					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P26S					Asiakirjan nimi: **Kolmansien osapuolten ja toimittajien tietoturvapolitiikka**							
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	Lauseke 8	Operatiiviset kontrollit kolmansia osapuolia ja toimittajasuhteita varten
ISO/IEC 27002:2022	Kontrollit 5.19–5.22	Toimittajaturvallisuuden kontrollit, sopimukselliset tietoturvavaatimukset, muutoksenhallinta, seuranta ja katselmointi
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Hankintaa, konfiguraationhallintaa, yhteenliittämissopimuksia ja ulkoista henkilöstöä koskevat kontrollit
EU:n GDPR	Artiklat 28, 32	Tietojenkäsittelysopimukset ja käsittelijöille asetettavat tietoturvavaatimukset
EU:n NIS2-direktiivi	Artiklat 21(2)(a)(b)(i), 23(1)	Toimitusketjuriskien hallinta, kolmannen osapuolen palvelujen valvonta
EU:n DORA-asetus	Artiklat 5(1)(2), 28(1)(2)	ICT-riskien hallinta kolmannen osapuolen palveluntarjoajien osalta
COBIT 2019	APO10, APO12, DSS05	Toimittajahallinta ja riskien integrointi

1. Tarkoitus

1.1 Tämä politiikka määrittää pakolliset tietoturvavaatimukset sellaisten kolmansien osapuolten ja toimittajien käyttöönotolle, hallinnalle ja sopimussuhteen päättämiselle, joilla on pääsy organisaation tietoihin, järjestelmiin tai palveluihin tai jotka vaikuttavat niihin.

1.2 Tämä politiikka varmistaa, että ulkoiset palveluntarjoajat, mukaan lukien IT-tukipalvelujen tarjoajat, pilvipalveluntarjoajat, ohjelmistokehittäjät ja liiketoimintaprosesseja tukevat sopimuskumppanit, käsittelevät yrityksen omaisuutta turvallisesti sovellettavan lainsäädännön ja standardien mukaisesti.

1.3 Tämä politiikka vähentää riskejä, kuten tietovuotoja, luvattomia järjestelmämuutoksia, sääntelyyn liittyviä seuraamusmaksuja tai liiketoiminnan keskeytyksiä, jotka johtuvat puutteellisesti suojatuista tai hallituista kolmannen osapuolen järjestelyistä.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia kolmansia osapuolia, jotka:

2.1.1 toimittavat ohjelmistoja, infrastruktuuria, hosting-palveluja tai pilvipalveluja

2.1.2 käyttävät tai hallinnoivat sisäisiä järjestelmiä, laitteita tai sovelluksia

2.1.3 käsittelevät yrityksen tietoja, asiakirjoja tai varmuuskopioita

2.1.4 tukevat liiketoimintaa, henkilöstöhallintoa, taloushallintoa tai asiakaspalvelua

2.2 Tämä politiikka koskee myös:

2.2.1 sisäistä henkilöstöä, joka osallistuu toimittajien valintaan, hankintaan tai valvontaan

2.2.2 henkilöstöä, joka hallinnoi toimittajien käyttöönottoa, sopimuksia, käyttöoikeuksia tai katselmointeja

2.2.3 järjestelmiä tai prosesseja, jotka ovat riippuvaisia kolmannen osapuolen komponenteista tai palveluista

3. Tavoitteet

3.1 Varmistaa, että kaikki toimittajat täyttävät selkeästi määritellyt tietoturvavaatimukset.

3.2 Varmistaa, että toimittajasopimukset sisältävät täytäntöönpanokelpoiset tietoturvaa, tietosuojaa ja poikkeamien käsittelyä koskevat velvoitteet.

3.3 Arvioida ja dokumentoida toimittajariskit ennen sopimusten allekirjoittamista tai käyttöoikeuksien myöntämistä.

3.4 Toteuttaa korkean riskin ja kriittisille toimittajille säännölliset katselmoinnit vaatimustenmukaisuuden varmistamiseksi.

3.5 Määrittää muodollinen menettely poikkeuksille, poikkeamien hallinnalle ja sopimuspäivityksille.

3.6 Tukea ISO/IEC 27001:2022 -standardin, EU:n GDPR:n, EU:n NIS2-direktiivin ja EU:n DORA-asetuksen velvoitteiden noudattamista toimittajahallinnan osalta.

4. Roolit ja vastuut

4.1 Toimitusjohtaja (GM)

4.1.1 Vastaa viime kädessä toimittajien valinnasta ja tietoturvaa koskevasta vaatimustenmukaisuudesta

4.1.2 Hyväksyy toimittajia koskevat sopimukset, poikkeukset ja eskaloinnit

4.1.3 Valvoo tietoturvapoikkeamiin reagointia ja päätöksentekoa tilanteissa, joissa toimittaja ei täytä velvoitteitaan

4.2 IT-palveluntarjoaja tai sisäinen tietoturvayhteyshenkilö

4.2.1 Arvioi toimittajien pyytämän teknisen pääsyn

4.2.2 Toteuttaa pääsynhallintaa koskevat säännöt, tarkastaa lokit ja varmistaa tietojen turvallisen käsittelyn

4.2.3 Tarkastaa soveltuvin osin tietoturvakontrolleja, sertifiointeja tai auditointituloksia koskevan näytön

[... 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 yhdessä IT-palveluntarjoajan tai toimittajahallinnasta vastaavan henkilön kanssa.

9.2 Tämä politiikka on katselmoitava myös:

9.2.1 merkittävän lakisääteisiin, sääntelyyn liittyviin tai sopimuksellisiin velvoitteisiin vaikuttavan muutoksen jälkeen

9.2.2 toimittajaan liittyvän tietoturvapoikkeaman tai auditointihavainnon jälkeen

9.2.3 otettaessa käyttöön uusia toimittajaluokkia (esim. kriittiset SaaS-ympäristöt)

9.3 Kaikkien päivitysten on oltava:

9.3.1 dokumentoituja versionhistorian ja perustelujen kanssa

9.3.2 toimitusjohtajan hyväksymiä

9.3.3 viestittyjä asianomaiselle sisäiselle henkilöstölle ja toimittajavastaaville

9.3.4 tallennettuja aiempien versioiden kanssa P14S – Tietojen säilytys- ja hävityspolitiikan mukaisesti

10. Liittyvät politiikat ja yhteydet

10.1 Tämän politiikan tehokas toimeenpano edellyttää koordinointia seuraavien pk-yrityksen tietoturvapolitiikkojen kanssa:

10.1.1 P2S – Hallinnointirooleja ja vastuita koskeva politiikka: määrittää vastuut toimittajien valvonnalle ja sopimusten toimeenpanolle.

10.1.2 P4S – Pääsynhallintapolitiikka: määrittää pääsyn rajoittamista koskevat säännöt, joita on sovellettava, kun toimittajille myönnetään järjestelmäkäyttöoikeuksia.

10.1.3 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: varmistaa, että henkilötietoja käsittelevät toimittajat noudattavat tietosuojaperiaatteita ja lakisääteisiä vaatimuksia.

10.1.4 P14S – Tietojen säilytys- ja hävityspolitiikka: koskee tietoja ja tallenteita, jotka on jaettu toimittajille tai joita toimittajat säilyttävät, ja määrittää turvallisen hävittämisen sopimuksen päättyessä.

10.1.5 P30S – Tietoturvapoikkeamien hallintapolitiikka: määrittää toimintatavan tilanteissa, joissa toimittaja aiheuttaa tietoturvapoikkeaman tai on siihen osallisena, mukaan lukien eskalointi sekä todentavan aineiston käsittelymenettelyt.

10.2 Nämä politiikat yhdessä varmistavat, että toimittajariskiä hallitaan koko sopimuksen elinkaaren ajan.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Lauseke 8.1 – edellyttää operatiivisten kontrollien toteuttamista, mukaan lukien kolmansia osapuolia ja toimittajasuhteita koskevat kontrollit.

11.2 ISO/IEC 27002

11.2.1 Kontrolli 5.19 – varmistaa, että toimittajien tietoturvatoimenpiteet ovat organisaation vaatimusten mukaisia.

11.2.2 Kontrolli 5.20 – edellyttää muodollisia sopimuksia, jotka kattavat tietoturvavaatimukset, vastuut ja tietoturvaloukkauksiin liittyvät velvoitteet.

11.2.3 Kontrolli 5.21 – hallitsee toimittajapalvelujen muutoksia, jotka voivat vaikuttaa tietoturvan tilaan.

11.2.4 Kontrolli 5.22 – edellyttää toimittajapalvelujen ja vaatimustenmukaisuuden seurantaa ja katselmointia.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – ohjaa ulkoisten järjestelmien ja palvelujen hankintaa ja edellyttää riskien arviointia sekä määriteltyjä odotuksia.

11.3.2 SA-10 – hallitsee kolmannen osapuolen hallinnoimiin järjestelmiin liittyviä konfiguraatio- ja muutosmenettelyjä.

11.3.3 CA-3 – edellyttää yhteenliittämissopimuksia järjestelmille, joihin osallistuu ulkoisia tahoja.

11.3.4 PS-7 – määrittää ulkoisen henkilöstön seulonnan ja vastuiden osoittamisen.

11.4 EU:n GDPR (2016/679)

11.4.1 Artikla 28 – edellyttää tietojenkäsittelysopimuksia toimittajien kanssa, kun nämä toimivat henkilötietojen käsittelijöinä.

11.4.2 Artikla 32 – velvoittaa toteuttamaan asianmukaiset tekniset ja organisatoriset tietoturvatoimenpiteet kaikille henkilötietojen käsittelijöille.

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

11.5.1 Artikla 21(2)(a), (b), (i) – velvoittaa hallitsemaan ICT-toimitusketjun riskejä ja toteuttamaan kolmansia osapuolia koskevat kontrollit.

11.5.2 Artikla 23(1) – edellyttää dokumentoitua kolmannen osapuolen palvelujen valvontaa keskeisille ja tärkeille toimijoille.

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

11.6.1 Artikla 5(1) – edellyttää ICT-riskienhallinnan viitekehystä, joka kattaa kaikki kriittiset kolmannen osapuolen palveluntarjoajat.

11.6.2 Artikla 5(2) – määrää ICT-palveluriippuvuuksia koskevista sopimuksellisista ja operatiivisista kontrolleista.

11.6.3 Artikla 28(1), (2) – määrittää finanssialan ICT-kolmannen osapuolen riskiä koskevat valvontasäännöt.

11.7 COBIT 2019

11.7.1 APO10 – "Manage Suppliers" määrittää hankinnan kontrollit ja suhteiden hallinnan odotukset.

11.7.2 APO12 – "Manage Risk" integroi toimittajariskin organisaation riskienhallintaan.

11.7.3 DSS05 – "Manage Security Services" koskee hallinnoituja kolmansia osapuolia ja ulkoistettuja palveluntarjoajia.