					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P26					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/säädös	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	Clause 8	Operatiivinen suunnittelu ja ohjaus: edellyttää muodollisia kontrolleja ISMS:ään vaikuttaville kolmannen osapuolen palveluille
ISO/IEC 27002:2022	Controls 5.19–5.22	Toimittajasuhteita koskevat politiikat ja menettelyt, toimittajariskien hallinta, toimittajapalvelujen toimituksen hallinta sekä toimittajien seuranta ja katselmointi
NIST SP 800-53 Rev. 5	SA-9, SA-10, CA-3, PS-7	Ulkoiset järjestelmäpalvelut, kehittäjän konfiguraationhallinta, järjestelmien väliset yhteydet sekä kolmannen osapuolen henkilöstöturvallisuus
EU:n GDPR	Articles 28, 32, 33	Käsittelijän velvollisuudet, käsittelyn turvallisuus sekä henkilötietojen tietoturvaloukkauksesta ilmoittaminen
EU:n NIS2-direktiivi	Article 21(2)(e–f)	Riskiperusteinen toimittajahallinta ja tietoturvan valvonta
EU:n DORA-asetus	Articles 28, 30	ICT-kolmannen osapuolen riskit sekä kriittisten ICT-kolmannen osapuolen palveluntarjoajien valvonta
COBIT 2019	BAI05, DSS02, MEA03	Organisaatiomuutosten käyttöönoton hallinta, palvelupyyntöjen ja poikkeamien hallinta sekä vaatimustenmukaisuuden seuranta, arviointi ja tarkastelu

1. Tarkoitus

1.1 Tämä politiikka määrittää tietoturvavaatimukset turvallisten suhteiden muodostamiselle, hallinnalle ja ylläpidolle kolmannen osapuolen toimittajien ja palveluntarjoajien kanssa.

1.2 Se varmistaa, että kaikki toimittajat, joilla on pääsy organisaation tietoihin, järjestelmiin tai infrastruktuuriin, kuuluvat koko palvelun elinkaaren ajan tiukkojen tietoturvakontrollien, sopimuksellisten suojatoimien ja jatkuvan valvonnan piiriin.

1.3 Tämä politiikka tukee ISO/IEC 27001:n liitteen A kontrolleja 5.19–5.22 sisällyttämällä tietoturvavaatimukset hankinnan, käyttöönoton, huolellisuusarvioinnin, sopimushallinnan, palvelujen seurannan ja palvelussuhteen päättämisen prosesseihin.

2. Soveltamisala

2.1 Tämä politiikka koskee:

2.1.1 kaikkia kolmannen osapuolen toimittajia, urakoitsijoita, pilvipalveluntarjoajia ja palveluorganisaatioita, jotka käsittelevät organisaation tietovaroja tai joilla on pääsy niihin

2.1.2 kaikkia sisäisiä rooleja, jotka osallistuvat toimittajien arviointiin, käyttöönottoon, sopimiseen, riskienhallintaan, seurantaan tai palvelussuhteen päättämiseen

2.1.3 kaikkia toimittajasuhteita, joihin sisältyy pääsy arkaluonteisiin tietoihin, integraatio tuotantopalveluihin tai tuki kriittisille liiketoimintatoiminnoille

2.2 Tämä politiikka kattaa soveltuvin osin sekä suorat toimittajat että niiden alihankkijat ja sisältää kolmannen osapuolen ohjelmistot, infrastruktuurin, tuen ja hallinnoidut palvelut.

3. Tavoitteet

3.1 Varmistaa, että toimittajiin liittyvät tietoturvariskit tunnistetaan, arvioidaan ja niitä lievennetään johdonmukaisesti koko sopimussuhteen elinkaaren ajan.

3.2 Sisällyttää vakioidut tietoturvavaatimukset kaikkiin toimittajasopimuksiin, mukaan lukien velvollisuudet ilmoittaa tietoturvaloukkauksista, auditointioikeutta koskevat ehdot ja tietosuojavastuut.

3.3 Edellyttää muodollista huolellisuusarviointia ja dokumentoituja riskienarviointeja ennen uusien toimittajien käyttöönottoa tai korkean riskin palvelusopimusten uusimista.

3.4 Luoda mekanismit toimittajien vaatimustenmukaisuuden jatkuvaan seurantaan, mukaan lukien suoritusarvioinnit, auditoinnit ja poikkeamien eskalointi.

3.5 Hallita toimittajapalveluihin tehtävät muutokset sekä varmistaa turvallinen palvelussuhteen päättäminen ja tietojen palautus tai hävittäminen sopimuksen päättyessä.

3.6 Yhdenmukaistaa kolmannen osapuolen tietoturvakontrollit sovellettavien sääntely- ja sopimusvelvoitteiden kanssa, mukaan lukien EU:n GDPR, EU:n NIS2-direktiivi, EU:n DORA-asetus ja ISO/IEC 27001.

4. Roolit ja vastuut

4.1 Tietoturvajohtaja (CISO)

4.1.1 Omistaa tämän politiikan ja varmistaa sen yhdenmukaisuuden koko ISMS:n, riskienhallinnan ja vaatimustenmukaisuusstrategian kanssa.

4.1.2 Hyväksyy toimittajien luokittelutasot, tietoturvakatselmusten tulokset ja korkean riskin poikkeukset.

4.1.3 Osallistuu vakavien toimittajapoikkeamien eskalointiin ja kriittisiä palveluja koskeviin sopimusneuvotteluihin.

4.2 Hankinta ja toimittajahallinta

4.2.1 Varmistaa, että kaikkiin uusiin ja uusittaviin toimittajasopimuksiin sisällytetään hyväksytyt tietoturva- ja tietosuojalausekkeet.

4.2.2 Ylläpitää keskitettyä toimittajarekisteriä ja koordinoi kolmannen osapuolen riskeihin liittyvää dokumentaatiota lakiasioiden ja vaatimustenmukaisuuden kanssa.

4.2.3 Käynnistää käyttöönottoprosessit ja varmistaa niiden yhdenmukaisuuden sopimusta edeltävien tietoturva-arviointien kanssa.

[... 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 tai aiemmin, jos tapahtuu jokin seuraavista:

9.1.1 olennaiset muutokset hankintastrategiassa tai toimittajaekosysteemissä

9.1.2 muutokset oikeudellisissa tai sääntelyä koskevissa viitekehyksissä (esim. EU:n DORA-asetus, EU:n GDPR)

9.1.3 merkittävät kolmannen osapuolen poikkeamat, tietomurrot tai auditointien epäonnistumiset

9.1.4 riskienarvioinneista tai ulkoisilta sertifiointielimiltä saadut havainnot

9.2 Katselmointiprosessin omistavat yhdessä tietoturvajohtaja (CISO), hankinta, lakiasiat ja vaatimustenmukaisuus sekä riskienhallintatoiminto.

9.3 Kaikki politiikan muutokset on dokumentoitava ISMS:n asiakirjahallintarekisteriin, pidettävä versiohallittuina ja viestittävä olennaisille sidosryhmille toimittajahallinnan kanavien ja henkilöstön tietoisuusohjelmien kautta.

9.4 Korvatut versiot on arkistoitava vähintään kolmeksi vuodeksi jäljitettävyyden ja oikeudellisen vaatimustenmukaisuuden varmistamiseksi.

10. Liittyvät politiikat ja yhteydet

10.1 P1 – Tietoturvapolitiikka. Määrittää yleisen sitoumuksen kaikkien organisaation toimintojen suojaamiseen, mukaan lukien riippuvuudet kolmannen osapuolen toimittajista ja ulkoisista palveluntarjoajista.

10.2 P6 – Riskienhallintapolitiikka. Ohjaa kolmannen osapuolen suhteisiin liittyvien riskien tunnistamista, arviointia ja lieventämistä, mukaan lukien toimittajaekosysteemeistä periytyvät tai järjestelmätason riskit.

10.3 P17 – Tietosuoja- ja yksityisyydensuojapolitiikka. Koskee kaikkia toimittajia, jotka käsittelevät henkilötietoja, ja edellyttää asianmukaisia sopimusehtoja, siirtojen suojatoimia ja sisäänrakennetun tietosuojan periaatteita.

10.4 P4 – Pääsynhallintapolitiikka. Määrittää, miten kolmannen osapuolen henkilöstö saa pääsyn organisaation järjestelmiin, ja toimeenpanee roolipohjaiset käyttöoikeudet, istunnon hallintatoimet ja käyttöoikeuksien perumismenettelyt.

10.5 P22 – Lokitus- ja valvontapolitiikka. Edellyttää, että toimittajien pääsyä järjestelmiin seurataan, kirjataan lokiin ja katselmoidaan erityisesti ympäristöissä, joissa tapahtuu etuoikeutettua käyttöä tai tietoihin kohdistuvia toimia.

10.6 P30 – Tietoturvapoikkeamien hallintapolitiikka. Määrittää eskalointimenettelyt ja tietoturvaloukkausten ilmoitusvaatimukset toimittajaperäisille tietoturvatapahtumille tai yhteisille tutkinnolle, jotka koskevat kolmannen osapuolen järjestelmiä.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001: Clause 8.1 – Operatiivinen suunnittelu ja ohjaus: edellyttää muodollisia kontrolleja ISMS:ään vaikuttaville kolmannen osapuolen palveluille.

11.2 ISO/IEC 27002:2022 – Kontrollit 5.19–5.22:

11.2.1 Liite A, kontrolli 5.19 – Toimittajasuhteita koskevat politiikat ja menettelyt: edellyttää kontrolleja toimittajavuorovaikutusten hallintaan.

11.2.2 Liite A, kontrolli 5.20 – Toimittajariskien hallinta: keskittyy toimittajien tietoturvan tilan tunnistamiseen, arviointiin ja jatkuvaan valvontaan.

11.2.3 Liite A, kontrolli 5.21 – Toimittajapalvelujen toimituksen hallinta: edellyttää suorituskyvyn ja tietoturvan yhdenmukaisuutta sopimuksellisten odotusten kanssa.

11.2.4 Liite A, kontrolli 5.22 – Toimittajien seuranta ja katselmointi: vahvistaa tarpeen jatkuvalle kolmannen osapuolen vaatimustenmukaisuuden varmennukselle ja uudelleenarvioinnille.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 SA-9 – Ulkoiset järjestelmäpalvelut: määrittää ulkoisten tahojen operoimien järjestelmien tietoturva- ja riskivaatimukset.

11.3.2 SA-10 – Kehittäjän konfiguraationhallinta: soveltuu tilanteisiin, joissa kolmannet osapuolet toimittavat ohjelmistoja tai ympäristöjä.

11.3.3 CA-3 – Järjestelmien väliset yhteydet: edellyttää valvontaa ja sopimista organisaatioiden välisten järjestelmien tietovirroista.

11.3.4 PS-7 – Kolmannen osapuolen henkilöstöturvallisuus: varmistaa, että toimeksisaajien ja toimittajien henkilöstö tarkistetaan ja sitä valvotaan asianmukaisesti.

11.4 EU:n GDPR (2016/679):

11.4.1 Artikla 28 – Käsittelijän velvollisuudet: edellyttää kirjallisia sopimuksia henkilötietojen käsittelijöiden kanssa, mukaan lukien tekniset ja organisatoriset toimenpiteet.

11.4.2 Artikla 32 – Käsittelyn turvallisuus: edellyttää asianmukaisia suojatoimia sekä rekisterinpitäjiltä että käsittelijöiltä.

11.4.3 Artikla 33 – Henkilötietojen tietoturvaloukkauksesta ilmoittaminen: edellyttää toimittajilta viivytyksetöntä ilmoitusta loukkauksen tapahtuessa.

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

11.5.1 Artikla 21(2)(e–f): edellyttää riskiperusteista toimittajahallintaa ja tietoturvan valvontaa erityisesti keskeisten ja tärkeiden toimijoiden digitaalisissa toimitusketjuissa.

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

11.6.1 Artikla 28 – ICT-kolmannen osapuolen riskit: asettaa velvoitteita riskien arvioinnille, sopimuksellisille tietoturvaehdoille ja irtautumisstrategioille finanssipalveluntarjoajille.

11.6.2 Artikla 30 – Kriittisten ICT-kolmannen osapuolen palveluntarjoajien valvonta: määrittää tehostetun seurannan ja valvonnalliset odotukset keskeisille toimittajille.

11.7 COBIT 2019:

11.7.1 BAI05 – Organisaatiomuutosten käyttöönoton hallinta: varmistaa, että toimittajasiirtymät hallitaan turvallisesti.

11.7.2 DSS02 – Palvelupyyntöjen ja poikkeamien hallinta: soveltuu toimittajien ilmoittamiin asioihin ja poikkeamien käsittelyn integrointiin.

11.7.3 MEA03 – Vaatimustenmukaisuuden seuranta, arviointi ja tarkastelu: vahvistaa toimittajien suorituskyvyn mittaamista ja vaatimustenmukaisuuden seurantaa.