					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P08S					Asiakirjan nimi: **tietoturvatietoisuus- ja koulutuspolitiikka**							
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	Huomio
ISO/IEC 27001:2022	Luku 7	
ISO/IEC 27002:2022	Kontrolli 6	
NIST SP 800-53 Rev.5	AT-2, AT-4	
EU:n NIS2-direktiivi	Artikla 21(2)(i)	
EU:n DORA-asetus	Artikla 13	
COBIT 2019	BAI08, DSS	
EU:n GDPR	Artikla 32, 39	

1. Tarkoitus

1.1. Tällä politiikalla varmistetaan, että kaikki työntekijät ja urakoitsijat ymmärtävät tietoturvaan liittyvät vastuunsa.

1.2. Politiikan tavoitteena on vähentää inhimillisten virheiden todennäköisyyttä, parantaa kykyä havaita ja ilmoittaa poikkeamia sekä edistää tietoturvatietoista toimintakulttuuria koko organisaatiossa.

1.3. Politiikka tukee ISO/IEC 27001:n, NIS2:n, GDPR:n ja DORA:n vaatimustenmukaisuutta tekemällä tietoturvatietoisuudesta osan päivittäistä työskentelyä ja roolipohjaisia odotuksia.

2. Soveltamisala

2.1. Tämä politiikka koskee kaikkia työntekijöitä, urakoitsijoita, harjoittelijoita ja kolmansia osapuolia, joilla on pääsy yrityksen järjestelmiin tai tietoihin.

2.2. Politiikka kattaa:

2.2.1. perehdytyksen aikaisen tietoturvatietoisuuskoulutuksen uudelle henkilöstölle

2.2.2. vuosittaisen kertauskoulutuksen

2.2.3. ad hoc -tietoisuustoimet (esim. poikkeamiin liittyvät tiedotteet, julisteet tai vinkit)

2.3. Politiikkaa sovelletaan kaikkiin työtehtäviin, osastoihin ja työskentelypaikkoihin.

3. Tavoitteet

3.1. Varmistetaan, että koko henkilöstö saa oikea-aikaista, ymmärrettävää ja olennaista tietoturvatietoisuuskoulutusta.

3.2. Työntekijöille annetaan valmiudet tunnistaa ja välttää yleisiä uhkia, kuten tietojenkalastelua, haittaohjelmia ja tietovuotoja.

3.3. Koulutusten suorittamisesta ylläpidetään dokumentaatiota, jolla voidaan osoittaa lakisääteisten, sopimuksellisten ja auditointivaatimusten noudattaminen.

3.4. Koulutussisältö pidetään ajan tasalla siten, että se vastaa organisaation politiikkoja, uhkia ja sovellettavia sääntelyvaatimuksia.

3.5. Henkilöstössä edistetään ennakoivaa toimintatapaa, jossa tietoturva nähdään osana päivittäistä vastuuta.

4. Roolit ja vastuut

4.1. Toimitusjohtaja

4.1.1. Hyväksyy koulutusvaatimukset ja varmistaa, että tarvittavat resurssit osoitetaan.

4.1.2. Katselmoi suoritusraportit ja eskaloi laiminlyönnit tarvittaessa.

4.2. Toimistopäällikkö / henkilöstöhallinto

4.2.1. Koordinoi uusien työntekijöiden koulutusten sekä vuosittaisten kertauskoulutusten toteutuksen.

4.2.2. Ylläpitää koulutustiedot ja koulutuslokit.

4.2.3. Varmistaa henkilöstön kuittaukset keskeisistä tietoturvapolitiikoista ja salassapitosopimuksista.

[... 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 ja henkilöstöhallinnon on katselmoitava tämä politiikka vuosittain varmistaakseen, että se vastaa ajantasaisia riskejä, sääntelyvaatimuksia ja henkilöstön tarpeita.

9.2. Väliin tulevat päivitykset

9.2.1. Politiikka ja koulutussisältö on lisäksi katselmoitava ja päivitettävä seuraavien tapahtumien jälkeen:

9.2.1.1. merkittävä tietoturvapoikkeama

9.2.1.2. oikeudelliset tai sopimukselliset muutokset

9.2.1.3. organisaatiomuutos tai järjestelmämigraatiot

9.3. Versionhallinta ja jakelu

9.3.1. Jokaisen päivityksen on sisällettävä:

9.3.1.1. versionumero ja voimaantulopäivä

9.3.1.2. yhteenveto muutoksista

9.3.1.3. toimitusjohtajan hyväksyntä

9.3.1.4. kaikkien aiempien versioiden arkisto, jota säilytetään vähintään kolme vuotta

9.4. Viestintä henkilöstölle

9.4.1. Politiikan päivityksistä on tiedotettava koko henkilöstölle, ja kuittaus on hankittava, jos muutokset ovat olennaisia.

10. Liittyvät politiikat ja yhteydet

10.1. Tämä politiikka tukee seuraavia politiikkoja:

10.1.1. P2S – Hallintoroolien ja -vastuiden politiikka: määrittää vastuut koulutuksen koordinoinnista ja valvonnasta

10.1.2. P3S – Hyväksyttävän käytön politiikka: vahvistaa koulutuksessa käsiteltäviä käyttäytymisodotuksia

10.1.3. P4S – Pääsynhallintapolitiikka: varmistaa, että käyttäjät ymmärtävät käyttöoikeuksien tietoturvan merkityksen

10.1.4. P7S – Perehdytys- ja työsuhteen päättämispolitiikka: sisällyttää koulutuksen osaksi aloittamisprosessia

10.1.5. P30S – Tietoturvapoikkeamien hallintapolitiikka: varmistaa, että henkilöstö osaa ilmoittaa poikkeamista viipymättä ja oikein

11. Viitestandardit ja viitekehykset

11.1. ISO/IEC 27001

11.1.1. Luku 7.3 – edellyttää, että organisaatio varmistaa henkilöstön tietoisuuden omista vastuistaan ja tietoturvavaikutuksista

11.2. ISO/IEC 27002

11.2.1. Kontrolli 6.3 – määrittää odotukset tietoturvakoulutuksen soveltamisalalle ja toteutukselle

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – edellyttää tietoisuuskoulutusta käyttäjille, joilla on pääsy järjestelmiin

11.3.2. AT-4 – kattaa roolipohjaisen koulutuksen ja vaatimustenvastaisuuden seuraukset

11.4. EU:n GDPR

11.4.1. Artikla 32 – edellyttää tietoturvatoimenpiteitä, mukaan lukien henkilöstön koulutus henkilötietojen suojaamiseksi

11.4.2. Artikla 39 – edellyttää, että tietosuojavastaava valvoo tietoisuus- ja koulutustoimia soveltuvin osin

11.5. EU:n NIS2-direktiivi

11.5.1. Artikla 21(2)(i) – edellyttää jatkuvia kyberturvallisuutta koskevia tietoisuus- ja koulutusohjelmia

11.6. EU:n DORA-asetus

11.6.1. Artikla 13 – edellyttää, että finanssialan toimijat toteuttavat koulutusta kaikelle henkilöstölle, jolla on tieto- ja viestintätekniikkaan liittyviä vastuita

11.7. COBIT 2019

11.7.1. BAI08 – Manage Knowledge: varmistaa, että henkilöstö on pätevää ja koulutettua

11.7.2. DSS05 – Manage Security Services: korostaa tietoisuutta keskeisenä suojaavana kontrollina