| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Lisää tähän rekisteröidyn oikeushenkilön nimi | | | | | | | |
| Asiakirjan numero:<br>P02 | | | | | Asiakirjan nimi:<br>**Hallinnointirooleja ja vastuita koskeva politiikka** | | | | | | | |
| Versio:<br>1.0 | | Voimaantulopäivä:<br>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 | Kohta 5.3; liitteen A kontrolli 5 | |
| ISO/IEC 27002:2022 | Kontrolli 5 | |
| NIST SP 800-53 Rev.5 | PL-1–PL-4, PM-1–PM-13 | |
| EU:n GDPR | Artiklat 5(1)(f), 24, 37 | |
| EU:n NIS2-direktiivi | Artikla 21(2)(a) | |
| EU:n DORA-asetus | Artikla 5 | |
| COBIT 2019 | EDM01, EDM02, APO01, APO12, MEA | |

**1. Tarkoitus**

1.1 Tämä politiikka määrittää hallinnointimallin sekä organisaatioroolit ja -vastuut, joita tarvitaan tehokkaan tietoturvallisuuden hallintajärjestelmän (ISMS) ylläpitämiseksi.

1.2 Se määrittää selkeät vastuita, päätöksentekovaltaa ja eskalointimenettelyjä koskevat linjaukset sen varmistamiseksi, että tietoturva on sisällytetty organisaation kaikille tasoille ja linjassa liiketoiminnan strategisten tavoitteiden kanssa.

1.3 Tämä politiikka toteuttaa ISO/IEC 27001:2022 -standardin kohdan 5.3 ja kontrollin A.5.2 vaatimukset varmistamalla, että tietoturvaan liittyvien toimintojen vastuut on määritetty, dokumentoitu, viestitty ja katselmoitu säännöllisesti.

1.4 Tämä politiikka muodostaa myös perustan integroidulle hallinnoinnille muiden osa-alueiden, kuten riskienhallinnan, vaatimustenmukaisuuden, IT-toimintojen ja lakiasioiden, kanssa.

**2. Soveltamisala**

**2.1 Tämä politiikka koskee kaikkia henkilöitä ja tahoja, jotka osallistuvat tietoturvan hallinnointiin, toteutukseen ja valvontaan ISMS:n soveltamisalan puitteissa. Tähän sisältyvät:**

2.1.1 ylimmän johdon edustajat, muu ylempi johto ja hallituksen jäsenet

2.1.2 ISMS-päälliköt, tietoturvajohtajat (CISO) ja kontrollien omistajat

2.1.3 prosessien omistajat ja omaisuuserien omistajat

2.1.4 toimeksisaajat ja kolmannen osapuolen palveluntarjoajat, joille on delegoitu tietoturvavastuita

2.2 Politiikka kattaa sekä sisäiset että ulkoistetut toiminnot (esim. ulkoistettu SOC tai pilvialustan ylläpitäjät), joissa hallinnointiroolit on määritetty muodollisesti tai sopimuksellisesti.

2.3 Tämä politiikka koskee myös organisaatioyksiköitä, osastoja ja projektitiimejä, jotka hallinnoivat tai muutoin vaikuttavat tietoturvan kannalta olennaisiin omaisuuseriin, järjestelmiin tai palveluihin.

**3. Tavoitteet**

3.1 Varmistaa, että tietoturvaroolit ja -vastuut on määritetty, osoitettu, viestitty ja dokumentoitu muodollisesti.

3.2 Ylläpitää hallinnointimallia, joka varmistaa tehtävien eriyttämisen, ehkäisee eturistiriidat ja mahdollistaa ratkaisemattomien tietoturvakysymysten eskaloinnin.

3.3 Varmistaa, että tietoturvaa koskeva vastuu ja päätösvalta jakautuvat liiketoimintavaikutuksen ja organisaatiorakenteen mukaisesti.

3.4 Luoda viitekehys delegointien, roolimuutosten ja osoitettujen vastuiden katselmoinnille.

3.5 Antaa sidosryhmille, mukaan lukien viranomaiset, auditoijat ja asiakkaat, varmuus siitä, että tietoturvaa hallinnoidaan tehokkaasti ja sovellettavien standardien mukaisesti.

## 4. Roolit ja vastuut

### 4.1 Ylin johto

4.1.1 Vastaa strategisesta ohjauksesta, resurssien kohdentamisesta ja siitä, että ISMS:n tavoitteet ovat linjassa liiketoiminnan tavoitteiden kanssa.

4.1.2 Hyväksyy keskeisen ISMS-dokumentaation, mukaan lukien tietoturvapolitiikan, riskienkäsittelysuunnitelmat ja auditointien korjaavia toimenpiteitä koskevat päätökset.

4.1.3 Osallistuu ISMS:n johdon katselmointeihin ja eskaloi päätökset, jotka edellyttävät hallitustason hyväksyntää.

4.1.4 Edistää tietoturvakulttuuria ja tukee tietoturvan hallinnoinnin periaatteiden noudattamista koko organisaatiossa.

### 4.2 Tietoturvan ohjausryhmä (ISSC)

4.2.1 Toimii poikkiorganisatorisena hallinnointielimenä ISMS:n ohjauksessa.

4.2.2 Katselmoi riskiasemaa, kontrollien suorituskykyä, auditointihavaintoja ja strategisia tietoturvahankkeita.

4.2.3 Edistää osastojen välistä koordinointia (esim. IT, lakiasiat, HR, riskienhallinta, vaatimustenmukaisuus ja operatiivinen toiminta).

4.2.4 Hyväksyy eskalointikynnykset, budjettikohdennukset ja politiikkamuutokset, jotka edellyttävät ylimmän johdon kannanottoa.

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

## 9. Katselmointi- ja päivitysvaatimukset

### 9.1 Katselmointiaikataulu

**9.1.1 Tämä politiikka on katselmoitava vähintään vuosittain tai silloin, kun tapahtuu jokin seuraavista:**

9.1.1.1 muutokset organisaatiorakenteessa tai johtoryhmässä

9.1.1.2 ISMS:n soveltamisalan laajentaminen tai uudelleenmäärittely

9.1.1.3 sääntelymuutokset, jotka vaikuttavat roolien osoittamiseen tai valvontaan

9.1.1.4 merkittävät auditointihavainnot tai hallinnointiepäonnistumiseen liittyvät poikkeamat

### 9.2 Katselmointi- ja hyväksymisprosessi

9.2.1 ISMS-päällikkö käynnistää ja johtaa katselmointiprosessia, mukaan lukien sidosryhmien näkemysten ja auditointipalautteen kerääminen.

9.2.2 Ehdotetut päivitykset on katselmoitava ISSC:ssä ja hyväksyttävä muodollisesti ylimmässä johdossa.

**9.2.3 Jokainen versio on kirjattava ISMS:n asiakirjarekisteriin, ja sen on sisällettävä seuraavat metatiedot:**

9.2.3.1 politiikan tunniste ja otsikko

9.2.3.2 versionumero ja muutosyhteenveto

9.2.3.3 voimaantulopäivä ja seuraavan katselmoinnin päivämäärä

9.2.3.4 politiikan omistaja ja hyväksyjä

9.2.3.5 asiakirjan luokitustaso

9.2.3.6 säilytys- ja arkistointihistoria

## 10. Liittyvät politiikat ja riippuvuudet

**10.1 Tätä politiikkaa on tulkittava yhdessä seuraavien politiikkojen kanssa:**

10.1.1 P1 – Tietoturvapolitiikka: määrittää yleisen tietoturvaohjelman ja kuvaa johdon vastuut politiikan hyväksynnässä ja strategisessa ohjauksessa.

10.1.2 P5 – Muutoksenhallintapolitiikka: varmistaa, että hallinnointirakenteisiin, rooleihin tai vastuisiin tehtäviin muutoksiin sovelletaan dokumentoitua hyväksyntää ja riskien tarkastelua.

10.1.3 P6 – Riskienhallintapolitiikka: tunnistaa ja käsittelee hallinnointiriskit, jotka johtuvat rooliristiriidoista, osoittamattomista tehtävistä tai eskaloinnin puutteesta.

10.1.4 P7 – Perehdytys- ja päättymispolitiikka: varmistaa kontrollien osoittamisen ja poistamisen henkilöstön elinkaaren muutostilanteissa.

10.1.5 P33 – Auditointi- ja vaatimustenmukaisuuden seurantapolitiikka: tukee hallinnoinnin tehokkuuden riippumatonta arviointia ja varmistaa korjaavat toimenpiteet vaatimustenvastaisuuksissa.

10.2 Nämä politiikat yhdessä tukevat yhtenäistä ja sovellettavaa ISMS:n hallinnointikehystä.

## 11. Viitestandardit ja viitekehykset

11.1 Tämä politiikka on yhdenmukainen maailmanlaajuisesti tunnettujen tietoturvan hallinnointia ja roolivastuuta koskevien standardien ja viitekehysten kanssa. Se varmistaa jäljitettävyyden sääntely- ja sertifiointivaatimuksiin sekä tukee perusteltavissa olevaa ISMS-rakennetta.

**11.2 ISO/IEC 27001**

11.2.1 Kohta 5.3 – Organisaation roolit, vastuut ja valtuudet: Tämä politiikka täyttää vaatimuksen, jonka mukaan tietoturvan kannalta olennaiset roolit on osoitettava, viestittävä ja dokumentoitava selkeästi.

11.2.2 Kohta 9.3 – Johdon katselmointi: Tämä politiikka varmistaa johdon valvonnan ISMS-rooleihin ja hallinnointiin neljännesvuosittaisten ja vuosittaisten katselmointien avulla.

11.2.3 Liitteen A kontrolli 5.2 – Tietoturvaroolit ja -vastuut: Määrittää roolit teknisellä, operatiivisella ja strategisella tasolla tehtävien eriyttämisen, riskinomistajuuden ja jäljitettävän vastuun varmistamiseksi.

**11.3 ISO/IEC 27002:2022 – Kontrolli 5**

11.3.1 Antaa toteutusohjeita tietoturvavastuiden osoittamiseen organisaatiossa. Tämä politiikka ottaa ohjeistuksen käyttöön määrittämällä roolityypit, delegointisäännöt, eskalointimenettelyt ja katselmointimekanismit.

**11.4 NIST SP 800-53 Rev.5**

11.4.1 PL-1–PL-4: Korostavat muodollisen suunnitteludokumentaation tarvetta, mukaan lukien politiikat, jotka määrittävät hallinnoinnin ja osoittavat tietoturvavastuut.

11.4.2 PM-1 (Information Security Program Plan) ja PM-2 (Senior Information Security Officer): Näkyvät tässä politiikassa CISO-/ISMS-päällikköroolin sekä muodollisten hallinnointiroolien osoittamisena.

11.4.3 PM-5–PM-13: Tämä politiikka täyttää vaatimukset roolidokumentoinnista, organisaation laajuisista riskirooleista, konfiguraationhallinnan valvonnasta ja integraatiosta tehtävä- ja liiketoimintatoimintoihin.

**11.5 EU:n GDPR (2016/679)**

11.5.1 Artikla 5(1)(f): Edellyttää, että henkilötietoja suojataan luvattomalta tai lainvastaiselta käsittelyltä. Tämä politiikka varmistaa, että tietosuojasta vastuulliset henkilöt on nimetty selkeästi ja että heidän toimintaansa seurataan.

11.5.2 Artikla 24: Edellyttää asianmukaisia organisatorisia toimenpiteitä, mukaan lukien hallinnointirakenteet.

11.5.3 Artikla 37: Edellyttää tietosuojavastaavan (DPO) nimeämistä, ja tämän on näyttävä organisaation hallinnointikehyksessä ja vastuuristerissä.

**11.6 EU:n NIS2-direktiivi (2022/2555)**

11.6.1 Artikla 21(2)(a): Velvoittaa organisaatioita ottamaan käyttöön riskianalyysiä ja tietojärjestelmien turvallisuutta koskevat politiikat, mukaan lukien roolikohtaiset vastuut. Tämä politiikka määrittää tällaiset roolit ja niiden hallinnointimekanismit.

**11.7 EU:n DORA-asetus (2022/2554)**

11.7.1 Artikla 5 – Hallinnointi- ja sisäisen valvonnan viitekehys: Edellyttää tieto- ja viestintäteknologian riskienhallinnan vastuiden, päätöksentekoroolien ja raportointikanavien muodollista osoittamista. Tämä politiikka muodostaa perustan tietoturvaan liittyvien roolien hallinnoinnille ICT-ympäristöissä.

**11.8 COBIT 2019**

11.8.1 EDM01 – Ensured Governance Framework Setting: Tämä politiikka varmistaa, että ISMS:llä on selkeästi määritelty hallinnointirakenne, joka vastaa organisaation tarpeita.

11.8.2 EDM02 – Ensured Benefits Delivery: Yhdistää rooliperusteiset tietoturvatoimet strategisiin ja operatiivisiin tavoitteisiin ja varmistaa vastuun sekä mitattavat tulokset.

11.8.3 APO01 – Managed I&T Management Framework ja APO12 – Managed Risk: Tämä politiikka tukee tietoturvaroolien jäsenneltyä hallintaa osana laajempaa IT-hallinnointi- ja riskienhallintakehystä.

11.8.4 MEA01 – Monitor, Evaluate and Assess Performance: Sisällyttää katselmointimekanismit sen varmistamiseksi, että hallinnointiroolit ovat tehokkaita, ajan tasalla ja niitä sovelletaan.