					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P18S					Asiakirjan nimi: **Salaus- ja kryptografisten hallintakeinojen 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**

Yhdenmukaisuus standardien ja sääntelyvaatimusten kanssa

Standardi/sääntely	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohta 8	
ISO/IEC 27002:2022	Hallintakeinot 8.24, 8.25	
NIST SP 800-53 Rev. 5	SC-12–SC-17	
EU:n NIS2-direktiivi	Artiklat 21(2)(d), 21(2)(e)	
EU:n DORA-asetus	Artiklat 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
EU:n GDPR	Artiklat 32(1)(a), 34	

1. Tarkoitus

1.1 Tämä politiikka määrittää pakolliset vaatimukset salauksen ja kryptografisten hallintakeinojen käytölle liiketoimintatietojen ja henkilötietojen luottamuksellisuuden, eheyden ja aitouden suojaamiseksi.

1.2 Tällä politiikalla varmistetaan, että kryptografisia työkaluja käytetään asianmukaisesti järjestelmissä, laitteissa ja pilvipalveluissa pk-yritysympäristössä.

1.3 Tämä politiikka tukee suoraan ISO/IEC 27001:2022 -sertifiointia ja auttaa organisaatiota täyttämään EU:n GDPR:n, EU:n NIS2-direktiivin ja DORA-asetuksen mukaiset lakisääteiset velvoitteet.

1.4 Tämän politiikan kattamiin kryptografisiin hallintakeinoihin kuuluvat tietojen salaus, varmenteiden hallinta, avainten turvallinen käsittely ja salatut varmuuskopiot.

2. Soveltamisala

2.1 Tätä politiikkaa sovelletaan seuraaviin:

2.1.1 kaikkiin työntekijöihin, sopimuskumppaneihin ja kolmansiin osapuoliin, jotka käsittelevät yrityksen tietoja

2.1.2 kaikkiin liiketoimintajärjestelmiin, päätelaitteisiin ja pilvialustoihin, joita käytetään luottamuksellisten tietojen tallentamiseen, siirtämiseen tai käyttöön

2.1.3 kaikkiin aineistoihin, jotka sisältävät henkilötietoja, taloudellisia, oikeudellisia tai muutoin arkaluonteisia tietoja ja jotka on luokiteltu organisaation tiedonluokittelupolitiikan mukaisesti

2.1.4 kaikkiin kryptografisiin hallintakeinoihin, mukaan lukien salausmenetelmät, avaimet, salasanat, varmenteet ja laitteistopohjaiset tietoturvamoduulit

2.2 Politiikka kattaa lepotilassa olevat tiedot, siirrettävät tiedot ja käytössä olevat tiedot. Se koskee myös varmuuskopioissa, sähköpostissa, ulkoisissa tiedonsiirroissa ja julkisilla verkkosivustoilla käytettävää salausta.

3. Tavoitteet

3.1 Varmistaa, että arkaluonteiset ja sääntelyn alaiset tiedot suojataan jatkuvasti asianmukaisilla kryptografisilla toimenpiteillä

3.2 Määrittää vastuut salaustyökalujen valinnasta, konfiguroinnista ja avainten hallinnasta

3.3 Estää luvaton pääsy, peukalointi ja tietovuodot toteuttamalla turvallisen siirron ja tallennuksen hallintakeinot

3.4 Täyttää lakisääteiset ja sääntelyyn perustuvat vaatimukset, jotka edellyttävät henkilötietojen ja liiketoimintatietojen salausta

3.5 Ylläpitää toiminnallista tietoturvaa ja saatavuutta hallitsemalla varmenteita ja kryptografisia avaimia tehokkaasti

4. Roolit ja vastuut

4.1 Toimitusjohtaja

4.1.1 hyväksyy tämän politiikan ja varmistaa, että kryptografisia vaatimuksia noudatetaan

4.1.2 katselmoi poikkeukset, tietoturvaloukkausilmoitukset ja toimittajien salausvaatimusten noudattamisen

4.1.3 varmistaa, että ulkoistetut palvelut ja pilvipalvelut täyttävät salausvaatimukset

4.2 IT-palveluntarjoaja / sisäinen IT-vastaava

4.2.1 toteuttaa ja ylläpitää salausratkaisuja, kuten koko levyn salausta, SSL/TLS-varmenteita ja VPN-yhteyksiä

4.2.2 hallitsee kryptografisten avainten elinkaarta ja turvallisia säilytysratkaisuja

4.2.3 konfiguroi ja valvoo salausta varmuuskopioiden, verkkosivustojen ja laitteiden suojaamiseksi

[... 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 Tämä politiikka on katselmoitava vähintään kerran vuodessa toimitusjohtajan toimesta yhteistyössä IT-palveluntarjoajan ja tietosuojakoordinaattorin kanssa

9.2 Väliaikaisen katselmoinnin herätteet

9.2.1 Katselmointi on tehtävä myös, jos:

9.2.1.1 kryptografiset standardit tai protokollat muuttuvat, kuten algoritmin käytöstäpoiston yhteydessä

9.2.1.2 käyttöön otetaan uusia järjestelmiä tai pilvipalveluita

9.2.1.3 tietoturvaloukkaus tai poikkeama liittyy vaarantuneeseen avaimeen tai varmenteeseen

9.2.1.4 lakisääteiset tai sääntelyyn liittyvät muutokset vaikuttavat salausvaatimuksiin

9.3 Versionhallinta ja viestintä

9.3.1 Kaikki politiikkamuutokset on dokumentoitava versiolokiin

9.3.2 Henkilöstölle on tiedotettava päivityksistä, ja aiemmat versiot on arkistoitava

9.3.3 Viimeisin hyväksytty versio on säilytettävä keskitetysti politiikkatietovarastossa

10. Liittyvät politiikat ja yhteydet

10.1 Tätä politiikkaa on sovellettava yhdessä seuraavien pk-yritykselle tarkoitettujen politiikkojen kanssa:

10.1.1 P12S – Omaisuudenhallintapolitiikka: varmistaa, että salaus kohdistetaan luokiteltuihin omaisuuseriin niiden tallennuksen, siirron ja hävittämisen aikana.

10.1.2 P14S – Tietojen säilytys- ja hävittämispolitiikka: määrittää säilytysajat ja edellyttää tietojen salausta niiden turvalliseen poistamiseen saakka.

10.1.3 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: yhdenmukaistaa salauksen tietosuojaperiaatteiden ja GDPR:n 32 artiklan mukaisten sääntelyodotusten kanssa.

10.1.4 P22S – Lokitus- ja valvontapolitiikka: edellyttää avainten käytön, salauksen epäonnistumisten ja varmenteiden vanhenemisen lokitusta auditointitarkoituksia varten.

10.1.5 P30S – Tietoturvapoikkeamien hallintapolitiikka: määrittää eskalointi-, rajaamis- ja ilmoitusmenettelyt tilanteissa, joissa salaus epäonnistuu tai avaimet vaarantuvat.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Kohta 8.1 – Edellyttää operatiivisten kontrollien, mukaan lukien salauksen, toteuttamista tietoturvariskien hallitsemiseksi.

11.2 ISO/IEC 27002

11.2.1 Hallintakeino 8.24 – Kuvaa salauksen soveltamista koskevat vaatimukset luottamuksellisuuden ja eheyden suojaamiseksi.

11.2.2 Hallintakeino 8.25 – Kuvaa kryptografisten avainten ja varmenteiden turvallisen hallinnan vaatimukset.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – Määrittää kryptografisten avainten muodostamista ja validointia koskevat vaatimukset.

11.3.2 SC-13 – Määrittää kryptografisten avainten luomista koskevat standardit.

11.3.3 SC-17 – Kattaa julkisen avaimen infrastruktuurin (PKI) ja varmenteiden elinkaaren hallinnan.

11.3.4 SC-28 – Edellyttää lepotilassa olevien tietojen salausta.

11.3.5 SC-12–SC-17 (tuoteperhe) – Varmistaa, että kryptografiset suojaukset toteutetaan asianmukaisesti kaikissa järjestelmissä.

11.4 EU:n GDPR

11.4.1 Artikla 32(1)(a) – Edellyttää organisaatioita toteuttamaan teknisiä toimenpiteitä, kuten salauksen, tietojen luottamuksellisuuden varmistamiseksi.

11.4.2 Artikla 34 – Toteaa, että salaus voi vapauttaa organisaation ilmoitusvelvollisuudesta tietoturvaloukkauksen yhteydessä, jos tiedot ovat olleet luvattomille henkilöille käsittämättömässä muodossa.

11.5 EU:n NIS2-direktiivi

11.5.1 Artikla 21(2)(d) – Edellyttää tehokasta salausta järjestelmien ja viestinnän suojaamiseksi.

11.5.2 Artikla 21(2)(e) – Korostaa tietojen suojaamista ja kyberuhkien lieventämistä salauksen avulla.

11.6 EU:n DORA-asetus

11.6.1 Artikla 6(2)(d) – Edellyttää, että ICT-järjestelmät ylläpitävät turvallisia viestintäkanavia ja salausta.

11.6.2 Artikla 9(2)(f) – Velvoittaa finanssialan toimijat käyttämään vahvaa salausta digitaalisen viestinnän ja tiedonvaihdon suojaamiseksi.

11.7 COBIT 2019

11.7.1 DSS05.01 – Edellyttää arkaluonteisten tietojen suojaamista salauksen ja kryptografisten protokollien avulla.

11.7.2 APO13.02 – Edellyttää tehokasta tietoturvakontrollien toteutusta, mukaan lukien kryptografiset suojatoimet, osana tietoturvallisuuden suunnittelua.