					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P12S					Dokumentum címe: **Eszközkezelési 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	8. pont	Eszközkezelési követelmények
ISO/IEC 27002:2022	5. kontrollterület	Eszközkezelési kontrollok
NIST SP 800-53 Rev.5	CM-8	Rendszerösszetevők nyilvántartása
EU NIS2	21. cikk (2) bekezdés a) pont	Az eszközök nyomon követése a hálózati és információs rendszerek védelme érdekében
EU DORA	5. cikk (8) bekezdés	IKT-eszköznyilvántartási követelmények
COBIT 2019	BAI	Az IT-eszközök életciklus-kezelése
EU GDPR	30. cikk	Az adatkezelési tevékenységek nyilvántartása

1. Cél

1.1 Jelen szabályzat meghatározza, hogy a szervezet miként azonosítja, tartja nyilván, védi és vonja ki az információs vagyon elemeit, beleértve a fizikai és digitális összetevőket is.

1.2 A cél az operatív és biztonsági kockázatok csökkentése azáltal, hogy a teljes életciklus során biztosított az összes üzleti eszköz átlátható, elszámoltatható és biztonságos kezelése.

1.3 A megbízható eszköznyilvántartás támogatja a jogszabályi megfelelést, az incidenskezelést, az üzletmenet-folytonossági tervezést és a kockázatkezelést.

1.4 Jelen szabályzat továbbá támogatja az ISO/IEC 27001 szerinti tanúsítást, és igazolja a GDPR, a NIS2 és a DORA szerinti jogi, pénzügyi és kiberbiztonsági kötelezettségekkel való összhangot.

1.5 A kis- és középvállalkozások (KKV-k) esetében az egyszerű, de rendszerszintű eszközkezelési megközelítés elengedhetetlen a nem kezelt eszközökből, az adatvesztésből vagy az auditmegállapításokból eredő kockázatok elkerüléséhez, különösen korlátozott technikai erőforrások mellett.

2. Hatály

2.1 Jelen szabályzat a szervezet tulajdonában álló, bérelt vagy egyéb módon kezelt valamennyi eszközre kiterjed, ideértve az alábbi környezetekben használt eszközöket is:

2.1.1 irodai munkavégzés

2.1.2 távoli vagy hibrid munkavégzés

2.1.3 terepi vagy mobil működés

2.1.4 felhőalapú és kiszervezett környezetek

2.2 A szabályzat hatálya alá tartozó eszköztípusok többek között az alábbiak:

2.2.1 Hardver: laptopok, asztali számítógépek, monitorok, telefonok, táblagépek, USB-meghajtók, routerek, nyomtatók, biztonsági mentési adathordozók

2.2.2 Szoftverek: telepített alkalmazások, SaaS-megoldások, operációs rendszerek, vírusvédelmi megoldások, licencek

2.2.3 Adatvagyon: üzleti adattárak, táblázatok, ügyfélnyilvántartások, forráskód

2.2.4 Digitális hitelesítő adatok és szolgáltatások: domainnevek, digitális tanúsítványok, API-kulcsok, e-mail-fiókok, felhőszolgáltatásokhoz tartozó bejelentkezési adatok

2.2.5 Hozzáférési eszközök: kulcsok, intelligens kártyák, beléptető tokenek, biometrikus azonosító eszközök

2.3 Jelen szabályzat hatálya kiterjed minden olyan munkavállalóra, szerződéses közreműködőre és harmadik fél szolgáltatóra, aki szervezeti eszközöket kezel.

2.4 A szabályzat a rövid távon használt eszközökre is kiterjed (például projektspecifikus laptopok), valamint a hosszú távon használt és a több munkatárs által közösen használt megosztott eszközökre is.

3. Célkitűzések

3.1 Valamennyi releváns eszköz teljes körű és pontos eszköznyilvántartásának kialakítása, folyamatos karbantartása és naprakészen tartása.

3.2 Annak biztosítása, hogy minden eszközhöz kijelölt tulajdonos tartozzon, aki felel annak használatáért, tárolásáért és visszaszolgáltatásáért.

3.3 Az eszközök osztályozása érzékenység, üzleti hatás vagy szabályozási relevancia alapján annak érdekében, hogy a megfelelő védelmi szintek alkalmazhatók legyenek.

3.4 Egyértelmű eljárások meghatározása az eszközök kiadására, átrendelésére, karbantartására, elvesztésének bejelentésére és kivonására.

3.5 Annak biztosítása, hogy az eszközök teljes életciklusuk során biztonságos kezelés alatt álljanak, és a rajtuk tárolt információk selejtezéskor megfelelően védettek legyenek vagy biztonságosan törlésre kerüljenek.

3.6 A nem nyilvántartott, vissza nem szolgáltatott vagy nem megfelelően használt szervezeti erőforrásokból eredő biztonsági incidensek valószínűségének csökkentése.

3.7 A vonatkozó jogszabályoknak való megfelelés támogatása, ideértve például a GDPR elszámoltathatósági elvét, valamint a kiberbiztonsági tanúsítási követelmények teljesítését.

4. Szerepkörök és felelősségi körök

4.1 Ügyvezető

4.1.1 Jelen szabályzat tulajdonosa, és felelős azért, hogy az eszközkezelési gyakorlatok a szervezet egészében bevezetésre és betartásra kerüljenek.

4.1.2 Felülvizsgálja és jóváhagyja az eszköznyilvántartás módosításait, valamint szükség esetén engedélyezi az eszközök kivonását vagy átruházását.

4.1.3 Minden jelentős eszközvesztésről, lopásról vagy visszaélésről értesíteni kell.

4.2 Informatikai vezető vagy kijelölt eszközfelelős

4.2.1 Fenntartja az eszköznyilvántartást (például táblázatban, jegykezelő rendszerben vagy egyszerű eszköznyilvántartó rendszerben).

4.2.2 Kijelöli az eszköztulajdonosi felelősséget, és nyomon követi az állapotváltozásokat (például új, használatban, javítás alatt, kivont).

4.2.3 Ellenőrzi, hogy minden kiadott eszköz dokumentált legyen, és egy konkrét személyhez vagy szervezeti egységhez legyen rendelve.

4.2.4 Biztosítja az osztályozási jelölések alkalmazását és betartását (például Belső használatú, Bizalmas).

4.2.5 Koordinálja az eszközök visszagyűjtését, adattörlését és deaktiválását kiléptetés vagy kivonás során.

4.2.6 Jelenti az ügyvezető részére a rendezetlen eszközeltéréseket.

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

9.1.1 új technológiák vagy eszköztípusok bevezetésekor

9.1.2 az eszköznyomonkövetési eljárások változásakor (például új eszközök vagy platformok bevezetése esetén)

9.1.3 amikor új szabályozási kötelezettségek érintik az eszközök visszakövethetőségét vagy selejtezését

9.1.4 amikor egy incidens vagy audit hiányosságot tár fel a jelenlegi eszközkezelési gyakorlatban

9.2 A felülvizsgálatokban részt kell vennie az ügyvezetőnek és az informatikai vezetőnek, és azoknak ki kell terjedniük az eszközkezelési eljárások, a nyilvántartási sablonok és az osztályozási útmutató frissítésére.

9.3 Minden módosítást dokumentálni kell, és közölni kell az érintett munkatársakkal. Verziókezelt változásnaplót kell megőrizni.

10. Kapcsolódó szabályzatok és összefüggések

10.1 P2S – Irányítási szerepkörök és felelősségek szabályzata: Meghatározza a szabályzattulajdonosi elszámoltathatóságot és az IT-üzemeltetéssel kapcsolatos felelősségi köröket.

10.2 P4S – Hozzáférés-szabályozási szabályzat: Összekapcsolja az eszközhasználatot (például laptopok, mobileszközök) a hozzáférési jogosultságokkal és az identitáskezeléssel.

10.3 P7S – Beléptetési és kiléptetési szabályzat: Biztosítja, hogy az eszközkiadás és az eszközvisszavétel beépüljön a személyzeti életciklus-folyamatokba.

10.4 P13S – Adatosztályozási és jelölési szabályzat: Szabályokat ad annak meghatározására, hogy egy eszközt Belső használatú vagy Bizalmas kategóriába kell-e sorolni.

10.5 P30S – Incidenskezelési szabályzat: Iránymutatást ad a reagálási eljárásokra abban az esetben, ha egy eszközzel kapcsolatos esemény biztonsági vagy adatvédelmi incidenshez vezet.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 8.1 pont: Előírja az eszközök kezelésére és a használatuk teljes időtartama alatti védelmére szolgáló operatív kontrollokat.

11.2 ISO/IEC 27002

11.2.1 5.9 kontroll: Részletezi, hogyan kell az eszközöket azonosítani, tulajdonost rendelni hozzájuk, osztályozni és biztonságosan kezelni.

11.3 NIST SP 800-53 Rev.5

11.3.1 CM-8: Előírja, hogy a szervezetek alakítsanak ki és tartsanak fenn nyilvántartást a rendszerösszetevőkről, beleértve a hardver-, szoftver- és virtuális eszközöket is.

11.4 EU GDPR

11.4.1 30. cikk: Előírja az adatkezelési tevékenységek dokumentálását, amelynek előfeltétele annak ismerete, hogy az adatok hol és milyen eszközökön kerülnek tárolásra.

11.5 EU NIS2

11.5.1 21. cikk (2) bekezdés a) pont: Technikai és szervezeti intézkedések alkalmazását írja elő, beleértve az eszközök nyomon követését is, a hálózati és információs rendszerek védelme érdekében.

11.6 EU DORA

11.6.1 5. cikk (8) bekezdés: Előírja, hogy a pénzügyi szervezetek az IKT-kockázatkezelés részeként részletes IKT-eszköznyilvántartást tartsanak fenn.

11.7 COBIT 2019

11.7.1 BAI09: Meghatározza, hogy az IT-eszközöket a teljes életciklusuk során kezelni kell — a beszerzéstől a kivonásig — egyértelmű tulajdonosi felelősség és kontrollok mellett.