					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P35					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**

Az alkalmazandó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	8. fejezet	
ISO/IEC 27002:2022	5.7, 5.23, 5.27, 5.31, 5.36 kontrollok	
NIST SP 800-53 Rev.5	SC-7, SI-4, CM-2, AC-6, PL-8	
GDPR	5., 25., 32. cikk	
NIS2 irányelv	21., 23. cikk	
DORA-rendelet	9., 10. cikk	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Cél

1.1 Jelen szabályzat meghatározza a szervezeten belüli Internet of Things (IoT) és Operational Technology (OT) rendszerek bevezetésére, üzemeltetésére, felügyeletére és kivonására vonatkozó kötelező információbiztonsági követelményeket.

1.2 Biztosítja, hogy e rendszerek a szervezet átfogó kiberbiztonsági irányítási rendszerébe integráltan működjenek, és védettek legyenek a kompromittálódással, a nem rendeltetésszerű használattal és az üzemeltetés szabotálásával szemben.

1.3 A szabályzat célja, hogy erős műszaki, szervezeti és eljárási kontrollokat írjon elő a fizikai infrastruktúrához, termelési folyamatokhoz és biztonságkritikus környezetekhez kapcsolódó IoT/OT rendszerek védelmére.

1.4 Támogatja a kiberbiztonságra, üzembiztonságra, környezeti felügyeletre és üzletmenet-folytonosságra vonatkozó szabályozási és szerződéses kötelezettségek teljesítését.

2. Hatály

2.1 Jelen szabályzat a szervezet működési, adminisztratív vagy termelési környezetében használt valamennyi IoT- és OT-rendszerre kiterjed, függetlenül attól, hogy azok a szervezet tulajdonában állnak, béreltek, vagy harmadik fél biztosítja őket.

2.2 Az érintett rendszerek különösen az alábbiakat foglalják magukban:

2.2.1 IoT-eszközök, például környezeti érzékelők, beléptetőrendszerek, intelligens világítási megoldások, megfigyelőberendezések és viselhető eszközök

2.2.2 OT-platformok, például PLC-k, SCADA-, DCS- és HMI-rendszerek, MES-interfészek és terepi vezérlők

2.2.3 Fizikai műveleteket felügyelő ipari vezérlőhálózatok vagy felhőkapcsolattal rendelkező eszközök

2.3 A szabályzat kiterjed:

2.3.1 Valamennyi környezetre (helyszíni, peremhálózati, felhőből felügyelt)

2.3.2 Valamennyi érintettre (belső felhasználók, integrátorok, külső beszállítók, szerződéses partnerek)

2.3.3 A teljes életciklus valamennyi szakaszára (tervezés, beszerzés, bevezetés, üzemeltetés, kivonás)

3. Célkitűzések

3.1 Az IoT- és OT-infrastruktúra védelme a belső és külső kiberbiztonsági fenyegetésekkel szemben, ideértve a szolgáltatásmegtagadásos támadásokat, a jogosulatlan hozzáférést, a zsarolóvírusok terjedését és a firmware jogosulatlan módosítását.

3.2 Annak biztosítása, hogy az IoT/OT platformok ne váljanak IT–OT közötti áthidaló támadások kiindulópontjává, és ne veszélyeztessék a biztonságkritikus rendszereket.

3.3 A beépített biztonság és a többrétegű védelem elveinek alkalmazása e technológiák teljes életciklusa során.

3.4 Az IoT- és OT-platformok megbízható, biztonságos és auditálható integrációjának biztosítása a szervezet biztonsági műveleti központjába (SOC) és az incidenskezelési tervekbe.

3.5 Annak biztosítása, hogy minden bevezetés összhangban legyen az ISO/IEC 27001 kontrolljaival és az alkalmazandó ágazati útmutatásokkal (pl. IEC 62443, ISO/IEC 27019, NIST SP 800-82).

4. Szerepkörök és felelősségek

4.1 Információbiztonsági vezető (CISO) / biztonsági vezető

4.1.1 Meghatározza az IoT/OT kiberbiztonságára vonatkozó szabályzatokat és műszaki szabványokat

4.1.2 Felügyeli a kockázatértékeléseket, a kontrollok megfelelőségének ellenőrzését és a szervezeti egységek közötti koordinációt

4.2 OT mérnökök / létesítmény- és üzemvezetők

4.2.1 Ellenőrzik az OT-rendszerek konfigurációit, és biztosítják a szabályzat betartását a termelési területeken

4.2.2 Fenntartják az OT-rendszerek sértetlenségét és biztonságos működését szolgáló fizikai és logikai védelmi intézkedéseket

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

9. Felülvizsgálati és módosítási követelmények

9.1 Jelen szabályzatot legalább évente felül kell vizsgálni, és az alábbiak alapján szükség szerint frissíteni kell:

9.1.1 Az OT- vagy IoT-rendszerarchitektúrában, a beszállítókban vagy a platformokban bekövetkező változások

9.1.2 Jelentős szabályozási változások (pl. a DORA, a NIS2 vagy ágazati irányelvek módosításai)

9.1.3 Új sérülékenységek vagy fenyegetési mintázatok megjelenése a vezérlőrendszerekben

9.1.4 Belső vagy külső auditok, behatolástesztek vagy red team gyakorlatok megállapításai

9.2 A felülvizsgálati folyamat közös megindításáért a CISO, az OT biztonsági vezető és az érintett szervezeti egységek vezetői felelősek.

9.3 Soron kívüli felülvizsgálatot kell kezdeményezni az alábbi esetekben:

9.3.1 Bármely, rendszerkiesést vagy adatvesztést eredményező IoT/OT incidens után

9.3.2 Jelentős új berendezések, felügyeleti szoftverek vagy firmware-platformok bevezetésekor

9.3.3 Intelligens peremhálózati számítástechnika vagy mesterséges intelligenciával támogatott automatizálás terepi szintű integrációja esetén

9.4 Valamennyi szabályzatmódosítást:

9.4.1 Dokumentálni kell a verziótörténetben és a szabályzatváltozási nyilvántartásban

9.4.2 Közölni kell minden érintett felhasználóval, beszállítóval és IT/OT-üzemeltetővel

9.4.3 A felsővezetésnek ismételten jóvá kell hagynia

10. Kapcsolódó szabályzatok és kapcsolódások

10.1 Jelen szabályzat az alábbi információbiztonsági szabályzatokkal együtt alkalmazandó, és azok támogatják annak végrehajtását:

10.1.1 P1 – Információbiztonsági szabályzat: Meghatározza azokat az alapvető biztonsági elveket, amelyek az IoT- és OT-rendszerek biztonságára is kiterjednek.

10.1.2 P3 – Elfogadható használati szabályzat: Meghatározza a személyes és jogosulatlan eszközhasználatra vonatkozó korlátozásokat, ideértve az üzemeltetési környezeteket is.

10.1.3 P6 – Kockázatkezelési szabályzat: Irányt ad a beágyazott és vezérlőrendszerekkel kapcsolatos kockázatok értékeléséhez, elfogadásához és csökkentéséhez.

10.1.4 P12 – Eszközkezelési szabályzat: Biztosítja, hogy valamennyi IoT- és OT-rendszer formálisan nyilvántartásba kerüljön, és kijelölt felelős tulajdonossal rendelkezzen.

10.1.5 P20 – Végpontvédelmi / rosszindulatú kódok elleni szabályzat: Vonatkozik a termelési környezethez kapcsolódó vezérlőkre, intelligens átjárókra és peremhálózati rendszerekre is.

10.1.6 P22 – Naplózási és felügyeleti szabályzat: Kiterjed az OT-környezetek naplógyűjtési és naplófelülvizsgálati eljárásaira.

10.1.7 P30 – Incidenskezelési szabályzat: Közvetlenül szabályozza az IoT/OT sérülések, anomáliák vagy rendszerhibák eszkalációját és kezelését.

10.1.8 P33 – Audit- és megfelelőségfelügyeleti szabályzat: Biztosítéki mechanizmusokat ad a jelen szabályzatnak való folyamatos megfelelés igazolására.

11. Hivatkozott szabványok és keretrendszerek

11.1 Jelen szabályzat összhangban van olyan nemzetközileg elismert szabványokkal és szabályozási keretrendszerekkel, amelyek biztosítják az Internet of Things (IoT) és Operational Technology (OT) rendszerek biztonságát, ellenálló képességét és megfelelőségét ipari, termelési és vállalati környezetben.

11.2 ISO/IEC 27002:2022 – 5.7, 5.23, 5.27, 5.31, 5.36 kontrollok

11.2.1 5.7 kontroll – Fenyegetettségi információk: Támogatja az OT-környezetek felügyeletét és az IoT-specifikus sérülékenységek azonosítását.

11.2.2 5.23 kontroll – Információbiztonság a felhőszolgáltatások használata során: Akkor alkalmazandó, amikor az IoT-eszközök telemetria, vezérlés vagy elemzés céljából felhőplatformokhoz kapcsolódnak.

11.2.3 5.27 kontroll – Biztonságos rendszerarchitektúra és mérnöki alapelvek: Szabályozza a beágyazott rendszerekre és vezérlőhálózatokra vonatkozó, tervezésbe épített biztonsági elveket.

11.2.4 5.31 kontroll – Biztonság a fejlesztési és támogatási folyamatokban: Előírja a szoftver- és firmware-ellenőrzést, a javításkezelési kontrollokat és a beszállítói követelményeket az OT-bevezetések során.

11.2.5 5.36 kontroll – Megfelelés jogi, jogszabályi, szabályozási és szerződéses követelményeknek: Biztosítja az OT-eszközök megfelelését a biztonsági, környezetvédelmi és szabályozási előírásoknak.

11.2.6 Ezek a kontrollok együttesen bevált gyakorlatokat határoznak meg az IoT/OT rendszerek teljes életcikluson át történő védelmére, ideértve az architektúratervezést, a biztonságos bevezetést, a javításkezelést, az anomáliaészlelést és az ágazati követelményeknek való megfelelést.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Határvédelem: Biztosítja, hogy az OT-hálózatok szegmentáltak legyenek, és védettek maradjanak a jogosulatlan hozzáféréssel szemben.

11.3.2 SI-4 – Rendszerfelügyelet: Előírja a folyamatos felügyeleti és anomáliaészlelési mechanizmusok bevezetését ICS-környezetekben.

11.3.3 CM-2 – Alapkonfiguráció: Előírja a konfigurációszabályozást és az IoT/OT-platformok megerősítését.

11.3.4 AC-6 – Legkisebb jogosultság elve: Alkalmazandó a felhasználói hozzáférésekre és a beágyazott vezérlőrendszerek beszállítói távoli szervizelésére.

11.3.5 PL-8 – Biztonsági és adatvédelmi architektúrák: Szabályozza a biztonságos rendszerintegráció tervezését, különösen az OT-modernizációs projektek esetében.

11.4 GDPR (2016/679)

11.4.1 5. cikk – A személyes adatok kezelésére vonatkozó alapelvek: Alkalmazandó azokra az IoT-platformokra, amelyek személyekhez kapcsolható érzékelőalapú vagy viselkedési adatokat kezelnek.

11.4.2 25. cikk – Beépített és alapértelmezett adatvédelem: Előírja az adatvédelmi garanciák beépítését az IoT-termékek tervezésébe és firmware-ébe.

11.4.3 32. cikk – Az adatkezelés biztonsága: Előírja a titkosítást, a hozzáférés-szabályozást és a biztonságos kommunikációt az intelligens eszközök adatátvitele során.

11.5 NIS2 irányelv (2022/2555)

11.5.1 21. és 23. cikk: Biztonsági kötelezettségeket ír elő az OT-rendszereket használó alapvető és fontos szervezetek számára. Ezek közé tartozik a kockázatértékelés, az incidensjelentés, valamint az IoT/OT beszállítók és a firmware sértetlenségének ellátásilánc-szintű ellenőrzése.

11.6 DORA-rendelet (2022/2554)

11.6.1 9. cikk – IKT-kockázatkezelés: Előírja a beágyazott rendszerek és az OT-technológiák biztonságos integrációját az IKT-kockázatkezelési programba.

11.6.2 10. cikk – IKT-biztonsági követelmények: Védelmi intézkedéseket ír elő a pénzügyi és kritikus szolgáltatási környezetekben használt, összekapcsolt OT-platformok esetében.

11.7 COBIT 2019

11.7.1 DSS05.01 – Védelem a rosszindulatú kódokkal szemben: Magában foglalja az ICS-specifikus fenyegetések és az IoT-t célzó rosszindulatú kampányok észlelését és kezelését.

11.7.2 BAI09.01 – Biztonsági követelmények meghatározása és fenntartása: Kapcsolódik az intelligens vagy beágyazott infrastruktúra biztonságos kialakításához és üzemeltetéséhez.

11.7.3 APO13.02 – Információbiztonsági terv kialakítása és fenntartása: Előírja az OT-rendszerek és sérülékenységeik bevonását a szervezetszintű kiberbiztonsági stratégiába.