					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P12					Asiakirjan nimi: **Omaisuudenhallintapolitiikka**							
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 pakolliset organisaatiotason vaatimukset tietovarojen tunnistamiselle, luokittelulle, hallinnalle ja suojaamiselle koko niiden elinkaaren ajan. Se tukee laitteistoihin, ohjelmistoihin, tietoihin, pilvipalveluihin ja aineettomiin tietovaroihin kohdistuvaa koko organisaation kattavaa hallintaa, mukaan lukien mobiili-, etä- ja kolmannen osapuolen hallinnoimat ympäristöt.

1.2 Tämän politiikan tarkoituksena on varmistaa täysi näkyvyys organisaation tietovaroihin, jotta tietoturvakontrollit voidaan toteuttaa tehokkaasti, omistajuudet voidaan määrittää, vaatimustenmukaisuus voidaan varmistaa ja käytöstäpoisto tai hävittäminen voidaan toteuttaa hallitusti.

1.3 Tämä politiikka on yhdenmukainen ISO/IEC 27001:2022 -standardin liitteen A kohdan 5.9 kanssa edellyttämällä tiedoista ja niihin liittyvistä omaisuuseristä ylläpidettävää keskitettyä luetteloa. Se varmistaa osoitusvelvollisuuden liittämällä jokaisen omaisuuserän omistajaan ja soveltamalla luokitukseen perustuvaa suojausta liiketoiminnan arkaluonteisuuden ja sääntelyvaatimusten perusteella.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia työntekijöitä, sopimuskumppaneita, kolmansia osapuolia ja palveluntarjoajia, jotka hallinnoivat, käyttävät, käsittelevät, tallentavat tai muutoin käsittelevät organisaation omistamia tai hallitsemia tietovaroja.

2.2 Soveltamisalaan kuuluvat kaikki omaisuuseräluokat, kuten:

2.2.1 Fyysiset omaisuuserät: kannettavat tietokoneet, pöytätietokoneet, mobiililaitteet, siirrettävät tallennusvälineet, tulostimet, verkkolaitteet

2.2.2 Digitaaliset omaisuuserät: ohjelmistot, sovellukset, järjestelmäkuvat, tietokannat, varmuuskopiotiedot, salausavaimet

2.2.3 Tietovarat: rakenteinen data, rakenteeton data, raportit, sähköpostit, immateriaalioikeudet

2.2.4 Pilvi- ja virtuaaliomaisuuserät: IaaS-, SaaS- ja PaaS-ympäristöt, virtuaalikoneet, kontit

2.2.5 Loogiset omaisuuserät: verkkotunnukset, lisenssit, käyttäjätilit, peruskonfiguraatiot

2.3 Tämä politiikka koskee myös etätyössä, hybridiympäristöissä tai ulkoistetuissa ympäristöissä käytettäviä omaisuuseriä ja varmistaa niiden suojauksen ja näkyvyyden myös silloin, kun omaisuuserät eivät sijaitse fyysisesti organisaation tiloissa.

3. Tavoitteet

3.1 Ylläpitää täydellistä, täsmällistä ja ajantasaista luetteloa kaikista organisaation tietovaroista sekä niiden omistajuus-, luokittelu- ja sijaintitiedoista.

3.2 Määrittää omaisuuserille omistajat, jotka vastaavat hallinnassaan olevien omaisuuserien luokittelusta, käsittelystä ja suojaamisesta tietojen hallintaa ja tietoturvapolitiikkoja koskevien vaatimusten mukaisesti.

3.3 Soveltaa asianmukaista luokittelua ja merkintöjä kaikkiin omaisuuseriin arkaluonteisuuden, kriittisyyden ja sääntelyvaatimusten perusteella.

3.4 Suojata omaisuuserät niiden luokituksen ja niihin liittyvän riskialtistuksen mukaisesti, mukaan lukien tallennus, pääsynhallinta, siirto ja hävittäminen.

3.5 Varmistaa omaisuuden palauttamista ja turvallista hävittämistä koskevien menettelyjen toteuttaminen työntekijän palvelussuhteen päättämisen, sopimuksen päättymisen tai omaisuuserän elinkaaren päättymisen yhteydessä.

3.6 Tukea ISO/IEC 27001:n, EU:n GDPR:n, EU:n NIS2-direktiivin, EU:n DORA-asetuksen ja COBIT 2019:n mukaista vaatimustenmukaisuutta rakenteellisella omaisuudenhallinnalla ja todennettavuudella.

4. Roolit ja vastuut

4.1 Ylin johto

4.1.1 Hyväksyy omaisuudenhallintapolitiikan ja varmistaa, että sen täysimääräiseen toimeenpanoon osoitetaan riittävät resurssit.

4.1.2 Vastaa viime kädessä siitä, että organisaation omaisuuserät suojataan ja niitä hallinnoidaan sääntelyyn ja sopimuksiin perustuvien velvoitteiden mukaisesti.

4.2 Tietoturvajohtaja (CISO)

4.2.1 Omistaa omaisuudenhallintapolitiikan ja varmistaa sen integroinnin organisaation tietoturvallisuuden hallintajärjestelmään (ISMS).

4.2.2 Käsittelee tähän politiikkaan liittyvät poikkeukset ja poikkeamat sekä varmistaa riskiperusteisten lieventävien toimenpiteiden soveltamisen.

4.2.3 Valvoo säännöllisiä auditointeja, jotka kohdistuvat omaisuuserien luokitteluun, omaisuusluettelon eheyteen ja omaisuuserien elinkaaren mukaiseen vaatimustenmukaisuuteen.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Tämä politiikka on katselmoitava vähintään vuosittain tai seuraavien muutosten yhteydessä:

9.1.1 Muutokset lakiin tai sääntelyyn perustuviin velvoitteisiin, jotka vaikuttavat omaisuuserien luokitteluun tai omaisuusrekisteriä koskeviin vaatimuksiin

9.1.2 Uusien omaisuuseräluokkien tai hallinta-alustojen käyttöönotto (esim. pilvinatiivit CMDB-ratkaisut)

9.1.3 Sisäisen tarkastuksen auditointihavainnot tai tietoturvapoikkeamat, jotka liittyvät omaisuuden virheelliseen hallintaan

9.1.4 Organisaatiomuutokset, jotka vaikuttavat omistajuuksiin tai elinkaarikontrolleihin

9.2 Katselmointiprosessin käynnistää IT-omaisuuspäällikkö, ja se koordinoidaan tietoturvajohtajan (CISO), hankinnan, laki- ja vaatimustenmukaisuustoiminnon sekä asianomaisten osastojen johtajien kanssa.

9.3 Välikatselmointeja voidaan käynnistää myös seuraavien tapahtumien perusteella:

9.3.1 Liiketoimintayksiköiden hankinta tai luovutus

9.3.2 Toimittajamuutokset, jotka vaikuttavat kolmannen osapuolen hallinnoimiin omaisuuseriin

9.3.3 Teknologiauudistukset, joihin liittyy laajamittainen käytöstäpoisto tai käyttöoikeuksien myöntäminen

9.4 Kaikkien tämän politiikan muutosten on:

9.4.1 Oltava versiohallittuja ja tallennettuja ISMS-tietovarastoon

9.4.2 Oltava ylimmän johdon hyväksymiä

9.4.3 Sisällettävä yhteenveto muutoksista ja niiden perusteista

9.4.4 Tultava viestityiksi kaikille asiaankuuluville sidosryhmille, mukaan lukien päivitetyt menettelyt tai järjestelmäkoulutus soveltuvin osin

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka toimii yhdessä seuraavien siihen liittyvien politiikkojen kanssa ja tukee niiden soveltamista:

10.1.1 P4 - Pääsynhallintapolitiikka: Varmistaa, että omaisuuserien näkyvyys on linjassa käyttöoikeuksien ja kontrollimekanismien kanssa eri järjestelmissä ja tietoympäristöissä.

10.1.2 P7 - Käyttöönotto- ja palvelussuhteen päättämispolitiikka: Määrittää fyysisten ja loogisten omaisuuserien oikea-aikaisen käyttöoikeuksien myöntämisen ja palauttamisen henkilöstömuutosten yhteydessä.

10.1.3 P13 - Tiedon luokittelu- ja merkintäpolitiikka: Määrittää omaisuuseriä koskevat pakolliset luokittelusäännöt, jotka ohjaavat merkintöjä, käsittelyä ja hävittämismenettelyjä.

10.1.4 P14 - Tietojen säilytys- ja hävittämispolitiikka: Määrittää digitaalisten ja fyysisten tietoa sisältävien omaisuuserien turvallisen hävittämisen aikataulun ja menetelmät.

10.1.5 P22 - Lokitus- ja valvontapolitiikka: Mahdollistaa omaisuuserien käytön ja pääsyn jäljitettävyyden järjestelmälokituksen, päätelaite-näkyvyyden ja käyttäytymisanalytiikan avulla.

10.1.6 P30 - Tietoturvapoikkeamien hallintapolitiikka: Tukee omaisuuseriin liittyvien loukkausten, kuten kadonneiden kannettavien tietokoneiden tai jäljittämättömien tallennusvälineiden, nopeaa rajaamista ja tutkintaa.

10.2 Nämä politiikat muodostavat yhtenäisen hallintarakenteen, joka varmistaa, että omaisuuseriä hallinnoidaan turvallisesti, ne inventoidaan tarkasti ja niitä käsitellään asianmukaisesti koko niiden elinkaaren ajan.

11. Viitestandardit ja viitekehykset

11.1 Tämä politiikka on yhdenmukainen kansainvälisesti tunnustettujen tietoturvastandardien ja sääntelyviitekehysten kanssa, jotka edellyttävät vahvaa omaisuudenhallintaa koko elinkaaren ajan.

11.2 ISO/IEC 27001:

11.2.1 Lauseke 8.1 - Edellyttää organisaatioita suunnittelemaan, toteuttamaan ja hallitsemaan prosessit, joita tarvitaan tietoturvavaatimusten täyttämiseksi, mukaan lukien omaisuuserien elinkaaren hallintaan liittyvät prosessit.

11.3 ISO/IEC 27002:2022 - Kontrollit 5.9–5.11

11.3.1 Kohta 5.9 - Tietojen ja muiden niihin liittyvien omaisuuserien luettelo: Edellyttää ajantasaista ja täydellistä luetteloa kaikista tietojen käsittelyn kannalta olennaisista omaisuuseristä.

11.3.2 Kohta 5.10 - Tietojen ja omaisuuserien hyväksyttävä käyttö: Tuetaan käyttösäännöillä, omistajuuksilla ja palautusprosesseilla.

11.3.3 Kohta 5.11 - Omaisuuserien palauttaminen: Toteutetaan muodollisilla luovutus- ja käytöstäpoistomenettelyillä.

11.3.4 Nämä kontrollit asettavat rakenteelliset vaatimukset organisaation omaisuuserien tunnistamiselle, merkitsemiselle, ylläpidolle ja seurannalle sekä määrittävät vastaavat vastuut omistajille ja haltijoille koko elinkaaren ajan.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 - Järjestelmäkomponenttien inventaario: Näkyy keskitettynä omaisuudenhallintana, reaaliaikaisena näkyvyytenä ja yhteytenä operatiivisiin konfiguraatioihin.

11.4.2 RA-3 - Riskien arviointi: Omaisuusrekisterit toimivat uhkamallinnuksen ja riskien arvioinnin perustana.

11.4.3 MP-6 - Tallennusvälineiden puhdistus: Toteutetaan turvallisilla hävitysmenetelmillä, jotka on määritetty omaisuuserien elinkaarikontrolleissa ja tietojen hävittämispolitiikassa.

11.5 EU:n GDPR (2016/679):

11.5.1 Artikla 30 - Käsittelytoimien selosteet: Edellyttää organisaatioita dokumentoimaan järjestelmät, laitteet ja tietovarastot, jotka tallentavat tai käsittelevät henkilötietoja.

11.5.2 Artikla 32 - Käsittelyn turvallisuus: Vastaa omaisuuseriin perustuvaa riskien arviointia ja luokiteltuihin omaisuuseriin sekä kriittiseen infrastruktuuriin sovitettuja suojatoimia.

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

11.6.1 Artikla 21(2)(a, b): Velvoittaa varmistamaan omaisuuserien näkyvyyden ja inventoinnin riskianalyysin, suojauksen ja kyberturvallisuuspoikkeamiin reagoinnin perustana.

11.6.2 Artikla 21(3): Korostaa rakenteellisen omaisuudenhallinnan välttämättömyyttä osana organisaation tietoturvakulttuuria.

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

11.7.1 Artikla 5 - ICT-hallinto ja sisäinen valvonta: Edellyttää finanssialan toimijoita hallinnoimaan ICT-omaisuuseriä selkeiden inventointi-, omistajuus- ja suojausvaatimusten mukaisesti.

11.7.2 Artikla 9 - ICT-riskienhallinnan viitekehys: Määrittää, että omaisuudenhallintaprosessien on tuettava uhkien lieventämistä, jatkuvuussuunnittelua ja palvelujen häiriönsietokykyä.

11.8 COBIT 2019:

11.8.1 BAI09 - Manage Assets: Vastaa suoraan yrityksen omaisuuserien rakenteellista tunnistamista, luokittelua, käyttöä ja hävittämistä.

11.8.2 DSS01 - Managed Operations: Tukee sellaisten kontrollien toteuttamista, joilla varmistetaan omaisuuserien suojaus ja operatiivisen hallinnan jatkuvuus.

11.8.3 MEA03 - Monitor, Evaluate, and Assess Compliance: Varmistaa omaisuudenhallinnan kontrollien ja niiden sääntelyn mukaisen tehokkuuden säännöllisellä auditoinnilla.