					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P14					Asiakirjan nimi: **Tietojen säilytys- ja hävittämispolitiikka**							
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	Kohdat 6.1.3, 8.1	
ISO/IEC 27002:2022	Kontrollit 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
EU:n GDPR	Artiklat 5(1)(e), 17, 32	
EU:n NIS2-direktiivi	Artikla 21(2)(a-e)	
EU:n DORA-asetus	Artiklat 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Tarkoitus

1.1 Tämän politiikan tarkoituksena on määrittää organisaation vaatimukset tietojen säilyttämiselle ja turvalliselle hävittämiselle tiedon elinkaaren kaikissa vaiheissa. Politiikka varmistaa sovellettavien lakisääteisten, sääntelyyn perustuvien ja sopimusperusteisten velvoitteiden noudattamisen sekä ehkäisee tietojen tarpeetonta tai riskialtista kertymistä.

1.2 Tämä politiikka tukee ISO/IEC 27001:2022 -standardin toimeenpanoa varmistamalla tietojen säilytysaikojen hallinnan ja peruuttamattomat hävittämiskäytännöt. Se mahdollistaa tallenteiden jäljitettävän dokumentoinnin, edellyttää tiedon luokituksen mukaista säilyttämistä tiedon herkkyyden perusteella sekä varmistaa valmiuden auditointeihin, viranomaistarkastuksiin ja oikeudelliseen tiedonhankintaan.

1.3 Lisäksi politiikan tavoitteena on ylläpitää tietojen luottamuksellisuutta, eheyttä ja saatavuutta sekä minimoida liiketoimintariskit, toiminnalliset tehottomuudet ja tietosuojaloukkauksiin liittyvä altistuminen, jotka johtuvat tietojen virheellisestä säilyttämisestä tai hävittämisestä.

2. Soveltamisala

2.1 Tätä politiikkaa sovelletaan kaikkiin organisaation omistamiin, käsittelemiin tai säilyttämiin fyysisiin ja digitaalisiin tietovaroihin, mukaan lukien kolmansien osapuolten, tytäryhtiöiden tai ulkoistuskumppaneiden hallinnassa olevat tietovarat.

2.2 Soveltamisalaan kuuluvat muun muassa seuraavat:

2.2.1 asiakirjat, tiedostot ja tallenteet (digitaaliset ja paperimuotoiset)

2.2.2 tietokannat ja arkistot

2.2.3 sähköpostit ja pikaviestilokit

2.2.4 varmuuskopiot, järjestelmälokit ja audit trail -tiedot

2.2.5 lähdekoodi, sovellustiedot ja pilvipalveluissa isännöidyt omaisuuserät

2.2.6 siirrettävät tallennusvälineet ja käytöstä poistettu laitteisto, joka sisältää tietoja

2.3 Tämä politiikka koskee sekä operatiivisia tallenteita että sääntelyn alaisia tietoaineistoja (esim. talous-, oikeudelliset, HR-, asiakas- ja auditointiin liittyvät sisällöt) tallennuspaikasta tai järjestelmästä riippumatta.

2.4 Tätä politiikkaa sovelletaan kaikkiin organisaation osastoihin sekä kaikkiin työntekijöihin, urakoitsijoihin ja toimittajiin, jotka osallistuvat tietojen luomiseen, säilyttämiseen, hallintaan tai hävittämiseen.

3. Tavoitteet

3.1 Varmistaa, että tietoja säilytetään vain niin kauan kuin se on lakisääteisesti, sopimusperusteisesti tai toiminnallisesti tarpeen, ja että tiedot hävitetään turvallisesti, kun niitä ei enää tarvita.

3.2 Estää sellaisten tallenteiden ennenaikainen, luvaton tai tahaton poistaminen, joita tarvitaan jatkuvassa toiminnassa, vaatimustenmukaisuuden varmistamisessa, oikeudenkäynneissä tai auditointitarkoituksissa.

3.3 Määrittää ja soveltaa yhdenmukaisia säilytysaikatauluja tiedon luokituksen, omaisuuserätyypin, sovellettavan lainsäädännön ja riskialtistuksen perusteella.

3.4 Suojata tietojen yksityisyys ja luottamuksellisuus niiden säilytysajan aikana ja hävittämishetkellä, mukaan lukien rekisteröidyn oikeuksien toteuttaminen (esim. poistaminen GDPR:n 17 artiklan mukaisesti).

3.5 Varmistaa, että kaikki tietojen hävittämismenetelmät ovat peruuttamattomia, asianmukaisesti dokumentoituja ja tunnustettujen standardien, kuten NIST SP 800-88:n, mukaisia.

3.6 Minimoida toiminnalliset tehottomuudet, kustannusrasitus ja oikeudellinen altistuminen, jotka johtuvat liian pitkästä säilyttämisestä tai seuraamattomasta historiadatasta.

3.7 Tukea liiketoiminnan jatkuvuuden ja katastrofipalautuksen tavoitteita integroidulla varmuuskopioiden säilytyksen hallinnalla ja todennettavissa olevilla tietojen arkistointikäytännöillä.

4. Roolit ja vastuut

4.1 Ylin johto

4.1.1 Hyväksyy tämän politiikan ja varmistaa asianmukaisen rahoituksen, resurssit sekä integroinnin yrityksen riskienhallintaan ja vaatimustenmukaisuusohjelmiin.

4.1.2 Vastaa kokonaisuutena tietojen säilyttämiseen ja turvalliseen hävittämiseen liittyvästä lakisääteisestä ja sääntelyyn perustuvasta vaatimustenmukaisuudesta.

4.2 Tietoturvajohtaja (CISO)

4.2.1 Omistaa tämän politiikan ja vastaa säilyttämisen ja hävittämisen hallinnan määrittämisestä ja katselmoinnista ISMS:n mukaisesti.

4.2.2 Varmistaa, että luokitukseen perustuvat säilytys- ja hävittämisvaatimukset toteutetaan liiketoimintayksiköissä ja teknisissä järjestelmissä.

4.2.3 Valvoo politiikan noudattamista ja varmistaa tarvittaessa korjaavien toimenpiteiden toteuttamisen.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Tämä politiikka on katselmoitava vuosittain tai kun jokin seuraavista ehdoista täyttyy:

9.1.1 sovellettavaan lainsäädäntöön tai sääntelyyn tulee muutoksia, jotka vaikuttavat tietojen säilyttämiseen (esim. päivitykset EU:n GDPR:ään, verosäännöksiin tai DORA-asetukseen)

9.1.2 luokitteluviitekehystä tai liiketoimintaprosesseja muutetaan siten, että tiedon elinkaaren vaiheet muuttuvat

9.1.3 käyttöön otetaan uusia IT-järjestelmiä, arkistointialustoja tai tallennusvälineiden hävittämisteknologioita

9.1.4 sisäisen tarkastuksen auditointihavainnot tai viranomaissuositukset osoittavat puutteita säilytys- tai hävittämiskäytännöissä

9.2 Katselmoinnista vastaa CISO yhdessä tietosuojavastaavan (DPO) kanssa, ja siihen osallistuvat laki- ja vaatimustenmukaisuustoiminnot, IT sekä liiketoimintayksiköt.

9.3 Tietojen pääsäilytysaikataulu (MDRS) ja hävitysrekisteri on katselmoitava rinnakkain sen varmistamiseksi, että:

9.3.1 aikataulut pysyvät täsmällisinä ja vastaavat toiminnallisia, lakisääteisiä ja sääntelyyn perustuvia tarpeita

9.3.2 hävittämisdokumentaatio on täydellistä ja todennettavissa

9.3.3 oikeudellisen säilytysvelvoitteen tallenteet validoidaan ja vapautetaan, kun se on asianmukaista

9.4 Kaikki politiikan päivitykset on:

9.4.1 versioitava muodollisesti ja säilytettävä ISMS:n dokumenttirekisterissä

9.4.2 sisällettävä muutoshistoria ja muutoksen perustelu

9.4.3 oltava ylimmän johdon hyväksymiä

9.4.4 viestittävä asianomaiselle henkilöstölle päivitetyn koulutus- tai ohjemateriaalin kanssa

9.5 Jos politiikkaan tehdään merkittäviä muutoksia, niiden kohteena olevien työntekijöiden on suoritettava kohdennettu koulutus 30 päivän kuluessa julkaisusta jatkuvan vaatimustenmukaisuuden varmistamiseksi.

9.6 Liittyvät politiikat ja yhteydet

10. Liittyvät politiikat ja yhteydet

10.1.1 P4 - Pääsynhallintapolitiikka: varmistaa, että vain valtuutetut henkilöt pääsevät tietoihin niiden säilytysajan aikana ja että vanhentuneiden tietojen pääsyä rajoitetaan hävittämistä odotettaessa.

10.1.2 P12 - Omaisuudenhallintapolitiikka: tunnistaa, mitkä omaisuuserät sisältävät tietoja, jotka edellyttävät aikataulutettua hävittämistä, ja seuraa niiden elinkaarta hankinnasta tuhoamiseen.

10.1.3 P13 - Tiedon luokittelu- ja merkintäpolitiikka: ohjaa luokittelupäätöksiä, jotka vaikuttavat suoraan siihen, kuinka pitkään tietoja säilytetään ja mitä hävittämismenetelmää vaaditaan.

10.1.4 P15 - Varmuuskopiointi- ja palautuspolitiikka: määrittää varmuuskopiointivälineiden ja replikoitujen tietovaraomaisuuserien säilytysajat ja hävittämismenettelyt.

10.1.5 P18 - Kryptografisten hallintakeinojen politiikka: tukee kryptografista poistoa hävittämisessä ja edellyttää salausta tietojen säilytyksen aikana hävittämiseen saakka.

10.1.6 P30 - Tietoturvapoikkeamien hallintapolitiikka: otetaan käyttöön tilanteissa, joissa virheellinen hävittäminen johtaa mahdolliseen tietojen menetykseen, tietomurtoon tai sääntelyrikkomukseen.

10.2 Jokaisella linkitetyllä politiikalla on rooli yhtenäisen tiedonhallintamallin toteuttamisessa luokittelun, elinkaaren hallinnan, pääsyn ja auditointivalmiuden osa-alueilla.

11. Viitestandardit ja viitekehykset

11.1 Tämä politiikka on yhdenmukainen kansainvälisesti tunnustettujen standardien ja sääntelyviitekehysten kanssa, jotka määrittävät turvalliset, vaatimustenmukaiset ja tehokkaat tiedon elinkaaren käytännöt.

11.2 ISO/IEC 27001:

11.2.1 Kohta 6.1.3 - Riskienkäsittelysuunnitelma: tukee liian pitkästä säilyttämisestä, tietomurroista tai hävittämisen epäonnistumisesta aiheutuvien riskien lieventämistä.

11.2.2 Kohta 8.1 - Toiminnan suunnittelu ja ohjaus: määrittää elinkaarikontrollit, joilla hallitaan säilyttämistä, arkistointia ja hävittämistä.

11.3 ISO/IEC 27002:2022 - Kontrollit 5.10, 5.12, 5.30, 5: antavat käytännön ohjeita tietojen hyväksyttävästä käytöstä, säilytysperusteista, hallitusta poistamisesta ja puolustettavissa olevasta tallenteiden hallinnasta organisaation riskinsietokyvyn mukaisesti.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - Auditointitallenteiden säilytys: varmistaa auditointilokien ja vaatimustenmukaisuusnäytön riittävän säilyttämisen.

11.4.2 MP-6 - Tallennusvälineiden puhdistaminen: edellyttää turvallisia, dokumentoituja hävittämismenetelmiä fyysisille ja sähköisille tallennusvälineille.

11.4.3 SI-12 - Tiedon käsittely: edellyttää asianmukaista tietojen käsittelyä säilytys- ja hävittämiskontrollien mukaisesti.

11.4.4 PL-2 - Järjestelmän tietoturva- ja tietosuojasuunnitelma: edellyttää järjestelmäkohtaista dokumentointia tiedon elinkaaren käsittelystä ja turvallisen hävittämisen menettelyistä.

11.5 EU:n GDPR (2016/679):

11.5.1 Artikla 5(1)(e) - Tietojen minimointi ja säilytyksen rajoittaminen: edellyttää, että tietoja ei säilytetä pidempään kuin on tarpeen.

11.5.2 Artikla 17 - Oikeus tietojen poistamiseen ("oikeus tulla unohdetuksi"): edellyttää henkilötietojen viipymätöntä ja pysyvää poistamista pätevän pyynnön perusteella.

11.5.3 Artikla 32 - Käsittelyn turvallisuus: vahvistaa tietosuojaa säilytyksen aikana ja edellyttää vanhentuneiden tallenteiden turvallista hävittämistä.

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

11.6.1 Artikla 21(2)(a-e): edellyttää, että toimijat ottavat käyttöön politiikat ja tekniset toimenpiteet tietojen turvallista käsittelyä varten, mukaan lukien säilytyksen rajoitukset ja hävittämismenetelmät.

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

11.7.1 Artikla 5 - Hallinnointi ja valvonta: edellyttää jäsenneltyä ICT-riskien hallintaa, mukaan lukien tiedon elinkaaren turvallinen hallinta.

11.7.2 Artikla 9 - ICT-riskien hallinnan viitekehys: edellyttää politiikkoja tietojen säilyttämiselle, hävittämiselle sekä digitaalisten toimintojen lakisääteiselle ja sääntelyyn perustuvalle vaatimustenmukaisuudelle.

11.8 COBIT 2019:

11.8.1 DSS01 - Hallitut operaatiot: tukee säilytyksen seurantaa ja yhdenmukaisuutta tietojärjestelmissä.

11.8.2 DSS05 - Hallitut tietoturvapalvelut: varmistaa tallennettujen ja arkistoitujen tietojen suojauksen turvalliseen hävittämiseen saakka.

11.8.3 MEA03 - Vaatimustenmukaisuuden seuranta, arviointi ja arviointi: mahdollistaa säilytyksen toteutuksen, poistomenettelyjen ja sääntelyvaatimusten täyttämisen auditoinnin.