					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P41					Asiakirjan nimi: **Toimittajariippuvuuden riskienhallintapolitiikka**							
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 säädösten kanssa

Standardi/säädös	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	6.1.3, 8.1, 9.1	
ISO/IEC 27002:2022	5.20, 5.21, 5.22, 5.23, 5.30	
NIST SP 800-53 Rev.5	SR-2, SR-3, SR-5, SR-6, SR-11, RA-3	
EU:n GDPR	Art. 28, Art. 32(1)(d)	
EU:n NIS2-direktiivi	Art. 21(2)(d), Art. 21(3), Art. 22	
EU:n DORA-asetus	Art. 28–30	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Tarkoitus

1.1 Vahvistaa organisaation toimitusketjun turvallisuuskäytäntöjä ottamalla käyttöön menettely kriittisten toimittaja- ja palveluntarjoajariippuvuuksien tunnistamiseksi ja hallitsemiseksi EU:n NIS2-direktiivin 21 artiklan 3 kohdan sekä unionitason toimitusketjun riskinarviointien edellyttämällä tavalla.

1.2 Varmistaa, että yksittäisiin toimittajiin kohdistuvat keskittymä- ja riippuvuusriskit tunnistetaan ja niitä lievennetään sekä että mahdolliset toimialakohtaiset toimitusketjuriskit, joita viranomaiset korostavat NIS2-direktiivin 22 artiklan nojalla, sisällytetään riskienhallintaan ja liiketoiminnan jatkuvuussuunnitteluun.

2. Soveltamisala

2.1 Tätä politiikkaa sovelletaan kaikkiin keskeisiin toimittajiin ja palveluntarjoajiin, joihin organisaatio tukeutuu kriittisissä toiminnoissaan, erityisesti ICT-toimitusketjussa (laitteisto, ohjelmisto, pilvipalvelut, televiestintä, hallinnoidut palvelut).

2.2 Se kattaa sisäiset toiminnot, mukaan lukien hankinta, toimittajahallinta, riskienhallinta ja asiaankuuluvat operatiiviset yksiköt. Se koskee myös kyseisiä toimittajia siltä osin kuin niiltä kerätään riskitietoja. Kriittisillä toimittajilla tarkoitetaan toimittajia, joiden vikaantuminen tai vaarantuminen voisi merkittävästi heikentää kykyämme tuottaa palveluja tai täyttää lakisääteiset velvoitteemme.

3. Tavoitteet

3.1 Saavuttaa näkyvyys toimitusketjuriippuvuuksiin tunnistamalla erityisesti yksittäiset vikapisteet tai korkeat keskittymäriskit toimittajakannassa (esimerkiksi riippuvuus yhdestä pilvipalveluntarjoajasta kaikkien palvelujen osalta).

3.2 Toteuttaa toimenpiteet toimittajiin liittyvien riskien vähentämiseksi ja hallitsemiseksi, kuten hajauttaminen, varautumissuunnitelmat tai toimittajien kontrollien parantamista koskevat vaatimukset, ja siten vahvistaa häiriönsietokykyä toimittajahäiriöitä ja toimitusketjusta alkavia hyökkäyksiä vastaan.

3.3 Yhdenmukaistaa toiminta EU:n NIS2-direktiivin vaatimusten kanssa sisällyttämällä kriittisiä toimitusketjuja koskevien koordinoitujen tietoturvariskien arviointien tulokset organisaation riskipäätöksiin sekä varmistamalla, että toimitusketjuriskien hallintamalli on dokumentoitu ja todennettavissa.

4. Roolit ja vastuut

4.1 Toimittajahallintatoiminto (VMO): omistaa toimittajariippuvuusrekisterin ja koordinoi riskien arviointia. Varmistaa, että jokaisen keskeisen toimittajan kriittisyys ja riippuvuustaso arvioidaan käyttöönoton yhteydessä ja sen jälkeen säännöllisesti.

4.2 Riskienhallinta (yritystason riskikomitea): katselmoi keskittymäriskit ja riippuvuusanalyysit, hyväksyy riskienkäsittelystrategiat (esimerkiksi vaihtoehtoisen toimittajan lisääminen tai lisävaraston ylläpito kriittisille komponenteille) sekä sisällyttää toimitusketjuriskit riskirekisteriin ja raportoi niistä ylimmälle johdolle.

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

9. Seuranta ja auditointi

9.1 Toimittajariippuvuusrekisteri ja riskien arvioinnit auditoidaan sisäisesti vuosittain. Sisäinen tarkastus varmistaa, että kaikki kriittiset toimittajat on kirjattu, että niiden riskiluokitukset ovat ajan tasalla ja että lieventämissuunnitelmat ovat olemassa ja etenevät. Lisäksi tarkastetaan, että ulkoiset riskinarviointisyötteet (22 artiklan raportit jne.) on huomioitu asianmukaisesti.

9.2 Hajauttamisen ja varautumistoimenpiteiden tehokkuutta testataan säännöllisesti. Esimerkiksi voidaan toteuttaa suunniteltu simulaatio, jossa oletetaan merkittävän toimittajan epäonnistuvan, jotta jatkuvuussuunnitelmat ja vaihtoehtoiset järjestelyt voidaan testata (vastaavalla tavalla kuin katastrofipalautusharjoitus, mutta toimittajahäiriön näkökulmasta). Testien tulokset dokumentoidaan, ja havaitut puutteet korjataan.

9.3 Mittarit: riskienhallintatoiminto seuraa mittareita, kuten "% kriittisistä palveluista, joille on käytettävissä vähintään yksi vaihtoehtoinen toimittaja tai ratkaisu" tai "5 merkittävintä toimittajariippuvuutta ja niiden riskitrendi". Nämä mittarit sisällytetään johdon riskimittaristoon. Riippuvuusriskin laskeva kehityssuunta ajan myötä on tavoite; jos mittarit osoittavat riippuvuuden kasvua, tämän on käynnistettävä johdon käsittely.

10. Katselmointi ja ylläpito

10.1 Toimittajahallinnan ja riskienhallinnan tiimit katselmoivat tämän politiikan vähintään kerran vuodessa. Katselmoinnissa huomioidaan muutokset toimittajakentässä (esimerkiksi jos uusi toimittaja muuttuu kriittiseksi tai vanha toimittaja poistetaan käytöstä) sekä uudet ulkoistamista tai kolmansien osapuolten riskejä koskevat sääntelyvaatimukset.

10.2 Jos toimialan viranomaiset julkaisevat päivitettyä ohjeistusta tai jos poikkeama paljastaa puutteita (esimerkiksi toimittajahäiriön vaikutus oli ennakoitua suurempi, mikä osoittaa, että riippuvuus oli arvioitu virheellisesti), politiikka päivitetään kriteerien tai lieventämisstrategioiden tarkentamiseksi.

10.3 Politiikan päivitetyt versiot on hyväksyttävä ylimmässä johdossa. Merkittävistä muutoksista tiedotetaan kaikille asiaankuuluville yksiköille, ja koulutusmateriaalit päivitetään vastaavasti uusien menettelyjen tai standardien huomioimiseksi.

11. Liittyvät politiikat ja yhteydet

11.1 P01 – Tietoturvapolitiikka. Määrittää vastuut toimittajariippuvuuksien hallinnalle.

11.2 P02 – Hallinnointirooleja ja vastuita koskeva politiikka. Selkeyttää toimittajariskejä koskevien päätösten omistajuuden.

11.3 P06 – Riskienhallintapolitiikka. Sisällyttää keskittymäriskin yritystason riskirekistereihin.

11.4 P26 – Kolmansien osapuolten ja toimittajaturvallisuuden politiikka. Määrittää perustason tietoturvan; P41 lisää riippuvuus- ja keskittymäriskin hallintakeinot.

11.5 P27 – Pilvipalvelujen käyttöpolitiikka. Soveltaa riippuvuuskriteereitä pilvipalvelujen käyttöönottoon ja exit-suunnitelmiin.

11.6 P28 – Ulkoistetun kehittämisen politiikka. Kattaa ulkoiseen suunnittelu- ja kehitystyöhön liittyvät riippuvuusriskit.

11.7 P32 – Liiketoiminnan jatkuvuus- ja katastrofipalautuspolitiikka. Määrittää toimittajahäiriö- ja korvaamisskenaariot.

11.8 P37 – Laki- ja vaatimustenmukaisuuspolitiikka. Varmistaa, että sopimukset ja velvoitteet sisältävät riippuvuusriskin hallintakeinot.

12. Viitteet

12.1 NIS2-direktiivi (EU 2022/2555), 21 artiklan 3 kohta (edellyttää kullekin suoralle toimittajalle tai palveluntarjoajalle ominaisia haavoittuvuuksia sekä niiden kyberturvallisuuden laatua koskevien seikkojen huomioimista, mukaan lukien koordinoitujen toimitusketjun riskinarviointien tulokset)

12.2 NIS2-direktiivi, 22 artiklan 1 kohta (kriittisiä toimitusketjuja koskevat unionitason koordinoidut tietoturvariskien arvioinnit, jotka tuottavat organisaatioille tietoa toimialan laajuisista toimittajariskeistä)

12.3 Komission täytäntöönpanoasetus (EU) 2024/2690, liitteen jakso 5 (toimitusketjun turvallisuusvaatimukset organisaatioille, mukaan lukien toimittajien valintaa, hajauttamista ja sopimusvelvoitteita koskevat kriteerit)

12.4 ENISAn hyvät käytännöt toimitusketjun kyberturvallisuudesta (2022) – suosituksia kriittisten toimittajien tunnistamisesta ja niihin liittyvien riskien hallinnasta

12.5 ISO/IEC 27001:2022 / ISO/IEC 27002:2022