					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P35					Asiakirjan nimi: **IoT-/OT-tietoturvapolitiikka**							
Versio: 1.0		Voimaantulopäivä: 01.01.2025			Asiakirjan omistaja:							
X	Politiikka		Standardi		Menettely		Lomake		Rekisteri		Muu	

Muutoshistoria				
Muutosnumero	**Muutospäivä**	**Muutokset**	**Tarkistanut**	**Prosessin omistaja**

Hyväksynnät			
Nimi	**Tehtävänimike**	**Päivämäärä**	**Allekirjoitus**

Yhdenmukaisuus standardien ja sääntelyn kanssa

Standardi/sääntely	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohta 8	
ISO/IEC 27002:2022	Hallintakeinot 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:n GDPR	Artiklat 5, 25, 32	
EU:n NIS2-direktiivi	Artiklat 21, 23	
EU:n DORA-asetus	Artiklat 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Tarkoitus

1.1 Tämä politiikka määrittää organisaation IoT- ja OT-järjestelmien käyttöönottoa, käyttöä, valvontaa ja käytöstäpoistoa koskevat pakolliset tietoturvavaatimukset.

1.2 Politiikalla varmistetaan, että tällaiset järjestelmät integroidaan osaksi organisaation laajempaa kyberturvallisuuden hallintajärjestelmää ja suojataan vaarantumiselta, väärinkäytöltä ja toiminnalliselta sabotaasilta.

1.3 Politiikan tavoitteena on edellyttää vahvojen teknisten, organisatoristen ja menettelyllisten hallintakeinojen toteuttamista sellaisten IoT-/OT-järjestelmien suojaamiseksi, jotka liittyvät fyysiseen infrastruktuuriin, tuotantoprosesseihin ja turvallisuuskriittisiin ympäristöihin.

1.4 Politiikka tukee kyberturvallisuuteen, turvallisuuteen, ympäristöhallintaan ja jatkuvuuteen liittyvien sääntely- ja sopimusvelvoitteiden täyttämistä.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia organisaation toiminnallisissa, hallinnollisissa tai tuotantoympäristöissä käytettäviä IoT- ja OT-järjestelmiä riippumatta siitä, ovatko ne organisaation omistamia, vuokrattuja vai kolmannen osapuolen toimittamia.

2.2 Soveltamisalaan kuuluvat muun muassa:

2.2.1 IoT-laitteet, kuten ympäristöanturit, kulunvalvontaratkaisut, älykäs valaistus, valvontalaitteet ja puettavat laitteet

2.2.2 OT-alustat, kuten PLC-, SCADA-, DCS- ja HMI-järjestelmät, MES-rajapinnat sekä kenttäohjaimet

2.2.3 Teolliset ohjausverkot tai pilveen liitetyt resurssit, joilla valvotaan fyysisiä toimintoja

2.3 Politiikka kattaa:

2.3.1 Kaikki ympäristöt (paikalliset ympäristöt, reunaympäristöt, pilvihallinnoidut ympäristöt)

2.3.2 Kaikki sidosryhmät (sisäiset käyttäjät, integraattorit, kolmannen osapuolen toimittajat, urakoitsijat)

2.3.3 Kaikki elinkaaren vaiheet (suunnittelu, hankinta, käyttöönotto, käyttö, käytöstäpoisto)

3. Tavoitteet

3.1 Suojata IoT- ja OT-infrastruktuuri sisäisiltä ja ulkoisilta kyberturvallisuusuhilta, mukaan lukien palvelunestohyökkäykset, luvaton pääsy, kiristysohjelmien leviäminen ja laiteohjelmiston manipulointi.

3.2 Varmistaa, etteivät IoT-/OT-alustat muodosta hyökkäysväylää IT- ja OT-ympäristöjen välille tai vaaranna turvallisuuskriittisiä järjestelmiä.

3.3 Soveltaa sisäänrakennetun tietoturvan ja kerroksellisen puolustuksen periaatteita näiden teknologioiden koko elinkaaren ajan.

3.4 Mahdollistaa IoT- ja OT-alustojen luotettava, turvallinen ja todennettavissa oleva integrointi organisaation tietoturvavalvomoon (SOC) ja poikkeamienhallintasuunnitelmiin.

3.5 Varmistaa, että kaikki käyttöönotot ovat ISO/IEC 27001:n hallintakeinojen ja soveltuvien toimialakohtaisten ohjeiden mukaisia (esim. IEC 62443, ISO 27019, NIST SP 800-82).

4. Roolit ja vastuut

4.1 Tietoturvajohtaja (CISO) / tietoturvavastaava

4.1.1 Määrittää IoT-/OT-kyberturvallisuutta koskevat politiikat ja tekniset standardit

4.1.2 Valvoo riskiarviointeja, hallintakeinojen validointia ja toimintojen välistä koordinointia

4.2 OT-insinöörit / kiinteistö- ja tuotantolaitosjohtajat

4.2.1 Varmistavat OT-järjestelmien konfiguraatiot ja huolehtivat politiikan noudattamisesta tuotantoalueilla

4.2.2 Ylläpitävät OT-ympäristön eheyttä ja turvallisuutta tukevia fyysisiä ja loogisia suojauskeinoja

[... Jaksot 4.3–8 eivät sisälly tähän esikatseluun. Osta koko asiakirja saadaksesi täyden sisällön. ...]

9. Katselmointi- ja päivitysvaatimukset

9.1 Tämä politiikka on katselmoitava vähintään vuosittain ja päivitettävä seuraavien perusteella:

9.1.1 Muutokset OT- tai IoT-järjestelmäarkkitehtuurissa, toimittajissa tai alustoissa

9.1.2 Merkittävät sääntelypäivitykset (esim. DORA-asetuksen, EU:n NIS2-direktiivin tai toimialakohtaisten direktiivien muutokset)

9.1.3 Uusien haavoittuvuuksien tai uhkamallien ilmeneminen ohjausjärjestelmissä

9.1.4 Sisäisten tai ulkoisten auditointien, tunkeutumistestausten tai red team -harjoitusten havainnot

9.2 Tietoturvajohtaja, OT-tietoturvavastaava ja asiaankuuluvien toimintojen johtajat vastaavat katselmointiprosessin käynnistämisestä yhdessä.

9.3 Välikatselmointi on käynnistettävä seuraavien jälkeen:

9.3.1 Mikä tahansa IoT-/OT-ympäristöön liittyvä poikkeama, joka johtaa järjestelmähäiriöön tai tietojen menetykseen

9.3.2 Merkittävän uuden laitteiston, valvontaohjelmiston tai laiteohjelmistoalustan käyttöönotto

9.3.3 Älykkään reunalaskennan tai tekoälyllä tehostetun automaation integrointi kenttätasolle

9.4 Kaikki politiikkamuutokset on:

9.4.1 Dokumentoitava versiohistoriassa ja politiikkamuutosrekisterissä

9.4.2 Viestittävä kaikille vaikutuksen piirissä oleville käyttäjille, toimittajille ja IT-/OT-operaattoreille

9.4.3 Hyväksytettävä uudelleen ylimmällä johdolla

10. Liittyvät politiikat ja kytkennät

10.1 Tätä politiikkaa sovelletaan yhdessä seuraavien tietoturvapolitiikkojen kanssa, jotka tukevat sen toimeenpanoa:

10.1.1 P1 – Tietoturvapolitiikka: Määrittää perustavanlaatuiset tietoturvaperiaatteet, jotka ulottuvat myös IoT- ja OT-järjestelmien tietoturvaan.

10.1.2 P3 – Hyväksyttävän käytön politiikka: Määrittää henkilökohtaisten ja luvattomien laitteiden käyttöä koskevat rajoitukset myös toiminnallisissa ympäristöissä.

10.1.3 P6 – Riskienhallintapolitiikka: Ohjaa sulautettuihin ja ohjausjärjestelmiin liittyvien riskien arviointia, hyväksyntää ja lieventämistä.

10.1.4 P12 – Omaisuudenhallintapolitiikka: Varmistaa, että kaikki IoT- ja OT-järjestelmät inventoidaan muodollisesti ja niille nimetään vastuulliset omistajat.

10.1.5 P20 – Päätelaitesuojaus- / haittaohjelmapolitiikka: Koskee tuotantoympäristön liitettyjä ohjaimia, älykkäitä yhdyskäytäviä ja reunajärjestelmiä.

10.1.6 P22 – Lokitus- ja seurantapolitiikka: Ulottuu myös OT-ympäristöjen lokien keräämiseen ja katselmointimenettelyihin.

10.1.7 P30 – Poikkeamienhallintapolitiikka: Määrittää suoraan, miten IoT-/OT-murrot, poikkeamat tai järjestelmähäiriöt on eskaloitava ja hallittava.

10.1.8 P33 – Auditointi- ja vaatimustenmukaisuuden seurantapolitiikka: Tarjoaa varmistusmekanismit tämän politiikan jatkuvan noudattamisen todentamiseksi.

11. Viitestandardit ja viitekehykset

11.1 Tämä politiikka on linjattu kansainvälisesti tunnustettujen standardien ja sääntelyviitekehysten kanssa, joilla varmistetaan teollisissa, tuotannollisissa ja yritysympäristöissä käytettävien esineiden internetin (IoT) ja operatiivisen teknologian (OT) järjestelmien tietoturva, toimintakyvyn palautumiskyky ja vaatimustenmukaisuus.

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

11.2.1 Hallintakeino 5.7 – Uhkatiedustelu: Tukee OT-ympäristöjen valvontaa ja IoT-ympäristöön liittyvien haavoittuvuuksien tunnistamista.

11.2.2 Hallintakeino 5.23 – Pilvipalvelujen käytön tietoturva: Soveltuu tilanteisiin, joissa IoT-laitteet liittyvät pilvialustoihin telemetriaa, ohjausta tai analytiikkaa varten.

11.2.3 Hallintakeino 5.27 – Turvallinen järjestelmäarkkitehtuuri ja suunnitteluperiaatteet: Ohjaa sisäänrakennetun tietoturvan periaatteita sulautetuissa järjestelmissä ja ohjausverkoissa.

11.2.4 Hallintakeino 5.31 – Tietoturva kehitys- ja tukiprosesseissa: Edellyttää ohjelmisto- ja laiteohjelmistovalidointia, päivityshallintaa ja toimittajavaatimuksia OT-käyttöönotossa.

11.2.5 Hallintakeino 5.36 – Lakiin ja sopimuksiin perustuvien vaatimusten noudattaminen: Varmistaa, että OT-omaisuus täyttää turvallisuuteen, ympäristöön ja sääntelyyn liittyvät vaatimukset.

11.2.6 Nämä hallintakeinot muodostavat yhdessä parhaat käytännöt IoT-/OT-järjestelmien suojaamiselle koko niiden elinkaaren ajan, mukaan lukien arkkitehtuurin suunnittelu, turvallinen käyttöönotto, päivitykset, poikkeamien havaitseminen ja toimialakohtaisten vaatimusten noudattaminen.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-7 – Rajasuojaukset: Varmistaa, että OT-verkot on segmentoitu ja suojattu luvattomalta pääsyltä.

11.3.2 SI-4 – Järjestelmien valvonta: Edellyttää jatkuvan valvonnan ja poikkeamien havaitsemismekanismien toteuttamista ICS-ympäristöissä.

11.3.3 CM-2 – Peruskonfiguraatio: Edellyttää IoT-/OT-alustojen konfiguraatiohallintaa ja koventamista.

11.3.4 AC-6 – Vähimmät oikeudet: Soveltuu käyttäjäoikeuksiin ja sulautettujen ohjausjärjestelmien toimittajien etähuoltoon.

11.3.5 PL-8 – Tietoturva- ja tietosuoja-arkkitehtuurit: Ohjaa turvallisen järjestelmäintegraation suunnittelua erityisesti OT-modernisointihankkeissa.

11.4 EU:n GDPR (2016/679)

11.4.1 Artikla 5 – Henkilötietojen käsittelyä koskevat periaatteet: Soveltuu IoT-alustoihin, jotka käsittelevät anturipohjaista tai käyttäytymiseen liittyvää tietoa, joka voidaan yhdistää yksilöihin.

11.4.2 Artikla 25 – Sisäänrakennettu ja oletusarvoinen tietosuoja: Edellyttää, että tietosuojatoimenpiteet sisällytetään IoT-tuotteiden suunnitteluun ja laiteohjelmistoon.

11.4.3 Artikla 32 – Käsittelyn turvallisuus: Edellyttää salausta, käyttöoikeuksien hallintaa ja suojattua viestintää älylaitteiden tiedonsiirrossa.

11.5 EU:n NIS2-direktiivi (2022/2555)

11.5.1 Artiklat 21 ja 23: Asettavat tietoturvavelvoitteita keskeisille ja tärkeille toimijoille, jotka käyttävät OT-järjestelmiä. Näihin kuuluvat riskiarviointi, poikkeamailmoitukset sekä IoT-/OT-toimittajien ja laiteohjelmiston eheyden arviointi toimitusketjussa.

11.6 EU:n DORA-asetus (2022/2554)

11.6.1 Artikla 9 – Tieto- ja viestintäteknologian riskienhallinta: Edellyttää sulautettujen järjestelmien ja OT-teknologioiden turvallista integrointia tieto- ja viestintäteknologian riskienhallinnan hallintamalliin.

11.6.2 Artikla 10 – Tieto- ja viestintäteknologian tietoturvavaatimukset: Edellyttää suojaavia toimenpiteitä toisiinsa liitetyille OT-alustoille, joita käytetään finanssi- ja kriittisten palvelujen ympäristöissä.

11.7 COBIT 2019

11.7.1 DSS05.01 – Suojaus haittaohjelmia vastaan: Kattaa ICS-ympäristöihin kohdistuvien uhkien ja IoT-haittaohjelmakampanjoiden havaitsemisen ja niihin vastaamisen.

11.7.2 BAI09.01 – Tietoturvavaatimusten määrittäminen ja ylläpito: Vastaa älykkään tai sulautetun infrastruktuurin turvallista toimittamista ja käyttöä.

11.7.3 APO13.02 – Tietoturvasuunnitelman määrittäminen ja ylläpito: Edellyttää OT-järjestelmien ja niiden haavoittuvuuksien sisällyttämistä organisaation laajuiseen kyberturvallisuusstrategiaan.