					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P35					Dokumenttitel: **Politik for sikkerhed i IoT- og OT-systemer**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Afstemt med standarder og regulering

Standard/regulering	Klausul/artikel	Bemærkning
ISO/IEC 27001:2022	Kapitel 8	
ISO/IEC 27002:2022	Kontroller 5.7, 5.23, 5.27, 5.31, 5.	
NIST SP 800-53 Rev.5	SC-7, SI-4, CM-2, AC-6, PL-8	
EU GDPR	Artikel 5, 25, 32	
EU NIS2	Artikel 21, 23	
EU DORA	Artikel 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.	

1. Formål

1.1 Denne politik fastsætter obligatoriske informationssikkerhedskrav til implementering, drift, overvågning og udfasning af Internet of Things (IoT)- og Operational Technology (OT)-systemer i organisationen.

1.2 Den skal sikre, at sådanne systemer integreres i organisationens overordnede ledelsessystem for cybersikkerhed og beskyttes mod kompromittering, misbrug og driftsmæssig sabotage.

1.3 Politikken skal sikre stærke tekniske, organisatoriske og proceduremæssige sikkerhedskontroller til beskyttelse af IoT-/OT-systemer, der er knyttet til fysisk infrastruktur, produktionsprocesser og sikkerhedskritiske miljøer.

1.4 Den understøtter regulatoriske og kontraktuelle forpligtelser inden for cybersikkerhed, sikkerhed, miljøstyring og forretningskontinuitet.

2. Anvendelsesområde

2.1 Denne politik gælder for alle IoT- og OT-systemer, uanset om de ejes af virksomheden, leases eller leveres af tredjepart, og som anvendes i organisationens drifts-, administrations- eller produktionsmiljøer.

2.2 Omfattede systemer inkluderer, men er ikke begrænset til:

2.2.1 IoT-enheder såsom miljøsensorer, adgangskontrolsystemer, intelligent belysning, overvågningsudstyr og wearables

2.2.2 OT-platforme såsom PLC'er, SCADA, DCS, HMI-paneler, MES-grænseflader og feltcontrollere

2.2.3 Industrielle kontrolnetværk eller cloudforbundne aktiver, der overvåger fysiske driftsprocesser

2.3 Politikken omfatter:

2.3.1 Alle miljøer (lokalt driftede, edge, cloudadministrerede)

2.3.2 Alle interessenter (interne brugere, integratorer, tredjepartsleverandører, kontraktansatte)

2.3.3 Alle livscyklusfaser (design, anskaffelse, implementering, drift, udfasning)

3. Mål

3.1 At beskytte IoT- og OT-infrastruktur mod interne og eksterne cybersikkerhedstrusler, herunder denial-of-service, uautoriseret adgang, spredning af ransomware og manipulation af firmware.

3.2 At sikre, at IoT-/OT-platforme ikke bliver angrebsvektorer via IT/OT-broer eller kompromitterer sikkerhedskritiske systemer.

3.3 At anvende principperne om security by design og defense in depth gennem hele disse teknologiers livscyklus.

3.4 At muliggøre pålidelig, sikker og revisionssporbar integration af IoT- og OT-platforme i organisationens Security Operations Center (SOC) og beredskabsplaner for hændelsesrespons.

3.5 At sikre, at alle implementeringer er i overensstemmelse med kontrollerne i ISO/IEC 27001 og relevant sektorspecifik vejledning (f.eks. IEC 62443, ISO 27019, NIST SP 800-82).

4. Roller og ansvar

4.1 Chief Information Security Officer (CISO) / informationssikkerhedschef

4.1.1 Fastsætter politikker og tekniske standarder for cybersikkerhed i IoT/OT

4.1.2 Fører tilsyn med risikovurderinger, kontrolvalidering og tværgående koordinering

4.2 OT-ingeniører / ledere af faciliteter og produktionsanlæg

4.2.1 Validerer konfigurationer af OT-systemer og sikrer efterlevelse af politikken i produktionsområder

4.2.2 Opretholder fysiske og logiske sikkerhedsforanstaltninger for OT-systemers integritet og sikkerhed

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1 Denne politik skal gennemgås mindst én gang årligt og opdateres på baggrund af:

9.1.1 Ændringer i OT- eller IoT-systemarkitektur, leverandører eller platforme

9.1.2 Væsentlige regulatoriske opdateringer (f.eks. ændringer i DORA, NIS2 eller sektorspecifikke direktiver)

9.1.3 Nye sårbarheder eller trusselsmønstre i kontrolsystemer

9.1.4 Resultater fra interne eller eksterne revisioner, penetrationstest eller red team-øvelser

9.2 CISO, den OT-sikkerhedsansvarlige og relevante afdelingsledere er i fællesskab ansvarlige for at iværksætte gennemgangsprocessen.

9.3 Ekstraordinære gennemgange skal iværksættes efter:

9.3.1 Enhver IoT-/OT-relateret hændelse, der medfører systemsvigt eller datatab

9.3.2 Indførelse af væsentligt nyt udstyr, ny overvågningssoftware eller nye firmwareplatforme

9.3.3 Integration af intelligent edge computing eller AI-understøttet automatisering på feltniveau

9.4 Alle ændringer i politikken skal:

9.4.1 Dokumenteres i versionshistorikken og registret over politikændringer

9.4.2 Kommunikeres til alle berørte brugere, leverandører og IT-/OT-operatører

9.4.3 Godkendes på ny af direktionen

10. Relaterede politikker og sammenhænge

10.1 Denne politik fungerer sammen med og understøttes af følgende informationssikkerhedspolitikker:

10.1.1 P1 – Informationssikkerhedspolitik: Fastlægger grundlæggende sikkerhedsprincipper, som også gælder for sikkerhed i IoT- og OT-systemer.

10.1.2 P3 – Politik for acceptabel brug: Fastlægger begrænsninger for personlig og uautoriseret brug af enheder, herunder i driftsmiljøer.

10.1.3 P6 – Politik for risikostyring: Regulerer vurdering, accept og reduktion af risici relateret til indlejrede systemer og kontrolsystemer.

10.1.4 P12 – Politik for aktivstyring: Sikrer, at alle IoT- og OT-systemer registreres formelt og tildeles ansvarlige ejere.

10.1.5 P20 – Politik for endpoint-beskyttelse / malware: Gælder for tilsluttede controllere, intelligente gateways og edge-systemer i produktionen.

10.1.6 P22 – Politik for logning og overvågning: Omfatter også procedurer for indsamling og gennemgang af logfiler i OT-miljøer.

10.1.7 P30 – Politik for hændelsesrespons: Regulerer direkte, hvordan brud, anomalier eller systemsvigt i IoT/OT skal eskaleres og håndteres.

10.1.8 P33 – Politik for revision og overvågning af efterlevelse: Sikrer, at efterlevelse af denne politik løbende kan valideres.

11. Referencestandarder og styringsrammer

11.1 Denne politik er afstemt med internationalt anerkendte standarder og regulatoriske rammer, der understøtter sikkerhed, robusthed og efterlevelse for Internet of Things (IoT)- og Operational Technology (OT)-systemer i industrielle miljøer, produktionsmiljøer og virksomhedsmiljøer.

11.2 ISO/IEC 27002:2022 – Kontroller 5.7, 5.23, 5.27, 5.31, 5

11.2.1 Kontrol 5.7 – Trusselsintelligens: Understøtter overvågning af OT-miljøer og identifikation af IoT-specifikke sårbarheder.

11.2.2 Kontrol 5.23 – Informationssikkerhed ved brug af cloudtjenester: Gælder, når IoT-enheder er forbundet til cloudplatforme for telemetri, styring eller analyse.

11.2.3 Kontrol 5.27 – Sikker systemarkitektur og tekniske principper: Regulerer security by design-principper for indlejrede systemer og kontrolnetværk.

11.2.4 Kontrol 5.31 – Sikkerhed i udviklings- og supportprocesser: Håndhæver validering af software/firmware, patchkontroller og leverandørkrav i OT-implementeringer.

11.2.5 Kontrol 5.36 – Efterlevelse af juridiske og kontraktuelle krav: Sikrer, at OT-aktiver efterlever krav vedrørende sikkerhed, miljø og regulering.

11.2.6 Disse kontroller udgør samlet bedste praksis for sikring af IoT-/OT-systemer gennem hele deres livscyklus, herunder arkitekturdesign, sikker implementering, patching, anomalidetektion og efterlevelse af sektorspecifikke krav.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Beskyttelse af systemgrænser: Sikrer, at OT-netværk er segmenteret og beskyttet mod uautoriseret adgang.

11.3.2 SI-4 – Systemovervågning: Kræver implementering af mekanismer til løbende overvågning og anomalidetektion i ICS-miljøer.

11.3.3 CM-2 – Baselinekonfiguration: Kræver konfigurationsstyring og hærdning af IoT-/OT-platforme.

11.3.4 AC-6 – Mindste privilegium: Gælder for brugeradgang og fjernservice fra leverandører på indlejrede kontrolsystemer.

11.3.5 PL-8 – Sikkerheds- og privatlivsarkitekturer: Regulerer planlægning af sikker systemintegration, særligt ved moderniseringsprojekter i OT.

11.4 EU GDPR (2016/679)

11.4.1 Artikel 5 – Principper for behandling af personoplysninger: Gælder for IoT-platforme, der behandler sensorbaserede eller adfærdsrelaterede data, som kan knyttes til enkeltpersoner.

11.4.2 Artikel 25 – Databeskyttelse gennem design og som standardindstilling: Kræver, at databeskyttelsesforanstaltninger indbygges i IoT-produktdesign og firmware.

11.4.3 Artikel 32 – Behandlingssikkerhed: Håndhæver kryptering, adgangskontrol og sikker kommunikation ved overførsel af data fra intelligente enheder.

11.5 EU NIS2-direktivet (2022/2555)

11.5.1 Artikel 21 og 23: Pålægger væsentlige og vigtige enheder sikkerhedsforpligtelser ved brug af OT-systemer. Dette omfatter risikovurdering, hændelsesrapportering og validering af forsyningskæden for IoT-/OT-leverandører og firmwareintegritet.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 9 – Risikostyring for IKT: Kræver sikker integration af indlejrede systemer og OT-teknologier i programmet for styring af IKT-risici.

11.6.2 Artikel 10 – Krav til IKT-sikkerhed: Kræver beskyttelsesforanstaltninger for sammenkoblede OT-platforme, der anvendes i finansielle miljøer og miljøer med kritiske tjenester.

11.7 COBIT 2019

11.7.1 DSS05.01 – Beskyt mod malware: Omfatter detektion af og respons på ICS-specifikke trusler og IoT-baserede malwarekampagner.

11.7.2 BAI09.01 – Etabler og vedligehold sikkerhedskrav: Kan knyttes til sikker klargøring og drift af intelligent eller indlejret infrastruktur.

11.7.3 APO13.02 – Etabler og vedligehold en plan for informationssikkerhed: Kræver, at OT-systemer og deres sårbarheder indgår i den virksomhedsdækkende cybersikkerhedsstrategi.