					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P01					Asiakirjan nimi: **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**

1. Tarkoitus

1.1 Tämä politiikka määrittää organisaation yleisen sitoutumisen tietoturvaan perustamalla muodollisen tietoturvallisuuden hallintajärjestelmän (ISMS).

1.2 Se määrittää strategisen suunnan ja perustavanlaatuiset vaatimukset kaikkien tietovarojen luottamuksellisuuden, eheyden, saatavuuden ja palautumiskyvyn suojaamiseksi fyysisissä, digitaalisissa ja pilviympäristöissä.

1.3 Tämä politiikka täyttää ISO/IEC 27001:2022 -standardin kohtien 5.1 ja 5.2 vaatimukset ilmaisemalla johdon tahtotilan, ylimmän johdon sitoutumisen ja tietoturvatoimien yhdenmukaisuuden organisaation tavoitteiden kanssa.

1.4 Tämä politiikka toimii ohjaavana viiteasiakirjana kaikille ISMS:n alaisille politiikoille, standardeille ja menettelyille, ja se on keskeinen riskiperusteisen, vaatimustenmukaisuutta tukevan ja jatkuvasti kehittyvän tietoturvaympäristön mahdollistaja.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia ISMS:n soveltamisalaan määriteltyjä henkilöitä, tietovaroja ja prosesseja, mukaan lukien:

2.1.1 Kaikki liiketoimintayksiköt, osastot, tytäryhtiöt ja toimipisteet

2.1.2 Työntekijät, alihankkijat, määräaikainen henkilöstö, konsultit ja kolmannen osapuolen palveluntarjoajat

2.1.3 Kaikki tiedot, tietojärjestelmät, sovellukset, infrastruktuuri ja viestintäkanavat

2.1.4 Kaikki fyysiset, pilvipohjaiset, etä- ja hybridiympäristöt, joissa yrityksen tietoja käsitellään tai joista niitä käytetään

2.2 Tämä politiikka on sitova kaikille organisaation tietoja käsitteleville tahoille, ja sitä sovelletaan tiedon elinkaaren kaikkiin vaiheisiin luonnista ja siirrosta säilytykseen ja hävittämiseen.

2.3 Kaikki tämän soveltamisalan rajaukset tai rajoitukset on dokumentoitava ISMS:n soveltamisalalausunnossa, ja niille on saatava ylimmän johdon muodollinen hyväksyntä.

3. Tavoitteet

3.1 Perustaa ISO/IEC 27001:2022 -standardin mukainen ISMS, joka tukee riskiperusteista päätöksentekoa koko organisaatiossa.

3.2 Varmistaa, että luottamuksellisuuden, eheyden ja saatavuuden tietoturvaperiaatteet sisällytetään kaikkiin organisaation toimintoihin, järjestelmiin ja kumppanuuksiin.

3.3 Mahdollistaa sääntely- ja sopimusvaatimusten noudattaminen määrittämällä mitattavat, politiikkaohjatut tietoturvatavoitteet ja integroimalla ne liiketoiminnan toimintaan.

3.4 Vähentää tietoturvapoikkeamien todennäköisyyttä ja vaikutuksia tehokkailla ennaltaehkäisevillä, havaitsevilla ja korjaavilla kontrolleilla.

3.5 Edistää tietoturvakyvykkyyden jatkuvaa parantamista määriteltyjen suorituskykymittareiden, auditointitulosten ja johdon katselmusten avulla.

3.6 Edistää vastuullisuuden, tietoisuuden ja palautumiskyvyn kulttuuria, jossa koko henkilöstö ymmärtää tietoturvavastuunsa ja toimii niiden mukaisesti.

4. Roolit ja vastuut

4.1 Ylin johto

4.1.1 Hyväksyy ja vahvistaa tietoturvapolitiikan ja ISMS-viitekehyksen.

4.1.2 Varmistaa tietoturvatavoitteiden ja liiketoimintastrategian yhdenmukaisuuden.

4.1.3 Näyttää esimerkkiä ja edistää vahvaa tietoturvakulttuuria.

4.1.4 Katselmoi ja hyväksyy merkittävät muutokset ISMS:n soveltamisalaan, riskien käsittelyyn ja hallintorakenteeseen.

4.2 Tietoturvajohtaja (CISO) / ISMS-päällikkö

4.2.1 Vastaa ISMS:stä ja ylläpitää tätä politiikkaa ISO/IEC 27001 -standardin mukaisesti.

4.2.2 Johtaa riskienarviointia, kontrollien toteutusta ja jatkuvan parantamisen prosesseja.

4.2.3 Varmistaa tietoturvatoimien poikkitoiminnallisen koordinoinnin ja valvoo alisteisia politiikkoja.

4.2.4 Raportoi ylimmälle johdolle ISMS:n tilasta, poikkeamista, auditointituloksista ja mittareista.

4.2.5 Varmistaa, että politiikan katselmoinnit ja päivitykset toteutetaan tämän asiakirjan kohdan 9 mukaisesti.

[... 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 on katselmoitava vähintään vuosittain tai jonkin seuraavan käynnistävän tekijän toteutuessa:

9.1.1.1 Merkittävät muutokset lakisääteisissä, sääntelyyn perustuvissa tai sopimusperusteisissa velvoitteissa

9.1.1.2 Olennaiset muutokset organisaation riskiprofiilissa

9.1.1.3 Sisäisten tai ulkoisten auditointien tulokset

9.1.1.4 Merkittävät poikkeamat tai kontrollien pettämiset

9.2 Katselmoinnin vastuu ja menettely

9.2.1 CISO tai nimetty ISMS-päällikkö johtaa katselmointiprosessia.

9.2.2 Katselmoinnin lähtötietojen on sisällettävä vähintään:

9.2.2.1 Sisäisten auditointien tulokset

9.2.2.2 Riskienarvioinnin trendit

9.2.2.3 Muutokset liiketoimintaprosesseissa ja teknologiassa

9.2.2.4 Suorituskyky suhteessa KPI-mittareihin ja riskirajoihin

9.2.3 Kaikkien päivitysten on:

9.2.3.1 Oltava versiohallittuja ja dokumentoituja

9.2.3.2 Oltava ylimmän johdon hyväksymiä

9.2.3.3 Tultava jaetuiksi kaikille asianosaisille virallisten viestintäkanavien kautta

9.2.3.4 Käynnistettävä tarvittavat päivitykset alisteiseen dokumentaatioon ja koulutuksiin

10. Liittyvät politiikat ja riippuvuudet

10.1 Tämä perustason politiikka liittyy suoraan seuraaviin organisaation tietoturvapolitiikkoihin ja viitekehyksiin:

10.1.1 P2 – Hallintoroolien ja vastuiden politiikka: Määrittää tässä asiakirjassa viitatun hallintorakenteen ja toimivaltahierarkian.

10.1.2 P3 – Hyväksyttävän käytön politiikka: Määrittää käyttäytymiseen liittyvät noudattamisvaatimukset ja tietovarojen hyväksyttävän käsittelyn.

10.1.3 P4 – Pääsynhallintapolitiikka: Toteuttaa käytännössä tästä ylemmän tason politiikasta johdetut pääsyyn liittyvät kontrollit.

10.1.4 P6 – Riskienhallintapolitiikka: Tarjoaa riskiperusteisen viitekehyksen kontrollien valinnalle ja jäännösriskien hyväksymiselle.

10.1.5 P33 – Auditointi- ja vaatimustenmukaisuuden seurannan politiikka: Kuvaa, miten sisäiset varmennusmekanismit todentavat politiikan noudattamisen.

10.2 Nämä keskinäiset riippuvuudet varmistavat kokonaisvaltaisen yhdenmukaisuuden ja jäljitettävyyden koko ISMS:ssä sekä tukevat yhtenäistä riskienhallintaa ja vaatimustenmukaisuuden hallintaa.

11. Viitestandardit ja viitekehykset

11.1 Tämä tietoturvapolitiikka on muodollisesti sovitettu yhteen seuraavien standardien ja viitekehysten kanssa täyden vaatimustenmukaisuuden, auditoinneissa osoitettavan vaatimustenmukaisuusvalmiuden ja sääntelyllisen puolustettavuuden varmistamiseksi:

11.2 ISO/IEC 27001

11.2.1 Kohta 5.1 – Johtajuus ja sitoutuminen: Tämä politiikka osoittaa ylimmän johdon sitoutumisen tietoturvaan sekä määrittää ISMS:n vastuut ja resurssien kohdentamisen.

11.2.2 Kohta 5.2 – Tietoturvapolitiikka: Tämä asiakirja toimii organisaation muodollisena tietoturvapolitiikkana, joka on yhdenmukainen määritettyjen tietoturvatavoitteiden, liiketoimintastrategian ja ISO/IEC 27001 -vaatimusten kanssa.

11.2.3 Kohta 6.1 – Riskien ja mahdollisuuksien käsittelyä koskevat toimenpiteet: Tässä politiikassa kuvattu riskiperusteinen lähestymistapa varmistaa, että tietoturvaresursseja kohdennetaan uhkiin nähden oikeasuhtaisesti.

11.2.4 Kohta 9.2 – Sisäinen auditointi ja kohta 10 – Parantaminen: Tämä politiikka on sisällytetty organisaation jatkuvan parantamisen elinkaareen, ja se kuuluu sisäisen auditoinnin todentamisen piiriin.

11.2.5 ISO/IEC 27002:2022 – Kontrolli 5.1: Määrittää ohjeet tietoturvapolitiikkojen laatimiselle ja ylläpidolle. Tämä politiikka vastaa ISO 27002:n suosituksia hierarkkisesta dokumentaatiosta, katselmointisykleistä ja toimeenpantavuudesta.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Tietoturvasuunnittelun politiikka ja menettelyt): Tämä politiikka täyttää vaatimuksen muodollisen, koko organisaation kattavan tietoturvapolitiikan laatimisesta, jakelusta ja katselmoinnista.

11.3.2 PM-1–PM-5: Kattaa ohjelmatason hallinnan, mukaan lukien tietoturvaroolit, resurssien kohdentamisen, riskistrategian ja tietoturvasuunnittelun integroinnin organisaation toimintaan.

11.4 EU:n GDPR (2016/679)

11.4.1 Artikla 5(2): Vahvistaa osoitusvelvollisuuden periaatteen. Tämä politiikka määrittää vastuutahot ja jäljitettävät toimeenpanotoimet.

11.4.2 Artikla 24: Edellyttää teknisten ja organisatoristen toimenpiteiden toteutusta, mukaan lukien riskeihin perustuvat politiikat.

11.4.3 Artikla 32: Tukee asianmukaisten toimenpiteiden toteutusta henkilötietojen turvallisuuden varmistamiseksi koko niiden elinkaaren ajan.

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

11.5.1 Artikla 21(2)(a): Velvoittaa organisaatiot toteuttamaan dokumentoidun tietoturvapolitiikan, joka käsittelee riskienhallintaa ja hallintaa. Tämä politiikka täyttää kyseisen vaatimuksen ja tukee laajemmin kyberturvallisuusvalmiutta sekä kriittisen infrastruktuurin suojausta.

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

11.6.1 Artikla 5(2): Edellyttää dokumentoitua sisäisen valvonnan viitekehystä ICT-riskien hallintaan. Tämä politiikka tukee finanssialan vaatimustenmukaisuutta osoittamalla DORA-asetuksen hallintaa koskevien odotusten mukaiset roolit, kontrollit ja valvontatoiminnot.

11.7 COBIT 2019

11.7.1 EDM01 – Hallintaviitekehyksen määrittäminen: Tämä politiikka tukee organisaation hallintaa määrittämällä ISMS:n roolit, johdon sitoumukset ja strategiset tavoitteet.

11.7.2 APO01 – Hallintaviitekehys: Tukee rakenteisen ISMS:n perustamista ja käyttöä.

11.7.3 APO12 – Riskienhallinta: Tarjoaa perustan tietoturvariskien hallinnalle.

11.7.4 MEA01/MEA03 – Seuranta, arviointi ja tarkastelu: Vahvistaa jatkuvaa suorituskyvyn arviointia ja sisäisen valvonnan seurantaa politiikan noudattamisen avulla.