					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P12S					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**

Yhdenmukaisuus standardien ja sääntelyvaatimusten kanssa

Standardi/sääntely	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohta 8	Omaisuudenhallinnan vaatimukset
ISO/IEC 27002:2022	Kontrolli 5	Omaisuudenhallinnan kontrollit
NIST SP 800-53 Rev.5	CM-8	Järjestelmäkomponenttien omaisuusluettelo
EU:n NIS2-direktiivi	Artikla 21(2)(a)	Omaisuuserien seuranta verkko- ja tietojärjestelmien suojaamiseksi
EU:n DORA-asetus	Artikla 5(8)	ICT-omaisuuseriä koskevat omaisuusluettelovaatimukset
COBIT 2019	BAI	IT-omaisuuserien elinkaaren hallinta
EU:n GDPR	Artikla 30	Käsittelytoimien dokumentointi

1. Tarkoitus

1.1 Tämä politiikka määrittää, miten organisaatio tunnistaa, seuraa, suojaa ja poistaa käytöstä tietovarallisuuden, mukaan lukien fyysiset ja digitaaliset omaisuuserät.

1.2 Tavoitteena on vähentää operatiivisia riskejä ja tietoturvariskejä varmistamalla kaikkien liiketoiminnan omaisuuserien näkyvyys, vastuun kohdentuminen ja turvallinen käsittely koko niiden elinkaaren ajan.

1.3 Luotettava omaisuusluettelo tukee vaatimustenmukaisuutta, tietoturvapoikkeamiin reagointia, jatkuvuussuunnittelua ja riskienhallintaa.

1.4 Tämä politiikka tukee myös ISO/IEC 27001 -sertifiointia ja osoittaa yhdenmukaisuuden GDPR:n, NIS2:n ja DORA:n kaltaisten viitekehysten mukaisten oikeudellisten, taloudellisten ja kyberturvallisuusvelvoitteiden kanssa.

1.5 Pienille ja keskisuurille yrityksille (pk-yrityksille) yksinkertainen mutta systemaattinen omaisuudenhallinnan toimintamalli on olennainen, jotta hallitsemattomat laitteet, tietojen häviäminen tai auditointiepäonnistumiset voidaan välttää erityisesti silloin, kun tekniset henkilöstöresurssit ovat rajalliset.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia organisaation omistamia, vuokraamia tai muutoin hallinnoimia omaisuuseriä, mukaan lukien omaisuuserät, joita käytetään seuraavissa ympäristöissä:

2.1.1 toimistotyössä

2.1.2 etä- tai hybridityössä

2.1.3 kenttätyössä tai liikkuvassa työssä

2.1.4 pilvipalveluissa ja ulkoistetuissa ympäristöissä

2.2 Soveltamisalaan kuuluvat omaisuuserätyypit sisältävät muun muassa seuraavat:

2.2.1 laitteisto: kannettavat tietokoneet, pöytätietokoneet, näytöt, puhelimet, tabletit, USB-muistit, reitittimet, tulostimet, varmuuskopiointivälineet

2.2.2 ohjelmistot: asennetut sovellukset, SaaS-työkalut, käyttöjärjestelmät, virustorjuntatyökalut, lisenssit

2.2.3 tiedot omaisuuserinä: liiketoiminnan tietovarannot, laskentataulukot, asiakastiedot, lähdekoodi

2.2.4 digitaaliset tunnisteet ja palvelut: verkkotunnukset, digitaaliset varmenteet, API-avaimet, sähköpostitilit, pilvipalvelujen kirjautumistunnukset

2.2.5 pääsynhallintavälineet: avaimet, älykortit, kulkutunnisteet, biometriset tunnisteet

2.3 Kaikki työntekijät, sopimuskumppanit ja kolmansien osapuolten palveluntarjoajat, jotka käsittelevät organisaation omaisuuseriä, kuuluvat tämän politiikan soveltamisalaan.

2.4 Tämä politiikka koskee sekä lyhytaikaisia omaisuuseriä (esimerkiksi projektikohtaisia kannettavia tietokoneita) että pitkäaikaisia omaisuuseriä sekä jaettuja omaisuuseriä, joita käyttää useampi henkilö.

3. Tavoitteet

3.1 Luoda ja ylläpitää täydellinen ja täsmällinen omaisuusluettelo kaikista merkityksellisistä omaisuuseristä sekä pitää se jatkuvasti ajan tasalla.

3.2 Varmistaa, että jokaiselle omaisuuserälle on nimetty omistaja, joka vastaa sen käytöstä, säilytyksestä ja palautuksesta.

3.3 Luokitella omaisuuserät arkaluonteisuuden, liiketoimintavaikutuksen tai sääntelymerkityksen perusteella, jotta niille voidaan määrittää eriytetyt suojaustasot.

3.4 Määrittää selkeät menettelyt omaisuuserien luovutukselle, uudelleenkohdentamiselle, ylläpidolle, katoamisilmoituksille ja käytöstäpoistolle.

3.5 Varmistaa, että omaisuuseriä käsitellään turvallisesti koko niiden elinkaaren ajan ja että niiden sisältämät tiedot joko suojataan tai poistetaan turvallisesti hävittämisen yhteydessä.

3.6 Vähentää sellaisten tietoturvapoikkeamien todennäköisyyttä, jotka johtuvat seuraamattomista, palauttamattomista tai väärinkäytetyistä organisaation resursseista.

3.7 Tukea sovellettavan lainsäädännön noudattamista (esimerkiksi GDPR:n osoitusvelvollisuuden osalta) sekä kyberturvallisuuden sertifiointivaatimuksia.

4. Roolit ja vastuut

4.1 Toimitusjohtaja

4.1.1 Omistaa tämän politiikan ja vastaa siitä, että omaisuudenhallinnan käytännöt otetaan käyttöön ja niitä noudatetaan koko organisaatiossa.

4.1.2 Katselmoi ja hyväksyy omaisuusluetteloon tehtävät päivitykset sekä valtuuttaa tarvittaessa omaisuuserien käytöstäpoiston tai siirron.

4.1.3 Hänelle on ilmoitettava kaikista merkittävistä omaisuuserien katoamisista, varkauksista tai väärinkäytöksistä.

4.2 IT-vastaava tai nimetty omaisuudenhallintavastaava

4.2.1 Ylläpitää omaisuusluetteloa (esimerkiksi laskentataulukossa, tikettijärjestelmässä tai kevyessä omaisuudenhallintaratkaisussa).

4.2.2 Määrittää omaisuuserien omistajuuden ja seuraa tilamuutoksia (esimerkiksi uusi, käytössä, korjattavana, poistettu käytöstä).

4.2.3 Varmistaa, että kaikki luovutetut omaisuuserät on dokumentoitu ja kohdistettu yksittäiselle henkilölle tai liiketoimintayksikölle.

4.2.4 Varmistaa, että luokitusmerkinnät otetaan käyttöön ja niitä noudatetaan (esimerkiksi Sisäinen, Luottamuksellinen).

4.2.5 Koordinoi omaisuuserien takaisinoton, puhdistamisen ja käytöstäpoiston palvelussuhteen päättymisen tai käytöstäpoiston yhteydessä.

4.2.6 Raportoi ratkaisemattomat omaisuuseriä koskevat poikkeamat toimitusjohtajalle.

[... 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 kerran vuodessa ja aina, kun:

9.1.1 otetaan käyttöön uusia teknologioita tai uusia omaisuuserätyyppejä

9.1.2 omaisuuserien seurantamenettelyt muuttuvat (esimerkiksi uusien työkalujen tai alustojen käyttöönoton myötä)

9.1.3 uudet sääntelyvelvoitteet vaikuttavat omaisuuserien jäljitettävyyteen tai hävittämiseen

9.1.4 poikkeama tai auditointi tunnistaa puutteen nykyisissä omaisuudenhallinnan käytännöissä

9.2 Katselmointiin on osallistuttava toimitusjohtajan ja IT-vastaavan, ja sen on sisällettävä päivitykset omaisuuserien käsittelymenettelyihin, omaisuusluettelopohjiin ja luokitusohjeistukseen.

9.3 Kaikki päivitykset on dokumentoitava ja viestittävä niitä koskevalle henkilöstölle. Versiohallittu muutosloki on säilytettävä.

10. Liittyvät politiikat ja yhteydet

10.1 P2S – Hallintoroolien ja vastuiden politiikka: määrittää vastuut politiikan omistajuudesta ja IT-operaatioista.

10.2 P4S – Pääsynhallintapolitiikka: yhdistää omaisuuserien käytön (esimerkiksi kannettavat tietokoneet, mobiililaitteet) käyttäjien käyttöoikeuksiin ja identiteetin- ja pääsynhallintaan.

10.3 P7S – Perehdytys- ja työsuhteen päättämispolitiikka: varmistaa, että omaisuuserien luovutus ja palautus sisältyvät henkilöstön elinkaariprosesseihin.

10.4 P13S – Tiedon luokittelu- ja merkintäpolitiikka: määrittää säännöt sille, milloin omaisuuserä on luokiteltava Sisäiseksi tai Luottamukselliseksi.

10.5 P30S – Tietoturvapoikkeamien hallintapolitiikka: ohjaa reagointimenettelyjä, jos omaisuuserään liittyvä tapahtuma johtaa tietoturva- tai tietosuojaloukkaukseen.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Kohta 8.1: edellyttää operatiivisia kontrolleja omaisuuserien hallintaan ja niiden suojaamiseen koko käytön ajan.

11.2 ISO/IEC 27002

11.2.1 Kontrolli 5.9: kuvaa, miten omaisuuserät tunnistetaan, niille nimetään omistaja, ne luokitellaan ja niitä hallitaan turvallisesti.

11.3 NIST SP 800-53 Rev

11.3.1 CM-8: edellyttää organisaatioita laatimaan ja ylläpitämään järjestelmäkomponenttien omaisuusluetteloa, mukaan lukien laitteisto, ohjelmistot ja virtuaaliset omaisuuserät.

11.4 EU:n GDPR

11.4.1 Artikla 30: edellyttää käsittelytoimien dokumentointia, mikä perustuu siihen, että tiedetään missä tietoja säilytetään ja millä omaisuuserillä.

11.5 EU:n NIS2-direktiivi

11.5.1 Artikla 21(2)(a): edellyttää teknisiä ja organisatorisia toimenpiteitä, mukaan lukien omaisuuserien seuranta, verkko- ja tietojärjestelmien suojaamiseksi.

11.6 EU:n DORA-asetus

11.6.1 Artikla 5(8): rahoitusalan toimijoiden on ylläpidettävä yksityiskohtaista ICT-omaisuuseräluetteloa osana ICT-riskien hallintaa.

11.7 COBIT 2019

11.7.1 BAI09: määrittää, että IT-omaisuuseriä on hallittava koko niiden elinkaaren ajan hankinnasta käytöstäpoistoon asti selkein omistajuuksin ja kontrollein.