemhez kapcsolódó felelősségi körök egyértelmű meghatározását.

11.1.2 8.1. pont: előírja az operatív tervezést és kontrollokat, beleértve az adatkategorizáláshoz kapcsolódó kontrollokat is.

11.2 ISO/IEC 27002

11.2.1 5.12 kontroll: iránymutatást ad az információk kockázat- és szabályozási követelményalapú osztályozásához.

11.2.2 5.13 kontroll: részletezi a gyakorlati jelölési mechanizmusokat és a kapcsolódó kezelési szabályokat.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16: előírja az információk megjelölését annak biztosítására, hogy a védelmi intézkedések összhangban legyenek az osztályozással.

11.3.2 MP-3 / MP-5: iránymutatást ad az adathordozók és kimenetek jelölésére és szabályozására.

11.4 EU GDPR

11.4.1 5. és 32. cikk: megfelelő osztályozási és kezelési védelmi intézkedések alkalmazásával írja elő az adattakarékosságot és a sértetlenséget.

11.5 EU NIS2

11.5.1 21. cikk (2) bekezdés a) pont: kockázatalapú adatvédelemhez szükséges technikai és szervezeti kontrollokat ír elő.

11.6 EU DORA

11.6.1 5. cikk (8) bekezdés: előírja, hogy a szervezetek adatvagyonukat az IKT-kockázatkezelési program részeként osztályozzák.

11.7 COBIT 2019

11.7.1 BAI03.05: előírja az információk osztályozását és a kockázathoz igazított védelmet.

11.7.2 DSS05.02: foglalkozik az osztályozásalapú kontrollok alkalmazásával és nyomon követésével.