					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P12					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**

1. Cél

1.1 Jelen szabályzat meghatározza az információs vagyonelemek azonosítására, osztályozására, kezelésére és védelmére vonatkozó kötelező szervezeti követelményeket a teljes életciklusuk során. Támogatja a hardver-, szoftver-, adat-, felhőalapú és immateriális információs vagyonelemek szervezetszintű irányítását, ideértve a mobil, távoli és harmadik fél által kezelt környezeteket is.

1.2 A szabályzat célja, hogy teljes körű átláthatóságot biztosítson a szervezet információsvagyon-környezetéről, lehetővé téve a hatékony biztonsági kontrollok működtetését, a tulajdonosi felelősségi körök kijelölését, a megfelelés biztosítását, valamint a szabályozott kivonást vagy selejtezést.

1.3 A szabályzat összhangban áll az ISO/IEC 27001:2022 A mellékletének 5.9. pontjával azáltal, hogy előírja az információk és a kapcsolódó vagyonelemek központi nyilvántartásának fenntartását. Biztosítja az elszámoltathatóságot azzal, hogy minden vagyonelemhez tulajdonost rendel, és üzleti érzékenység, valamint jogszabályi követelmények alapján osztályozáson alapuló védelmet ír elő.

2. Hatály

2.1 Jelen szabályzat valamennyi munkavállalóra, szerződéses közreműködőre, harmadik fél beszállítóra és szolgáltatóra vonatkozik, akik a szervezet tulajdonában álló vagy általa ellenőrzött információs vagyonelemeket kezelik, használják, elérik, tárolják vagy feldolgozzák.

2.2 A hatály valamennyi vagyonelem-kategóriára kiterjed, beleértve az alábbiakat:

2.2.1 Fizikai eszközök: laptopok, asztali számítógépek, mobileszközök, cserélhető adathordozók, nyomtatók, hálózati berendezések

2.2.2 Digitális vagyonelemek: szoftverek, alkalmazások, rendszerképek, adatbázisok, biztonsági mentések, titkosítási kulcsok

2.2.3 Információs vagyon: strukturált és strukturálatlan adatok, jelentések, e-mailek, szellemi tulajdon

2.2.4 Felhő- és virtuális vagyonelemek: IaaS-, SaaS- és PaaS-környezetek, virtuális gépek, konténerek

2.2.5 Logikai vagyonelemek: domainnevek, licencek, felhasználói fiókok, előírt alapkonfigurációk

2.3 A szabályzat kiterjed továbbá a távmunkában, hibrid vagy kiszervezett környezetben használt vagyonelemekre is, biztosítva azok védelmét és nyomon követhetőségét akkor is, ha fizikailag nem a szervezet telephelyén találhatók.

3. Célkitűzések

3.1 A szervezet valamennyi információs vagyonelemére vonatkozó teljes körű, pontos és naprakész eszköznyilvántartás fenntartása, meghatározott tulajdonosi, osztályozási és elhelyezkedési attribútumokkal.

3.2 Olyan eszközgazdák kijelölése, akik felelősek az irányításuk alá tartozó vagyonelemek osztályozásáért, kezeléséért és védelméért, az adatirányítási és információbiztonsági szabályzatokkal összhangban.

3.3 Megfelelő osztályozás és címkézés alkalmazása minden vagyonelemre érzékenység, kritikus jelleg és jogszabályi szempontok alapján.

3.4 A vagyonelemek védelme az osztályozásuknak és a kapcsolódó kockázati kitettségnek megfelelően, beleértve a tárolást, hozzáférést, továbbítást és selejtezést.

3.5 Az eszközök visszaszolgáltatására és biztonságos megsemmisítésére vonatkozó eljárások érvényesítése munkavállalói kiléptetés, szerződés megszűnése vagy a vagyonelem életciklusának lezárása esetén.

3.6 Az ISO/IEC 27001, a GDPR, a NIS2, a DORA és a COBIT 2019 követelményeinek való megfelelés támogatása strukturált eszközkezeléssel és auditálhatósággal.

4. Szerepkörök és felelősségi körök

4.1 Felső vezetés

4.1.1 Jóváhagyja az Eszközkezelési szabályzatot, és biztosítja a teljes körű végrehajtásához szükséges erőforrásokat.

4.1.2 Végső elszámoltathatósággal tartozik azért, hogy a szervezeti vagyonelemek védelme és kezelése a jogszabályi és szerződéses kötelezettségekkel összhangban történjen.

4.2 Információbiztonsági vezető

4.2.1 Az Eszközkezelési szabályzat szakmai felelőse, és biztosítja annak integrációját a szervezet átfogó információbiztonsági irányítási rendszerébe (IBIR).

4.2.2 Felülvizsgálja a jelen szabályzat alóli kivételeket és eltéréseket, és érvényesíti a kockázatalapú kockázatcsökkentő intézkedéseket.

4.2.3 Felügyeli az eszközosztályozásra, az eszköznyilvántartás sértetlenségére és az eszközök életciklusára vonatkozó megfelelés időszakos auditjait.

[... 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, vagy az alábbi esetekben kell felülvizsgálni:

9.1.1 Az eszközosztályozást vagy a nyilvántartási követelményeket érintő jogi vagy szabályozási kötelezettségek változása

9.1.2 Új eszközkategóriák vagy kezelési platformok bevezetése (pl. felhőnatív CMDB-k)

9.1.3 Belső auditmegállapítások vagy az eszközök nem megfelelő kezelésével kapcsolatos biztonsági incidensek

9.1.4 Olyan szervezeti átalakítás, amely érinti a tulajdonosi felelősséget vagy az életciklus-kontrollokat

9.2 A felülvizsgálati folyamatot az IT-eszközkezelési vezető indítja el, és azt az információbiztonsági vezetővel, a beszerzéssel, a jogi és megfelelőségi területtel, valamint az érintett szervezeti egységek vezetőivel összehangoltan kell végrehajtani.

9.3 Soron kívüli felülvizsgálatok az alábbi esetekben is kezdeményezhetők:

9.3.1 Üzleti egységek felvásárlása vagy értékesítése

9.3.2 Harmadik fél által kezelt eszközöket érintő beszállítói változások

9.3.3 Tömeges kivonással vagy jogosultságkiosztással járó technológiai megújítások

9.4 A jelen szabályzat valamennyi módosítása esetén:

9.4.1 Verziókezelést kell alkalmazni, és a dokumentumot az IBIR adattárában kell tárolni

9.4.2 A módosítást a felső vezetésnek jóvá kell hagynia

9.4.3 Tartalmaznia kell a változások összefoglalását és indoklását

9.4.4 A módosításokat közölni kell valamennyi érintett féllel, beleértve adott esetben a frissített eljárásokat vagy a rendszerhasználati képzést is

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat az alábbi kapcsolódó szabályzatokkal együtt alkalmazandó, és támogatja azok betartását:

10.1.1 P4 - Hozzáférés-szabályozási szabályzat: Biztosítja, hogy az eszközök átláthatósága összhangban legyen a hozzáférési jogosultságokkal és a rendszereken, valamint adatkörnyezetekben alkalmazott kontrollmechanizmusokkal.

10.1.2 P7 - Beléptetési és kiléptetési szabályzat: Szabályozza a fizikai és logikai eszközök időben történő jogosultságkiosztását és visszaszolgáltatását a munkatársi állomány változásai során.

10.1.3 P13 - Adatosztályozási és címkézési szabályzat: Meghatározza az eszközökre vonatkozó kötelező osztályozási szabályokat, amelyek a címkézési, kezelési és selejtezési eljárásokat irányítják.

10.1.4 P14 - Adatmegőrzési és adatselejtezési szabályzat: Meghatározza a digitális és fizikai, információt tartalmazó eszközök biztonságos selejtezésének határidejét és módszereit.

10.1.5 P22 - Naplózási és felügyeleti szabályzat: Lehetővé teszi az eszközhozzáférés és eszközhasználat visszakövethetőségét rendszernaplózás, végponti átláthatóság és viselkedéselemzés útján.

10.1.6 P30 - Incidenskezelési szabályzat: Támogatja az eszközökhöz kapcsolódó incidensek, például elveszett laptopok vagy nem nyomon követett tárolóadathordozók gyors elszigetelését és kivizsgálását.

10.2 Ezek a szabályzatok egységes irányítási struktúrát alkotnak annak biztosítására, hogy a vagyonelemek a teljes életciklusuk során biztonságosan legyenek kezelve, pontosan legyenek nyilvántartva, és megfelelő eljárások szerint legyenek használva.

11. Hivatkozott szabványok és keretrendszerek

11.1 Jelen szabályzat összhangban áll azokkal a nemzetközileg elismert információbiztonsági szabványokkal és szabályozási keretrendszerekkel, amelyek a teljes életciklus során erős eszközkezelést írnak elő.

11.2 ISO/IEC 27001:

11.2.1 8.1. pont - Előírja, hogy a szervezetek tervezzék meg, valósítsák meg és szabályozzák az információbiztonsági követelmények teljesítéséhez szükséges folyamatokat, beleértve az eszközök életciklus-kezelésére vonatkozó folyamatokat is.

11.3 ISO/IEC 27002:2022 - 5.9–5.11. pont szerinti kontrollok

11.3.1 5.9. pont - Az információk és egyéb kapcsolódó vagyonelemek nyilvántartása: Előírja minden, információfeldolgozás szempontjából releváns eszköz naprakész és teljes nyilvántartását.

11.3.2 5.10. pont - Az információk és eszközök elfogadható használata: A használati szabályok, a tulajdonosi felelősség és a visszaszolgáltatási folyamatok támogatják.

11.3.3 5.11. pont - Eszközök visszaszolgáltatása: Formális átadási és kivonási eljárásokon keresztül valósul meg.

11.3.4 Ezek a kontrollok strukturált követelményeket határoznak meg a szervezeti vagyonelemek azonosítására, címkézésére, fenntartására és nyomon követésére, a tulajdonosok és kezelők életcikluson átívelő felelősségeivel együtt.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 CM-8 - Rendszerkomponens-nyilvántartás: Megjelenik a központi eszközkezelésben, a valós idejű átláthatóságban és az operatív konfigurációkkal való összekapcsolásban.

11.4.2 RA-3 - Kockázatértékelés: Az eszköznyilvántartások alapvető kiindulási elemet képeznek a fenyegetésmodellezéshez és a kockázatértékeléshez.

11.4.3 MP-6 - Adathordozók biztonságos törlése: Az eszközök életciklus-kontrolljaiban és az Adatselejtezési szabályzatban meghatározott biztonságos selejtezési módszerekkel kerül érvényesítésre.

11.5 GDPR (2016/679):

11.5.1 30. cikk - Adatkezelési tevékenységek nyilvántartása: Előírja azoknak a rendszereknek, eszközöknek és adattáraknak a dokumentálását, amelyek személyes adatokat tárolnak vagy kezelnek.

11.5.2 32. cikk - Az adatkezelés biztonsága: Összhangban áll az eszközalapú kockázatértékeléssel és az osztályozott eszközökhöz, valamint a kritikus infrastruktúrához igazított védelmi intézkedésekkel.

11.6 NIS2 irányelv (2022/2555):

11.6.1 21. cikk (2) bekezdés a), b): Előírja az eszközök átláthatóságát és nyilvántartását mint a kockázatelemzés, a védelem és a kiberbiztonsági incidenskezelés alapját.

11.6.2 21. cikk (3): Megerősíti a strukturált eszközirányítás szükségességét a szervezeti biztonsági kultúra részeként.

11.7 DORA-rendelet (2022/2554):

11.7.1 5. cikk - IKT-irányítás és belső kontroll: Előírja, hogy a pénzügyi szervezetek egyértelmű nyilvántartási, tulajdonosi és védelmi követelmények mentén tartsák ellenőrzés alatt IKT-eszközeiket.

11.7.2 9. cikk - IKT-kockázatkezelési keretrendszer: Meghatározza, hogy az eszközkezelési folyamatoknak támogatniuk kell a fenyegetések csökkentését, az üzletmenet-folytonossági tervezést és a szolgáltatások rezilienciáját.

11.8 COBIT 2019:

11.8.1 BAI09 - Eszközök kezelése: Közvetlenül illeszkedik a szervezeti eszközök strukturált azonosításához, osztályozásához, használatához és selejtezéséhez.

11.8.2 DSS01 - Kezelt üzemeltetés: Támogatja azon kontrollok bevezetését, amelyek biztosítják az eszközök védelmét és a folyamatos operatív irányítást.

11.8.3 MEA03 - A megfelelés monitorozása, értékelése és felmérése: Biztosítja az eszközkezelési kontrollok és azok szabályozási megfelelésben betöltött hatékonyságának rendszeres auditját.