					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P14S					Dokumentum címe: **Adatmegőrzési és megsemmisítési 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	6.1.3 és 8. pont	Lefedi a kockázatkezelést, az operatív kontrollokat és a megőrzési követelményeket
ISO/IEC 27002:2022	5. kontroll	Iránymutatást ad a megőrzési időtartamok és a biztonságos megsemmisítési módszerek meghatározásához
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12	Auditnaplók megőrzése, adathordozók biztonságos törlése, adatmegőrzési korlátok és azok érvényesítése
EU NIS2	21. cikk (2) bekezdés a) pont	Előírja a kockázatarányos életciklus-kezelési szabályzatot
EU DORA	5. cikk (1) bekezdés	IKT-kockázatkezelés: adatok rendelkezésre állása és eltávolítása
COBIT 2019	BAI03.04, DSS01	Információ-életciklus kontrollok, biztonságos megsemmisítés
GDPR	5. cikk (1) bekezdés e) pont, 17. cikk	Az adatokat nem lehet a szükségesnél hosszabb ideig megőrizni; törléshez való jog

1. Cél

1.1 Jelen szabályzat célja, hogy meghatározza az információk megőrzésére és biztonságos megsemmisítésére vonatkozó, kikényszeríthető szabályokat KKV-környezetben. Biztosítja, hogy a nyilvántartások kizárólag a jogszabályi, szerződéses vagy üzleti szükségesség által indokolt ideig kerüljenek megőrzésre, majd ezt követően biztonságosan megsemmisítésre kerüljenek.

1.2 Jelen szabályzat célja az információbiztonsági kockázatok csökkentése, a jogi kitettség kezelése, valamint a redundáns vagy elavult adatok tárolásának korlátozása. Támogatja az ISO/IEC 27001 és az olyan adatvédelmi keretrendszerek szerinti megfelelést, mint a GDPR, a személyes vagy érzékeny adatok jogosulatlan megőrzésének minimalizálásával.

1.3 A megfelelően kialakított megőrzési és megsemmisítési keretrendszer csökkenti a működési költségeket, javítja a rendszerek teljesítményét, és növeli az auditkészültséget. Korlátozott IT-kapacitással működő KKV-k esetében gyakorlati megoldást nyújt a digitális eszközök és a fizikai információs vagyon felelős kezelésére.

2. Hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 A szervezet által létrehozott, gyűjtött, feldolgozott vagy tárolt valamennyi nyilvántartásra, állományra, naplóra, kommunikációra és adathalmazra

2.1.2 Valamennyi munkavállalóra, vállalkozóra és a szervezeti adatokat kezelő külső szolgáltatóra

2.1.3 Minden adatformátumra (pl. papír, elektronikus, kép-, hang- vagy naplóadat), valamint minden adathordozóra és tárolási megoldásra (pl. helyi meghajtók, felhőszolgáltatások, e-mail-szerverek, biztonsági mentések)

2.2 A hatály különösen az alábbiakra terjed ki:

2.2.1 Üzleti dokumentumokra (pl. számlák, szerződések, projektjelentések)

2.2.2 Működési nyilvántartásokra (pl. naplók, hozzáférési előzmények, biztonsági mentési pillanatképek)

2.2.3 Személyes adatokra (pl. HR-nyilvántartások, ügyfélkommunikáció, támogatási nyilvántartások)

2.2.4 Belső, külső vagy hibrid rendszerekben tárolt adatokra

2.2.5 Archivált és biztonsági mentett adatokra, függetlenül attól, hogy aktív vagy inaktív állapotúak

2.3 Az adatok életciklusának valamennyi szakasza a hatály alá tartozik, a létrehozástól az engedélyezett megsemmisítésig.

3. Célkitűzések

3.1 Egységes megőrzési szabályok meghatározása jogi, működési és szabályozási szempontok alapján.

3.2 A kritikus nyilvántartások idő előtti törlésének megelőzése és a szükségtelen adatfelhalmozás megszüntetése.

3.3 Az adatok biztonságos, visszafordíthatatlan megsemmisítésének biztosítása, amikor a megőrzés már nem indokolt.

3.4 A megőrzési és törlési döntések végrehajtásához kapcsolódó tulajdonosi felelősség kijelölése KKV-szintű erőforráskorlátok mellett.

3.5 Olyan auditképes dokumentáció biztosítása, amely igazolja a kellő gondosságot az ISO 27001, a GDPR, a NIS2 és más keretrendszerek szerinti megfelelés érdekében.

3.6 Az adatok biztonságos életciklus-kezelésének elősegítése anélkül, hogy szükségtelen műszaki terhet róna a nem szakértő munkatársakra.

4. Szerepkörök és felelősségi körök

4.1 Ügyvezető

4.1.1 Jóváhagyja jelen szabályzatot, és felelős annak érvényesítéséért.

4.1.2 Biztosítja, hogy a megőrzési és megsemmisítési eljárások a jogi és üzleti kockázatokkal összhangban kerüljenek végrehajtásra.

4.1.3 Szükség esetén jóváhagyja a kivételeket és a jogi zárolást.

4.1.4 Kezdeményezi a szabályzat felülvizsgálatát, és jóváhagyja a módosításokat üzleti vagy szabályozási változások alapján.

4.2 Kijelölt adatgazda

4.2.1 Adatkategóriánként kerül kijelölésre (pl. pénzügyi, HR- vagy ügyfélnyilvántartások).

4.2.2 Osztályozza a nyilvántartásokat, és a szabályzat, valamint a jogi iránymutatás alapján meghatározza a megfelelő megőrzési időtartamot.

4.2.3 Engedélyezi a törlést, ha a megőrzési követelmények teljesültek.

4.2.4 A megőrzési logika és a megsemmisítési események bemutatásával támogatja a belső auditokat.

[... 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 évente legalább egyszer, valamint az alábbi esetekben felül kell vizsgálni:

9.1.1 Az alkalmazandó jogszabályok változása esetén (pl. adatvédelem, pénzügyi beszámolás)

9.1.2 Olyan új rendszerek vagy folyamatok bevezetése esetén, amelyek hatással vannak az adatok életciklusára

9.1.3 Olyan auditmegállapítások vagy incidensek esetén, amelyek hiányosságokat tárnak fel a megőrzési gyakorlatban

9.2 A felülvizsgálatoknak biztosítaniuk kell, hogy a Megőrzési nyilvántartás teljes legyen, és tartalmazza valamennyi fő nyilvántartási kategóriát.

9.3 A szabályzat módosításait az ügyvezetőnek kell jóváhagynia, és azokat közölni kell az érintett munkatársakkal. A legfrissebb verziónak hozzáférhetőnek és verziókövetettnek kell lennie.

10. Kapcsolódó szabályzatok és összefüggések

10.1 P2S – Irányítási szerepkörök és felelősségek szabályzata: Meghatározza a szabályzat tulajdonosi felelősségét és a kivételek jóváhagyási jogosultságát.

10.2 P13S – Adatosztályozási és címkézési szabályzat: Meghatározza, hogy a megőrzési szabályok hogyan illeszkednek az adatosztályozáshoz.

10.3 P12S – Eszközkezelési szabályzat: Szabályozza a megőrzési és megsemmisítési kötelezettség alá tartozó adatokat tartalmazó adathordozókat.

10.4 P17S – Adatvédelmi és magánszféra-védelmi szabályzat: Biztosítja az adattakarékosságot, és támogatja a GDPR szerinti jogszerű információkezelést.

10.5 P30S – Incidenskezelési szabályzat: Akkor alkalmazandó, ha a megsemmisítési vagy megőrzési hibák potenciális adatkitettséget eredményeznek.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 6.1.3. pont: Előírja az információval kapcsolatos kockázatok kezelését, ideértve a megőrzéssel kapcsolatos kockázatokat is.

11.1.2 8.1. pont: Meghatározza az életciklushoz kapcsolódó operatív kontrollokat.

11.2 ISO/IEC 27002

11.2.1 5.33. kontroll: Iránymutatást ad a megőrzési időtartamok és a biztonságos megsemmisítési módszerek meghatározásához.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: Előírja az auditnaplók megőrzését.

11.3.2 MP-6: Meghatározza az adathordozók biztonságos törlésére vonatkozó eljárásokat.

11.3.3 SI-12: Az adatmegőrzési korlátokat és azok alkalmazását tárgyalja.

11.4 GDPR

11.4.1 5. cikk (1) bekezdés e) pont: Az adatokat nem lehet a szükségesnél hosszabb ideig megőrizni.

11.4.2 17. cikk: A törléshez való jog alkalmazandó, ha az adat megőrzése már nem jogszerű.

11.5 EU NIS2

11.5.1 21. cikk (2) bekezdés a) pont: Előírja a kockázatarányos szervezeti szabályzatokat, beleértve az életciklus-kezelést is.

11.6 EU DORA

11.6.1 5. cikk (1) bekezdés: Az IKT-kockázatkezelés magában foglalja az adatok rendelkezésre állását és eltávolítását.

11.7 COBIT 2019

11.7.1 BAI03.04: Információ-életciklus kontrollokat ír elő.

11.7.2 DSS01.06: Biztonságos megsemmisítési eljárások az információs vagyon védelmének részeként.