					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P14S					Asiakirjan nimi: **Tietojen säilytys- ja hävityspolitiikka**							
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 6.1.3, 8	Kattaa riskien käsittelyn, operatiiviset kontrollit ja säilytysvaatimukset
ISO/IEC 27002:2022	Kontrolli 5	Ohjeistaa säilytysaikojen määrittämistä ja turvallisia hävitysmenetelmiä
NIST SP 800-53 Rev.5	AU-11, MP-6, SI-12	Auditointitallenteiden säilytys, tallennusvälineiden sanitointi, tietojen säilytysrajat ja niiden soveltaminen
EU:n NIS2-direktiivi	Artikla 21(2)(a)	Edellyttää riskiin nähden tarkoituksenmukaista tiedon elinkaaren hallintaa koskevaa politiikkaa
EU:n DORA-asetus	Artikla 5(1)	ICT-riskien hallinta: tietojen saatavuus ja poistaminen
COBIT 2019	BAI03.04, DSS01	Tiedon elinkaaren kontrollit, turvallinen hävittäminen
EU:n GDPR	Artiklat 5(1)(e), 17	Tietoja ei säilytetä pidempään kuin on tarpeen; oikeus tietojen poistamiseen

1. Tarkoitus

1.1 Tämän politiikan tarkoituksena on määrittää toimeenpantavat säännöt tietojen säilyttämisestä ja turvallisesta hävittämisestä pk-yritysympäristössä. Se varmistaa, että tallenteita säilytetään vain lain, sopimusvelvoitteen tai liiketoiminnallisen tarpeen edellyttämän ajan ja että ne hävitetään tämän jälkeen turvallisesti.

1.2 Tämän politiikan tavoitteena on vähentää tietoriskejä, hallita oikeudellista altistumista ja rajoittaa päällekkäisten tai vanhentuneiden tietojen säilyttämistä. Se tukee ISO/IEC 27001:n sekä EU:n GDPR:n kaltaisten tietosuojaa koskevien viitekehysten mukaista vaatimustenmukaisuutta minimoimalla henkilötietojen tai muiden arkaluonteisten tietojen perusteettoman säilyttämisen.

1.3 Hyvin jäsennelty säilytys- ja hävitysviitekehys vähentää operatiivisia kustannuksia, parantaa järjestelmien suorituskykyä ja tukee auditointivalmiutta. Rajallisen IT-kapasiteetin pk-yrityksille se tarjoaa käytännöllisen tavan hallita digitaalisia ja fyysisiä tietovaroja vastuullisesti.

2. Soveltamisala

2.1 Tämä politiikka koskee seuraavia:

2.1.1 Kaikkia organisaation luomia, keräämiä, käsittelemiä tai säilyttämiä tallenteita, tiedostoja, lokeja, viestejä ja tietoaineistoja

2.1.2 Kaikkia työntekijöitä, sopimuskumppaneita ja ulkoisia palveluntarjoajia, jotka käsittelevät organisaation tietoja

2.1.3 Kaikkia tietomuotoja (esim. paperi, sähköinen aineisto, kuva, ääni tai loki) ja kaikkia tallennusvälineitä (esim. paikalliset levyasemat, pilvipalvelut, sähköpostipalvelimet, varmuuskopiot)

2.2 Soveltamisalaan sisältyvät seuraavat:

2.2.1 Liiketoiminnan tallenteet (esim. laskut, sopimukset, projektiraportit)

2.2.2 Operatiiviset tallenteet (esim. lokit, käyttöoikeushistoria, varmuuskopioiden tilannevedokset)

2.2.3 Henkilötiedot (esim. HR-tiedostot, asiakasviestintä, tukitallenteet)

2.2.4 Sisäisesti, ulkoisesti tai hybridiympäristöissä ylläpidetyt tiedot

2.2.5 Arkistoidut tiedot ja varmuuskopiot riippumatta siitä, ovatko ne aktiivisia vai passiivisia

2.3 Soveltamisalaan kuuluvat kaikki tiedon elinkaaren vaiheet tiedon luomisesta valtuutettuun hävittämiseen.

3. Tavoitteet

3.1 Määrittää yhdenmukaiset säilytyssäännöt oikeudellisten, operatiivisten ja sääntelyyn liittyvien kriteerien perusteella.

3.2 Estää kriittisten tallenteiden ennenaikainen poistaminen ja ehkäistä tarpeetonta tietojen kertymistä.

3.3 Varmistaa tietojen turvallinen ja peruuttamaton hävittäminen, kun säilyttäminen ei ole enää tarpeen.

3.4 Määrittää omistajuus säilytys- ja poistopäätösten toteuttamiselle pk-yrityksen henkilöstöresurssit huomioiden.

3.5 Tuottaa auditointivalmiuden edellyttämät dokumentoidut tiedot huolellisuuden osoittamiseksi ISO 27001:n, EU:n GDPR:n, EU:n NIS2-direktiivin ja muiden viitekehysten mukaisesti.

3.6 Edistää tietojen turvallista käsittelyä koko elinkaaren ajan asettamatta tarpeetonta teknistä kuormitusta ei-erikoistuneelle henkilöstölle.

4. Roolit ja vastuut

4.1 Toimitusjohtaja

4.1.1 Hyväksyy tämän politiikan ja omistaa sen.

4.1.2 Varmistaa, että säilytys- ja hävitysmenettelyt toteutetaan oikeudellisen riskin ja liiketoimintariskin mukaisesti.

4.1.3 Hyväksyy tarvittaessa poikkeukset ja oikeudellista säilytysvelvoitetta koskevat tapaukset.

4.1.4 Käynnistää politiikan katselmoinnit ja hyväksyy päivitykset liiketoiminnallisten tai sääntelyyn liittyvien muutosten perusteella.

4.2 Nimetty tiedon omistaja

4.2.1 Nimetään kutakin tietoluokkaa varten (esim. talous-, HR- ja asiakastallenteet).

4.2.2 Luokittelee tallenteet ja määrittää asianmukaisen säilytysajan politiikan ja oikeudellisen ohjeistuksen perusteella.

4.2.3 Valtuuttaa poistamisen, kun säilytysvaatimukset on täytetty.

4.2.4 Tukee sisäisiä auditointeja antamalla taustatiedot säilytysperusteista ja hävitystapahtumista.

[... 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 kerran vuodessa tai seuraavien muutosten yhteydessä:

9.1.1 Sovellettavaan lainsäädäntöön tehdyt muutokset (esim. tietosuoja, taloudellinen raportointi)

9.1.2 Uusien järjestelmien tai prosessien käyttöönotto, joka vaikuttaa tiedon elinkaareen

9.1.3 Auditointihavainnot tai poikkeamat, jotka osoittavat puutteita säilytyskäytännöissä

9.2 Katselmoinneissa on varmistettava, että säilytysrekisteri pysyy täydellisenä ja kattaa kaikki merkittävät tallenneluokat.

9.3 Politiikkapäivitykset on hyväksytettävä toimitusjohtajalla ja viestittävä niistä henkilöstölle, jota ne koskevat. Uusimman version on oltava saatavilla ja versiohallittu.

10. Liittyvät politiikat ja yhteydet

10.1 P2S – Hallinnointirooleja ja vastuita koskeva politiikka: Määrittää politiikan omistajuuden ja poikkeuksiin liittyvän toimivallan.

10.2 P13S – Tiedon luokittelu- ja merkintäpolitiikka: Määrittää, miten säilytyssäännöt suhteutuvat tiedon luokitteluun.

10.3 P12S – Omaisuudenhallintapolitiikka: Ohjaa sellaisten tallennusvälineiden hallintaa, jotka sisältävät säilytys- tai hävitysvaatimusten alaisia tietoja.

10.4 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: Varmistaa tietojen minimoinnin ja tukee lainmukaista käsittelyä EU:n GDPR:n mukaisesti.

10.5 P30S – Tietoturvapoikkeamien hallintapolitiikka: Aktivoidaan, kun hävittämisen tai säilyttämisen epäonnistuminen johtaa mahdolliseen tietojen altistumiseen.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Lauseke 6.1.3: Edellyttää tietoihin liittyvien riskien, mukaan lukien säilyttämiseen liittyvien riskien, käsittelyä.

11.1.2 Lauseke 8.1: Määrittää elinkaaren aikaiset operatiiviset kontrollit.

11.2 ISO/IEC 27002

11.2.1 Kontrolli 5.33: Ohjeistaa säilytysaikojen määrittämistä ja turvallisia hävitysmenetelmiä.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: Edellyttää auditointitallenteiden säilytystä.

11.3.2 MP-6: Määrittää tallennusvälineiden sanitointimenettelyt.

11.3.3 SI-12: Käsittelee tietojen säilytysrajoja ja niiden soveltamista.

11.4 EU:n GDPR

11.4.1 Artikla 5(1)(e): Tietoja ei saa säilyttää pidempään kuin on tarpeen.

11.4.2 Artikla 17: Oikeus tietojen poistamiseen soveltuu, kun tietojen säilyttämiselle ei ole enää lainmukaista perustetta.

11.5 EU:n NIS2-direktiivi

11.5.1 Artikla 21(2)(a): Edellyttää riskiin nähden tarkoituksenmukaisia organisatorisia politiikkoja, mukaan lukien elinkaaren hallinta.

11.6 EU:n DORA-asetus

11.6.1 Artikla 5(1): ICT-riskien hallinta kattaa tietojen saatavuuden ja poistamisen.

11.7 COBIT 2019

11.7.1 BAI03.04: Edellyttää tiedon elinkaaren kontrolleja.

11.7.2 DSS01.06: Turvalliset hävitysmenettelyt osana tietovarojen suojaamista.