					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P35					Documenttitel: **IoT-OT-beveiligingsbeleid**							
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:							
X	Beleid		Standaard		Procedure		Formulier		Register		Overig	

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Afgestemd op normen en regelgeving waar van toepassing

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausule 8	
ISO/IEC 27002:2022	Beheersmaatregelen 5.7, 5.23, 5.27, 5.31, 5.36	
NIST SP 800-53 Rev.5	SC-7, SI-4, CM-2, AC-6, PL-8	
AVG	Artikelen 5, 25, 32	
EU NIS2	Artikelen 21, 23	
EU DORA	Artikelen 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Doel

1.1 Dit beleid stelt de verplichte informatiebeveiligingseisen vast voor de implementatie, exploitatie, monitoring en buitengebruikstelling van Internet of Things (IoT)- en operationele technologie (OT)-systemen binnen de organisatie.

1.2 Het waarborgt dat dergelijke systemen worden geïntegreerd in het bredere cyberbeveiligingsmanagementsysteem van de organisatie en worden beschermd tegen compromittering, misbruik en operationele sabotage.

1.3 Dit beleid heeft tot doel robuuste technische, organisatorische en procedurele beheersmaatregelen af te dwingen ter bescherming van IoT-/OT-systemen die zijn gekoppeld aan fysieke infrastructuur, productieprocessen en veiligheidskritieke omgevingen.

1.4 Het ondersteunt wettelijke, regelgevende en contractuele verplichtingen op het gebied van cyberbeveiliging, veiligheid, omgevingsbeheersing en continuïteit.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle IoT- en OT-systemen — ongeacht of deze eigendom zijn van de organisatie, geleased zijn of door derden worden geleverd — die worden gebruikt binnen de operationele, administratieve of productieomgevingen van de organisatie.

2.2 Onder de reikwijdte vallende systemen omvatten onder meer:

2.2.1 IoT-apparaten zoals omgevingssensoren, toegangscontrolesystemen, slimme verlichting, bewakingsapparatuur en wearables

2.2.2 OT-platforms zoals PLC's, SCADA, DCS, HMI-panelen, MES-interfaces en veldcontrollers

2.2.3 Industriële besturingsnetwerken of met de cloud verbonden bedrijfsmiddelen die fysieke processen bewaken

2.3 Dit beleid omvat:

2.3.1 Alle omgevingen (on-premises, edge en cloudbeheerd)

2.3.2 Alle belanghebbenden (interne gebruikers, integrators, externe leveranciers en opdrachtnemers)

2.3.3 Alle levenscyclusfasen (ontwerp, inkoop, implementatie, exploitatie en buitengebruikstelling)

3. Doelstellingen

3.1 Het beveiligen van IoT- en OT-infrastructuur tegen interne en externe cyberdreigingen, waaronder denial-of-service, ongeautoriseerde toegang, verspreiding van ransomware en manipulatie van firmware.

3.2 Waarborgen dat IoT-/OT-platforms geen aanvalsvector vormen voor IT-OT-brugaanvallen en geen veiligheidskritieke systemen compromitteren.

3.3 Het toepassen van de principes van security by design en defense in depth gedurende de gehele levenscyclus van deze technologieën.

3.4 Het mogelijk maken van betrouwbare, veilige en auditeerbare integratie van IoT- en OT-platforms binnen het Security Operations Center (SOC) en de incidentresponsplannen van de organisatie.

3.5 Waarborgen dat alle implementaties in lijn zijn met de beheersmaatregelen van ISO/IEC 27001 en toepasselijke sectorspecifieke richtlijnen (bijvoorbeeld IEC 62443, ISO 27019, NIST SP 800-82).

4. Rollen en verantwoordelijkheden

4.1 Chief Information Security Officer (CISO) / informatiebeveiligingsverantwoordelijke

4.1.1 Stelt beleid en technische standaarden vast voor IoT-/OT-cyberbeveiliging

4.1.2 Houdt toezicht op risicobeoordelingen, validatie van beheersmaatregelen en interdisciplinaire afstemming

4.2 OT-engineers / facility- en plantmanagers

4.2.1 Valideren configuraties van OT-systemen en zien toe op naleving van dit beleid in productieomgevingen

4.2.2 Beheren fysieke en logische beveiligingsmaatregelen ter waarborging van de integriteit en veiligheid van OT

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Eisen voor herziening en actualisatie

9.1 Dit beleid moet ten minste jaarlijks worden herzien en bijgewerkt op basis van:

9.1.1 Wijzigingen in de architectuur, leveranciers of platforms van OT- of IoT-systemen

9.1.2 Belangrijke regelgevende actualisaties (bijvoorbeeld herzieningen van DORA, NIS2 of sectorspecifieke richtlijnen)

9.1.3 Het ontstaan van nieuwe kwetsbaarheden of dreigingspatronen in besturingssystemen

9.1.4 Bevindingen uit interne of externe audits, penetratietests of red-teamoefeningen

9.2 De CISO, de OT-beveiligingsverantwoordelijke en de relevante afdelingshoofden zijn gezamenlijk verantwoordelijk voor het initiëren van het herzieningsproces.

9.3 Tussentijdse herzieningen moeten worden gestart na:

9.3.1 Elk IoT-/OT-gerelateerd incident dat resulteert in systeemuitval of gegevensverlies

9.3.2 Introductie van belangrijke nieuwe apparatuur, monitoringsoftware of firmwareplatforms

9.3.3 Integratie van slimme edge computing of AI-verrijkte automatisering op veldniveau

9.4 Alle beleidswijzigingen moeten:

9.4.1 Worden gedocumenteerd in de versiehistorie en het register voor beleidswijzigingen

9.4.2 Worden gecommuniceerd aan alle betrokken gebruikers, leveranciers en IT-/OT-operators

9.4.3 Opnieuw worden goedgekeurd door het topmanagement

10. Gerelateerde beleidsdocumenten en samenhang

10.1 Dit beleid functioneert in samenhang met en wordt ondersteund door de volgende informatiebeveiligingsbeleidsdocumenten:

10.1.1 P1 – Informatiebeveiligingsbeleid: Stelt de basisprincipes voor beveiliging vast die ook van toepassing zijn op de beveiliging van IoT- en OT-systemen.

10.1.2 P3 – Beleid inzake aanvaardbaar gebruik: Definieert beperkingen op persoonlijk gebruik en gebruik van ongeautoriseerde apparaten, ook binnen operationele omgevingen.

10.1.3 P6 – Risicobeheerbeleid: Geeft richting aan de beoordeling, acceptatie en beperking van risico's met betrekking tot embedded systemen en besturingssystemen.

10.1.4 P12 – Activabeheerbeleid: Waarborgt dat alle IoT- en OT-systemen formeel worden opgenomen in de activainventaris en aan verantwoordelijke eigenaren worden toegewezen.

10.1.5 P20 – Beleid inzake endpointbeveiliging / malware: Is van toepassing op aangesloten controllers, slimme gateways en edge-systemen in productieomgevingen.

10.1.6 P22 – Logging- en monitoringbeleid: Is ook van toepassing op procedures voor het vastleggen en beoordelen van loggegevens in OT-omgevingen.

10.1.7 P30 – Incidentresponsbeleid: Regelt rechtstreeks hoe IoT-/OT-inbreuken, anomalieën of systeemuitval moeten worden geëscaleerd en beheerd.

10.1.8 P33 – Beleid inzake audit en nalevingsmonitoring: Biedt assurance-mechanismen om de voortdurende naleving van dit beleid te valideren.

11. Referentienormen en -kaders

11.1 Dit beleid is afgestemd op internationaal erkende normen en regelgevende kaders die de beveiliging, weerbaarheid en naleving van Internet of Things (IoT)- en operationele technologie (OT)-systemen in industriële, productie- en bedrijfsomgevingen waarborgen.

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

11.2.1 Beheersmaatregel 5.7 – Threat Intelligence: Ondersteunt de monitoring van OT-omgevingen en de identificatie van IoT-specifieke kwetsbaarheden.

11.2.2 Beheersmaatregel 5.23 – Informatiebeveiliging bij het gebruik van clouddiensten: Is van toepassing wanneer IoT-apparaten gekoppeld zijn aan cloudplatforms voor telemetrie, besturing of analyse.

11.2.3 Beheersmaatregel 5.27 – Veilige systeemarchitectuur en engineeringprincipes: Regelt security-by-design-principes voor embedded systemen en besturingsnetwerken.

11.2.4 Beheersmaatregel 5.31 – Beveiliging in ontwikkel- en ondersteuningsprocessen: Dwingt software-/firmwarevalidatie, patchbeheer en leveranciersvereisten af bij OT-implementaties.

11.2.5 Beheersmaatregel 5.36 – Naleving van wettelijke en contractuele vereisten: Waarborgt dat OT-activa voldoen aan vereisten op het gebied van veiligheid, milieu en regelgeving.

11.2.6 Deze beheersmaatregelen vormen gezamenlijk best practices voor het beveiligen van IoT-/OT-systemen gedurende hun volledige levenscyclus, waaronder architectuurontwerp, veilige implementatie, patchbeheer, anomaliedetectie en naleving van sectorspecifieke vereisten.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Grensbeveiliging: Waarborgt dat OT-netwerken zijn gesegmenteerd en beschermd tegen ongeautoriseerde toegang.

11.3.2 SI-4 – Systeembewaking: Vereist de implementatie van continue monitoring en mechanismen voor anomaliedetectie in ICS-omgevingen.

11.3.3 CM-2 – Baselineconfiguratie: Verplicht configuratiebeheer en hardening van IoT-/OT-platforms.

11.3.4 AC-6 – Minimale bevoegdheden: Is van toepassing op gebruikerstoegang en onderhoud op afstand door leveranciers van embedded besturingssystemen.

11.3.5 PL-8 – Beveiligings- en privacyarchitecturen: Regelt de planning van veilige systeemintegratie, in het bijzonder voor moderniseringsprojecten in OT.

11.4 AVG (2016/679)

11.4.1 Artikel 5 – Beginselen inzake verwerking van persoonsgegevens: Is van toepassing op IoT-platforms die op sensoren gebaseerde of gedragsgegevens verwerken die herleidbaar zijn tot personen.

11.4.2 Artikel 25 – Gegevensbescherming door ontwerp en door standaardinstellingen: Vereist privacywaarborgen die zijn ingebouwd in het productontwerp en de firmware van IoT-oplossingen.

11.4.3 Artikel 32 – Beveiliging van de verwerking: Verplicht encryptie, toegangsbeheersing en veilige communicatie voor gegevensoverdracht door slimme apparaten.

11.5 EU NIS2-richtlijn (2022/2555)

11.5.1 Artikelen 21 en 23: Leggen beveiligingsverplichtingen op aan essentiële en belangrijke entiteiten die OT-systemen gebruiken. Deze omvatten risicobeoordeling, incidentrapportage en validatie van de toeleveringsketen van IoT-/OT-leveranciers en firmware-integriteit.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 9 – ICT-risicobeheer: Vereist veilige integratie van embedded systemen en OT-technologieën binnen het ICT-risicogovernanceprogramma.

11.6.2 Artikel 10 – ICT-beveiligingsvereisten: Verplicht beschermende maatregelen voor onderling verbonden OT-platforms die worden gebruikt in financiële en kritieke dienstverleningsomgevingen.

11.7 COBIT 2019

11.7.1 DSS05.01 – Beschermen tegen malware: Omvat detectie van en respons op ICS-specifieke dreigingen en IoT-malwarecampagnes.

11.7.2 BAI09.01 – Vaststellen en onderhouden van beveiligingsvereisten: Sluit aan op veilige toegangsverlening en exploitatie van slimme of embedded infrastructuur.

11.7.3 APO13.02 – Vaststellen en onderhouden van een informatiebeveiligingsplan: Vereist opname van OT-systemen en hun kwetsbaarheden in de organisatiebrede cyberbeveiligingsstrategie.