					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P35S					Dokumenttitel: **Policy för säkerhet i IoT-/OT-system**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Anpassning till standarder och regelverk

Standard/reglering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausuler 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontroller 5.23, 5.31	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
EU:s dataskyddsförordning (GDPR)	Artikel 32	
EU:s NIS2-direktiv	Artikel 21(2)(a), (d), (f)	
EU:s DORA-förordning	Artikel 9(2), 10(1)	

1. Syfte

1.1. Denna policy fastställer obligatoriska regler för säker användning och hantering av Internet of Things (IoT) och operativa tekniska system (OT-system) inom organisationen. Dessa enheter kan omfatta smarta sensorer, säkerhetskameror, produktionsmaskiner, HVAC-styrenheter eller andra industriella system som är anslutna till nätverk.

1.2. Syftet med denna policy är att:

1.2.1. skydda fysisk och digital verksamhet mot störningar eller manipulation via bristfälligt säkrade uppkopplade enheter

1.2.2. säkerställa säker driftsättning, övervakning och underhåll av IoT- och OT-system

1.2.3. säkerställa efterlevnad av ISO/IEC 27001:2022, EU:s NIS2-direktiv och relaterade regelverk

1.2.4. tillhandahålla praktiska och verkställbara kontroller för små och medelstora företag som verkar i kontors-, lager- eller produktionsmiljöer

2. Omfattning

2.1. Denna policy gäller för alla personer som deltar i planering, installation, konfiguration, användning, support eller avveckling av IoT- eller OT-enheter. Detta omfattar:

2.1.1. anställda, entreprenörer, tredjepartsleverantörer och praktikanter med fysisk åtkomst eller fjärråtkomst till enheter

2.1.2. tredjepartsleverantörer eller servicetekniker som installerar eller underhåller uppkopplade system

2.1.3. verkställande direktör eller personal med ansvar för tillsyn av säkerhetspolicyer

2.2. Policyn omfattar:

2.2.1. IoT-enheter såsom smarta lås, övervakningssystem, smarta mätare eller skrivare

2.2.2. OT-system, inklusive PLC:er (programmerbara logikstyrningar), SCADA-paneler eller industriella gateway-enheter

2.2.3. stödjande hårdvara, administrationsapplikationer och kommunikationsnätverk som används av dessa system

2.3. Denna policy gäller på samtliga arbetsplatser: kontorsmiljöer, fjärrplatser, produktionsgolv och molnplattformar som gränssnittar med dessa enheter.

3. Mål

3.1. Säker driftsättning: Säkerställa att alla IoT-/OT-system är säkert konfigurerade innan de tas i drift i produktionsmiljön.

3.2. Begränsad exponering: Förhindra obehörig åtkomst, missbruk eller övertagande av uppkopplade enheter genom starka åtkomstkontroller och nätverkssegmentering.

3.3. Kontinuerlig övervakning: Upprätthålla insyn i IoT-/OT-driften genom aktivitetsloggning och övervakning av avvikande beteenden.

3.4. Leverantörsansvar: Säkerställa att tredjepartsleverantörer följer säkra rutiner för installation, konfiguration och underhåll.

3.5. Regulatorisk efterlevnad: Påvisa full efterlevnad av tillämpliga standarder såsom ISO/IEC 27001, EU:s dataskyddsförordning (GDPR) (om personuppgifter samlas in) och EU:s NIS2-direktiv för motståndskraft i kritisk infrastruktur.

4. Roller och ansvar

4.1. verkställande direktör (VD)

4.1.1. har det övergripande ansvaret för säkerheten i IoT- och OT-system

4.1.2. godkänner denna policy och säkerställer att den tillämpas i alla verksamhetsområden

4.1.3. verifierar att leverantörer och entreprenörer följer säkra rutiner för installation och underhåll

4.1.4. godkänner nätverksåtkomst för varje IoT-/OT-system

4.2. utsedd medarbetare eller driftansvarig (om sådan har utsetts)

4.2.1. ansvarar för tillgångsförteckning, placering och konfiguration av IoT-/OT-enheter

4.2.2. registrerar varje enhets placering, nätverkstilldelning och supportdokumentation

4.2.3. säkerställer att alla ändringar (t.ex. firmwareuppdateringar eller utbyte av enheter) dokumenteras

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Krav för granskning och uppdatering

9.1. Årlig granskning

9.1.1. Denna policy ska granskas minst en gång per år av VD

9.1.2. Granskningen ska bedöma om policyn fortsatt är effektiv, omfattar aktuella enhetstyper och är anpassad till nya risker eller tekniker

9.2. Utlösande faktorer för uppdatering

9.2.1. Policyuppdateringar ska också initieras när:

9.2.2. nya typer av IoT- eller OT-system införs

9.2.3. leverantörer utfärdar säkerhetsråd eller meddelanden om avveckling

9.2.4. en incident eller revision identifierar brister i IoT-/OT-kontroller

9.2.5. nya lagar eller standarder medför ytterligare krav

9.3. Dokumentation och versionshantering

9.3.1. Alla uppdateringar ska dokumenteras, inklusive datum, versionsnummer och ändringssammanfattning

9.3.2. VD ska bevara historiska versioner av policyn för revisionsändamål

9.4. Kommunikation av ändringar

9.4.1. Alla uppdateringar av policyn ska kommuniceras till relevant personal och relevanta leverantörer

9.4.2. Uppdaterade versioner ska göras tillgängliga via delade mappar eller tryckt material på installationsplatser eller i kontrollcentraler

10. Relaterade policyer och kopplingar

10.1. Denna policy ska tillämpas i linje med följande relaterade SME-policyer:

10.1.1. P4S – Åtkomstkontrollpolicy: reglerar inloggningskontroller på enhetsnivå, användning av starka lösenord och godkända åtkomstförfaranden för IoT- och OT-plattformar

10.1.2. P9S – Policy för distansarbete: förhindrar användning av fjärråtkomst till IoT-/OT-paneler via osäkra eller icke godkända kanaler

10.1.3. P17S – Policy för dataskydd och integritet: gäller om IoT-enheter (t.ex. säkerhetskameror) behandlar eller spelar in personuppgifter och säkerställer efterlevnad av EU:s dataskyddsförordning (GDPR)

10.1.4. P30S – Policy för incidenthantering: fastställer rutiner för att upptäcka, rapportera och hantera IoT- eller OT-incidenter, inklusive misstänkt manipulation eller driftfel

10.1.5. P36S – Policy för sociala medier och extern kommunikation: säkerställer att information om enheter eller nätverkstopologi inte delas externt utan godkännande

10.2. Varje relaterad policy stärker tillämpningen och den praktiska användningen av denna policy genom riktad processvägledning.

11. Referensstandarder och ramverk

11.1. ISO/IEC 27001

11.1.1. Klausul 6.1 – Riskidentifiering och riskbehandling: kräver att risker relaterade till IoT- och OT-system bedöms systematiskt och hanteras med riskreducerande åtgärder

11.1.2. Klausul 8.1 – Operativ planering och styrning: säkerställer säker operativ styrning av uppkopplade enheter

11.2. ISO/IEC 27002

11.2.1. Kontroll 5.23 – Informationssäkerhet vid användning av operativ teknik: definierar säker användning av OT i fysiska och digitala miljöer

11.2.2. Kontroll 5.31 – Säker konfiguration av informationssystem: kräver härdade konfigurationer för IoT-/OT-enheter och att osäkra standardinställningar undviks

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – Programvaru-, firmware- och informationsintegritet: kräver validering av integriteten hos firmware och uppdateringar

11.3.2. CM-7 – principen om minsta funktionalitet: enheter får inte ha oanvända eller osäkra funktioner aktiverade

11.3.3. AC-6 – principen om minsta privilegium: åtkomst till enheter ska begränsas till behöriga användare

11.3.4. PE-20 – övervakning av tillgångar: fysisk och operativ övervakning av IoT- och OT-tillgångar

11.3.5. SC-7 – gränsskydd: segmentering och styrning av nätverkskommunikation för uppkopplade system

11.4. EU:s dataskyddsförordning (GDPR) (2016/679)

11.4.1. Artikel 32 – Säkerhet i behandlingen: om personuppgifter registreras (t.ex. via övervakningskameror) ska organisationen införa lämpliga tekniska och organisatoriska åtgärder (TOM) för att skydda sådan behandling

11.5. EU:s NIS2-direktiv (2022/2555)

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

11.5.2. Artikel 21(2)(d) – säker konfiguration och användning av enheter

11.5.3. Artikel 21(2)(f) – säkerhet i leveranskedjan och systemsäkerhet

11.6. EU:s DORA-förordning (2022/2554)

11.6.1. Artikel 9(2) – omfattning för IKT-riskhantering: omfattar industriella och inbyggda enheter som används i operativa miljöer

11.6.2. Artikel 10(1) – IKT-kontinuitet: kräver att enhetskonfigurationer stödjer motståndskraft och återhämtningsåtgärder

11.7. COBIT 2019

11.7.1. DSS01 – Hantera drift: gäller tillsyn över teknikdrift, inklusive fysiska enheter

11.7.2. DSS05 – Hantera säkerhetstjänster: säkerställer att uppkopplade system övervakas och skyddas på ett korrekt sätt

11.7.3. APO13 – Hantera säkerhet: förstärker policyer för skydd av operativa tillgångar i små och medelstora företag