					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P27					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	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohta 8	Pilvipalvelujen operatiivista suunnittelua ja hallintaa koskevat vaatimukset.
ISO/IEC 27002:2022	Kontrollit 5.23–5.25	Pilvipalvelujen käyttöä, käyttöpolitiikkaa ja tietoturvaa koskevat vaatimukset.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12 – SC-28, SR-5	Ulkoisten järjestelmien käyttö, sopimukselliset ja tekniset vaatimukset, kryptografiset suojatoimet, toimitusketjun suojaus.
EU:n GDPR	Artiklat 28, 32, luku V	Pilvipalvelujen henkilötietojen käsittelijää koskevat vaatimukset, käsittelyn turvallisuus ja tiedonsiirrot.
EU:n NIS2-direktiivi	Artikla 21(2)(f, i)	Kolmansien osapuolten riskejä ja toimitusketjua koskevat vaatimukset.
EU:n DORA-asetus	Artiklat 5(2), 28	ICT-riskien ja kolmansien osapuolten (pilvipalvelut) valvonta finanssialan toimijoille.
COBIT 2019	BAI04, DSS01, DSS05	Pilvipalvelujen saatavuus, operointi ja tietoturvan hallinta.

1. Tarkoitus

1.1 Tämä politiikka määrittää organisaation pakolliset vaatimukset pilvipalvelujen turvalliselle, vaatimustenmukaiselle ja vastuulliselle käytölle Infrastructure-as-a-Service (IaaS)-, Platform-as-a-Service (PaaS)- ja Software-as-a-Service (SaaS) -toimitusmalleissa.

1.2 Politiikan tavoitteena on varmistaa, että pilvipalvelut otetaan käyttöön ja niitä hallitaan tavalla, joka suojaa tietovarantojen luottamuksellisuutta, eheyttä ja saatavuutta sekä täyttää sääntelyyn, lainsäädäntöön ja sopimuksiin perustuvat velvoitteet.

1.3 Politiikka määrittää kontrollit pilviriskien hallintaan, tietojen suojaamiseen, palveluntarjoajien vaatimustenmukaisuuden seurantaan ja luvattoman käytön estämiseen. Lisäksi se tukee liiketoiminnan uudistumista pilvialustojen avulla yhteensovittamalla tietoturvan, operatiivisen luotettavuuden ja kustannustehokkuuden.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia työntekijöitä, toimeksisaajia, kolmansien osapuolten palveluntarjoajia ja ulkoisia konsultteja, jotka organisaation puolesta myöntävät käyttöoikeuksia pilvipalveluihin, määrittävät, käyttävät, hallinnoivat tai muutoin hyödyntävät pilvipalveluja.

2.2 Politiikka koskee kaikkia ympäristöjä, joissa organisaation tietoja tai työkuormia käsitellään, mukaan lukien:

2.2.1 Julkiset, yksityiset, hybridi- ja yhteisöpilvitoteutukset

2.2.2 Kaikki pilvipalvelumallit (IaaS, PaaS, SaaS)

2.2.3 Monipilvi- ja federoidut arkkitehtuurit

2.2.4 Varjo-IT:n tai henkilökohtaisten pilvitilien käyttö liiketoimintatarkoituksiin

2.3 Politiikka kattaa kaikki tiedon luokittelutasot ja koskee sekä sisäisiä järjestelmiä että toimittajien ylläpitämiä alustoja, joissa organisaation omistamia tai sääntelyn alaisia tietoja säilytetään tai käsitellään.

3. Tavoitteet

3.1 Varmistaa pilviteknologioiden turvallinen ja yhdenmukainen käyttö selkeästi määritettyjen käyttöohjeiden, tietoturvan perusmääritysten ja hallinnointiroolien avulla.

3.2 Minimoida pilvipalveluihin liittyvät operatiiviset ja sääntelyyn liittyvät riskit, mukaan lukien luvaton pääsy, tietomurrot, virheelliset määritykset, vaatimustenvastaisuus ja palveluhäiriöt.

3.3 Varmistaa tietoturva- ja tietosuojavaatimusten toteutuminen kaikkien pilvipalvelutoimittajien osalta sekä todentaa vaatimustenmukaisuus sopimuslausekkeilla, arvioinneilla ja auditointioikeuksilla.

3.4 Mahdollistaa skaalautuva ja häiriönsietokykyinen pilvipalvelujen käyttöönotto vaarantamatta tietoturvan tasoa, lakisääteisiä vaatimuksia tai liiketoiminnan jatkuvuutta.

3.5 Yhdenmukaistaa pilvipalvelujen hallinnointi ja käyttö organisaation tietoturvallisuuden hallintajärjestelmän (ISMS), lakisääteisten velvoitteiden (esim. GDPR, DORA), toimialakohtaisten ohjeistusten ja yleisesti tunnustettujen parhaiden käytäntöjen (esim. NIST, COBIT) kanssa.

4. Roolit ja vastuut

4.1 Ylin johto

4.1.1 Hyväksyy pilvipalvelujen käyttöpolitiikan ja pilvipalvelujen käyttöönoton strategisen tiekartan.

4.1.2 Tarkastelee ja hyväksyy korkean riskin poikkeukset pilvipalvelujen hallinnoinnin vakiovaatimuksista.

4.1.3 Varmistaa, että pilvihankkeille osoitetaan riittävä rahoitus, valvonta ja yhdenmukaisuus organisaation riskienhallinnan viitekehysten kanssa.

4.2 Tietoturvajohtaja (CISO)

4.2.1 Omistaa tämän politiikan ja organisaation pilvipalvelurekisterin.

4.2.2 Hyväksyy uusien pilvipalveluntarjoajien käyttöönoton huolellisuusarvioinnin ja riskienarvioinnin perusteella.

4.2.3 Tarkastaa palveluntarjoajien vaatimustenmukaisuusdokumentaation ja varmistaa tietoturvakontrollien yhdenmukaisuuden.

[... 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 vuosittain ja päivitettävä tarpeen mukaan, jotta se säilyy yhdenmukaisena seuraavien kanssa:

9.1.1 kehittyvät oikeudelliset ja sääntelyyn liittyvät vaatimukset (esim. GDPR, NIS2, DORA)

9.1.2 ISO/IEC 27001- tai ISO/IEC 27002 -standardien muutokset

9.1.3 organisaation pilviarkkitehtuurin, riskiympäristön tai palveluportfolion muutokset

9.1.4 poikkeamien tutkinnat, auditointitulokset tai operatiivisesta käytöstä saadut opit

9.2 Tietoturvajohtaja (CISO) vastaa katselmoinnin käynnistämisestä ja asianomaisten sidosryhmien koollekutsumisesta, mukaan lukien:

9.2.1 pilviturvallisuusarkkitehti

9.2.2 laki- ja vaatimustenmukaisuustiimi

9.2.3 hankinta- ja toimittajahallinnasta vastaavat henkilöt

9.2.4 palveluomistajat ja IT-operaatiot

9.3 Kaikkien päivitysten on oltava:

9.3.1 versionhallittuja ja päivättyjä

9.3.2 ylimmän johdon hyväksymiä

9.3.3 tiedotettuja vaikutuksen alaisille osapuolille, mukaan lukien työntekijät, toimeksisaajat ja kolmannet osapuolet

9.3.4 arkistoituja sisäisten dokumentointipolitiikkojen mukaisesti

9.4 Väliaikaisia katselmointeja voidaan käynnistää seuraavissa tilanteissa:

9.4.1 uudet CSP-palvelusitoumukset tai merkittävät migraatiot

9.4.2 pilvi-infrastruktuuriin kohdistuvat esiin nousevat uhat

9.4.3 olennaiset muutokset sopimuksellisissa, oikeudellisissa tai toimialakohtaisissa velvoitteissa

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka liittyy läheisesti seuraaviin sisäisiin politiikkoihin ja on niistä riippuvainen:

10.1.1 P1 – Tietoturvapolitiikka: Määrittää järjestelmien ja palvelujen turvallista käyttöä koskevat yleiset periaatteet, joita tämä politiikka soveltaa pilviympäristöissä.

10.1.2 P5 – Muutoksenhallintapolitiikka: Kaikkien pilvimääritysten muutosten on noudatettava P5:ssä määritettyjä muutoksenhallintamenettelyjä.

10.1.3 P13 – Tiedon luokittelu- ja merkintäpolitiikka: Määrittää, miten tiedot arvioidaan ennen siirtoa pilveen ja miten kontrollit, kuten salaus ja tietojen sijainti, otetaan käyttöön.

10.1.4 P18 – Kryptografisten hallintakeinojen politiikka: Määrittää salauksen, avaintenhallinnan ja kryptografisten algoritmien käytön standardit, joita sovelletaan suoraan pilvipalvelujen määrityksiin.

10.1.5 P22 – Lokitus- ja valvontapolitiikka: Määrittää lokien keräämistä, säilytystä ja analysointia koskevat vaatimukset, jotka on toteutettava pilviympäristöissä.

10.1.6 P30 – Tietoturvapoikkeamien hallintapolitiikka: Määrittää pilvipalveluihin liittyvien tietoturvatapahtumien eskalointi-, rajaamis- ja korjausmenettelyt.

10.1.7 P33 – Auditointi- ja vaatimustenmukaisuuden seurantapolitiikka: Tukee auditointivalmiutta ja jatkuvaa varmistusta siitä, että pilvikontrollit on toteutettu ja niitä seurataan.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001: Kohta 8.1 – Operatiivinen suunnittelu ja hallinta: Edellyttää, että organisaatiot toteuttavat ja hallitsevat prosesseja, joita tarvitaan tietoturvavaatimusten täyttämiseen, mukaan lukien pilviympäristöihin liittyvät prosessit.

11.2 ISO/IEC 27002:2022 – Kontrollit 5.23–5.25:

11.2.1 Liite A, kontrolli 5.23 – Pilvipalvelujen käyttö: Edellyttää riskiperusteista arviointia, muodollista valtuutusta ja pilvipalvelujen käytön dokumentointia.

11.2.2 Liite A, kontrolli 5.24 – Pilvipalvelujen käyttöpolitiikka: Edellyttää organisaation tarpeisiin ja riskeihin perustuvien muodollisten pilvipalvelujen käyttöpolitiikkojen laatimista ja soveltamista.

11.2.3 Liite A, kontrolli 5.25 – Tietoturva pilvipalveluissa: Edellyttää tietoturvan integrointia, sopimuksellisia suojatoimia sekä pilvessä toimivien työkuormien ja tietojen seurantaa.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – Ulkoisten järjestelmien käyttö: Edellyttää määriteltyjä sääntöjä ja ehtoja organisaation resurssien käyttämiselle ulkoisista tai pilvipohjaisista järjestelmistä.

11.3.2 SA-9(5) – Ulkoisten tietojärjestelmäpalvelujen käyttö: Edellyttää sopimukseen perustuvia tietoturvavaatimuksia, valvontaa ja jatkuvaa seurantaa kolmannen osapuolen pilvijärjestelmille.

11.3.3 SC-12 – SC-28 – Kryptografiset suojatoimet, rajasuojaukset ja siirron eheys: Tukevat salaukseen, identiteettiin ja pääsyyn liittyviä vaatimuksia pilvessä toimiville palveluille ja siirrettäville tiedoille.

11.3.4 SR-5 – Toimitusketjun suojaus: Tukee pilvipalvelutoimitukseen osallistuvien palveluntarjoajien arviointia ja sopimuksellista hallintaa.

11.4 EU:n GDPR (2016/679):

11.4.1 Artikla 28 – Henkilötietojen käsittelijän velvollisuudet: Edellyttää muodollisia sopimuksia pilvipalveluntarjoajien kanssa henkilötietojen käsittelyn turvallisuuden, luottamuksellisuuden ja todennettavuuden varmistamiseksi.

11.4.2 Artikla 32 – Käsittelyn turvallisuus: Tukee salauksen, pääsynhallinnan, lokituksen ja muiden suojatoimien soveltamista pilviympäristöissä.

11.4.3 Luku V – Kansainväliset tiedonsiirrot: Edellyttää tietojen lainmukaista siirtoa EU:n/ETA:n ulkopuolelle käyttäen suojatoimia, kuten SCC-lausekkeita tai tietosuojan riittävyyttä koskevia päätöksiä.

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

11.5.1 Artikla 21(2)(f, i): Edellyttää, että organisaatiot hallitsevat kolmannen osapuolen pilvipalveluntarjoajiin liittyviä riskejä ja varmistavat digitaalisen toimitusketjun eheyden sopimuksellisilla ja teknisillä toimenpiteillä.

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

11.6.1 Artikla 5(2) – ICT-riskien hallinnointi: Edellyttää, että ICT-kolmannen osapuolen riskit, mukaan lukien pilvipalvelut, integroidaan kokonaisvaltaiseen riskienhallintaan.

11.6.2 Artikla 28 – Kriittisten ICT-kolmannen osapuolen palveluntarjoajien valvonta: Edellyttää, että finanssialan toimijat seuraavat, hallitsevat ja raportoivat pilvipalveluntarjoajariippuvuuksia, tietoturvan tasoa ja häiriönsietokykyä.

11.7 COBIT 2019:

11.7.1 BAI04 – Saatavuuden ja kapasiteetin hallinta: Varmistaa, että pilvipalvelut ovat häiriönsietokykyisiä, valvottuja ja täyttävät määritetyt suorituskykykriteerit.

11.7.2 DSS01 – Operaatioiden hallinta: Tukee operatiivista integraatiota, poikkeamien käsittelyä ja perusmäärityksiä pilvessä toimivilla alustoilla.

11.7.3 DSS05 – Tietoturvapalvelujen hallinta: Ohjaa pilvikohtaisten tietoturvakontrollien toteutusta, valvontaa ja tietoturvapoikkeamien ennaltaehkäisyä digitaalisissa palveluissa.