					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P30					Asiakirjan nimi: **Tietoturvapoikkeamien hallintapolitiikka**							
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	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohta 8.1, kohta 9	Jäsennetyt prosessit riskienhallintaa ja tietoturvapoikkeamiin reagointia varten
ISO/IEC 27002:2022	Kontrollit 5.25–5.27	Poikkeamien roolit, raportointi, reagointi ja jatkuva parantaminen
NIST SP 800-53 Rev.5	IR-1–IR-9	Kattava tietoturvapoikkeamiin reagoinnin elinkaari
EU:n GDPR	Artikla 33(1), 33(3)(a)–(d), 34(1), 34(2)(a)–(c)	Tietoturvaloukkausten ilmoitusmääräajat, raportointi ja viestintä rekisteröidyille
EU:n NIS2-direktiivi	Artikla 23(1)–(4)	Ilmoittaminen kansalliselle toimivaltaiselle viranomaiselle ja jäsennelty raportointi
EU:n DORA-asetus	Artikla 17(1)–(3)	Merkittävien ICT-poikkeamien ilmoittaminen finanssialan toimijoilla
COBIT 2019	DSS02, DSS04, MEA	Poikkeamien hallinnan, jatkuvuuden ja arvioinnin määrittäminen, seuranta ja arviointi

1. Tarkoitus

1.1 Tämä politiikka määrittää muodollisen toimintamallin organisaatioon vaikuttavien tietoturvapoikkeamien tunnistamiseen, ilmoittamiseen, analysointiin, rajaamiseen, käsittelyyn, palautumiseen ja jälkiarviointiin.

1.2 Tavoitteena on varmistaa oikea-aikainen, koordinoitu ja tehokas reagointi siten, että toiminnalliset häiriöt, taloudelliset menetykset, mainehaitta ja sääntelyvaatimusten noudattamatta jättäminen minimoidaan.

1.3 Politiikka tukee myös organisaation kyberhäiriönsietokyvyn jatkuvaa parantamista hyödyntämällä oppeja sekä integroimalla jälkiarviointien havainnot hallintamalliin, työkaluihin ja koulutusohjelmiin.

2. Soveltamisala

2.1 Tämä politiikka koskee:

2.1.1 koko henkilöstöä, mukaan lukien työntekijät, urakoitsijat, konsultit ja kolmannen osapuolen palveluntarjoajat

2.1.2 kaikkia tietojärjestelmiä, sovelluksia, infrastruktuuria, verkkoja ja tietoja riippumatta siitä, sijaitsevatko ne omissa tiloissa, pilvipalveluissa tai hybridiympäristöissä

2.1.3 kaikkia tietoturvapoikkeamien tyyppejä, mukaan lukien muun muassa:

2.1.3.1 luvaton pääsy tai käyttöoikeuksien korottaminen

2.1.3.2 haittaohjelma- ja kiristysohjelmahyökkäykset

2.1.3.3 palvelunestohyökkäykset (DoS/DDoS)

2.1.3.4 tietojen menetys, vuotaminen tai luvaton siirto

2.1.3.5 sisäinen väärinkäyttö tai politiikkarikkomukset

2.1.3.6 fyysisen turvallisuuden loukkaukset, jotka vaikuttavat digitaalisiin omaisuuseriin

2.2 Politiikka kattaa havaitsemisen, poikkeamien luokittelun ja priorisoinnin, tutkinnan, eskaloinnin, rajaamisen, todistusaineiston käsittelyn, ilmoitukset, palautumisen ja juurisyyanalyysin.

3. Tavoitteet

3.1 Luoda toistettava ja skaalautuva tietoturvapoikkeamiin reagointikyvykkyys, joka mahdollistaa tietoturvapoikkeamien nopean havaitsemisen, luokittelun ja lieventämisen.

3.2 Minimoida tietoturvatapahtumien liiketoimintavaikutukset jäsenneltyjen rajaamis-, poistamis- ja järjestelmien palauttamismenettelyjen avulla.

3.3 Varmistaa, että poikkeamien ilmoittaminen ja käsittely ovat yhdenmukaisia lakisääteisten, sääntelyyn perustuvien ja sopimusvelvoitteiden kanssa, erityisesti tietoturvaloukkausten ilmoitusmääräaikojen ja todistusaineiston käsittelyn osalta.

3.4 Tukea läpinäkyvyyttä ja vastuun osoitettavuutta asianmukaisen lokituksen, dokumentoinnin ja mittareiden seurannan avulla kaikissa tietoturvapoikkeamissa.

3.5 Edistää jatkuvaa parantamista jälkiarviointien, korjaavien toimenpiteiden ja sidosryhmien koulutuksen avulla.

4. Roolit ja vastuut

4.1 Tietoturvajohtaja (CISO)

4.1.1 Omistaa tietoturvapoikkeamiin reagoinnin viitekehyksen, varmistaa politiikan toimeenpanon ja valvoo koko organisaation laajuista poikkeamien koordinointia.

4.1.2 Toimii ensisijaisena yhteyshenkilönä viranomaisten, ylimmän johdon ja ulkoisen oikeudellisen neuvonannon suuntaan merkittävien poikkeamien aikana.

4.2 Tietoturvapoikkeamiin reagoinnin koordinaattori

4.2.1 Koordinoi poikkitoiminnallisia reagointitiimejä, hallinnoi työnkulkuja sekä seuraa rajaamisen ja palautumisen tilaa.

4.2.2 Käynnistää ja johtaa poikkeamien jälkiarvioinnit (PIR) sekä varmistaa, että korjaavat toimenpiteet kirjataan ja toteutetaan.

[... 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 ja päivitettävä tarvittaessa siten, että siihen sisällytetään:

9.1.1 muutokset uhkaympäristössä, poikkeamatyypeissä tai hyökkäysvektoreissa

9.1.2 merkittävistä poikkeamista, läheltä piti -tilanteista tai sääntelyhavainnoista saadut opit

9.1.3 sovellettavaan lainsäädäntöön ja sääntelyyn tehdyt muutokset (esim. EU:n GDPR, EU:n DORA-asetus, EU:n NIS2-direktiivi)

9.1.4 palaute tietoturvapoikkeamiin reagoinnin harjoituksista ja jälkiarvioinneista

9.2 Tietoturvajohtaja (CISO) vastaa katselmointiprosessin käynnistämisestä ja koordinoinnista kuullen seuraavia tahoja:

9.2.1.1 oikeudellinen neuvonta ja tietosuojavastaava

9.2.1.2 SOC ja IT-operaatiot

9.2.1.3 liiketoiminnan jatkuvuus- ja riskienhallintatiimit

9.2.1.4 ylin johto

9.3 Politiikkamuutokset on:

9.3.1 dokumentoitava versionhallittuun tietovarastoon

9.3.2 viestittävä kaikille vaikutuksen kohteena oleville tiimeille ja sisällytettävä tietoisuuskoulutukseen

9.3.3 validoitava pöytäharjoituksilla tai käytännön tietoturvapoikkeamiin reagoinnin harjoituksilla kolmen kuukauden kuluessa hyväksynnästä

9.4 Esiin nousevien uhkien, auditointihavaintojen tai uusien lakisääteisten velvoitteiden käynnistämät kiireelliset päivitykset on toteutettava välittömästi ja kirjattava politiikan muutoshistoriaan.

10. Liittyvät politiikat ja yhteydet

10.1 Tätä politiikkaa tukevat seuraavat organisaation politiikat, joihin se myös tukeutuu:

10.1.1 P1 – Tietoturvapolitiikka: määrittää yleisen vaatimuksen riskiperusteiselle ja poikkeamavalmiille toiminnalle.

10.1.2 P5 – Muutoksenhallintapolitiikka: varmistaa, että infrastruktuuriin tai palveluihin kohdistuvat rajaamis- ja palautumistoimet noudattavat muodollisia menettelyjä.

10.1.3 P13 – Tiedon luokittelu- ja merkintäpolitiikka: tukee poikkeamien vakavuusluokittelua tiedon arkaluonteisuuden perusteella.

10.1.4 P15 – Varmuuskopiointi- ja palautuspolitiikka: mahdollistaa palautumisen kiristysohjelmista tai tuhoavista hyökkäyksistä eheyden varmistamisen yhteydessä.

10.1.5 P18 – Kryptografisten hallintakeinojen politiikka: määrittää salauskeinot, jotka pienentävät poikkeamien vaikutuksia ja tietojen altistumisen riskejä.

10.1.6 P22 – Lokitus- ja valvontapolitiikka: tarjoaa tehokkaan havaitsemisen ja forensiikan edellyttämän perustan tapahtumien näkyvyydelle, hälytyksille ja lokien säilytykselle.

10.1.7 P29 – Testitietojen ja testiympäristöjen politiikka: varmistaa, että myös ei-tuotantoympäristöihin vaikuttavat poikkeamat käsitellään jäsennellysti ja turvallisesti.

10.1.8 P33 – Auditointi- ja vaatimustenmukaisuuden seurantapolitiikka: validoi poikkeamavalmiuden ja reagoinnin tehokkuuden jäsenneltyjen auditointien ja vaatimustenmukaisuuden arviointien avulla.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001: kohta 8.1 – Operational Planning and Control: jäsennetyt prosessit riskien hallintaan ja tietoturvapoikkeamiin reagoinnin suunnitteluun.

11.2 ISO/IEC 27002:2022 – kontrollit 5.25–5.27: vastuut poikkeamien hallinnasta, ilmoittamisesta, reagoinnista, viestinnästä ja parantamisesta.

11.3 NIST SP 800-53 Rev.5: IR-1–IR-9, AU-6, PL-2: kattavat vaatimukset tietoturvapoikkeamiin reagoinnin elinkaarelle, auditoinnille ja tietoturvasuunnittelulle.

11.4 EU:n GDPR: artiklat 33/34: ilmoitusvelvollisuudet valvontaviranomaisille sekä rekisteröityjen informointivaatimukset (määritellyin poikkeuksin).

11.5 EU:n NIS2-direktiivi (2022/2555): artikla 23: pakollinen kansallinen ilmoittaminen sekä väli- ja loppuraportointivelvoitteet.

11.6 EU:n DORA-asetus (2022/2554): artikla 17: finanssilaitosten viranomaisille kohdistuvat ICT-poikkeamien ilmoitusvaatimukset.

11.7 COBIT 2019: DSS02, DSS04, MEA01: palvelupoikkeamien ja jatkuvuuden hallinta sekä suorituskyvyn ja vaatimustenmukaisuuden seuranta.