					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P06S					Asiakirjan nimi: **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**

Yhdenmukaistettu standardien ja sääntelyvaatimusten kanssa

Standardi/sääntely	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohdat 6.1, 6.1.3	
ISO/IEC 27002:2022	5.4, 5.25	
NIST SP 800-53 Rev. 5	RA-1–RA-7, PM-9	
EU:n NIS2-direktiivi	Artikla 21(2)(a–d)	
EU:n DORA-asetus	Artikla 5	
COBIT 2019	APO12, MEA01	

1. Tarkoitus

1.1 Tässä politiikassa määritellään, miten organisaatio tunnistaa, arvioi ja hallitsee tietoturvaan, toimintaan, teknologiaan ja kolmannen osapuolen palveluihin liittyviä riskejä.

1.2 Tällä politiikalla varmistetaan, että riskienhallinta on kiinteä osa suunnittelua, projektien toteutusta, toimittajavalintaa ja tietoturvapoikkeamien hallintaa ISO 27001:n, ISO 31000:n ja sääntelyvaatimusten mukaisesti.

1.3 Politiikka tukee tietoista päätöksentekoa, tietovarojen suojaamista ja keskeisten liiketoimintatoimintojen häiriönsietokykyä.

2. Soveltamisala

2.1 Tämä politiikka koskee:

2.1.1 kaikkia organisaation osastoja, järjestelmiä ja käyttäjiä

2.1.2 kaikkea tietoa, palveluja ja omaisuutta, joita hallitaan sisäisesti tai kolmansien osapuolten kautta

2.1.3 riskienhallintaan liittyviä toimintoja, mukaan lukien projektikatselmoinnit, järjestelmäpäivitykset, ulkoistaminen ja sääntelyvaatimusten noudattaminen

2.2 Se kattaa kaikki riskityypit, kuten:

2.2.1 kyberturvallisuusuhat ja järjestelmien haavoittuvuudet

2.2.2 toiminnalliset häiriöt ja palvelukatkokset

2.2.3 oikeudelliset, vaatimustenmukaisuuteen tai maineeseen kohdistuvat riskit

2.2.4 kolmannen osapuolen ja toimitusketjun riskit

2.3 Kaikkien työntekijöiden, urakoitsijoiden ja palveluntarjoajien on noudatettava tätä politiikkaa tunnistaessaan tai raportoidessaan riskejä.

3. Tavoitteet

3.1 Yksinkertaiset ja toistettavat riskienarviointimenettelyt on integroitava osaksi normaalia liiketoimintaa.

3.2 On tunnistettava ja priorisoitava riskit, jotka voivat vaikuttaa luottamuksellisuuteen, eheyteen, saatavuuteen tai oikeudellisten vaatimusten noudattamiseen.

3.3 Kaikille merkittäville riskeille on osoitettava omistaja ja määriteltävä riskienkäsittelytoimet.

3.4 Ajantasaista ja paikkansapitävää riskirekisteriä on ylläpidettävä auditointivalmiuden varmistamiseksi ja riskien seurannan tukemiseksi.

3.5 Johdon osallistuminen riskinsietotason ja merkittävien riskienkäsittelysuunnitelmien hyväksymiseen on varmistettava.

4. Roolit ja vastuut

4.1 Toimitusjohtaja

4.1.1 Määrittää organisaation riskinottohalukkuuden ja hyväksyy riskienhallinnan viitekehyksen.

4.1.2 Hyväksyy merkittäviä riskienkäsittelyä koskevat päätökset ja niihin tarvittavat resurssit.

4.1.3 Katselmoi merkittävimmät riskit neljännesvuosittain riskikoordinaattorin kanssa.

4.2 Riskikoordinaattori (tai ISMS:n omistaja)

4.2.1 Tukee riskien arviointeja ja ylläpitää riskirekisteriä.

4.2.2 Varmistaa, että riskipisteytys, riskinomistajuus ja riskienkäsittelytoimet dokumentoidaan.

4.2.3 Järjestää vähintään yhden muodollisen riskikatselmoinnin vuodessa.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Politiikan vuosittainen katselmointi

9.1.1 Toimitusjohtajan ja riskikoordinaattorin on katselmoitava tämä politiikka vähintään kerran vuodessa sen ajantasaisuuden ja kattavuuden varmistamiseksi.

9.2 Päivitystä edellyttävät herätteet

9.2.1 Katselmointi ja päivitys on tehtävä aiemmin, jos:

9.2.1.1 merkittävä poikkeama tai auditointihavainto paljastaa riskienhallinnan puutteita

9.2.1.2 käyttöön otetaan uusia liiketoimintayksiköitä, teknologioita tai kumppanuuksia

9.2.1.3 sääntelyyn tai sopimusvaatimuksiin tulee muutoksia

9.3 Versionhallinta

9.3.1 Kaikki tämän politiikan päivitykset on versionhallittava seuraavilla metatiedoilla:

9.3.1.1 versionumero ja voimaantulopäivä

9.3.1.2 yhteenveto muutoksista

9.3.1.3 hyväksyjä (toimitusjohtaja)

9.3.1.4 auditointitarkoituksia varten arkistoidut aiemmat versiot

9.4 Viestintä ja tietoisuus

9.4.1 Politiikan päivitetyt versiot ja merkittävät riskienkäsittelysuunnitelmat on viestittävä niille työntekijöille, joita ne koskevat. Vuosittaisen tietoisuuskoulutuksen on sisällettävä riskitietoisuuden perusperiaatteet.

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka toimii yhdessä useiden muiden politiikkojen kanssa kattavan tietoturvan hallintamallin varmistamiseksi:

10.1.1 P2S – Hallinnointirooleja ja -vastuita koskeva politiikka: määrittelee, kenelle riskinomistajuus ja päätöksenteko on osoitettu.

10.1.2 P5S – Muutoksenhallintapolitiikka: edellyttää riskien arviointia ennen teknisten tai prosessiin liittyvien muutosten toteuttamista.

10.1.3 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: käsittelee henkilötietojen käsittelyyn liittyviä sääntelyriskejä.

10.1.4 P30S – Tietoturvapoikkeamiin reagointia koskeva politiikka: varmistaa, että riskienkäsittely jatkuu tietoturvapoikkeamien aikana ja niiden jälkeen.

10.1.5 P33S – Liiketoiminnan jatkuvuuspolitiikka: tunnistaa jäännösriskit ja palautumistoimenpiteet kriittisille palveluille.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001:

11.1.1 Kohta 6.1 – edellyttää muodollisen riskienhallintaprosessin ja riskienkäsittelyn suunnittelun määrittämistä.

11.1.2 Kohta 6.1.3 – edellyttää, että organisaatio säilyttää dokumentoidut riskienkäsittelysuunnitelmat ja hyväksynnät.

11.2 ISO/IEC 27002:

11.2.1 Kontrollit 5.4, 5.25 – antavat toteutusohjeita riskinomistajuudesta, priorisoinnista ja elinkaaren hallinnasta.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 RA-1–RA-7 – määrittelevät riskien arvioinnin, vaste-strategiat, dokumentoinnin ja katselmointimekanismit.

11.4 PM-9 – edellyttää johdonmukaista johdon tason valvontaa organisaation riskeihin.

11.5 EU:n NIS2-direktiivi

11.5.1 Artikla 21(2)(a–d) – asettaa olennaisille ja tärkeille toimijoille pakolliset riskien arviointia, lieventämistä ja hallintaa koskevat kontrollit.

11.6 EU:n DORA-asetus

11.6.1 Artikla 5 – edellyttää säännellyiltä toimijoilta tieto- ja viestintäteknologiaan kohdistuvien riskienhallinnan viitekehysten määrittämistä ja hallintaa, mukaan lukien tunnistaminen, luokittelu ja reagointi.

11.7 COBIT 2019

11.7.1 APO12 – Hallitse riskejä: integroi riskit strategiseen ja operatiiviseen suunnitteluun.

11.7.2 MEA01 – Seuraa, arvioi ja tarkastele: varmistaa riskiprosessien ja toimenpiteiden tehokkuuden ja vaatimustenmukaisuuden.