					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P17					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/säädös	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	Lausekkeet 5.1, 6.1.3, 8.1, 10	Asiaankuuluvat yleiset, tekniset ja jatkuvan parantamisen tietosuojakontrollit
ISO/IEC 27002:2022	Kontrollit 5.34, 8.10, 8.11, 8.12	Henkilötietojen käsittelyä, säilyttämistä, poistamista, anonymisointia ja rekisteröidyn oikeuksia koskevat kontrollit
NIST SP 800-53 Rev.5	AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	Hallinnointia, riskienhallintaa, käyttöoikeuksien hallintaa, lokitusta, tietoturvaloukkausten käsittelyä ja tietosuojaohjelmaa koskevat vaatimukset
EU:n GDPR	Artiklat 5, 6, 12–23, 25, 28, 30, 32–34; johdanto-osan kappale 78	Keskeiset tietosuojan, osoitusvelvollisuuden, rekisteröidyn oikeuksien, DSR-pyyntöjen, tietoturvaloukkausten sekä sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet
EU:n NIS2-direktiivi	Artikla 21(2)(e), (f)	Riskiperusteiset tietoturvakontrollit keskeisille ja tärkeille toimijoille
EU:n DORA-asetus	Artiklat 6(2)(d), 11(1)(c), 15(1), 17	Hallinnointia, kolmansien osapuolten riskejä ja käsittelyn turvallisuutta koskevat vaatimukset
COBIT 2019	APO12, DSS01, DSS05, MEA	Riskienhallinta, turvalliset operatiiviset toiminnot ja vaatimustenmukaisuuden valvonta

1. Tarkoitus

1.1 Tämä politiikka määrittää pakolliset organisatoriset periaatteet ja tekniset vaatimukset henkilötietojen suojaamiselle sekä sisäänrakennetun tietosuojan toteuttamiselle kaikissa ympäristöissä.

1.2 Tämä politiikka täsmentää organisaation vastuut kansainvälisten standardien ja sääntelykehysten mukaisesti ja varmistaa, että henkilötietoja kerätään, käsitellään, säilytetään, jaetaan ja hävitetään lainmukaisesti, turvallisesti ja läpinäkyvästi.

1.3 Tämä politiikka vahvistaa myös sovellettavan tietosuojalainsäädännön ja viitekehysten noudattamisen, mukaan lukien EU:n yleinen tietosuoja-asetus (GDPR), EU:n NIS2-direktiivi, EU:n DORA-asetus, ISO/IEC 27001:2022 ja COBIT 2019.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia organisaatioyksiköitä, henkilöstöä ja järjestelmiä, jotka osallistuvat henkilötietojen käsittelyyn, mukaan lukien:

2.1.1 työntekijät, urakoitsijat, konsultit ja kolmannen osapuolen palveluntarjoajat.

2.1.2 kaikissa liiketoiminnoissa sisäisistä ja ulkoisista lähteistä kerätyt tiedot.

2.1.3 fyysiset ja digitaaliset tallennusvälineet, mukaan lukien pilvipalvelut, SaaS-ympäristöt, mobiililaitteet ja paperimuotoiset tallenteet.

2.1.4 kaikki ympäristöt, mukaan lukien tuotanto-, kehitys-, testi- ja varmuuskopiointijärjestelmät, joissa henkilötietoja voi olla.

2.2 Se kattaa kaikki sovellettavan tietosuojalainsäädännön ja standardien piiriin kuuluvat käsittelytoimet, mukaan lukien muun muassa:

2.2.1 henkilötietojen kerääminen, säilyttäminen, käyttö, siirtäminen ja hävittäminen.

2.2.2 rekisteröidyn oikeuksien toteuttaminen, käsittelyn oikeusperusteen dokumentointi ja suostumusten hallinta.

2.2.3 rajat ylittävät siirrot, tietoturvaloukkauksista ilmoittaminen ja tietojen jakaminen kolmansille osapuolille.

2.2.4 turvallinen suunnittelu sekä oletusarvoisen tietosuojan toteuttaminen järjestelmissä ja prosesseissa.

3. Tavoitteet

3.1 Varmistaa henkilötietojen lainmukainen, läpinäkyvä ja osoitusvelvollisuuden täyttävä käsittely ISO/IEC 27001:2022 -standardin ja siihen liittyvien oikeudellisten velvoitteiden mukaisesti.

3.2 Sisällyttää sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet kaikkiin tietojärjestelmiin, palveluihin ja liiketoimintaprosesseihin.

3.3 Toteuttaa tekniset ja organisatoriset toimenpiteet (TOM), joilla suojataan henkilötietojen luottamuksellisuus, eheys ja saatavuus koko niiden elinkaaren ajan.

3.4 Määrittää tietosuojan hallintoroolit ja vastuurakenteet, mukaan lukien tietosuojavastaavan, tietoturvatoiminnon, laki- ja vaatimustenmukaisuustoiminnon sekä tiedon omistajien vastuut.

3.5 Mahdollistaa täysimääräinen vaatimustenmukaisuus GDPR:n artiklojen 5, 6, 25, 30 ja 32 sekä NIS2:n ja DORA:n riskien vähentämistä ja häiriönsietokykyä koskevien vaatimusten kanssa.

3.6 Turvata rekisteröidyn oikeudet, mukaan lukien oikeus saada pääsy tietoihin, oikeus tietojen oikaisuun, poistamiseen, käsittelyn rajoittamiseen, siirrettävyyteen, vastustamiseen sekä suojaan automaattista päätöksentekoa vastaan.

3.7 Lieventää sääntelyyn, maineeseen, oikeudellisiin seuraamuksiin ja operatiiviseen toimintaan liittyviä riskejä, jotka aiheutuvat henkilötietojen luvattomasta käytöstä, väärinkäytöstä tai menetyksestä.

4. Roolit ja vastuut

4.1 Ylin johto

4.1.1 Vastaa strategisesta ohjauksesta ja osoittaa riittävät resurssit tietosuojaohjelman tueksi.

4.1.2 Hyväksyy tämän politiikan ja varmistaa sen toimeenpanon koko organisaatiossa.

4.2 Tietosuojavastaava (DPO)

4.2.1 Toimii riippumattomasti valvoakseen tietosuojasääntelyn noudattamista.

4.2.2 Ylläpitää GDPR:n artiklan 30 mukaista selostetta käsittelytoimista (RoPA).

4.2.3 Vastaa viranomaisyhteistyöstä, toteuttaa tietosuojaa koskevat vaikutustenarvioinnit (DPIA) ja hallinnoi tietoturvaloukkauksista ilmoittamisen prosesseja.

4.2.4 Katselmoi tietosuojaa koskevat poikkeukset ja ylläpitää tietosuojapoikkeusrekisteriä.

[... 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 aiemmin seuraavissa tilanteissa:

9.1.1 merkittävät oikeudelliset tai sääntelyyn liittyvät päivitykset (esim. GDPR:n muutokset tai DORA-asetuksen määräajat)

9.1.2 uudet järjestelmät tai henkilötietoja sisältävät käsittelytoimet

9.1.3 sisäisen tarkastuksen havainnot, jotka osoittavat politiikan puutteita

9.1.4 olennaiset tietoturvaloukkaustapaukset tai valvontaviranomaisen palaute

9.2 Katselmointivastuut

9.2.1 Tietosuojavastaava käynnistää politiikan katselmoinnin ja koordinoi sitä laki- ja vaatimustenmukaisuustoiminnon, riskienhallinnan, tietoturvallisuuden ja ylimmän johdon kanssa.

9.2.2 Kaikki päivitykset on kirjattava ISMS:n asiakirjojen ohjausrekisteriin ja jaettava vaikutuksen kohteena oleville sidosryhmille.

9.3 Muutoksenhallinta

9.3.1 Kaikki tämän politiikan muutokset on hyväksyttävä muodollisesti ylimmän johdon toimesta.

9.3.2 Vanhentuneet versiot on arkistoitava turvallisesti, ja päivitetyn version on sisällettävä dokumentoitu muutoshistoria.

10. Liittyvät politiikat ja yhteydet

10.1 P1 – Tietoturvapolitiikka. Määrittää yleiset tietoturvan hallinnan periaatteet, joihin tämä tietosuojapolitiikka perustuu. P1 tukee henkilötietojen luottamuksellisuutta, eheyttä ja saatavuutta kaikissa järjestelmissä ja palveluissa.

10.2 P6 – Riskienhallintapolitiikka. Määrittää organisaation riskienkäsittelymenetelmän, joka on välttämätön tietosuojariskien, DPIA-prosessien ja GDPR:n sekä ISO/IEC 27001:n lausekkeen 6.1.3 edellyttämien jäännösriskien arvioinnissa.

10.3 P13 – Tiedon luokittelu- ja merkintäpolitiikka. Ohjaa henkilötietojen ja arkaluonteisten tietojen luokittelua ja muodostaa perustan asianmukaisten tietosuojakontrollien soveltamiselle, mukaan lukien säilytyksen toimeenpano, pääsyn rajoittaminen ja turvallinen hävittäminen.

10.4 P14 – Tietojen säilytys- ja hävityspolitiikka. Tukee suoraan GDPR:n artiklojen 5(1)(e) ja 17 mukaisia tietosuojavaatimuksia varmistamalla, että henkilötietoja säilytetään vain niin kauan kuin on tarpeen ja että ne hävitetään turvallisesti oikeudellisten velvoitteiden mukaisesti.

10.5 P16 – Tietojen peittämisen ja pseudonymisoinnin politiikka. Määrittää kontrollit, joilla henkilötietojen tunnistettavuutta vähennetään teknisillä toimenpiteillä, kuten tokenisoinnilla, dynaamisella peittämisellä ja pseudonymisoinnilla, ja toteuttaa siten GDPR:n artiklan 32 sekä ISO/IEC 27002:n kontrollin 5.34 vaatimuksia.

10.6 P30 – Tietoturvapoikkeamien hallintapolitiikka. Kuvaa pakolliset tietoturvaloukkausten käsittelymenettelyt, jotka tukevat GDPR:n artiklojen 33 ja 34 edellyttämiä käsittely- ja ilmoitusmääräaikoja.

10.7 P33 – Auditointi- ja vaatimustenmukaisuuden seurantapolitiikka. Toteuttaa aikataulutetut arvioinnit tietosuojaohjelman tehokkuudesta, politiikan soveltamisesta ja korjaavien toimenpiteiden seurannasta organisaatioyksiköissä ja kolmannen osapuolen henkilötietojen käsittelijöillä.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Lauseke 5.1 – Johtajuus ja sitoutuminen: määrittää ylimmän johdon vastuun henkilötietojen suojaamisesta ja tietosuojaperiaatteiden toteuttamisesta.

11.1.2 Lauseke 6.1.3 – Tietoturvariskien hallinta: tukee tietosuojariskien tunnistamista, arviointia ja käsittelyä DPIA-arviointien ja poikkeusten avulla.

11.1.3 Lauseke 8.1 – Toiminnan suunnittelu ja ohjaus: edellyttää teknisiä ja menettelyllisiä suojatoimia henkilötietojen turvallisen käsittelyn varmistamiseksi.

11.1.4 Lauseke 10.1 – Jatkuva parantaminen: edellyttää tietosuojaohjelman säännöllistä arviointia ja mukauttamista.

11.2 ISO/IEC 27002:2022 kontrollit 5.34, 8.10, 8.11, 8.12: antavat ohjeistusta henkilötietojen käsittelystä, säilytyksen toimeenpanosta, poistamisesta, anonymisoinnista ja rekisteröidyn oikeuksien läpinäkyvyydestä.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: määrittävät hallinnoinnin, roolien, osoitusvelvollisuuden ja tietosuojakoulutuksen vastuut.

11.3.2 PL-2, PL-8: edellyttävät tietosuojakontrollien integrointia järjestelmien elinkaareen ja yritysarkkitehtuuriin.

11.3.3 AC-2, AC-6: toteuttavat vähimmän oikeuden periaatteen ja käyttäjätilien hallinnan henkilötietojen suojaamiseksi.

11.3.4 AU-2, AU-6, AU-9: edellyttävät lokitusta, jäljitettävyyttä ja auditoinnin eheyttä henkilötietoihin kohdistuvassa pääsyssä.

11.3.5 IR-4, IR-5, IR-6: määrittävät rakenteiset havaitsemisen, analysoinnin ja raportoinnin prosessit tietosuojaloukkauksille.

11.3.6 PM-1, PM-21, PM-23: muodostavat kattavan tietosuojaohjelman, joka on yhdenmukainen strategisten riskien ja tiedonhallinnan tavoitteiden kanssa.

11.4 EU:n GDPR (2016/679)

11.4.1 Artiklat 5, 6, 12–23, 25, 28, 30, 32–34: säätelevät lainmukaista käsittelyä, käyttötarkoitussidonnaisuutta, rekisteröidyn oikeuksia, osoitusvelvollisuutta, sisäänrakennettua ja oletusarvoista tietosuojaa, kolmansien osapuolten velvoitteita ja tietoturvaloukkausten hallintaa.

11.4.2 Johdanto-osan kappale 78: vahvistaa sisäänrakennetun tietosuojan periaatteita.

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

11.5.1 Artikla 21(2)(e) ja (f): edellyttää riskiperusteisten tietoturvakontrollien toteuttamista ja henkilötietojen suojaamista direktiivin soveltamisalaan kuuluvissa keskeisissä ja tärkeissä toimijoissa.

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

11.6.1 Artikla 6(2)(d): edellyttää tietojen käsittelyyn liittyvien ICT-riskien sisäistä hallintaa.

11.6.2 Artikla 11(1)(c): edellyttää dataan liittyvien palveluiden kolmannen osapuolen riskien valvontaa.

11.6.3 Artiklat 15(1) ja 17: edellyttävät palveluntarjoajilta turvallista tietojen käsittelyä sekä oikea-aikaisia viranomaisilmoituksia ICT-liitännäisten poikkeamien jälkeen.

11.7 COBIT 2019

11.7.1 APO12 – Riskienhallinta: sisällyttää tietosuojariskit laajempaan yritystason riskien valvontaan.

11.7.2 DSS01 – Hallitut operatiiviset toiminnot ja DSS05 – Tietoturvapalvelut: varmistavat turvalliset operatiiviset toiminnot, mukaan lukien pääsynhallinta, säilytys ja järjestelmien eheys.

11.7.3 MEA03 – Vaatimustenmukaisuuden seuranta: edellyttää jatkuvaa vaatimustenmukaisuustilan katselmointia suhteessa sääntelyyn ja politiikkoihin perustuviin tietosuojavelvoitteisiin.