					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P17S					Asiakirjan nimi: **Tietosuoja- ja yksityisyydensuojapolitiikka**							
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	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	Lausekkeet 5.1, 6.1.3, 8	
ISO/IEC 27002:2022	Kontrollit 5.34, 8.10–8.12	
NIST SP 800-53 Rev. 5	AR-2, PL-5, AC-6, IR-4	
EU:n GDPR	Artiklat 5, 6, 12–23, 30, 32–34	
EU:n NIS2-direktiivi	Artikla 21(2)(e), 21(2)(f)	
EU:n DORA-asetus	Artiklat 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA03	

1. Tarkoitus

1.1. Tämä politiikka määrittää, miten organisaatio suojaa henkilötietoja lakisääteisten velvoitteiden, sääntelykehysten ja kansainvälisten tietoturvastandardien mukaisesti.

1.2. Se varmistaa, että henkilötietoja – riippumatta siitä, koskevatko ne asiakkaita, henkilöstöä tai kumppaneita – kerätään, käytetään, säilytetään ja poistetaan lainmukaisesti, asianmukaisesti ja turvallisesti.

1.3. Tämä politiikka tukee myös ISO/IEC 27001:2022 -standardin vaatimusten noudattamista ja auditointivalmiutta edellyttämällä johdonmukaista, riskiperusteista lähestymistapaa tietosuojan toteuttamiseen.

1.4. Tämän politiikan avulla organisaatio osoittaa osoitusvelvollisuuden toteutumista ja vahvistaa asiakkaiden luottamusta korostamalla läpinäkyvyyttä, tietojen minimointia ja vahvaa tietosuojan hallintaa.

2. Soveltamisala

2.1. Tämä politiikka koskee:

2.1.1. kaikkia työntekijöitä, sopimuskumppaneita ja palveluntarjoajia, jotka käyttävät, käsittelevät tai hallinnoivat henkilötietoja

2.1.2. kaikkia järjestelmiä, sovelluksia ja sijainteja, joissa henkilötietoja säilytetään tai välitetään

2.1.3. kaikkia henkilötietoja riippumatta siitä, säilytetäänkö niitä sähköisessä muodossa, paperimuodossa, pilvipalveluissa tai mobiililaitteissa

2.2. Tämä politiikka koskee asiakkaisiin, henkilöstöön, toimittajiin ja muihin tunnistettuihin tai tunnistettavissa oleviin henkilöihin liittyviä tietoja.

2.3. Tätä politiikkaa sovelletaan riippumatta siitä, käsitelläänkö tietoja organisaation sisällä vai kolmannen osapuolen palveluntarjoajan toimesta.

3. Tavoitteet

3.1. Varmistaa, että henkilötietoja käsitellään tietosuojalainsäädännön ja tietoturvastandardien, mukaan lukien GDPR:n, NIS2-direktiivin ja ISO 27001:n, mukaisesti.

3.2. Suojata henkilötiedot luvattomalta pääsyltä, väärinkäytöltä, muuttamiselta ja häviämiseltä selkeillä teknisillä ja organisatorisilla kontrolleilla.

3.3. Turvata rekisteröityjen oikeudet, mukaan lukien oikeus saada pääsy tietoihinsa sekä oikeus tietojen oikaisuun ja poistamiseen.

3.4. Määrittää organisaation tietosuojaan liittyvät roolit ja vastuut selkeästi.

3.5. Varmistaa tietojen minimointi, turvallinen säilyttäminen ja oikea-aikainen poistaminen kaikissa järjestelmissä ja prosesseissa.

3.6. Vähentää vaatimustenvastaisuuden, oikeudellisten seuraamusten, mainehaitan ja asiakkaiden luottamuksen heikkenemisen riskiä.

4. Roolit ja vastuut

4.1. Toimitusjohtaja

4.1.1. hyväksyy tämän politiikan ja varmistaa sen toimeenpanon

4.1.2. varmistaa riittävät resurssit tietosuojariskien hallintaan ja poikkeamien käsittelyyn

4.1.3. vastaa kokonaisuutena tietosuojalainsäädännön ja standardien noudattamisesta

4.2. Tietosuojakoordinaattori (sisäinen tai ulkoistettu)

4.2.1. ylläpitää selostetta henkilötietojen käsittelytoimista

4.2.2. käsittelee rekisteröityjen pyynnöt ja viranomaistiedustelut

4.2.3. tukee riskien arviointia, koulutusta ja politiikan toimeenpanoa

4.2.4. dokumentoi henkilötietojen tietoturvaloukkaukset ja tekee tarvittaessa ilmoitukset viranomaisille

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

9. Katselmointi- ja päivitysvaatimukset

9.1. Säännölliset katselmoinnit

9.1.1. tietosuojakoordinaattorin on katselmoitava tämä politiikka vähintään kerran 12 kuukaudessa, ja toimitusjohtajan on hyväksyttävä se

9.1.2. katselmoinnissa on arvioitava politiikan ajantasaisuus, yhdenmukaisuus sääntelyvaatimusten kanssa ja toiminnallinen tehokkuus

9.2. Katselmoinnin käynnistävät herätteet

9.2.1. politiikan päivitykset on käynnistettävä myös seuraavissa tilanteissa:

9.2.1.1. uudet tai päivitetyt tietosuojalait (esim. GDPR, DORA)

9.2.1.2. henkilötietoihin liittyvät tietoturvapoikkeamat tai tietosuojaloukkaukset

9.2.1.3. uusien järjestelmien, työkalujen tai palvelujen käyttöönotto, joissa käsitellään henkilötietoja

9.2.1.4. olennaiset auditointihavainnot tai viranomaisen suositukset

9.3. Muutostenhallinta ja viestintä

9.3.1. kaikki politiikkaan tehtävät muutokset on dokumentoitava muodollisesti muutoslokiin

9.3.2. päivitetyt versiot on jaettava kaikille työntekijöille ja asiaankuuluville urakoitsijoille

9.3.3. arkistoidut versiot on säilytettävä vaatimustenmukaisuuden audit trailia varten

10. Liittyvät politiikat ja kytkennät

10.1. Tätä politiikkaa sovelletaan yhdessä muiden pk-yrityksen politiikkojen kanssa kattavan ja toimeenpantavan tietosuoja- ja yksityisyydensuojan viitekehyksen muodostamiseksi:

10.1.1. P13S – Tiedon luokittelu- ja merkintäpolitiikka: varmistaa, että henkilötiedot luokitellaan asianmukaisesti, jotta tietosuojatoimenpiteet voidaan toteuttaa riskiperusteisesti.

10.1.2. P14S – Tietojen säilytys- ja hävityspolitiikka: määrittää selkeät säännöt sille, kuinka kauan henkilötietoja on säilytettävä ja mitä turvallisia menetelmiä niiden hävittämisessä on käytettävä säilytysajan päätyttyä.

10.1.3. P16S – Tietojen peittämis- ja pseudonymisointipolitiikka: määrittää, miten henkilötunnisteet on muunnettava ennen tietojen käyttöä ei-tuotantoympäristöissä tai ennen niiden jakamista organisaation ulkopuolelle.

10.1.4. P30S – Tietoturvapoikkeamien hallintapolitiikka: kattaa vaiheet, joita henkilötietojen tietoturvaloukkauksiin reagointi edellyttää, mukaan lukien ilmoitukset viranomaisille ja asianomaisille henkilöille vaadituissa määräajoissa.

10.1.5. P2S – Hallinnointirooleja ja vastuita koskeva politiikka: selventää vastuurakenteen ja päätöksentekoroolit, joita sovelletaan tietosuojan toimeenpanoon ja valvontaan.

10.2. Nämä liittyvät politiikat on katselmoitava ja niitä on sovellettava yhdessä, jotta varmistetaan järjestelmät, henkilöstö ja toimittajat kattava päästä päähän -tietosuoja.

11. Viitestandardit ja viitekehykset

11.1. ISO/IEC 27001

11.1.1. Lauseke 5.1 – Edellyttää, että ylin johto osoittaa johtajuutta ja sitoutumista henkilötietojen suojaamiseen.

11.1.2. Lauseke 6.1.3 – Edellyttää henkilötietojen käsittelyyn liittyvien riskien käsittelyä.

11.1.3. Lauseke 8.1 – Edellyttää operatiivisten kontrollien toteuttamista tietojen suojaamiseksi koko niiden elinkaaren ajan.

11.2. ISO/IEC 27002

11.2.1. Kontrolli 5.34 – Antaa toteutusohjeita tietosuojan varmistamiseen ja henkilötietojen turvalliseen käsittelyyn.

11.2.2. Kontrolli 8.10 – Käsittelee henkilötietojen turvallista hävittämistä jäännöstietojen paljastumisen estämiseksi.

11.2.3. Kontrolli 8.11 – Tukee peittämisen ja pseudonymisoinnin käyttöä minimoinnin toteuttamisessa.

11.2.4. Kontrolli 8.12 – Estää tietojen luvattoman vuotamisen kontrolloimalla tietojen käyttöä ja pääsyä niihin.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AR-2 – Määrittää tietosuojariskien hallinnan roolit ja vastuut.

11.3.2. PL-5 – Edellyttää tietosuunnitelman dokumentointia tietojen käyttöä ja suojaamista varten.

11.3.3. AC-6 – Edellyttää vähimmän oikeuden periaatteen ja pääsynhallinnan soveltamista henkilötietoihin.

11.3.4. IR-4 – Edellyttää poikkeamien käsittelyprosesseja henkilötietoihin liittyville loukkauksille.

11.4. EU:n GDPR

11.4.1. Artikla 5 – Määrittää lainmukaisen, asianmukaisen ja läpinäkyvän henkilötietojen käsittelyn keskeiset periaatteet.

11.4.2. Artikla 6 – Edellyttää voimassa olevaa oikeusperustetta jokaiselle henkilötietojen käsittelytoimelle.

11.4.3. Artiklat 12–23 – Määrittävät rekisteröityjen oikeudet, mukaan lukien oikeus saada pääsy tietoihin, tietojen oikaisu, poistaminen ja vastustaminen.

11.4.4. Artikla 30 – Edellyttää selostetta käsittelytoimista.

11.4.5. Artikla 32 – Edellyttää asianmukaisia teknisiä ja organisatorisia tietoturvatoimenpiteitä.

11.4.6. Artiklat 33–34 – Määrittävät tietoturvaloukkauksia koskevat ilmoitusvelvollisuudet viranomaisille ja rekisteröidyille.

11.5. EU:n NIS2-direktiivi

11.5.1. Artikla 21(2)(e) – Edellyttää toimenpiteitä tietosuojan varmistamiseksi kyberturvallisuuspolitiikkojen mukaisesti.

11.5.2. Artikla 21(2)(f) – Edellyttää mekanismeja henkilötietojen ja luottamuksellisten tietojen turvallisuuden hallintaan ICT-järjestelmissä.

11.6. EU:n DORA-asetus

11.6.1. Artikla 6 – Edellyttää sisäisiä hallintakehyksiä tietoriskien ja tietosuojan hallintaan.

11.6.2. Artikla 15 – Velvoittaa finanssialan toimijat varmistamaan, että kolmannen osapuolen palveluntarjoajat suojaavat henkilötietoja ja tukevat sääntelyvaatimusten noudattamista.

11.6.3. Artikla 17 – Edellyttää varmistamaan, että henkilötietoja käsittelevät ICT-järjestelmät ovat turvallisia, häiriönsietokykyisiä ja valvottuja.

11.7. COBIT 2019

11.7.1. APO12 – Manage Risk: edellyttää tietosuoja- ja henkilötietoriskien tunnistamista ja käsittelyä.

11.7.2. DSS05 – Manage Security Services: edellyttää suojatoimia henkilötietoihin kohdistuvan luvattoman pääsyn estämiseksi.

11.7.3. MEA03 – Monitor Compliance: edellyttää, että organisaatiot varmistavat tietosuoja- ja henkilötietolainsäädännön jatkuvan noudattamisen.