					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P02S					Asiakirjan nimi: **Hallinnointirooleja ja vastuita koskeva politiikka**							
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**

Yhdenmukaistettu standardien ja sääntelyvaatimusten kanssa

Standardi/sääntely	Kohta/artikla	Huomio
ISO/IEC 27001:2022	Kohta 5	
ISO/IEC 27002:2022	Toimenpiteet: 5.2, 5.3, 5.4	
NIST SP 800-53 Rev.5	PM-1, PL-1, PL-4, CA-1, AC-1	
EU:n GDPR	Artiklat 5(2), 32	

1. Tarkoitus

1.1 Tämä politiikka määrittää, miten tietoturvan hallinnointiin liittyvät vastuut organisaatiossa osoitetaan, delegoidaan ja hallitaan ISO/IEC 27001:2022 -standardin sekä muiden sovellettavien sääntelyvaatimusten noudattamisen varmistamiseksi.

1.2 Politiikka varmistaa vastuiden selkeän kohdentamisen kaikilla tasoilla ja tukee toiminnallista tehokkuutta määrittämällä selkeästi, kuka vastaa kustakin tietoturvaan liittyvästä tehtävästä.

1.3 Tämä politiikka tukee auditointivalmiutta ja vahvistaa asiakkaiden luottamusta osoittamalla muodollisen tietoturvan hallintamallin myös organisaatioissa, joissa tekninen henkilöstö on rajallinen tai IT-toimintoja on ulkoistettu.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia henkilöitä, jotka käsittelevät organisaation järjestelmiä tai tietoja, mukaan lukien:

2.1.1 liiketoimintavastaavat ja toimitusjohtaja

2.1.2 työntekijät ja sopimuskumppanit

2.1.3 ulkoiset IT-palveluntarjoajat ja konsultit

2.2 Politiikka kattaa kaikki järjestelmät, ympäristöt ja palvelut, joita käytetään liiketoiminta- tai asiakastietojen käsittelyyn, siirtämiseen tai tallentamiseen, mukaan lukien:

2.2.1 toimiston IT-infrastruktuuri ja etätyölaitteet

2.2.2 pilvipalvelut ja sähköpostipalvelut

2.2.3 fyysiset tallenteet ja jaetut verkkoasemat

2.3 Soveltamisala kattaa sekä sisäiset että ulkoistetut toiminnot, joihin liittyy tietoturvan hallinnointi.

3. Tavoitteet

3.1 Määrittää selkeä vastuunjako kaikille tietoturvaan liittyville tehtäville, mukaan lukien politiikkojen hallinta, käyttöoikeuksien hallinta, poikkeamien käsittely ja seuranta.

3.2 Mahdollistaa tehtävien asianmukainen eriyttäminen eturistiriitojen ja väärinkäytösriskien vähentämiseksi.

3.3 Varmistaa, että tietoturvatehtävät ja -roolit dokumentoidaan selkeästi ja katselmoidaan säännöllisesti.

3.4 Mahdollistaa tietoon perustuvan päätöksenteon, eskaloinnin sekä IT- ja tietoturvariskien valvonnan.

3.5 Tukea ISO/IEC 27001:2022 -sertifiointia sekä vahvistaa asiakkaiden, kumppaneiden ja auditoijien luottamusta.

4. Roolit ja vastuut

4.1 Toimitusjohtaja / liiketoimintavastaava

4.1.1 Vastaa tämän politiikan toimeenpanosta ja valvonnasta kokonaisuutena.

4.1.2 Hyväksyy kaikki tietoturvaroolit, vastuut ja delegointipäätökset.

4.1.3 Valvoo noudattamista ja tekee lopulliset päätökset politiikkaa koskevista poikkeuksista ja eskaloinneista.

4.2 Nimetty tietoturvakoordinaattori (jos nimetty)

4.2.1 Roolissa voi toimia henkilöstön jäsen tai luotettu konsultti.

4.2.2 Mikroyritysympäristössä tämän roolin voi hoitaa toimitusjohtaja tai ulkoinen palveluntarjoaja.

4.2.3 Avustaa käyttöoikeuksien hallinnan, tietoturvapoikkeamiin reagoinnin ja perustason teknisten tietoturvatehtävien päivittäisessä toteutuksessa.

4.2.4 Raportoi suoraan toimitusjohtajalle kaikista tietoturvaan liittyvistä asioista ja riskeistä.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Vuosittainen katselmointi

9.1.1 Toimitusjohtajan on katselmoitava tämä politiikka 12 kuukauden välein varmistaakseen, että se vastaa edelleen oikeudellisia velvoitteita, toiminnallisia tarpeita ja ISO/IEC 27001 -sertifioinnin vaatimuksia.

9.2 Katselmoinnit katselmointijaksojen välillä

9.2.1 Katselmointi on tehtävä myös silloin, kun:

9.2.1.1 organisaatiossa tapahtuu merkittäviä muutoksia

9.2.1.2 uusi palveluntarjoaja otetaan käyttöön

9.2.1.3 tapahtuu vakava tietoturvapoikkeama

9.2.1.4 EU:n GDPR:ää, EU:n NIS2-direktiiviä tai EU:n DORA-asetusta päivitetään

9.3 Versionhallinta ja dokumentointi

9.3.1 Kaikkien katselmointien on sisällettävä:

9.3.1.1 katselmoinnin päivämäärä

9.3.1.2 yhteenveto tehdyistä muutoksista

9.3.1.3 toimitusjohtajan allekirjoitus tai dokumentoitu hyväksyntä

9.3.1.4 arkistoidut aiemmat versiot auditointia varten

9.4 Muutoksista viestiminen

9.4.1 Kaikista politiikan päivityksistä on viestittävä viipymättä henkilöstölle ja palveluntarjoajille sähköpostitse, sisäisten portaalien kautta tai virallisilla tiedotteilla.

10. Liitännäiset politiikat ja yhteydet

10.1 Tämä politiikka on toimeenpantava yhdessä seuraavien SME-politiikkojen kanssa täyden vaikuttavuuden varmistamiseksi:

10.1.1 P4S – Käyttöoikeuksien hallintapolitiikka: määrittää, miten käyttöoikeudet myönnetään, hallitaan ja poistetaan suhteessa osoitettuihin rooleihin ja valvontaan.

10.1.2 P8S – Tietoturvatietoisuuden ja koulutuksen politiikka: vahvistaa roolikohtaisia vastuita ja odotuksia.

10.1.3 P17S – Tietosuojan ja yksityisyyden politiikka: määrittää EU:n GDPR:n mukaiset oikeudelliset velvoitteet, jotka osoitetaan tässä hallinnointipolitiikassa määritellyille rooleille.

10.1.4 P30S – Tietoturvapoikkeamien hallintapolitiikka: edellyttää määriteltyjä vastuita poikkeamien ilmoittamiseen, eskalointiin ja ratkaisemiseen.

10.2 Yhdessä nämä politiikat mahdollistavat yhdenmukaisen soveltamisen, sisäisen vastuunjaon ja ulkoisten vaatimusten noudattamisen.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Kohta 5.3 – Organisaation roolit, vastuut ja valtuudet: edellyttää, että roolit osoitetaan selkeästi ja että ylin johto tukee niitä.

11.2 ISO/IEC 27002

11.2.1 Toimenpiteet 5.2–5.4: edellyttävät tietoturvaroolien selkeää dokumentointia, tehtävien eriyttämistä ja johdon valvontaa.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: määrittää yleisen tietoturvaohjelman, jossa vastuut on määritelty.

11.3.2 PL-1–PL-4: edellyttävät suunnittelukontrolleja, mukaan lukien politiikkojen laatiminen ja dokumentoidut roolimäärittelyt.

11.3.3 CA-1: edellyttää määriteltyjä arviointi- ja valtuutusrooleja.

11.3.4 AC-1: liittää roolipohjaisen käyttöoikeuksien hallinnan osoitettuihin hallinnointivastuisiin.

11.4 EU:n GDPR

11.4.1 Artikla 5(2) – Osoitusvelvollisuus: edellyttää, että organisaatio kykenee osoittamaan vaatimustenmukaisuuden roolien ja vastuiden avulla.

11.4.2 Artikla 32 – Käsittelyn turvallisuus: korostaa tehtävien selkeää osoittamista henkilötietojen suojaamiseksi.

11.5 EU:n NIS

11.5.1 Artikla 21(2)(a): edellyttää hallinnointirakenteita, joihin sisältyvät muodollisesti määritellyt roolit kyberriskien ja poikkeamien hallintaan.

11.6 EU:n DORA

11.6.1 Artiklat 9 ja 10: edellyttävät, että finanssialan toimijat osoittavat ja valvovat tieto- ja viestintätekniikkaan sekä tietoturvaan liittyvät vastuut selkeästi.

11.7 COBIT 2019

11.7.1 EDM03 – Varmista riskien optimointi: edellyttää selkeästi määriteltyjä rooleja ja eskalointipolkuja tietoturvariskien hallintaan.

11.7.2 APO13 – Hallitse tietoturvaa: osoittaa strategiset ja operatiiviset tietoturvatehtävät henkilöille ja rooleille.

11.7.3 DSS05 – Hallitse tietoturvapalveluja: edellyttää rakennetta ja jäljitettävyyttä ulkoisten ja sisäisten tietoturvapalvelujen vastuille.