					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P35					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**

Anpassad till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Kapitel 8	
ISO/IEC 27002:2022	Kontroller 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	
EU:s GDPR	Artiklarna 5, 25, 32	
EU:s NIS2-direktiv	Artiklarna 21, 23	
EU:s DORA-förordning	Artiklarna 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Syfte

1.1 Denna policy fastställer obligatoriska informationssäkerhetskrav för driftsättning, drift, övervakning och avveckling av IoT-system och operativ teknik (OT-system) inom organisationen.

1.2 Den säkerställer att sådana system integreras i organisationens övergripande ledningssystem för cybersäkerhet och skyddas mot kompromettering, missbruk och operativt sabotage.

1.3 Policyn syftar till att införa robusta tekniska, organisatoriska och processuella kontroller för att skydda IoT-/OT-system som har gränssnitt mot fysisk infrastruktur, produktionsprocesser och säkerhetskritiska miljöer.

1.4 Den stöder regulatoriska skyldigheter och avtalskrav inom cybersäkerhet, säkerhet, miljöstyrning och kontinuitet.

2. Omfattning

2.1 Denna policy gäller för alla IoT- och OT-system, oavsett om de ägs av organisationen, leasas eller tillhandahålls av tredje part, som används i organisationens operativa, administrativa eller produktionsmiljöer.

2.2 System som omfattas inkluderar, men är inte begränsade till:

2.2.1 IoT-enheter såsom miljösensorer, passerkontrollsystem, smart belysning, övervakningsutrustning och kroppsburna enheter

2.2.2 OT-plattformar såsom programmerbara logikstyrningar (PLC), övervaknings- och styrsystem med datainsamling (SCADA), distribuerade styrsystem (DCS), HMI-paneler, MES-gränssnitt och fältstyrenheter

2.2.3 Industriella styrnätverk eller molnanslutna tillgångar som övervakar fysiska verksamhetsprocesser

2.3 Policyn omfattar:

2.3.1 Alla miljöer (lokala miljöer, edge och hanterade molnmiljöer)

2.3.2 Alla intressenter (interna användare, integratörer, tredjepartsleverantörer och entreprenörer)

2.3.3 Alla livscykelfaser (design, upphandling, driftsättning, drift och avveckling)

3. Mål

3.1 Att skydda IoT- och OT-infrastruktur mot interna och externa cybersäkerhetshot, inklusive överbelastningsattacker, obehörig åtkomst, spridning av utpressningsprogram och manipulation av firmware.

3.2 Att säkerställa att IoT-/OT-plattformar inte utgör vektorer för bryggattacker mellan IT och OT och inte komprometterar säkerhetskritiska system.

3.3 Att tillämpa principerna säkerhet genom design och försvar på djupet genom hela dessa teknologiers livscykel.

3.4 Att möjliggöra tillförlitlig, säker och verifierbar integration av IoT- och OT-plattformar i organisationens Security Operations Center (SOC) och incidenthanteringsplaner.

3.5 Att säkerställa att alla driftsättningar är i linje med kontroller enligt ISO/IEC 27001 och tillämplig sektorsspecifik vägledning (t.ex. IEC 62443, ISO/IEC 27019, NIST SP 800-82).

4. Roller och ansvar

4.1 Informationssäkerhetschef (CISO) / säkerhetsansvarig

4.1.1 Fastställer policyer och tekniska standarder för cybersäkerhet i IoT/OT.

4.1.2 Övervakar riskbedömningar, kontrollvalidering och samordning mellan avdelningar.

4.2 OT-ingenjörer / fastighets- och anläggningsansvariga

4.2.1 Validerar konfigurationer för OT-system och säkerställer efterlevnad av policyn i produktionsmiljöer.

4.2.2 Upprätthåller fysiska och logiska skyddsåtgärder för OT-systemens integritet och säkerhet.

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

9. Krav på granskning och uppdatering

9.1 Denna policy ska granskas minst årligen och uppdateras utifrån:

9.1.1 Förändringar i arkitektur, leverantörer eller plattformar för OT- eller IoT-system

9.1.2 Väsentliga regulatoriska uppdateringar (t.ex. ändringar i DORA-förordningen, EU:s NIS2-direktiv eller sektorsspecifika direktiv)

9.1.3 Nya sårbarheter eller hotmönster i styrsystem

9.1.4 Resultat från interna eller externa revisioner, penetrationstester eller red team-övningar

9.2 CISO, OT-säkerhetsansvarig och berörda avdelningschefer ansvarar gemensamt för att initiera granskningsprocessen.

9.3 Extra granskningar ska initieras efter:

9.3.1 Varje IoT-/OT-relaterad incident som leder till systemfel eller dataförlust

9.3.2 Införande av större ny utrustning, ny övervakningsprogramvara eller nya firmwareplattformar

9.3.3 Integration av smart edge computing eller AI-förstärkt automatisering på fältnivå

9.4 Alla policyändringar ska:

9.4.1 Dokumenteras i versionshistoriken och i registret för policyändringar

9.4.2 Kommuniceras till alla berörda användare, leverantörer och IT-/OT-operatörer

9.4.3 Godkännas på nytt av verkställande ledning

10. Relaterade policyer och kopplingar

10.1 Denna policy ska tillämpas tillsammans med och stöds av följande informationssäkerhetspolicyer:

10.1.1 P1 – Informationssäkerhetspolicy: Fastställer grundläggande säkerhetsprinciper som även gäller för säkerhet i IoT- och OT-system.

10.1.2 P3 – Policy för godtagbar användning: Definierar begränsningar för personlig och obehörig användning av enheter, även i operativa miljöer.

10.1.3 P6 – Riskhanteringspolicy: Vägleder bedömning, acceptans och riskreducering av risker kopplade till inbyggda system och styrsystem.

10.1.4 P12 – Policy för tillgångshantering: Säkerställer att alla IoT- och OT-system formellt inventeras och tilldelas ansvariga ägare.

10.1.5 P20 – Policy för slutpunktsskydd / skadlig kod: Gäller för anslutna styrenheter, smarta gateways och edge-system i produktion.

10.1.6 P22 – Loggnings- och övervakningspolicy: Omfattar även rutiner för insamling och granskning av loggar i OT-miljöer.

10.1.7 P30 – Policy för incidenthantering: Styr direkt hur överträdelser, avvikelser eller systemfel i IoT/OT ska eskaleras och hanteras.

10.1.8 P33 – Policy för övervakning av revision och regelefterlevnad: Tillhandahåller mekanismer för att säkerställa fortlöpande efterlevnad av denna policy.

11. Referensstandarder och ramverk

11.1 Denna policy är anpassad till internationellt erkända standarder och regulatoriska ramverk som säkerställer säkerhet, motståndskraft och regelefterlevnad för Internet of Things (IoT) och operativ teknik (OT-system) i industriella miljöer, produktionsmiljöer och verksamhetsmiljöer.

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

11.2.1 Kontroll 5.7 – hotinformation: Stödjer övervakning av OT-miljöer och identifiering av IoT-specifika sårbarheter.

11.2.2 Kontroll 5.23 – informationssäkerhet vid användning av molntjänster: Gäller när IoT-enheter har gränssnitt mot molnplattformar för telemetri, styrning eller analys.

11.2.3 Kontroll 5.27 – säker systemarkitektur och tekniska principer: Styr principer för säkerhet genom design för inbyggda system och styrnätverk.

11.2.4 Kontroll 5.31 – säkerhet i utvecklings- och supportprocesser: Säkerställer validering av programvara och firmware, patchkontroller samt leverantörskrav vid driftsättning i OT-miljöer.

11.2.5 Kontroll 5.36 – efterlevnad av rättsliga krav samt avtalskrav: Säkerställer att OT-tillgångar uppfyller krav avseende säkerhet, miljö och regulatorisk efterlevnad.

11.2.6 Dessa kontroller etablerar sammantaget bästa praxis för att skydda IoT-/OT-system genom hela deras livscykel, inklusive arkitekturdesign, säker driftsättning, patchning, anomalidetektering och efterlevnad av sektorsspecifika krav.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – gränsskydd: Säkerställer att OT-nätverk segmenteras och skyddas mot obehörig åtkomst.

11.3.2 SI-4 – systemövervakning: Kräver kontinuerlig övervakning och mekanismer för anomalidetektering i ICS-miljöer.

11.3.3 CM-2 – baskonfiguration: Kräver konfigurationsstyrning och enhetshärdning för IoT-/OT-plattformar.

11.3.4 AC-6 – principen om minsta privilegium: Gäller för användaråtkomst och leverantörers fjärrservice av inbyggda styrsystem.

11.3.5 PL-8 – säkerhets- och dataskyddsarkitekturer: Styr planering av säker systemintegration, särskilt vid moderniseringsprojekt inom OT.

11.4 EU:s GDPR (2016/679)

11.4.1 Artikel 5 – principer för behandling av personuppgifter: Gäller för IoT-plattformar som behandlar sensorbaserade data eller beteendedata som kan kopplas till individer.

11.4.2 Artikel 25 – dataskydd genom design och som standard: Kräver att dataskyddsåtgärder byggs in i IoT-produktdesign och firmware.

11.4.3 Artikel 32 – säkerhet i behandlingen: Kräver kryptering, åtkomstkontroll och säker kommunikation för dataöverföring från smarta enheter.

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

11.5.1 Artiklarna 21 och 23: Medför säkerhetsskyldigheter för väsentliga och viktiga verksamhetsutövare som använder OT-system. Dessa omfattar riskbedömning, incidentrapportering samt validering av leveranskedjan för IoT-/OT-leverantörer och firmwareintegritet.

11.6 EU:s DORA-förordning (2022/2554)

11.6.1 Artikel 9 – IKT-riskhantering: Kräver säker integration av inbyggda system och OT-teknik i styrningen av IKT-risker.

11.6.2 Artikel 10 – IKT-säkerhetskrav: Kräver skyddsåtgärder för sammanlänkade OT-plattformar som används i finansiella miljöer och miljöer för kritiska tjänster.

11.7 COBIT 2019

11.7.1 DSS05.01 – skydd mot skadlig kod: Omfattar detektering och hantering av ICS-specifika hot och kampanjer med skadlig kod riktade mot IoT.

11.7.2 BAI09.01 – fastställa och upprätthålla säkerhetskrav: Motsvarar säker tilldelning och drift av smart eller inbyggd infrastruktur.

11.7.3 APO13.02 – fastställa och upprätthålla en informationssäkerhetsplan: Kräver att OT-system och deras sårbarheter inkluderas i den verksamhetsövergripande cybersäkerhetsstrategin.