					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P35S					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 sääntelyvaatimusten kanssa

Standardi/sääntely	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohdat 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontrollit 5.23, 5	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
EU:n GDPR	Artikla 32	
EU:n NIS2-direktiivi	Artikla 21(2)(a), (d), (f)	
EU:n DORA-asetus	Artikla 9(2), 10(1)	

1. Tarkoitus

1.1. Tämä politiikka määrittää pakolliset vaatimukset esineiden internetin (IoT) ja operatiivisen teknologian (OT) laitteiden turvalliselle käytölle ja hallinnalle organisaatiossa. Näihin laitteisiin voivat kuulua esimerkiksi älyanturit, valvontakamerat, tuotantokoneet, LVI-ohjaimet tai muut verkkoon liitetyt teolliset järjestelmät.

1.2. Tämän politiikan tarkoituksena on:

1.2.1. suojata fyysisiä ja digitaalisia toimintoja häiriöiltä tai manipuloinnilta, joita puutteellisesti suojatut verkkoon liitetyt laitteet voivat aiheuttaa

1.2.2. varmistaa IoT- ja OT-järjestelmien turvallinen käyttöönotto, valvonta ja ylläpito

1.2.3. varmistaa vaatimustenmukaisuus ISO/IEC 27001:2022 -standardin, EU:n NIS2-direktiivin ja muiden sovellettavien sääntelykehysten kanssa

1.2.4. tarjota käytännölliset ja toimeenpantavat kontrollit pk-yrityksille, jotka toimivat toimisto-, varasto- tai tuotantoympäristöissä

2. Soveltamisala

2.1. Tätä politiikkaa sovelletaan kaikkiin henkilöihin, jotka osallistuvat IoT- tai OT-laitteiden suunnitteluun, asennukseen, konfigurointiin, käyttöön, tukemiseen tai käytöstä poistoon. Näihin kuuluvat:

2.1.1. työntekijät, sopimuskumppanit tai harjoittelijat, joilla on fyysinen pääsy laitteisiin tai etäkäyttöoikeus niihin

2.1.2. kolmannet osapuolet tai huoltoteknikot, jotka asentavat tai ylläpitävät verkkoon liitettyjä järjestelmiä

2.1.3. toimitusjohtaja tai henkilöstö, joka vastaa tietoturvapolitiikkojen valvonnasta

2.2. Politiikka kattaa:

2.2.1. IoT-laitteet, kuten älylukot, valvontajärjestelmät, älymittarit tai tulostimet

2.2.2. OT-järjestelmät, mukaan lukien ohjelmoitavat logiikkaohjaimet (PLC), SCADA-paneelit tai teolliset yhdyskäytävät

2.2.3. näiden järjestelmien käyttämät tukilaitteistot, hallintasovellukset ja viestintäverkot

2.3. Tätä politiikkaa sovelletaan kaikissa toimintaympäristöissä: toimistoympäristöissä, etäkohteissa, tuotantotiloissa ja pilvialustoilla, jotka ovat yhteydessä näihin laitteisiin.

3. Tavoitteet

3.1. Turvallinen käyttöönotto: varmistetaan, että kaikki IoT-/OT-järjestelmät on konfiguroitu turvallisesti ennen niiden liittämistä tuotantoympäristöön.

3.2. Altistumisen rajoittaminen: estetään verkkoon liitettyjen laitteiden luvaton käyttö, väärinkäyttö tai haltuunotto toteuttamalla vahva pääsynhallinta ja verkon segmentointi.

3.3. Jatkuva valvonta: ylläpidetään näkyvyyttä IoT-/OT-toimintoihin kirjaamalla toimintaa lokiin ja seuraamalla poikkeavaa käyttäytymistä.

3.4. Toimittajavastuu: varmistetaan, että kolmannen osapuolen palveluntarjoajat noudattavat turvallisia asennus-, konfigurointi- ja ylläpitokäytäntöjä.

3.5. Sääntelyvaatimusten noudattaminen: osoitetaan yhdenmukaisuus sovellettavien standardien, kuten ISO 27001:n, EU:n GDPR:n (jos henkilötietoja kerätään) ja EU:n NIS2-direktiivin kanssa kriittisen infrastruktuurin häiriönsietokyvyn osalta.

4. Roolit ja vastuut

4.1. toimitusjohtaja

4.1.1. vastaa kokonaisuudessaan IoT- ja OT-järjestelmien tietoturvasta

4.1.2. hyväksyy tämän politiikan ja varmistaa, että sitä sovelletaan kaikissa toimintaympäristöissä

4.1.3. varmistaa, että toimittajat ja sopimuskumppanit noudattavat turvallisia käyttöönotto- ja ylläpitokäytäntöjä

4.1.4. hyväksyy kaikkien IoT-/OT-järjestelmien liittämisen verkkoon

4.2. nimetty työntekijä tai operatiivinen päällikkö (jos nimetty)

4.2.1. vastaa IoT-/OT-laitteiden inventoinnista, sijoittelusta ja konfiguroinnista

4.2.2. kirjaa kunkin laitteen sijainnin, verkkoliitynnän ja tukidokumentaation

4.2.3. varmistaa, että kaikki muutokset, kuten laiteohjelmistopäivitykset tai laitevaihdot, dokumentoidaan

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

9. Katselmointi- ja päivitysvaatimukset

9.1. Vuosittainen katselmointi

9.1.1. Toimitusjohtajan on katselmoitava tämä politiikka vähintään kerran vuodessa

9.1.2. Katselmoinnissa on arvioitava, onko politiikka edelleen tehokas, kattaako se nykyiset laitetyypit ja vastaako se uusiin riskeihin tai teknologioihin

9.2. Tapahtumaperusteiset päivitykset

9.2.1. Politiikan päivitys on käynnistettävä myös silloin, kun:

9.2.2. otetaan käyttöön uusia IoT- tai OT-järjestelmätyyppejä

9.2.3. toimittajat julkaisevat tietoturvatiedotteita tai elinkaaren päättymistä koskevia ilmoituksia

9.2.4. tietoturvapoikkeama tai auditointi tunnistaa puutteita IoT-/OT-kontrolleissa

9.2.5. uudet lait tai standardit asettavat lisävaatimuksia

9.3. Dokumentointi ja versionhallinta

9.3.1. Kaikki päivitykset on dokumentoitava, mukaan lukien päivämäärä, versionumero ja muutosten yhteenveto

9.3.2. Toimitusjohtajan on säilytettävä politiikan aiemmat versiot auditointitarkoituksia varten

9.4. Muutoksista tiedottaminen

9.4.1. Kaikista politiikan päivityksistä on tiedotettava kaikille asiaankuuluville työntekijöille ja toimittajille

9.4.2. Päivitetyt versiot on asetettava saataville yhteiskäyttöisissä kansioissa tai painettuina aineistoina asennuspaikoissa tai ohjauskeskuksissa

10. Liittyvät politiikat ja yhteydet

10.1. Tämä politiikka on toimeenpantava yhdenmukaisesti seuraavien siihen liittyvien pk-yrityksen politiikkojen kanssa:

10.1.1. P4S – Pääsynhallintapolitiikka: määrittää laitetason kirjautumiskontrollit, vahvojen salasanojen käytön ja valtuutettua pääsyä koskevat menettelyt IoT- ja OT-alustoille

10.1.2. P9S – Etätyöpolitiikka: estää etäkäytön IoT-/OT-hallintanäkymiin suojaamattomien tai hyväksymättömien kanavien kautta

10.1.3. P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: sovelletaan, jos IoT-laitteet, kuten valvontakamerat, käsittelevät tai tallentavat henkilötietoja, jotta EU:n GDPR:n vaatimukset täyttyvät

10.1.4. P30S – Tietoturvapoikkeamien hallintapolitiikka: määrittää menettelyt IoT- tai OT-poikkeamien havaitsemiselle, ilmoittamiselle ja ratkaisemiselle, mukaan lukien epäilty manipulointi tai operatiivinen häiriö

10.1.5. P36S – Sosiaalisen median ja ulkoisen viestinnän politiikka: varmistaa, ettei laitteita koskevia tietoja tai verkkorakennetta jaeta organisaation ulkopuolelle ilman hyväksyntää

10.2. Kukin liittyvä politiikka tukee tämän politiikan soveltamista ja käytännön toimeenpanoa tarjoamalla kohdennettua menettelyohjeistusta

11. Viitestandardit ja viitekehykset

11.1. ISO/IEC 27001

11.1.1. Kohta 6.1 – riskien tunnistaminen ja käsittely: edellyttää, että IoT- ja OT-järjestelmiin liittyvät riskit arvioidaan ja niitä käsitellään järjestelmällisesti

11.1.2. Kohta 8.1 – toiminnan suunnittelu ja ohjaus: varmistaa verkkoon liitettyjen laitteiden turvallisen operatiivisen hallinnan

11.2. ISO/IEC 27002

11.2.1. Kontrolli 5.23 – operatiivisen teknologian käytön tietoturvallisuus: määrittää OT:n turvallisen käytön fyysisissä ja digitaalisissa ympäristöissä

11.2.2. Kontrolli 5.31 – tietojärjestelmien turvallinen konfigurointi: edellyttää IoT-/OT-laitteiden kovennettuja asetuksia ja turvattomien oletusasetusten välttämistä

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – ohjelmistojen, laiteohjelmistojen ja tiedon eheys: edellyttää laiteohjelmistojen ja päivitysten eheyden validointia

11.3.2. CM-7 – vähimmäistoiminnallisuus: laitteissa ei saa olla käytössä käyttämättömiä tai turvattomia toimintoja

11.3.3. AC-6 – vähimmän etuoikeuden periaate: laitteiden käyttö on rajoitettava vain valtuutetuille käyttäjille

11.3.4. PE-20 – omaisuuden seuranta: IoT- ja OT-omaisuuserien fyysinen ja operatiivinen seuranta

11.3.5. SC-7 – rajasuojaukset: verkkoon liitettyjen järjestelmien verkkoviestinnän segmentointi ja hallinta

11.4. EU:n GDPR (2016/679)

11.4.1. Artikla 32 – käsittelyn turvallisuus: jos henkilötietoja kerätään esimerkiksi valvontakameroiden kautta, organisaation on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet tällaisen käsittelyn suojaamiseksi

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

11.5.1. Artikla 21(2)(a) – riskienhallintatoimenpiteet

11.5.2. Artikla 21(2)(d) – laitteiden turvallinen konfigurointi ja käyttö

11.5.3. Artikla 21(2)(f) – toimitusketjun ja järjestelmien tietoturva

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

11.6.1. Artikla 9(2) – ICT-riskien hallinnan soveltamisala: kattaa operatiivisissa ympäristöissä käytettävät teolliset ja sulautetut laitteet

11.6.2. Artikla 10(1) – ICT-jatkuvuus: edellyttää, että laitemääritykset tukevat häiriönsietokykyä ja palautumistoimia

11.7. COBIT 2019

11.7.1. DSS01 – operaatioiden hallinta: soveltuu teknologiaoperaatioiden valvontaan, mukaan lukien fyysiset laitteet

11.7.2. DSS05 – tietoturvapalvelujen hallinta: varmistaa, että verkkoon liitettyjä järjestelmiä valvotaan ja suojataan asianmukaisesti

11.7.3. APO13 – tietoturvan hallinta: vahvistaa politiikkoja operatiivisten omaisuuserien suojaamiseksi pk-yrityksissä