					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P32					Asiakirjan nimi: **Liiketoiminnan jatkuvuus- ja katastrofipalautuspolitiikka**							
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	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	Kohta 8	
ISO/IEC 27002:2022	Kontrollit 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-1–CP-11	
NIST SP 800-34 Rev.1	Contingency Planning	Viitekehys
ISO 22301:2019		Liiketoiminnan jatkuvuuden hallintajärjestelmän vaatimukset
EU:n yleinen tietosuoja-asetus (GDPR)	Artikla 32	
EU:n NIS2-direktiivi	Artikla 21(2)(f)	
DORA-asetus	Artikla 10	
COBIT 2019	DSS04	

1. Tarkoitus

1.1. Tämä politiikka määrittää pakolliset kontrollit ja vastuut organisaation kyvykkyyden varmistamiseksi ylläpitää tai palauttaa kriittiset liiketoimintatoiminnot ja niitä tukevat ICT-palvelut häiriötilanteen aikana ja sen jälkeen.

1.2. Politiikan tavoitteena on suojata henkeä, toiminnan vakautta, lakisääteisten velvoitteiden täyttämistä, asiakassitoumuksia ja organisaation mainetta vahvistamalla häiriönsietokykyä ennakoivan suunnittelun ja validoitujen palautuskyvykkyyksien avulla.

1.3. Tämä politiikka muodostaa perustan organisaation liiketoiminnan jatkuvuuden hallinnan (BCM) ja katastrofipalautuksen (DR) viitekehykselle sekä varmistaa sovellettavien sääntely-, sopimus- ja toimialavaatimusten noudattamisen.

2. Soveltamisala

2.1. Tätä politiikkaa sovelletaan kaikkiin organisaation yksiköihin, tietojärjestelmiin, liiketoimintaprosesseihin, henkilöstöön ja kolmansien osapuolten palveluihin, jotka on luokiteltu kriittisiksi tai olennaisiksi liiketoimintavaikutusten arvioinnin (BIA) perusteella.

2.2. Politiikka kattaa:

2.2.1. luonnon aiheuttamat ja ihmisen aiheuttamat häiriöt, mukaan lukien kyberhyökkäykset, infrastruktuuriviat, konesalikatkokset, pandemiat ja toimittajien palvelukatkokset

2.2.2. liiketoiminnan jatkuvuussuunnitelmien (BCP/DRP) suunnittelun, testauksen ja jatkuvan parantamisen

2.2.3. roolit ja vastuut hätätilanteisiin reagoinnissa, palautumisen koordinoinnissa ja poikkeamien eskaloinnissa

2.3. Kaikki henkilöt, joilla on jatkuvuuteen tai palautumiseen liittyviä vastuita, mukaan lukien IT, liiketoimintavastaavat, kriisijohto ja toimittajat, kuuluvat tämän politiikan soveltamisalaan.

3. Tavoitteet

3.1. Varmistaa liiketoiminnan ja palvelujen jatkuvuus ennalta määritellyillä ja testatuilla menettelyillä sekä minimoida toiminnalliset, mainehaitat ja oikeudelliset vaikutukset.

3.2. Palauttaa ICT-palvelut määritettyjen toipumisaikatavoitteiden (RTO) ja palautuspistetavoitteiden (RPO) puitteissa liiketoiminnan riskinsietokyvyn mukaisesti.

3.3. Määrittää omistajuus liiketoiminnan jatkuvuuden ja katastrofipalautuksen suunnittelulle, toteutukselle ja hallinnalle koko organisaatiossa.

3.4. Varmistaa, että jatkuvuuskyvykkyyksiä testataan, ylläpidetään ja parannetaan säännöllisesti realististen skenaarioiden ja auditointihavaintojen perusteella.

3.5. Täyttää ISO-standardien, NISTin, EU:n yleisen tietosuoja-asetuksen, DORA-asetuksen ja EU:n NIS2-direktiivin vaatimustenmukaisuusvelvoitteet sekä tukea asianmukaista huolellisuutta toiminnan häiriönsietokyvyn ja saatavuuden varmistamisessa.

4. Roolit ja vastuut

4.1. Ylin johto

4.1.1. Hyväksyy liiketoiminnan jatkuvuus- ja katastrofipalautuspolitiikan ja varmistaa sen strategisen yhdenmukaisuuden.

4.1.2. Osoittaa budjetin ja resurssit liiketoiminnan jatkuvuuden, hätätilanteisiin reagoinnin ja palautusharjoitusten tukemiseksi.

4.2. Liiketoiminnan jatkuvuuspäällikkö (BCM-vastuuhenkilö)

4.2.1. Vastaa organisaation laajuisten liiketoiminnan jatkuvuussuunnitelmien laatimisesta ja ylläpidosta sekä jatkuvuustestauksen koordinoinnista.

4.2.2. Ylläpitää BIA-aikataulua, tukee koulutuksen toteutusta ja varmistaa, että dokumentaatio täyttää vaatimustenmukaisuusvaatimukset.

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

9. Katselmointi- ja päivitysvaatimukset

9.1. Liiketoiminnan jatkuvuuspäällikön ja tietoturvajohtajan (CISO) on katselmoitava tämä politiikka vuosittain sen varmistamiseksi, että se on yhdenmukainen seuraavien kanssa:

9.1.1. muutokset liiketoiminnassa, kriittisissä järjestelmissä tai infrastruktuurissa

9.1.2. poikkeamista, auditoinneista, pöytäharjoituksista tai DR-testeistä saadut opit

9.1.3. päivitetyt sääntelyyn tai sopimuksiin liittyvät velvoitteet (esim. DORA-asetus, EU:n yleinen tietosuoja-asetus, asiakkaiden RTO-/RPO-vaatimukset)

9.1.4. muutokset organisaation riskinottohalukkuudessa tai jatkuvuusstrategiassa

9.2. Katselmointien on sisällettävä:

9.2.1. suunnitelmien asianmukaisuuden ja yhteystietojen validointi

9.2.2. RTO-, RPO- ja palautusluokituksen uudelleenarviointi

9.2.3. varmuuskopiointi- ja DR-palvelukapasiteetin arviointi

9.2.4. palaute sidosryhmiltä, jotka ovat toteuttaneet viimeaikaisia palautussuunnitelmia tai testejä

9.3. Kaikkien politiikkamuutosten on oltava:

9.3.1. versionhallittuja, dokumentoidulla perustelulla ja sidosryhmien hyväksynnällä varustettuja

9.3.2. viestittyjä keskeiselle henkilöstölle ja tiimeille, joiden vastuut ovat muuttuneet

9.3.3. huomioituja päivitetyissä koulutuksissa, tietoisuusmateriaaleissa ja toimintamenettelyissä

9.4. Kiireelliset väliaikaiset päivitykset on julkaistava, jos merkittävä organisaatiomuutos, oikeudellinen velvoite tai kriittinen havainto tekee nykyisistä suunnitelmista tai politiikasta toteuttamiskelvottoman.

10. Liittyvät politiikat ja yhteydet

10.1. Tätä politiikkaa sovelletaan yhdessä seuraavien keskeisten asiakirjojen kanssa:

10.1.1. P1 – Tietoturvapolitiikka: asettaa vaatimuksen riskiperusteiselle ja häiriönsietokykyä tukevalle toiminnalle kaikissa olosuhteissa.

10.1.2. P5 – Muutoksenhallintapolitiikka: varmistaa, että kaikki palautumiseen liittyvät konfiguraatio- tai infrastruktuurimuutokset noudattavat dokumentoituja ja hyväksyttyjä työnkulkuja.

10.1.3. P14 – Tietojen säilytys- ja hävityspolitiikka: ohjaa jatkuvuustoiminnassa käytettävien varmuuskopiointivälineiden ja palautettujen tietojen elinkaarta.

10.1.4. P15 – Varmuuskopiointi- ja palautuspolitiikka: asettaa kontrollit varmuuskopiointitiheydelle, tietoturvalle ja palautusten varmennukselle.

10.1.5. P18 – Kryptografisten hallintakeinojen politiikka: varmistaa, että palautusprosessit noudattavat salausta ja luottamuksellisuutta koskevia vaatimuksia.

10.1.6. P22 – Lokitus- ja valvontapolitiikka: tukee jatkuvuuteen vaikuttavien tapahtumien havaitsemista ja eskalointia.

10.1.7. P30 – Tietoturvapoikkeamien hallintapolitiikka: määrittää jatkuvuuteen liittyvien herätteiden mukaiset rajaamisen, eskaloinnin ja juurisyyn selvittämisen prosessit.

10.1.8. P33 – Auditointi- ja vaatimustenmukaisuuden seurantapolitiikka: varmistaa jatkuvuus- ja palautuskäytäntöjen eheyden ja tehokkuuden järjestelmissä ja prosesseissa.

11. Viitestandardit ja viitekehykset

11.1. Tämä politiikka on yhdenmukainen kansainvälisesti hyväksyttyjen liiketoiminnan jatkuvuuden ja katastrofipalautuksen standardien kanssa ja tukee todennettavuutta, häiriönsietokykyä ja oikeudellista vaatimustenmukaisuutta.

11.2. ISO/IEC 27002

11.2.1. Liite A, kontrolli 5.29 – Tietoturvallisuus häiriötilanteen aikana: edellyttää tietoturvakontrollien jatkuvuutta haitallisissa olosuhteissa.

11.2.2. Liite A, kontrolli 5.30 – ICT-valmius liiketoiminnan jatkuvuutta varten: edellyttää ICT-palautuskyvykkyyksien valmistelua, testausta ja validointia.

11.3. ISO 22301:2019 – Liiketoiminnan jatkuvuuden hallintajärjestelmät

11.3.1. Tarjoaa viitekehyksen BCM-käytäntöjen perustamiselle, toteutukselle ja ylläpidolle organisaation tavoitteiden ja riskikynnyksen mukaisesti.

11.4. NIST SP 800-34 Rev.1 – Varautumissuunnittelun ohjeistus

11.4.1. Kuvaa parhaat käytännöt IT-järjestelmien varautumissuunnitelmille, mukaan lukien jatkuvuusstrategian laatiminen, vaikutusanalyysi ja suunnitelmien testaus.

11.5. EU:n yleinen tietosuoja-asetus (2016/679)

11.5.1. Artikla 32 – käsittelyn turvallisuus: edellyttää käsittelyjärjestelmien häiriönsietokykyä sekä saatavuuden ja henkilötietoihin pääsyn oikea-aikaista palauttamista poikkeaman jälkeen.

11.6. EU:n NIS2-direktiivi (2022/2555)

11.6.1. Artikla 21(2)(f): edellyttää liiketoiminnan jatkuvuuteen ja kriisinhallintaan liittyviä toimenpiteitä verkko- ja tietojärjestelmien turvallisuuden tukemiseksi.

11.7. DORA-asetus (2022/2554)

11.7.1. Artikla 10 – ICT-liiketoiminnan jatkuvuus: edellyttää, että finanssialan toimijat laativat ja testaavat ICT-jatkuvuussuunnitelmia, mukaan lukien riskiperusteiset RTO-/RPO-tavoitteet ja failover-valmiudet.

11.8. COBIT 2019

11.8.1. DSS04 – Jatkuvuuden hallinta: kattaa kaikki jatkuvuussuunnittelun osa-alueet, mukaan lukien uhkien tunnistaminen, vaikutusanalyysi, palautusstrategia ja säännöllinen testaus.