				Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P35S				Documenttitel: **IoT-OT-beveiligingsbeleid - MKB**						
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

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausules 6.1, 6.2, 8	
ISO/IEC 27002:2022	Beheersmaatregelen 5.23, 5.31	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
AVG	Artikel 32	
NIS2-richtlijn	Artikel 21(2)(a), (d), (f)	
DORA	Artikel 9(2), 10(1)	

1. Doel

1.1. Dit beleid stelt verplichte regels vast voor het veilige gebruik en beheer van Internet of Things (IoT)- en operationele technologie (OT)-systemen binnen de organisatie. Deze systemen kunnen onder meer bestaan uit slimme sensoren, beveiligingscamera's, productiemachines, HVAC-regelaars of andere industriële systemen met netwerkverbinding.

1.2. Het doel van dit beleid is om:

1.2.1. de fysieke en digitale bedrijfsvoering te beschermen tegen verstoring of manipulatie via onvoldoende beveiligde verbonden apparaten

1.2.2. de veilige implementatie, monitoring en het veilige onderhoud van IoT- en OT-systemen af te dwingen

1.2.3. naleving van ISO/IEC 27001:2022, de NIS2-richtlijn en gerelateerde wettelijke en regelgevende kaders te waarborgen

1.2.4. praktische en afdwingbare beheersmaatregelen te bieden voor mkb-organisaties die opereren in kantoor-, magazijn- of productieomgevingen

2. Reikwijdte

2.1. Dit beleid is van toepassing op alle personen die betrokken zijn bij de planning, installatie, configuratie, het gebruik, de ondersteuning of de afvoer van IoT- of OT-apparaten. Hieronder vallen:

2.1.1. werknemers, opdrachtnemers of stagiairs met fysieke of externe toegang tot apparaten

2.1.2. externe leveranciers of servicemonteurs die verbonden systemen installeren of onderhouden

2.1.3. algemeen directeuren of medewerkers die verantwoordelijk zijn voor het toezicht op het beveiligingsbeleid

2.2. Dit beleid heeft betrekking op:

2.2.1. IoT-apparaten zoals slimme sloten, camerabewakingssystemen, slimme meters of printers

2.2.2. OT-systemen, waaronder PLC's (programmeerbare logische controllers), SCADA-panelen of industriële gateways

2.2.3. ondersteunende hardware, beheerapplicaties en communicatienetwerken die door deze systemen worden gebruikt

2.3. Dit beleid geldt voor alle werklocaties: kantooromgevingen, externe locaties, productievloeren en cloudplatforms die met deze apparaten zijn gekoppeld.

3. Doelstellingen

3.1. Veilige implementatie: waarborgen dat alle IoT-/OT-systemen veilig zijn geconfigureerd voordat zij in de operationele omgeving in gebruik worden genomen.

3.2. Beperking van blootstelling: voorkomen van ongeautoriseerde toegang, misbruik of overname van verbonden apparaten door sterke toegangsbeheersing en netwerksegmentatie af te dwingen.

3.3. Continue zichtbaarheid: zicht behouden op IoT-/OT-activiteiten door gebeurtenissen vast te leggen en afwijkend gedrag te monitoren.

3.4. Verantwoordelijkheid van leveranciers: waarborgen dat externe leveranciers veilige installatie-, configuratie- en onderhoudspraktijken volgen.

3.5. Naleving van wet- en regelgeving: aantonen van volledige afstemming op toepasselijke normen zoals ISO 27001, de AVG (indien persoonsgegevens worden verzameld) en NIS2 voor de weerbaarheid van kritieke infrastructuur.

4. Rollen en verantwoordelijkheden

4.1. Algemeen directeur (GM)

4.1.1. draagt de eindverantwoordelijkheid voor de beveiliging van IoT- en OT-systemen

4.1.2. keurt dit beleid goed en ziet erop toe dat het in alle werkgebieden wordt gehandhaafd

4.1.3. verifieert dat leveranciers en opdrachtnemers veilige installatie- en onderhoudspraktijken volgen

4.1.4. autoriseert netwerktoegang voor elk IoT-/OT-systeem

4.2. Aangewezen medewerker of operationeel manager, indien aangewezen

4.2.1. houdt toezicht op de inventarisatie, plaatsing en configuratie van IoT-/OT-apparaten

4.2.2. registreert per apparaat de locatie, netwerktoewijzing en ondersteunende documentatie

4.2.3. ziet erop toe dat wijzigingen, zoals firmware-updates of vervanging van apparaten, worden gedocumenteerd

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

9. Vereisten voor herziening en actualisering

9.1. Jaarlijkse beoordeling

9.1.1. Dit beleid moet ten minste eenmaal per jaar door de GM worden beoordeeld

9.1.2. Bij de beoordeling moet worden vastgesteld of het beleid doeltreffend blijft, de huidige apparaattypen afdekt en aansluit op nieuwe risico's of technologieën

9.2. Actualisering op basis van triggers

9.2.1. Actualisering van het beleid moet ook worden gestart wanneer:

9.2.2. nieuwe typen IoT- of OT-systemen worden geïntroduceerd

9.2.3. leveranciers dreigingsadviezen of end-of-life-kennisgevingen uitbrengen

9.2.4. een incident of audit tekortkomingen in de IoT-/OT-beheersmaatregelen identificeert

9.2.5. nieuwe wet- en regelgeving of normen aanvullende vereisten opleggen

9.3. Documentatie en versiebeheer

9.3.1. Alle wijzigingen moeten worden gedocumenteerd, inclusief datum, versienummer en samenvatting van de wijzigingen

9.3.2. De GM moet historische beleidsversies bewaren ten behoeve van audits

9.4. Communicatie van wijzigingen

9.4.1. Wijzigingen in dit beleid moeten worden gedeeld met alle relevante medewerkers en leveranciers

9.4.2. Bijgewerkte versies moeten toegankelijk worden gemaakt via gedeelde schijven of in gedrukte vorm op installatielocaties of in controlecentra

10. Gerelateerde beleidsdocumenten en samenhang

10.1. Dit beleid moet worden geïmplementeerd in samenhang met de volgende gerelateerde mkb-beleidsdocumenten:

10.1.1. P4S – Beleid inzake toegangscontrole: dwingt toegangsbeheersmaatregelen op apparaatniveau, het gebruik van sterke wachtwoorden en geautoriseerde toegangsprocedures voor IoT- en OT-platforms af

10.1.2. P9S – Beleid inzake werken op afstand: voorkomt het gebruik van externe toegang tot IoT-/OT-dashboards via onveilige of niet-goedgekeurde kanalen

10.1.3. P17S – Beleid inzake gegevensbescherming en privacy: is van toepassing indien IoT-apparaten, zoals beveiligingscamera's, persoonsgegevens verwerken of vastleggen, en waarborgt naleving van de AVG

10.1.4. P30S – Incidentresponsbeleid: definieert procedures voor het detecteren, melden en afhandelen van IoT- of OT-incidenten, waaronder vermoedelijke manipulatie of operationeel falen

10.1.5. P36S – Beleid inzake sociale media en externe communicatie: waarborgt dat geen apparaatinformatie of netwerkinrichting extern wordt gedeeld zonder goedkeuring

10.2. Elk gerelateerd beleidsdocument versterkt de handhaving en praktische toepassing van dit beleid door gerichte procedurele richtlijnen te bieden.

11. Referentienormen en -kaders

11.1. ISO/IEC 27001

11.1.1. Clausule 6.1 – Risico-identificatie en risicobehandeling: vereist dat risico's met betrekking tot IoT- en OT-systemen systematisch worden beoordeeld en gemitigeerd

11.1.2. Clausule 8.1 – Operationele planning en beheersing: waarborgt veilige operationele beheersing van verbonden apparaten

11.2. ISO/IEC 27002

11.2.1. Beheersmaatregel 5.23 – Informatiebeveiliging voor het gebruik van operationele technologie: definieert veilig gebruik van OT in fysieke en digitale omgevingen

11.2.2. Beheersmaatregel 5.31 – Veilige configuratie van informatiesystemen: vereist geharde configuraties voor IoT-/OT-apparaten en het vermijden van onveilige standaardinstellingen

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – Integriteit van software, firmware en informatie: vereist validatie van de integriteit van firmware en updates

11.3.2. CM-7 – Beginsel van minimale functionaliteit: apparaten mogen geen ongebruikte of onveilige functies ingeschakeld hebben

11.3.3. AC-6 – Beginsel van minimale bevoegdheden: apparaattoegang moet beperkt blijven tot uitsluitend geautoriseerde gebruikers

11.3.4. PE-20 – Monitoring van bedrijfsmiddelen: fysieke en operationele monitoring van IoT- en OT-activa

11.3.5. SC-7 – Grensbeveiliging: segmentatie en beheersing van netwerkcommunicatie voor verbonden systemen

11.4. AVG (Verordening (EU) 2016/679)

11.4.1. Artikel 32 – Beveiliging van de verwerking: indien persoonsgegevens worden vastgelegd, bijvoorbeeld via beveiligingscamera's, moet de organisatie passende technische en organisatorische maatregelen (TOM's) implementeren om die verwerking te beveiligen

11.5. NIS2-richtlijn (Richtlijn (EU) 2022/2555)

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

11.5.2. Artikel 21(2)(d) – Veilige configuratie en veilig gebruik van apparaten

11.5.3. Artikel 21(2)(f) – Beveiliging van de toeleveringsketen en systemen

11.6. DORA (Verordening (EU) 2022/2554)

11.6.1. Artikel 9(2) – Reikwijdte van ICT-risicobeheer: omvat industriële en ingebedde apparaten die in operationele omgevingen worden gebruikt

11.6.2. Artikel 10(1) – ICT-continuïteit: vereist dat apparaatconfiguraties herstelbaarheid en weerbaarheidsmaatregelen ondersteunen

11.7. COBIT 2019

11.7.1. DSS01 – Manage Operations: van toepassing op het toezicht op technologieactiviteiten, waaronder fysieke apparaten

11.7.2. DSS05 – Manage Security Services: waarborgt dat verbonden systemen naar behoren worden gemonitord en beschermd

11.7.3. APO13 – Manage Security: versterkt beleidsdocumenten voor de bescherming van operationele activa binnen mkb-organisaties