					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P27S					Asiakirjan nimi: **Pilvipalveluiden käyttöpolitiikka**							
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	Vaatimus/artikla	Kommentti
ISO/IEC 27001:2022	Lauseke 8	
ISO/IEC 27002:2022	Kontrollit 5.23–5.25	
NIST SP 800-53 Rev. 5	AC-20, SC-12, SC-13, SR-5	
EU:n GDPR	Artiklat 28, 32 ja luku V	
EU:n NIS2-direktiivi	Artikla 21(2)(f), (i)	
EU:n DORA-asetus	Artiklat 5(2), 28	
COBIT 2019	DSS01, DSS05, BAI04	

1. Tarkoitus

1.1 Tämä politiikka määrittää, miten pilvipalveluita saa käyttää turvallisesti organisaatiossa. Sen tavoitteena on varmistaa, että pilvessä käsiteltävät tai tallennettavat tiedot suojataan, käyttöoikeuksia hallitaan ja riskejä hallitaan asianmukaisesti.

1.2 Se auttaa pk-yrityksiä täyttämään lakisääteiset velvoitteensa ja asiakkaiden odotukset arkaluonteisten tietojen suojaamisesta, tietovuotojen estämisestä ja pilvipalveluihin liittyvien riskien tehokkaasta hallinnasta ilman laajamittaista yritystason infrastruktuuria.

1.3 Tämä politiikka tukee ISO/IEC 27001 -sertifiointia, EU:n GDPR:n mukaista vaatimustenmukaisuutta ja toimitusketjun hallinnan varmistamista yhdenmukaisella kaikkien kolmansien osapuolten pilvipalveluiden hallinnalla.

2. Soveltamisala

2.1 Tätä politiikkaa sovelletaan seuraaviin:

2.1.1 kaikkiin pilvipohjaisiin palveluihin, joita käytetään yrityksen tietojen tallentamiseen, käsittelyyn tai siirtämiseen

2.1.2 kaikkiin työntekijöihin, sopimuskumppaneihin ja palveluntarjoajiin, jotka käyttävät pilvipalveluita organisaation puolesta

2.1.3 maksuttomiin ja maksullisiin pilviratkaisuihin, mukaan lukien sähköpostialustat, asiakirjojen jakopalvelut, SaaS-työkalut, varmuuskopiointialustat, videoneuvottelupalvelut ja asiakasalustat

2.1.4 kaikkiin laitteisiin (työasemat, mobiililaitteet, tabletit), joilla käytetään yrityksen tietoja pilvisovellusten kautta

2.2 Tähän kuuluvat muun muassa seuraavat:

2.2.1 Microsoft 365, Google Workspace, Dropbox Business

2.2.2 Zoom, Microsoft Teams, Google Meet

2.2.3 AWS, Azure, GCP

2.2.4 pilvipohjaiset varmuuskopiointi- ja katastrofipalautustyökalut

2.2.5 jaetut kansiot tai sovellukset, joita käytetään laskutukseen, projektinhallintaan tai asiakasviestintään

3. Tavoitteet

3.1 Estää hyväksymättömien pilvipalveluiden luvaton tai korkean riskin käyttö.

3.2 Varmistaa, että pilvessä tallennetut sääntelyn alaiset tai arkaluonteiset tiedot suojataan asianmukaisilla teknisillä ja hallinnollisilla kontrolleilla.

3.3 Määrittää selkeät roolit pilvipalveluiden hyväksynnälle, konfiguroinnille, valvonnalle ja käytöstä poistolle.

3.4 Hallita tietovirtoja sekä toteuttaa pilveen tallennettuja tietoja koskevat säilytys-, poistamis- ja tietosuojavelvoitteet.

3.5 Vähentää riippuvuutta henkilökohtaisista tileistä tai valvomattomista työkaluista edellyttämällä, että kaikki liiketoimintatarkoituksiin käytettävät pilvijärjestelmät hyväksytään.

3.6 Täyttää ISO/IEC 27001:2022:n, EU:n GDPR:n, NIS2:n ja DORA:n vaatimukset ulkoisten pilvipalveluriippuvuuksien hallinnassa.

4. Roolit ja vastuut

4.1 toimitusjohtaja

4.1.1 hyväksyy kaikkien uusien pilvipalveluiden käyttöönoton

4.1.2 katselmoi pilvipalveluntarjoajiin ja palvelutyyppeihin liittyvät riskit

4.1.3 vastaa politiikan toimeenpanosta ja poikkeuspäätösten valvonnasta

4.2 ulkoinen IT-palveluntarjoaja tai IT-tukipalveluntarjoaja

4.2.1 arvioi ja toteuttaa pilvipalveluiden turvalliset määritykset

4.2.2 perustaa tilit, käyttöoikeuksien hallinnan ja varmuuskopioinnin

4.2.3 valvoo salasanoihin, monivaiheiseen todennukseen ja tietoturva-asetuksiin liittyvien vaatimusten noudattamista

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Toimitusjohtajan on katselmoitava tämä politiikka vähintään vuosittain yhteistyössä IT-palveluntarjoajan kanssa.

9.2 Muodollinen katselmointi on tehtävä myös seuraavissa tilanteissa:

9.2.1 pilvipalveluihin liittyvän tietoturvapoikkeaman jälkeen (esim. tietomurto, tietojen menetys)

9.2.2 kun käyttöön otetaan uusi merkittävä pilvialusta

9.2.3 jos lakisääteiset tai sääntelyvaatimukset muuttuvat (esim. EU:n GDPR-, NIS2- tai DORA-päivitykset)

9.2.4 jos seurantatoimenpiteet paljastavat väärinkäyttöä tai uusia riskejä

9.3 Toimitusjohtajan on varmistettava, että:

9.3.1 pilvipalvelurekisteri päivitetään uusilla tai käytöstä poistetuilla palveluilla

9.3.2 lakisääteiset ja tietosuojavaatimukset täyttyvät edelleen

9.3.3 kaikki muutokset viestitään asiaankuuluville käyttäjille ja sidosryhmille

9.4 Arkistoidut versiot on säilytettävä turvallisesti, ja vanhoja politiikkaversioita on käsiteltävä organisaation P14S – Tietojen säilytys- ja hävityspolitiikan mukaisesti.

10. Liittyvät politiikat ja yhteydet

10.1 Tätä politiikkaa on sovellettava yhdessä seuraavien pk-yrityksille yhdenmukaistettujen tietoturvapolitiikkojen kanssa:

10.1.1 P2S – Hallinnointirooleja ja vastuita koskeva politiikka: määrittää vastuut pilvipalveluiden hyväksynnästä ja palveluntarjoajasuhteiden hallinnasta.

10.1.2 P4S – Pääsynhallintapolitiikka: tukee pilvialustoilla vaadittuja turvallisia kirjautumis-, istunnonhallinta- ja käyttöoikeuksien poistamiskäytäntöjä.

10.1.3 P14S – Tietojen säilytys- ja hävityspolitiikka: ohjaa, miten pilvipohjaiset tiedot varmuuskopioidaan, säilytetään ja poistetaan lakisääteisten velvoitteiden mukaisesti.

10.1.4 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: varmistaa, että pilvipalveluihin tallennetut henkilötiedot käsitellään EU:n GDPR:n periaatteiden mukaisesti.

10.1.5 P30S – Tietoturvapoikkeamien hallintapolitiikka: määrittää rakenteiset menettelyt pilvipalveluihin liittyviin tietoturvapoikkeamiin reagoimiseksi, mukaan lukien näytön kerääminen ja ulkoinen ilmoittaminen.

10.2 Yhdessä nämä politiikat varmistavat, että pilvipalveluiden käyttö on turvallista, vaatimustenmukaista ja toiminnallisesti häiriönsietokykyistä.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Lauseke 8.1 – edellyttää organisaatioita toteuttamaan operatiiviset kontrollit tietojen käsittelylle, mukaan lukien pilvipohjaisiin järjestelmiin liittyvät kontrollit.

11.2 ISO/IEC 27002

11.2.1 Kontrolli 5.23 – edellyttää pilvipalveluiden käytön ja kolmannen osapuolen SaaS-työkalujen hallintaa.

11.2.2 Kontrolli 5.24 – edellyttää määriteltyä pilvipalveluiden käyttöpolitiikkaa, joka on yhdenmukainen riskien ja sääntelyvaatimusten kanssa.

11.2.3 Kontrolli 5.25 – edellyttää, että organisaatiot varmistavat pilviympäristöjen tietoturvakontrollien vastaavan organisaation tarpeita.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AC-20 – edellyttää muodollisia käyttösääntöjä ulkoisille järjestelmille, kuten pilvipalveluille.

11.3.2 SC-12, SC-13 – käsittelevät siirrettävien tietojen ja levossa olevien tietojen salausta pilviympäristöissä.

11.3.3 SR-5 – kattaa pilvipalveluihin ja kolmansien osapuolten riskeihin liittyvät toimitusketjukontrollit.

11.4 EU:n GDPR (2016/679)

11.4.1 Artikla 28 – edellyttää, että henkilötietojen käsittelijöinä toimivat pilvipalveluntarjoajat noudattavat sitovia sopimusvelvoitteita.

11.4.2 Artikla 32 – edellyttää teknisiä ja organisatorisia kontrolleja pilvipohjaiseen henkilötietojen käsittelyyn.

11.4.3 Luku V – kieltää pilveen tallennettujen henkilötietojen luvattomat kansainväliset siirrot.

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

11.5.1 Artikla 21(2)(f), (i) – edellyttää keskeisiä ja tärkeitä toimijoita toteuttamaan asianmukaiset politiikat pilvipalveluiden tietoturvaa ja toimitusketjun hallintaa varten.

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

11.6.1 Artikla 5(2) – edellyttää rahoitusalan pk-yrityksiä integroimaan pilvipalveluiden tietoturvan ICT-riskienhallinnan viitekehyksiinsä.

11.6.2 Artikla 28 – määrittää kriittisiä kolmannen osapuolen ICT-palveluntarjoajia, mukaan lukien pilvipalveluntarjoajia, koskevat valvontasäännöt.

11.7 COBIT 2019

11.7.1 DSS01 – "Manage Operations" käsittelee pilvipalveluiden operatiivista eheyttä.

11.7.2 DSS05 – "Manage Security Services" sisältää pilvipalvelukohtaiset suojaustoimenpiteet ja valvonnan.

11.7.3 BAI04 – "Manage Availability and Capacity" varmistaa liiketoiminnan jatkuvuuden ja suorituskyvyn pilviympäristöissä.