					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P18					Asiakirjan nimi: **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	Kontrollit 8.24, 8.25, 8	-
NIST SP 800-53 Rev.5	SC-12–SC-17, SC-28, SC-28(1), SC-12(3)	-
EU:n GDPR	Artikla 32, artiklat 33–34, johdanto-osan kappale 83	-
EU:n NIS2-direktiivi	Artikla 21(2)(d)	-
EU:n DORA-asetus	Artiklat 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA	-

1. Tarkoitus

1.1 Tämä politiikka määrittää pakolliset vaatimukset kryptografisten hallintakeinojen turvalliselle ja vaatimustenmukaiselle käytölle koko organisaatiossa, jotta arkaluonteisten ja sääntelyn alaisten tietojen luottamuksellisuus, eheys ja aitous varmistetaan.

1.2 Kryptografian käyttö muodostaa perustan luottamukselle tietoturvatoimintojen toteutuksessa, tukee turvallista viestintää, toteuttaa pääsynhallintaa ja mahdollistaa sääntelyvaatimusten noudattamisen tehokkaiden salaus- ja avaintenhallintakäytäntöjen avulla.

1.3 Tämä politiikka on yhdenmukainen ISO/IEC 27001:2022 -standardin kohdan 8.1 ja liitteen A kontrollin 8.24 kanssa ja tukee GDPR:n 32 artiklan, DORA-asetuksen 6(2)(d) artiklan ja NIS2-direktiivin 21 artiklan mukaisia oikeudellisia ja operatiivisia velvoitteita. Se tukee myös COBIT 2019 -viitekehyksen tavoitteita tietoturvapalveluille ja tietovarojen suojaamiselle.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia organisaatioyksiköitä, liiketoimintatoimintoja, henkilöstöä ja kolmannen osapuolen palveluntarjoajia, jotka osallistuvat kryptografisten työkalujen ja menetelmien käyttöön, hallintaan tai toteutukseen.

2.2 Soveltamisalaan kuuluvat tuotanto-, kehitys-, testaus-, varmuuskopiointi- ja katastrofipalautusjärjestelmät, joissa arkaluonteisia tietoja siirretään, käsitellään tai säilytetään.

2.3 Soveltamisala kattaa kaikki kryptografiset komponentit ja käyttötapaukset, mukaan lukien seuraavat:

2.3.1 Symmetrinen ja epäsymmetrinen salaus

2.3.2 Digitaaliset allekirjoitukset ja digitaaliset varmenteet

2.3.3 Tiivistealgoritmit

2.3.4 Avainten turvallinen luonti, jakelu ja tuhoaminen

2.3.5 Transport Layer Security (TLS), koko levyn salaus (FDE) ja ohjelmointirajapintatason salaus

2.3.6 Turvalliset komponentit, kuten laitteistoturvamoduulit (HSM), Trusted Platform Module -moduulit (TPM) ja avaintenhallintajärjestelmät (KMS)

2.4 Tämä politiikka ohjaa kryptografian käyttöä seuraavissa yhteyksissä:

2.4.1 Tiedot, jotka on luokiteltu luottamuksellisiksi, erittäin luottamuksellisiksi tai sääntelyn alaisiksi

2.4.2 Todennus ja digitaalisen identiteetin varmentaminen

2.4.3 Turvallinen viestintä ulkoisten osapuolten kanssa

2.4.4 Avainten hallussapito ja kahden henkilön valvontamekanismit

3. Tavoitteet

3.1 Varmistaa, että kryptografiset teknologiat valitaan, hyväksytään, toteutetaan ja ylläpidetään liiketoimintariskien, kansainvälisten standardien ja sääntelyvaatimusten mukaisesti.

3.2 Määrittää standardoitu hallintamalli kryptografisten palvelujen hallintaan siten, että vastuut toteutuksesta, validoinnista ja poikkeusten käsittelystä ovat selkeät.

3.3 Estää kryptografisten algoritmien ja hallintakeinojen luvaton käyttö, virheelliset määritykset tai vanhentuminen muodollisen hyväksyntä- ja katselmointiprosessin avulla.

3.4 Varmistaa, että kryptografiset hallintakeinot sisällytetään järjestelmien suunnitteluvaiheeseen ja validoidaan säännöllisesti tietojen altistumisen, avainten vaarantumisen tai protokollien heikkenemisen estämiseksi.

3.5 Toteuttaa kaikkien kryptografisten avainten elinkaaren hallinta, mukaan lukien luonti, säilytys, käyttö, kierto, peruminen ja turvallinen tuhoaminen.

3.6 Noudattaa kansainvälisiä ja alueellisia säädöksiä, jotka edellyttävät salausta ja turvallista tietojen käsittelyä, mukaan lukien GDPR, DORA, NIS2 ja COBIT 2019.

4. Roolit ja vastuut

4.1 ISMS-päällikkö / tietoturvajohtaja (CISO)

4.1.1 Omistaa tämän politiikan ja varmistaa sen yhdenmukaisuuden ISMS:n ja ISO/IEC 27001:n liitteen A kontrollin 8.24 kanssa.

4.1.2 Hyväksyy kryptografisten algoritmien ja hallintakeinojen käytön ja varmistaa politiikan noudattamisen koko organisaatiossa.

4.2 Kryptografisten operaatioiden vastuuhenkilö / tietoturva-arkkitehti

4.2.1 Vastaa kryptografisten järjestelmien päivittäisestä käytöstä ja ylläpidosta.

4.2.2 Ylläpitää hyväksyttyjen kryptografisten menetelmien luetteloa (ACML) ja avaintenhallintarekisteriä.

4.2.3 Suorittaa kryptografisen suunnittelun katselmointeja (CDR) ja arvioi uusia kryptografisia teknologioita.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 ISMS-päällikön ja kryptografisten operaatioiden vastuuhenkilön on katselmoitava tämä politiikka vuosittain.

9.2 Katselmoinnin käynnistäviä tekijöitä ovat:

9.2.1 Kryptografisten haavoittuvuuksien havaitseminen (esim. algoritmin heikentyminen, kvanttihyökkäykset)

9.2.2 Sääntelymuutokset, jotka edellyttävät päivitettyjä salausstandardeja

9.2.3 Operatiiviset havainnot tai auditointihavainnot, jotka paljastavat politiikan puutteita

9.2.4 Kryptografisten työkalujen päivitykset tai arkkitehtuurimuutokset

9.3 Päivitykset on pidettävä versionhallittuina ISMS:n asiakirjahallintarekisterissä ja viestittävä seuraaville:

9.3.1 Kaikille ylläpitäjille, joilla on kryptografisia käyttöoikeusrooleja

9.3.2 Kehitystiimeille ja DevSecOps-vastuuhenkilöille

9.3.3 Kolmannen osapuolen palveluntarjoajille, joihin kohdistuu sopimusperusteisia salausvelvoitteita

9.4 ISMS-tiimin on varmistettava, että korvatut versiot arkistoidaan eikä niihin enää viitata toimintamenettelyissä.

10. Liittyvät politiikat ja yhteydet

10.1 P1 - Tietoturvapolitiikka. Määrittää perustavan hallintakehyksen kaikille tietoturvatoimenpiteille, mukaan lukien kryptografisten hallintakeinojen soveltaminen, omaisuuden suojaaminen ja turvallinen viestintä.

10.2 P4 - Pääsynhallintapolitiikka. Varmistaa, että looginen pääsy kryptografiseen materiaaliin ja salauksen hallintajärjestelmiin on rajoitettu tiukasti vähimmän oikeuden periaatteen ja tehtävien eriyttämisen mukaisesti.

10.3 P6 - Riskienhallintapolitiikka. Tukee kryptografisiin hallintakeinoihin liittyvien riskien arviointia ja dokumentoi riskien käsittelyn strategian poikkeuksille, algoritmien vanhentumiselle tai avainten vaarantumisskenaarioille.

10.4 P12 - Omaisuudenhallintapolitiikka. Edellyttää arkaluonteisten tietojen ja laitteisto-omaisuuserien luokittelua, mikä määrittää suoraan kryptografiset vaatimukset ja avainten hallussapitoa koskevat velvoitteet.

10.5 P13 - Tiedon luokittelu- ja merkintäpolitiikka. Määrittää luokittelutasot (esim. luottamuksellinen, sääntelyn alainen), jotka käynnistävät tietyt salausvaatimukset siirron aikana ja lepotilassa.

10.6 P14 - Tietojen säilytys- ja hävityspolitiikka. Määrittää menettelyt salattujen tallennusvälineiden ja kryptografisen avainmateriaalin turvalliselle hävittämiselle elinkaaren päättyessä.

10.7 P30 - Tietoturvapoikkeamien hallintapolitiikka. Kuvaa organisaation toimintamallin avainten vaarantumiseen, varmenteiden väärinkäyttöön tai epäiltyihin algoritmisiin haavoittuvuuksiin, mukaan lukien nopea peruminen ja tietoturvaloukkauksista ilmoittaminen.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Kohta 8.1 - Operatiivinen suunnittelu ja ohjaus: Edellyttää teknisten tietoturvakontrollien, mukaan lukien kryptografisten toimenpiteiden, toteutusta osana operatiivisia suojatoimia.

11.2 ISO/IEC 27002:2022

11.2.1 Kontrollit 8.24, 8.25, 8: Antaa toteutusohjeet kryptografisten hallintakeinojen tavoitteista, algoritmien valinnasta, protokollien pakottamisesta ja varmenteiden elinkaaren hallinnasta.

11.3 NIST SP 800-53 Rev.

11.3.1 SC-12 - Kryptografisten avainten muodostaminen: Varmistaa salausavainten turvallisen luonnin ja vaihdon. P18 määrittää, miten symmetriset ja epäsymmetriset avaimet on luotava ja vaihdettava hyväksytyillä algoritmeilla ja protokollilla.

11.3.2 SC-13 - Kryptografinen suojaus: Edellyttää kryptografian käyttöä tietojen luottamuksellisuuden ja eheyden suojaamiseen. P18 edellyttää salausta lepotilassa oleville tiedoille ja siirrettäville tiedoille tiedon luokittelun perusteella siten, että algoritmistandardit ovat yhdenmukaiset NIST FIPS 140-3:n kanssa.

11.3.3 SC-17 - Julkisen avaimen infrastruktuurin (PKI) varmenteet: Edellyttää PKI:n käyttöönottoa todennuksen ja digitaalisten allekirjoitusten tukemiseksi. P18 määrittää PKI:n käytön viestinnän, järjestelmäidentiteettien ja hallinnollisen pääsyn suojaamiseen.

11.3.4 SC-28, SC-28(1) - Lepotilassa olevien ja siirrettävien tietojen suojaus: Edellyttää tietojen salausta, kun niitä säilytetään tai siirretään ei-luotetuissa verkoissa. P18 määrittää TLS:n, VPN-tunnelien, koko levyn salauksen ja turvallisten säilytysmenetelmien käytön arkaluonteisille tiedoille.

11.3.5 SC-12(3) - Symmetristen avainten luonti turvallista säilytystä ja jakelua varten: Keskittyy symmetristen avainten turvalliseen luontiin ja käsittelyyn. P18 edellyttää vahvojen

satunnaislukugeneraattorien käyttöä, avainten kiertokäytäntöjä ja turvallisia avainholveja kryptografisissa toiminnoissa.

11.4 EU:n GDPR (2016/679)

11.4.1 Artikla 32 - Käsittelyn turvallisuus: Suosittelee nimenomaisesti salausta henkilötietojen riskien vähentämistoimenpiteenä.

11.4.2 Johdanto-osan kappale 83: Korostaa salausta hallintakeinona luvattoman pääsyn estämiseksi tietoihin.

11.4.3 Artiklat 33 ja 34: Tehokas salaus voi vapauttaa organisaation pakollisista tietoturvaloukkausilmoituksista.

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

11.5.1 Artikla 21(2)(d): Edellyttää teknisiä ja organisatorisia toimenpiteitä, mukaan lukien kryptografinen suojaus, palvelujen saatavuuden ja eheyden ylläpitämiseksi.

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

11.6.1 Artikla 6(2)(d): Finanssialan toimijoiden on suojattava tiedot, mukaan lukien kriittiset tiedot, vahvalla salauksella.

11.6.2 Artikla 11(1)(c): Edellyttää turvallisia tietojenkäsittelyn hallintakeinoja ICT-kolmannen osapuolen palveluntarjoajille.

11.7 COBIT 2019

11.7.1 DSS05.01 - Tietovarojen suojaaminen: Edellyttää salauksen ja avaintenhallinnan käyttöä tietojen suojaamiseksi luvattomalta käytöltä.

11.7.2 DSS06.06 - Hallittu tietoturvatestaus: Suosittelee kryptografisen vaatimustenmukaisuuden validointia osana haavoittuvuuksien arviointia.

11.7.3 MEA03 - Vaatimustenmukaisuuden seuranta, arviointi ja tarkastelu: Edellyttää kryptografisten hallintakeinojen tehokkuuden jatkuvaa varmistamista.