					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P35S					Dokumentum címe: **IoT / OT biztonsági 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., 6.2., 8. pont	
ISO/IEC 27002:2022	5.23., 5.31. kontroll	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
GDPR	32. cikk	
NIS2 irányelv	21. cikk (2) bekezdés a), d), f) pont	
DORA-rendelet	9. cikk (2) bekezdés, 10. cikk (1) bekezdés	

1. Cél

1.1. Jelen szabályzat meghatározza az Internet of Things (IoT) és az operatív technológiai (OT) eszközök szervezeten belüli biztonságos használatára és kezelésére vonatkozó kötelező szabályokat. Ezen eszközök közé tartozhatnak többek között intelligens érzékelők, biztonsági kamerák, gyártóberendezések, HVAC-vezérlők, valamint bármely hálózatra csatlakozó ipari rendszer.

1.2. Jelen szabályzat célja:

1.2.1. a fizikai és digitális működés védelme a nem megfelelően védett, hálózatra csatlakozó eszközökön keresztül megvalósuló zavarás vagy manipuláció ellen;

1.2.2. az IoT- és OT-rendszerek biztonságos telepítésének, felügyeletének és karbantartásának kikényszerítése;

1.2.3. az ISO/IEC 27001:2022, a NIS2 irányelv és a kapcsolódó szabályozási keretrendszerek követelményeinek való megfelelés biztosítása;

1.2.4. gyakorlati, kikényszeríthető kontrollok meghatározása irodai, raktári vagy termelési környezetben működő KKV-k számára.

2. Hatály

2.1. Jelen szabályzat minden olyan személyre alkalmazandó, aki IoT- vagy OT-eszközök tervezésében, telepítésében, konfigurálásában, használatában, támogatásában vagy selejtezésében részt vesz. Ide tartoznak:

2.1.1. a munkavállalók, vállalkozók vagy gyakornokok, akik fizikai vagy távoli hozzáféréssel rendelkeznek az eszközökhöz;

2.1.2. a csatlakoztatott rendszereket telepítő vagy karbantartó harmadik fél beszállítók vagy szerviztechnikusok;

2.1.3. az ügyvezető vagy a biztonsági szabályzatok felügyeletéért felelős munkatársak.

2.2. A szabályzat hatálya kiterjed:

2.2.1. az olyan IoT-eszközökre, mint az intelligens zárak, megfigyelőrendszerek, intelligens mérőórák vagy nyomtatók;

2.2.2. az olyan OT-rendszerekre, mint a programozható logikai vezérlők (PLC-k), SCADA-panelek vagy ipari átjárók;

2.2.3. az e rendszerek által használt támogató hardverekre, felügyeleti alkalmazásokra és kommunikációs hálózatokra.

2.3. Jelen szabályzat valamennyi munkavégzési helyszínre alkalmazandó: irodai környezetekre, távoli telephelyekre, termelési területekre és az ezekhez az eszközökhöz kapcsolódó felhőplatformokra.

3. Célkitűzések

3.1. Biztonságos telepítés: biztosítani kell, hogy minden IoT-/OT-rendszer biztonságos konfigurációval kerüljön a működési környezetbe.

3.2. Kitettség korlátozása: meg kell előzni a csatlakoztatott eszközökhöz való jogosulatlan hozzáférést, a visszaélésszerű használatot vagy az eszközök feletti jogosulatlan átvételt erős hozzáférés-szabályozás és hálózati szegmentáció alkalmazásával.

3.3. Folyamatos felügyelet: az IoT-/OT-környezet átláthatóságát a tevékenységek naplózásával és a szokatlan viselkedés figyelésével fenn kell tartani.

3.4. Beszállítói elszámoltathatóság: biztosítani kell, hogy a harmadik fél szolgáltatók biztonságos telepítési, konfigurálási és karbantartási gyakorlatokat kövessenek.

3.5. Jogszabályi megfelelés: igazolni kell az alkalmazandó szabványokkal és előírásokkal való teljes összhangot, különösen az ISO/IEC 27001, a GDPR (amennyiben személyes adatok gyűjtése történik) és a kritikus infrastruktúrák rezilienciájára vonatkozó NIS2-követelmények tekintetében.

4. Szerepkörök és felelősségek

4.1. Ügyvezető igazgató (GM)

4.1.1. általános felelősséget visel az IoT- és OT-rendszerek biztonságáért;

4.1.2. jóváhagyja jelen szabályzatot, és biztosítja annak betartatását valamennyi munkaterületen;

4.1.3. ellenőrzi, hogy a beszállítók és vállalkozók biztonságos telepítési és karbantartási gyakorlatokat alkalmaznak-e;

4.1.4. jóváhagyja bármely IoT-/OT-rendszer hálózati hozzáférését.

4.2. Kijelölt munkavállaló vagy üzemeltetési vezető (amennyiben kijelölésre került)

4.2.1. felügyeli az IoT-/OT-eszközök nyilvántartását, elhelyezését és konfigurációját;

4.2.2. rögzíti az egyes eszközök helyét, hálózati hozzárendelését és a kapcsolódó támogatási dokumentációt;

4.2.3. biztosítja, hogy minden változás (pl. firmware-frissítés vagy eszközcsere) dokumentálásra kerüljön.

[... A 4.3–8. szakaszok nem szerepelnek ebben az előnézetben. A teljes tartalom eléréséhez vásárolja meg a teljes dokumentumot. ...]

9.1. Éves felülvizsgálat

9.1.1. Jelen szabályzatot az ügyvezetőnek legalább évente egyszer felül kell vizsgálnia.

9.1.2. A felülvizsgálatnak értékelnie kell, hogy a szabályzat továbbra is eredményes-e, lefedi-e az aktuális eszköztípusokat, valamint összhangban van-e az új kockázatokkal és technológiákkal.

9.2. Eseményalapú frissítések

9.2.1. A szabályzat frissítését akkor is kezdeményezni kell, ha:

9.2.2. új típusú IoT- vagy OT-rendszerek kerülnek bevezetésre;

9.2.3. a beszállítók biztonsági tájékoztatókat vagy életciklus-végi értesítéseket adnak ki;

9.2.4. incidens vagy audit hiányosságokat tár fel az IoT-/OT-kontrollokban;

9.2.5. új jogszabályok vagy szabványok további követelményeket írnak elő.

9.3. Dokumentálás és verziókezelés

9.3.1. Minden frissítést dokumentálni kell, beleértve a dátumot, a verziószámot és a változások összefoglalását.

9.3.2. Az ügyvezető köteles a szabályzat korábbi verzióit auditcélból megőrizni.

9.4. A változások kommunikálása

9.4.1. A szabályzat minden frissítését meg kell osztani valamennyi érintett munkatárssal és beszállítóval.

9.4.2. A frissített verziókat elérhetővé kell tenni megosztott mappákban vagy nyomtatott formában a telepítési helyszíneken vagy vezérlőközpontokban.

10. Kapcsolódó szabályzatok és összefüggések

10.1. Jelen szabályzatot az alábbi kapcsolódó KKV-szabályzatokkal összhangban kell végrehajtani:

10.1.1. P4S – Hozzáférés-szabályozási szabályzat: érvényesíti az eszközszintű bejelentkezési kontrollokat, az erős jelszóhasználatot és az IoT- és OT-platformokra vonatkozó engedélyezett hozzáférési eljárásokat;

10.1.2. P9S – Távmunka-szabályzat: megakadályozza az IoT-/OT-irányítópultokhoz való távoli hozzáférést nem biztonságos vagy nem jóváhagyott csatornákon keresztül;

10.1.3. P17S – Adatvédelmi és magánszféra-védelmi szabályzat: alkalmazandó, ha az IoT-eszközök (pl. biztonsági kamerák) személyes adatokat kezelnek vagy rögzítenek, biztosítva a GDPR-nak való megfelelést;

10.1.4. P30S – Incidenskezelési szabályzat: meghatározza az IoT- vagy OT-incidensek észlelésére, bejelentésére és kezelésére szolgáló eljárásokat, beleértve a feltételezett manipulációt vagy működési hibát;

10.1.5. P36S – Közösségimédia- és külsőkommunikációs szabályzat: biztosítja, hogy eszközadatok vagy hálózati topológiai információk ne kerüljenek külső fél részére átadásra jóváhagyás nélkül.

10.2. Minden kapcsolódó szabályzat célzott eljárásrendi útmutatással támogatja jelen szabályzat betartatását és gyakorlati alkalmazását.

11. Hivatkozott szabványok és keretrendszerek

11.1. ISO/IEC 27001

11.1.1. 6.1. pont – Kockázatok azonosítása és kezelése: előírja az IoT- és OT-rendszerekhez kapcsolódó kockázatok szisztematikus értékelését és csökkentését.

11.1.2. 8.1. pont – Működéstervezés és -szabályozás: biztosítja a csatlakoztatott eszközök feletti biztonságos operatív kontrollt.

11.2. ISO/IEC 27002

11.2.1. 5.23. kontroll – Az operatív technológia használatának információbiztonsága: meghatározza az OT biztonságos használatát a fizikai és digitális környezetekben.

11.2.2. 5.31. kontroll – Az információs rendszerek biztonságos konfigurálása: előírja az IoT-/OT-eszközök megerősített beállításait és a nem biztonságos alapértelmezések elkerülését.

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – Szoftver-, firmware- és információintegritás: előírja a firmware és a frissítések integritásának ellenőrzését.

11.3.2. CM-7 – Minimálisan szükséges funkcionalitás: az eszközökön nem lehetnek engedélyezve nem használt vagy nem biztonságos funkciók.

11.3.3. AC-6 – Legkisebb jogosultság elve: az eszközökhöz való hozzáférést kizárólag jogosult felhasználókra kell korlátozni.

11.3.4. PE-20 – Eszközök felügyelete: az IoT- és OT-eszközök fizikai és működési felügyelete.

11.3.5. SC-7 – Határvédelem: a csatlakoztatott rendszerek hálózati kommunikációjának szegmentálása és szabályozása.

11.4. GDPR (2016/679)

11.4.1. 32. cikk – Az adatkezelés biztonsága: ha személyes adatok rögzítése történik (pl. megfigyelő kamerák révén), a szervezet köteles megfelelő technikai és szervezési intézkedéseket bevezetni az ilyen adatkezelés védelme érdekében.

11.5. NIS2 irányelv (2022/2555)

11.5.1. 21. cikk (2) bekezdés a) pont – Kockázatkezelési intézkedések

11.5.2. 21. cikk (2) bekezdés d) pont – Az eszközök biztonságos konfigurálása és használata

11.5.3. 21. cikk (2) bekezdés f) pont – Ellátási lánc és rendszerbiztonság

11.6. DORA-rendelet (2022/2554)

11.6.1. 9. cikk (2) bekezdés – Az IKT-kockázatkezelés hatálya: magában foglalja a működési környezetben használt ipari és beágyazott eszközöket.

11.6.2. 10. cikk (1) bekezdés – IKT-folytonosság: előírja, hogy az eszközkonfigurációk támogassák a rezilienciát és a helyreállítási műveleteket.

11.7. COBIT 2019

11.7.1. DSS01 – Műveletek kezelése: alkalmazandó a technológiai műveletek – beleértve a fizikai eszközöket is – felügyeletére.

11.7.2. DSS05 – Biztonsági szolgáltatások kezelése: biztosítja, hogy a csatlakoztatott rendszerek megfelelő felügyelet és védelem alatt álljanak.

11.7.3. APO13 – Biztonság kezelése: megerősíti a KKV-kon belüli működési vagyonelemek védelmére vonatkozó szabályzatokat.