					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P06					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**

Sovellettavat standardit ja säädökset

Standardi/säädös	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohdat 6.1, 8.32, 10	Riskien tunnistamisen ja hallinnan ydin, integrointi muutoksenhallintaan, jatkuva parantaminen
ISO/IEC 27005:2024	Koko riskienhallinnan elinkaarimenetelmä	Koko riskienhallintaprosessi standardin mukaisesti
ISO 31000:2018	Riskienhallinnan periaatteet ja viitekehys	Viitekehykseen omaksutut riskienhallinnan periaatteet
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Ohjeistus ja rakenne riskien arviointiin, tasokohtainen riskienhallinta
EU:n GDPR	Artiklat 24, 25, 32	Tietosuojariskejä koskevat prosessit ja hallintakeinot
EU:n NIS2-direktiivi	Artikla 21(2)(a–d)	Riskien ja turvallisuuden arviointia koskevat velvoitteet
EU:n DORA-asetus	Artiklat 5, 6	ICT-riskienhallinta ja operatiivinen häiriönsietokyky
COBIT 2019	APO12, MEA	Riskienhallinnan rakenne ja valvonta

1. Tarkoitus

1.1 Tämä politiikka määrittää yhtenäisen ja muodollisen viitekehyksen tietoturvariskien tunnistamiseen, analysointiin, arviointiin, käsittelyyn, seurantaan ja katselmointiin koko organisaatiossa.

1.2 Politiikka varmistaa riskiperusteisten periaatteiden johdonmukaisen soveltamisen tietovarallisuuden luottamuksellisuuden, eheyden ja saatavuuden suojaamiseksi ISO/IEC 27001:2022 -standardin kohdan 6.1 ja ISO 31000:2018 -standardin mukaisesti.

1.3 Politiikka integroi tietoturvariskienhallinnan organisaation päätöksentekoprosesseihin sisäisten strategisten tavoitteiden ja ulkoisten sääntelyvaatimusten täyttämiseksi.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia organisaatioyksiköitä, liiketoimintaprosesseja, järjestelmiä, henkilöstöä ja kolmansien osapuolten toimeksiantoja, jotka liittyvät tietovarallisuuden käsittelyyn, kehittämiseen, säilyttämiseen tai hallintaan.

2.2 Soveltamisala kattaa fyysiset, digitaaliset ja pilvipalveluissa isännöidyt omaisuuserät, mukaan lukien strukturoitu ja strukturoimaton tieto, sovellukset, infrastruktuurin, verkot ja palvelut.

2.3 Politiikka kattaa tietoturvariskit strategisella, operatiivisella, projekti- ja teknisellä tasolla, ja se on pakollinen kaikille työntekijöille, sopimuskumppaneille ja palveluntarjoajille, jotka osallistuvat ISMS:n toimintoihin.

2.4 Riskienhallintaa on sovellettava seuraavissa tilanteissa:

2.4.1 uuden projektin tai järjestelmän käyttöönotto

2.4.1.1 merkittävät muutokset (esim. arkkitehtuuri, omistajuus, prosessit)

2.4.1.2 toimittajan käyttöönotto ja kolmansien osapuolten sopimukset

2.4.1.3 tietoturvapoikkeamien hallinta ja poikkeamien jälkiarvioinnit

2.4.1.4 säännölliset organisaation riskikatselmoinnit tai auditoinnit

3. Tavoitteet

3.1 Tavoitteena on määrittää ja ottaa käyttöön toistettava, koko organisaation kattava riskienhallintaprosessi, joka perustuu ISO/IEC 27005- ja ISO 31000 -menetelmiin.

3.2 Tavoitteena on varmistaa, että riskit tunnistetaan, analysoidaan, arvioidaan ja käsitellään rakenteisilla ja jäljitettävillä menetelmillä, mukaan lukien riskinomistajuuden määrittäminen ja yhteydet hallintakeinoihin.

3.3 Tavoitteena on ylläpitää keskitettyä ja versionhallittua riskirekisteriä ja riskienkäsittelysuunnitelmaa, jotka kuvaavat ajantasaisen riskitilan, kontrollien kattavuuden ja lieventämistoimenpiteiden etenemisen.

3.4 Tavoitteena on yhdenmukaistaa riskipäätökset dokumentoidun riskinottohalukkuuden ja riskinsietotason kanssa sekä mahdollistaa tietoon perustuvat hallintopäätökset riskin hyväksymisestä, lieventämisestä, siirtämisestä tai välttämisestä.

3.5 Tavoitteena on seurata jatkuvasti riskitrendejä ja varmistaa riskienkäsittelytoimien tehokkuus sekä mahdollistaa ennakoivat muutokset uhkaympäristön kehittymisen tai liiketoiminnan muutosten perusteella.

4. Roolit ja vastuut

4.1 Ylin johto / hallitus

4.1.1 Hyväksyy riskienhallinnan viitekehyksen ja määrittää hyväksyttävän riskinottohalukkuuden ja riskinsietotason rajat.

4.1.2 Hyväksyy riskienkäsittelystrategiat jäännösriskeille, jotka ylittävät riskinsietotason.

4.1.3 Osoittaa resurssit ja valvonnan riskienhallintaohjelman tehokkaaseen toteuttamiseen.

4.2 ISMS-päällikkö / riskivastaava

4.2.1 Vastaa tästä politiikasta ja ylläpitää sen yhdenmukaisuutta ISO/IEC 27001- ja ISO/IEC 27005 -standardien kanssa.

4.2.2 Johtaa organisaation riskienarviointiprosessia ja ylläpitää riskirekisteriä sekä riskienkäsittelysuunnitelmaa.

4.2.3 Varmistaa keskeisten riskien säännöllisen katselmoinnin ja eskaloinnin ylimmälle johdolle tai ISMS-ohjausryhmälle.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Tämä politiikka ja siihen liittyvä viitekehys on katselmoitava vuosittain tai:

9.1.1 merkittävän riskitapahtuman tai tietoturvapoikkeaman jälkeen

9.1.2 merkittävän organisatorisen tai teknisen muutoksen jälkeen

9.1.3 auditointihavaintojen tai uusien sääntelyvaatimusten johdosta

9.2 ISMS-päällikkö, riskivastaava ja vaatimustenmukaisuustiimi vastaavat yhdessä seuraavista:

9.2.1 katselmointisyklin käynnistäminen

9.2.2 lähtötietojen kerääminen liiketoimintayksiköiltä

9.2.3 menettelyjen ja kynnysarvojen päivittäminen tarpeen mukaan

9.3 Kaikkien muutosten on oltava:

9.3.1 versionhallittuja ja lokiin kirjattuja

9.3.2 ylimmän johdon hyväksymiä

9.3.3 sidosryhmille viestittyjä

9.3.4 vähintään 5 vuoden ajan auditointitietovarastossa säilytettäviä

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka on riippuvuussuhteessa seuraaviin tietoturvapolitiikkoihin:

10.1.1 P1 – Tietoturvapolitiikka: Määrittää yleisen tietoturvan hallintamallin, jonka puitteissa tätä riskipolitiikkaa sovelletaan.

10.1.2 P2 – Hallinnointirooleja ja vastuita koskeva politiikka: Määrittää vastuutahot ja hallinnointitasot, joihin riskien eskalointimatriisissa viitataan.

10.1.3 P5 – Muutoksenhallintapolitiikka: Käynnistää riskien uudelleenarvioinnin infrastruktuuria ja organisaatiota koskevissa muutoksissa.

10.1.4 P13 – Tiedon luokittelu- ja merkintäpolitiikka: Tukee vaikutusten arviointia riskien tunnistamisen yhteydessä.

10.1.5 P33 – Auditointi- ja vaatimustenmukaisuuden seurantapolitiikka: Varmistaa politiikkojen noudattamisen, mukaan lukien riskirekisterin täydellisyyden ja näytön riskienkäsittelytoimista.

11. Viitestandardit ja viitekehykset

11.1 Tämä politiikka on nimenomaisesti yhdenmukaistettu seuraavien standardien ja viitekehysten kanssa sen varmistamiseksi, että se täyttää kansainväliset parhaat käytännöt ja sääntelyodotukset tietoturvariskienhallinnassa:

11.2 ISO/IEC 27001:

11.2.1 Kohta 6.1: Määrittää vaatimukset riskien ja mahdollisuuksien tunnistamiselle, mukaan lukien tietoturvariskien arviointien ja käsittelyjen koko elinkaari. Tämä politiikka toteuttaa kohdat 6.1.2 ja 6.1.3 rakenteisen viitekehyksen avulla, joka edellyttää dokumentoituja menettelyjä riskien tunnistamiseen, analysointiin, arviointiin, käsittelyyn ja jäännösriskin hyväksyntään.

11.2.2 Kohta 8.32: Riskiperusteisen ajattelun integrointi muutoksenhallintaprosesseihin varmistaa, että kaikki merkittävät organisatoriset muutokset käynnistävät muodolliset riskien uudelleenarvioinnit.

11.2.3 Kohta 10: Jatkuva parantaminen on sisällytetty politiikkaan säännöllisten politiikkakatselmusten, riskitrendien analysoinnin ja riskitietojen perusteella tehtävien SoA-päivitysten kautta.

11.3 ISO/IEC 27005:

11.3.1 Tarjoaa erikoistunutta ja yksityiskohtaista ohjeistusta tietoturvariskienhallintaan. Tämä politiikka toteuttaa ISO/IEC 27005 -standardin koko riskiprosessimallin: toimintaympäristön määrittäminen, riskien tunnistaminen, riskianalyysi, riskien arviointi, riskien käsittely, riskin hyväksyminen, riskiviestintä sekä riskien seuranta ja katselmointi.

11.4 ISO 31000:

11.4.1 Tämä politiikka integroi ISO 31000 -standardin periaatteet, kuten johdon sitoutumisen, päätöksentekoon integroitumisen ja jatkuvan parantamisen. Se varmistaa, että riskienhallinta on sisällytetty organisaation kulttuuriin ja toimintaan.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Vastaa NISTin riskien arviointia koskevaa ohjeistusta, mukaan lukien uhkien tunnistaminen, haavoittuvuusanalyysi, todennäköisyyden arviointi ja vaikutusten määrittäminen. Tämän politiikan rakenne vastaa NISTin määrittämiä riskien arvioinnin vaiheita ja soveltaa niitä sekä teknisiin että liiketoimintaprosesseihin.

11.6 NIST SP 800-39:

11.6.1 Tukee organisaatiotason riskienhallintaa korostamalla tasokohtaista riskienhallintaa organisaation, tehtävä-/liiketoimintaprosessin ja tietojärjestelmän tasoilla. Politiikka varmistaa, että

riskinomistajuus on määritelty selkeästi kaikilla tasoilla ja sisältää organisaatiotason käsittelystrategiat.

11.7 EU:n GDPR:

11.7.1 Artikla 24: Edellyttää asianmukaisten teknisten ja organisatoristen toimenpiteiden toteuttamista sen varmistamiseksi, että tietosuojariskejä hallitaan asianmukaisesti — tämä toteutetaan politiikan rakenteisen riskiprosessin kautta.

11.7.2 Artikla 25: "Sisäänrakennettu ja oletusarvoinen tietosuoja" vastaa riskien käsittelyn sisällyttämistä järjestelmien ja prosessien suunnitteluun.

11.7.3 Artikla 32: Edellyttää riskiperusteista lähestymistapaa turvallisuustoimenpiteisiin — tämä toteutetaan vaikutusperusteisen riskien arvioinnin ja hallintakeinojen valinnan kautta.

11.8 EU:n NIS2-direktiivi:

11.8.1 Artikla 21(2)(a–d): Edellyttää, että toimijat suorittavat riskien arviointeja, toteuttavat riskianalyysiä koskevat politiikat ja varmistavat oikeasuhtaiset turvallisuustoimenpiteet. Tämä politiikka täyttää nämä velvoitteet riskienhallinnan elinkaaren jatkuvalla soveltamisella ja dokumentoidulla hallinnoinnilla.

11.9 EU:n DORA-asetus:

11.9.1 Artikla 5: Edellyttää dokumentoitua ICT-riskienhallintakehystä — tämä politiikka kattaa sen kokonaisuudessaan, mukaan lukien SoA-kohdistukset ja keskeiset riski-indikaattorit.

11.9.2 Artikla 6: Edellyttää riskienhallinnan integrointia operatiivisen häiriönsietokyvyn strategioihin, mikä toteutetaan eskalointimatriisien ja kriittisten omaisuuserien seurannan avulla.

11.10 COBIT 2019:

11.10.1 APO12 – Riskien hallinta: Vastaa suoraan organisaation rakenteista riskienhallintatapaa, jossa määritetään roolit, seurataan käsittelytoimia ja varmistetaan hallitustason vastuun osoitettavuus.

11.10.2 MEA01 – Suorituskyvyn ja vaatimustenmukaisuuden seuranta, arviointi ja tarkastelu: Näkyy tämän politiikan painotuksessa riskitrendien analysointiin, keskeisten riski-indikaattorien seurantaan ja auditointipalautteen integrointiin jatkuvan parantamisen sykliin.