					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P08					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	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	Lauseke 7.3, liitteen A kontrolli 6.3	Määrittää tämän politiikan kattamat tietoisuus- ja koulutusvaatimukset
ISO/IEC 27002:2022	Kontrolli 6	Tukee tehtävärooliin soveltuvaa roolipohjaista tietoisuus- ja koulutustoimintaa
NIST SP 800-53 Rev.5	AT-1–AT-5	Vastaa politiikkoja ja menettelyjä, tietoisuuskoulutusta, roolipohjaista koulutusta, koulutustallenteita ja yhteydenpitoa tietoturvaryhmiin koskevia vaatimuksia
EU:n GDPR	Artiklat 32, 39; johdanto-osan kappale 78	Edellyttää henkilötietoja käsittelevän henkilöstön kouluttamista sekä henkilöstön yleisen tietoisuuden varmistamista
EU:n NIS2-direktiivi	Artiklat 21(2)(a, b), 21(3)	Edellyttää riski- ja tietoturvakoulutusta koskevia politiikkoja ja tietoisuusaloitteita
EU:n DORA-asetus	Artiklat 5, 8, 13	Edellyttää ICT-riskitietoisuutta ja koulutusta osana häiriönsietokykyä tukevia kontrollitoimia
COBIT 2019	APO07, DSS05, MEA	Vahvistaa henkilöstön tietoisuutta, käyttäjäkoulutusta ja vaatimustenmukaisuuden seurantaa

1. Tarkoitus

1.1 Tämä politiikka määrittää muodollisen viitekehyksen sen varmistamiseksi, että koko henkilöstö on tietoinen tietoturvavastuistaan ja saa koulutuksen, joka on tarpeen tietovarantojen luottamuksellisuuden, eheyden ja saatavuuden suojaamiseksi.

1.2 Se tukee ISO/IEC 27001 -standardin lauseketta 7.3 ja liitteen A kontrollia 6.3 edellyttämällä jäsenneltyä ja riskitietoista tietoisuus- ja koulutusohjelmaa, joka on mukautettu organisaation rooleihin ja muuttuviin uhkiin.

1.3 Politiikka edistää inhimillisiin tekijöihin liittyvien haavoittuvuuksien vähentämistä, tietoturvatietoisen käyttäytymisen vahvistamista ja turvallisten käytäntöjen jatkuvaa juurruttamista sääntely- ja sopimusvaatimusten mukaisesti.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia sisäisiä ja ulkoisia henkilöitä, joilla on pääsy organisaation tietojärjestelmiin, tietoihin tai toimitiloihin, mukaan lukien:

2.1.1 työntekijät (vakituinen, osa-aikainen, määräaikainen)

2.1.2 urakoitsijat, konsultit, toimittajat ja harjoittelijat

2.1.3 kolmannet osapuolet, joilla on looginen tai fyysinen pääsy palvelusopimusten perusteella

2.2 Soveltamisalaan kuuluvat:

2.2.1 perehdytyksen yhteydessä annettava tietoturvatietoisuuskoulutus

2.2.2 roolikohtainen koulutus (esim. kehittäjät, taloushallinto, etuoikeutetut käyttäjät)

2.2.3 säännöllinen kertauskoulutus ja tietoisuuskampanjat

2.2.4 tapauskohtainen koulutus tietoturvapoikkeamien tai uusien uhkien seurauksena

2.3 Tämän politiikan kattamiin koulutuksen toteutustapoihin kuuluvat verkkokoulutus, lähitilaisuudet, simulaatiot, osaamistestit, julisteet, uutiskirjeet ja pakolliset kuittaukset.

3. Tavoitteet

3.1 Varmistaa, että koko henkilöstö ymmärtää vastuunsa organisaation omaisuuden suojaamisessa ja tietoturvapolitiikkojen noudattamisessa.

3.2 Tarjota jatkuvaa ja mitattavaa tietoisuus- ja koulutustoimintaa, joka on linjassa roolipohjaisen riskialtistuksen kanssa.

3.3 Vakiinnuttaa turvallinen toiminta osaksi päivittäistä työtä vahvistamalla käytäntöjä, kuten salasanojen turvallista käyttöä, poikkeamien ilmoittamista ja tietojenkalastelun tunnistamista.

3.4 Varmistaa sääntelyvaatimusten noudattaminen ja auditointivalmius tietoturvakoulutusvelvoitteiden osalta eri toimialoilla ja oikeudenkäyttöalueilla.

3.5 Vähentää huolimattomuudesta, tietämättömyydestä tai heikosta harkinnasta johtuvia tietoturvapoikkeamia käyttäytymisen ohjauksen ja jatkuvan vahvistamisen avulla.

4. Roolit ja vastuut

4.1 Ylin johto

4.1.1 Hyväksyy organisaation tietoturvakoulutusstrategian ja varmistaa, että sille on osoitettu riittävät resurssit ja että se on sisällytetty organisaation prioriteetteihin.

4.1.2 Seuraa vaatimustenmukaisuutta johdon tasolla ja varmistaa politiikkojen noudattamisen kaikissa yksiköissä.

4.2 Tietoturvajohtaja (CISO) / ISMS-päällikkö

4.2.1 Vastaa tästä politiikasta ja määrittää tietoisuus- ja koulutusviitekehyksen riskien, vaatimustenmukaisuuden ja liiketoiminnan tarpeiden mukaisesti.

4.2.2 Valvoo kaikkien tietoturvakoulutushankkeiden suunnittelua, toteutusta, seurantaa ja katselmointia.

4.2.3 Varmistaa, että koulutusta päivitetään säännöllisesti ja että se vastaa muuttuvia uhkia ja uusia teknologioita.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Katselmointitiheys

9.1.1 Tämä politiikka ja siihen liittyvä koulutusohjelma on katselmoitava:

9.1.1.1 vuosittain, tai

9.1.1.2 merkittävien inhimilliseen virheeseen tai sisäiseen uhkaan liittyvien poikkeamien jälkeen

9.1.1.3 merkittävien uusien teknologioiden tai uhkien käyttöönoton yhteydessä

9.1.1.4 oikeudellisten, sopimuksellisten tai sertifiointivelvoitteiden muuttuessa

9.2 Katselmointiprosessi

9.2.1 Katselmointia johtaa tietoturvajohtaja (CISO) yhteistyössä seuraavien kanssa:

9.2.1.1 henkilöstöhallinto ja koulutustoiminnot

9.2.1.2 laki- ja vaatimustenmukaisuustoiminnot sekä tietosuojavastaavat

9.2.1.3 IT-, tietoturva- ja operatiivisen riskienhallinnan toiminnot

9.2.2 Kaikkien päivitysten on oltava:

9.2.2.1 ISMS-ohjausryhmän hyväksymiä

9.2.2.2 versiohallittuja ja dokumentoituja ISMS-asiakirjarekisteriin

9.2.2.3 viestittyjä käyttäjille, jos olennaiset muutokset vaikuttavat koulutuksen soveltamisalaan tai vastuisiin

9.3 Sisällön päivitysten hallinta

9.3.1 Koulutusmoduulit ja tietoisuusmateriaalit on katselmoitava 12 kuukauden välein sen varmistamiseksi, että:

9.3.1.1 ne vastaavat uhkaympäristöä

9.3.1.2 ne ovat sääntelyn osalta paikkansapitäviä

9.3.1.3 ne ovat muodoltaan yhteensopivia (esim. saavutettavuus, lokalisointi)

9.3.2 Vanhentunut tai harhaanjohtava sisältö on poistettava viipymättä käytöstä ja korvattava hyväksytyillä vaihtoehdoilla.

10. Liittyvät politiikat ja yhteydet

10.1 Tätä politiikkaa tukevat seuraavat politiikat, ja se tukee niiden soveltamista:

10.1.1 P01 – Tietoturvapolitiikka: Määrittää tietoturvatietoisuuden organisaation tietoturvallisuuden hallintajärjestelmän perustavanlaatuiseksi kontrolliksi.

10.1.2 P03 – Hyväksyttävän käytön politiikka: Edellyttää käyttäjän kuittausta koulutuksen yhteydessä ja selventää päivittäiseen teknologian käyttöön liittyviä vastuita.

10.1.3 P07 – Perehdytys- ja työsuhteen päättämispolitiikka: Varmistaa, että koulutus sisällytetään työsuhteen alkuun ja että sitä seurataan koko työsuhteen ajan.

10.1.4 P06 – Riskienhallintapolitiikka: Yhdistää ihmislähtöisen koulutuksen uhkamallinnukseen ja jäännösriskin vähentämisstrategioihin.

10.1.5 P33 – Auditointi- ja vaatimustenmukaisuuden seurantapolitiikka: Varmistaa auditoinneissa, että tietoisuuskontrollit ovat käytössä, mitattavia ja tehokkaita.

10.2 Yhdessä nämä politiikat muodostavat kattavan käyttäytymiseen vaikuttavan kontrolliviitekehyksen, joka yhdistää tietoisuuden, vastuun osoitettavuuden ja kulttuurin vahvistamisen.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Lauseke 7.3 – Tietoisuus: Edellyttää, että organisaatiot varmistavat työntekijöiden olevan tietoisia tietoturvapolitiikoista ja omista vastuistaan. Tämä politiikka toteuttaa kyseisen vaatimuksen jäsennellyn perehdytyksen, säännöllisen koulutuksen ja mitattavan kampanjaosallistumisen avulla.

11.1.2 Liitteen A kontrolli 6.3 – Tietoturvatietoisuus, koulutus ja opastus: Katettu täysimääräisesti alkuvaiheen, roolipohjaisten ja jatkuvien koulutusohjelmien kautta, jotka on mukautettu käyttäjien riskiprofiileihin.

11.2 ISO/IEC 27002:2022 – Kontrolli 6

11.2.1 Tukee työrooleihin soveltuvan tietoisuus- ja koulutustoiminnan kehittämistä ja toteutusta painottaen turvallisen käyttäytymisen vahvistamista sekä uhkatiedusteluun ja auditointipalautteeseen perustuvia säännöllisiä päivityksiä.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1–AT-5 (Awareness and Training -tuoteperhe): Tämä politiikka on linjassa kohtien AT-1 (Policy and Procedures), AT-2 (Awareness Training), AT-3 (Role-Based Training), AT-4 (Security Training Records) ja AT-5 (Contact with Security Groups) kanssa.

11.3.2 IA-5, AC-2: Vahvistaa käyttäjän vastuuta turvallisesta todennuksesta ja hyväksyttävästä käytöstä, jotka ovat tietoisuusohjelmien keskeisiä käyttäytymistavoitteita.

11.3.3 IR-1–IR-8: Tietoturvapoikkeamiin reagoinnin valmiutta vahvistetaan kohdennetuilla tietoisuuskampanjoilla ja simulaatioilla.

11.4 EU:n GDPR (2016/679)

11.4.1 Artikla 32 – käsittelyn turvallisuus: Edellyttää, että henkilötietoja käsittelevä henkilöstö koulutetaan tunnistamaan, ehkäisemään ja ilmoittamaan henkilötietoihin kohdistuvia riskejä. Tämä politiikka varmistaa, että henkilötietojen käsittelijät ja kaikki muut asiaankuuluvat roolit koulutetaan tämän mukaisesti.

11.4.2 Artikla 39 – tietosuojavastaavan tehtävät: Sisältää henkilöstön tietoisuuden lisäämisen ja käsittelytoimiin osallistuvan henkilöstön kouluttamisen.

11.4.3 Johdanto-osan kappale 78: Kannustaa tarkoituksenmukaisiin tietoisuustoimenpiteisiin vahvojen tietoturvakäytäntöjen ja politiikkojen noudattamisen varmistamiseksi.

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

11.5.1 Artikla 21(2)(a, b): Edellyttää yhteisöjä ottamaan käyttöön riskianalyysiä ja tietoturvakoulutusta koskevia politiikkoja kaikelle asiaankuuluvalle henkilöstölle. Tämä politiikka täyttää vaatimuksen ottamalla käyttöön jatkuvat ja rooliherkät koulutusprosessit.

11.5.2 Artikla 21(3): Kannustaa edistämään kyberturvallisuusriskien tietoisuutta johdon ja henkilöstön keskuudessa tietoisuusaloitteiden ja simulaatioiden avulla.

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

11.6.1 Artikla 13 – digitaalisen operationaalisen häiriönsietokyvyn strategia: Edellyttää, että ICT-riskitietoisuus ja koulutus ovat osa hallintamallia. Tämä politiikka varmistaa, että inhimillinen riski käsitellään jatkuvan koulutuksen ja uhkasimulaatioiden avulla.

11.6.2 Artiklat 5 ja 8: Korostavat sisäisen valvonnan viitekehyksen merkitystä, jossa tietoisuus ja koulutus ovat ICT:n häiriönsietokyvyn ja kyberhygienian perustavia osatekijöitä.

11.7 COBIT 2019

11.7.1 APO07 – Managed Human Resources: Korostaa tarvetta kehittää tietoisuutta tietoturvavastuista ja sisällyttää tämä osaksi henkilöstön hallintaa.

11.7.2 DSS05 – Managed Security Services: Määrittää kontrollit käyttäjäkoulutukselle ja poikkeamien ilmoittamiselle, jotka molemmat ovat tämän politiikan olennaisia osia.

11.7.3 MEA03 – Monitor, Evaluate, and Assess Compliance: Edellyttää käyttäjäkäyttäytymisen ja politiikkojen noudattamisen tehokkuuden arviointia; tässä politiikassa tämä toteutetaan tietojenkalastelutestien, tietotestien ja tietoisuuskampanjamittareiden avulla.