					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P35S					Dokumenttitel: **Politik for IoT-/OT-sikkerhed**							
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**

Tilpasset relevante standarder og lovkrav

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontrol 5.23, 5	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
EU GDPR	Artikel 32	
EU NIS2	Artikel 21(2)(a), (d), (f)	
EU DORA	Artikel 9(2), 10(1)	

1. Formål

1.1. Denne politik fastsætter obligatoriske krav for sikker anvendelse og styring af Internet of Things (IoT)- og Operational Technology (OT)-enheder i organisationen. Disse enheder kan omfatte smarte sensorer, sikkerhedskameraer, produktionsmaskiner, HVAC-styreenheder eller andre netværkstilsluttede industrielle systemer.

1.2. Formålet med denne politik er at:

1.2.1. Beskytte fysiske og digitale driftsaktiviteter mod afbrydelser eller manipulation som følge af utilstrækkeligt sikrede forbundne enheder

1.2.2. Sikre sikker idriftsættelse, overvågning og vedligeholdelse af IoT- og OT-systemer

1.2.3. Sikre overholdelse af ISO/IEC 27001:2022, NIS2-direktivet og relaterede regulatoriske rammeværker

1.2.4. Fastlægge praktiske og ensartede sikkerhedskontroller for SMV'er, der opererer i kontor-, lager- eller produktionsmiljøer

2. Omfang

2.1. Denne politik gælder for alle personer, der deltager i planlægning, installation, konfiguration, brug, support eller bortskaffelse af IoT- eller OT-enheder. Dette omfatter:

2.1.1. Medarbejdere, kontrahenter eller praktikanter med fysisk adgang eller fjernadgang til enheder

2.1.2. Tredjepartsleverandører eller serviceteknikere, der installerer eller vedligeholder forbundne systemer

2.1.3. Direktører eller medarbejdere med ansvar for tilsyn med sikkerhedspolitikker

2.2. Politikken omfatter:

2.2.1. IoT-enheder såsom smarte låse, overvågningssystemer, smarte målere eller printere

2.2.2. OT-systemer, herunder PLC'er (programmerbare logiske styringer), SCADA-paneler eller industrielle gateways

2.2.3. Understøttende hardware, administrationsapplikationer og kommunikationsnetværk, der anvendes af disse systemer

2.3. Denne politik gælder på alle arbejdssteder: kontormiljøer, fjernlokationer, produktionsområder og cloudplatforme, der har grænseflader til disse enheder.

3. Mål

3.1. Sikker idriftsættelse: Sikre, at alle IoT-/OT-systemer er konfigureret sikkert, før de tages i brug i driftsmiljøet.

3.2. Begrænse eksponering: Forebygge uautoriseret adgang, misbrug eller kompromittering af forbundne enheder ved at håndhæve stærk adgangsstyring og netværkssegmentering.

3.3. Løbende overvågning: Opretholde synlighed i IoT-/OT-driften gennem aktivitetslogning og overvågning af usædvanlig adfærd.

3.4. Leverandøransvarlighed: Sikre, at tredjepartsleverandører følger sikker praksis for installation, konfiguration og vedligeholdelse.

3.5. Regulatorisk overholdelse: Dokumentere fuld tilpasning til gældende standarder såsom ISO 27001, GDPR (hvis der indsamles personoplysninger) og NIS2 med henblik på robusthed i kritisk infrastruktur.

4. Roller og ansvar

4.1. Direktør (GM)

4.1.1. Har det overordnede ansvar for sikkerheden i IoT- og OT-systemer

4.1.2. Godkender denne politik og sikrer, at den håndhæves på alle arbejdssteder

4.1.3. Verificerer, at leverandører og kontrahenter følger sikker praksis for opsætning og vedligeholdelse

4.1.4. Godkender netværksadgang for alle IoT-/OT-systemer

4.2. Udpeget medarbejder eller driftsansvarlig (hvis udpeget)

4.2.1. Fører tilsyn med aktivfortegnelsen samt placering og konfiguration af IoT-/OT-enheder

4.2.2. Registrerer hver enheds placering, netværkstilknytning og supportdokumentation

4.2.3. Sikrer, at alle ændringer (f.eks. firmwareopdateringer eller udskiftning af enheder) dokumenteres

[... 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. Årlig gennemgang

9.1.1. Denne politik skal gennemgås mindst én gang om året af GM

9.1.2. Gennemgangen skal vurdere, om politikken fortsat er effektiv, dækker aktuelle enhedstyper og er tilpasset nye risici eller teknologier

9.2. Opdateringer udløst af hændelser eller ændringer

9.2.1. Opdateringer af politikken skal også iværksættes, når:

9.2.2. Nye typer IoT- eller OT-systemer introduceres

9.2.3. Leverandører udsender sikkerhedsmeddelelser eller meddelelser om end of life

9.2.4. En hændelse eller revision identificerer mangler i IoT-/OT-kontroller

9.2.5. Nye love eller standarder fastsætter yderligere krav

9.3. Dokumentation og versionsstyring

9.3.1. Alle opdateringer skal dokumenteres, herunder dato, versionsnummer og et resumé af ændringer

9.3.2. GM skal opbevare historiske versioner af politikken til revisionsformål

9.4. Kommunikation af ændringer

9.4.1. Enhver opdatering af politikken skal deles med alle relevante medarbejdere og leverandører

9.4.2. Opdaterede versioner skal være tilgængelige via fællesdrev eller trykte materialer på installationssteder eller i kontrolcentre

10. Relaterede politikker og sammenhænge

10.1. Denne politik skal implementeres i overensstemmelse med følgende relaterede SME-politikker:

10.1.1. P4S – Politik for adgangskontrol: Håndhæver login-kontroller på enhedsniveau, brug af stærke adgangskoder og procedurer for godkendt adgang til IoT- og OT-platforme

10.1.2. P9S – Politik for fjernarbejde: Forhindrer brug af fjernadgang til IoT-/OT-administrationsgrænseflader via usikre eller ikke-godkendte kanaler

10.1.3. P17S – Databeskyttelses- og privatlivspolitik: Gælder, hvis IoT-enheder (f.eks. sikkerhedskameraer) behandler eller optager personoplysninger, og sikrer overholdelse af GDPR

10.1.4. P30S – Politik for hændelseshåndtering: Fastlægger procedurer for detektion, rapportering og håndtering af IoT- eller OT-hændelser, herunder mistanke om manipulation eller driftsfejl

10.1.5. P36S – Politik for sociale medier og ekstern kommunikation: Sikrer, at oplysninger om enheder eller netværksopsætning ikke deles eksternt uden godkendelse

10.2. Hver relateret politik styrker håndhævelsen og den praktiske anvendelse af denne politik ved at give målrettet proceduremæssig vejledning.

11. Referencestandarder og rammeværker

11.1. ISO/IEC 27001

11.1.1. Klausul 6.1 – Risikoidentifikation og risikobehandling: Kræver, at risici relateret til IoT- og OT-systemer vurderes systematisk og afbødes

11.1.2. Klausul 8.1 – Operationel planlægning og styring: Sikrer sikker driftsmæssig kontrol med forbundne enheder

11.2. ISO/IEC 27002

11.2.1. Kontrol 5.23 – Informationssikkerhed ved brug af Operational Technology (OT): Definerer sikker brug af OT på tværs af fysiske og digitale miljøer

11.2.2. Kontrol 5.31 – Sikker konfiguration af informationssystemer: Kræver hærdede konfigurationer for IoT-/OT-enheder og undgåelse af usikre standardindstillinger

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – Software-, firmware- og informationsintegritet: Kræver integritetsvalidering af firmware og opdateringer

11.3.2. CM-7 – Mindst nødvendig funktionalitet: Enheder må ikke have ubrugte eller usikre funktioner aktiveret

11.3.3. AC-6 – Mindste privilegium: Adgang til enheder skal begrænses til autoriserede brugere

11.3.4. PE-20 – Overvågning af aktiver: Fysisk og driftsmæssig overvågning af IoT- og OT-aktiver

11.3.5. SC-7 – Beskyttelse af systemgrænser: Segmentering og kontrol af netværkskommunikation for forbundne systemer

11.4. EU GDPR (2016/679)

11.4.1. Artikel 32 – Behandlingssikkerhed: Hvis personoplysninger indsamles (f.eks. via overvågningskameraer), skal organisationen implementere passende tekniske og organisatoriske foranstaltninger til at sikre denne behandling

11.5. EU NIS2-direktivet (2022/2555)

11.5.1. Artikel 21(2)(a) – Risikostyringsforanstaltninger

11.5.2. Artikel 21(2)(d) – Sikker konfiguration og brug af enheder

11.5.3. Artikel 21(2)(f) – Sikkerhed i forsyningskæden og systemsikkerhed

11.6. EU DORA (2022/2554)

11.6.1. Artikel 9(2) – Omfang af styring af IKT-risiko: Omfatter industrielle og indlejrede enheder, der anvendes i driftsmiljøer

11.6.2. Artikel 10(1) – IKT-kontinuitet: Kræver, at enhedskonfigurationer understøtter robusthed og genopretning

11.7. COBIT 2019

11.7.1. DSS01 – Styring af driftsaktiviteter: Gælder for tilsyn med teknologidrift, herunder fysiske enheder

11.7.2. DSS05 – Styring af sikkerhedstjenester: Sikrer, at forbundne systemer overvåges og beskyttes korrekt

11.7.3. APO13 – Styring af sikkerhed: Understøtter politikker til beskyttelse af driftsaktiver i SMV'er