					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P32S					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	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohdat 6.1, 6.3, 8	
ISO/IEC 27002:2022	Kontrollit 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
EU:n GDPR	Artiklat 32, 33	
EU:n NIS2-direktiivi	Artikla 21(2)(f)	
EU:n DORA-asetus	Artikla 10	
COBIT 2019	DSS04	

1. Tarkoitus

1.1 Tämän politiikan tarkoituksena on varmistaa, että organisaatio kykenee ylläpitämään toimintaansa ja palauttamaan olennaiset IT-palvelut häiriötilanteiden aikana ja niiden jälkeen, kuten sähkökatkojen, kyberhyökkäysten, kiristyshaittaohjelmatartuntojen tai järjestelmähäiriöiden yhteydessä.

1.2 Tämä politiikka määrittää selkeän viitekehyksen liiketoiminnan jatkuvuuden ja katastrofipalautuksen (BC/DR) suunnittelulle pk-yritysympäristöissä, joissa ei ole erillisiä IT-tiimejä.

1.3 Tämä politiikka tukee organisaatiota sovellettavien standardi- ja sääntelyvaatimusten täyttämisessä, mukaan lukien ISO/IEC 27001:2022, EU:n GDPR, EU:n NIS2-direktiivi, EU:n DORA-asetus ja COBIT 2019, sekä vahvistaa operatiivista häiriönsietokykyä ja asiakkaiden luottamusta.

2. Soveltamisala

2.1 Tämä politiikka koskee:

2.1.1 kaikkia liiketoimintakriittisiä järjestelmiä ja palveluita (esim. sähköposti, pilvitallennuspalvelut, laskutusalustat, asiakastiedot)

2.1.2 kaikkia työntekijöitä ja ulkoisia IT-palveluntarjoajia, jotka vastaavat BC/DR-valmiudesta ja sen toteutuksesta

2.1.3 kaikkia häiriötyyppejä, mukaan lukien kyberpoikkeamat, laitteistoviat, sähkökatkot, tulvat ja toimitiloihin pääsyn estyminen

2.2 Tämä politiikka kattaa:

2.2.1 varmuuskopioinnin hallinnan

2.2.2 liiketoiminnan jatkuvuussuunnittelun (BCP)

2.2.3 katastrofipalautustoiminnot

2.2.4 henkilöstön koulutuksen ja testauksen

2.2.5 lakisääteiset ja sääntelyyn liittyvät reagointimenettelyt

3. Tavoitteet

3.1 Suojata organisaation kykyä tuottaa keskeisiä palveluja suunnittelemattomista häiriöistä huolimatta.

3.2 Varmistaa järjestelmien ja tietojen oikea-aikainen palauttaminen ennalta määritettyjen toipumisaikatavoitteiden (RTO) mukaisesti.

3.3 Varmistaa, että koko henkilöstö pystyy noudattamaan jatkuvuusmenettelyjä kriisitilanteissa mahdollisimman vähäisin epäselvyyksin.

3.4 Varmistaa tietosuojaa ja operatiivista häiriönsietokykyä koskevien lakien noudattaminen, mukaan lukien EU:n GDPR:n artikla 32 ja EU:n NIS2-direktiivin artikla 21.

3.5 Määrittää käytännöllinen ja testattavissa oleva jatkuvuus- ja palautusstrategia, joka soveltuu pk-yrityksille.

4. Roolit ja vastuut

4.1 Toimitusjohtaja

4.1.1 omistaa BC/DR-prosessin ja tämän politiikan

4.1.2 hyväksyy liiketoiminnan jatkuvuussuunnitelman (BCP)

4.1.3 koordinoi poikkeamien hallintaa ja sisäistä viestintää häiriötilanteiden aikana

4.1.4 tekee tarvittavat viranomaisilmoitukset (esim. EU:n GDPR:n mukaiset tietoturvaloukkausilmoitukset)

4.2 IT-palveluntarjoaja / järjestelmänvalvoja

4.2.1 ylläpitää ja testaa varmuuskopioita

4.2.2 toteuttaa katastrofipalautusmenettelyt, kun ne aktivoidaan

4.2.3 dokumentoi kaikki palautustoimet ja järjestelmien palautustapahtumat

4.2.4 ilmoittaa kriittisistä IT-poikkeamista toimitusjohtajalle välittömästi

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Politiikan ja suunnitelman vuosittainen katselmointi

9.1.1 Toimitusjohtajan tulee varmistaa, että tämä politiikka ja siihen liittyvä liiketoiminnan jatkuvuussuunnitelma (BCP) katselmoidaan muodollisesti vähintään kerran vuodessa.

9.1.2 Katselmoinnin tulee sisältää:

9.1.2.1 uusien tai nousevien riskien arviointi

9.1.2.2 RTO-/RPO-tavoitteiden uudelleenvahvistus

9.1.2.3 toimittaja- ja yhteystietojen varmentaminen

9.1.2.4 yhdenmukaisuuden varmistaminen IT-järjestelmissä, lakisääteisissä velvoitteissa tai toiminnassa tapahtuneiden muutosten kanssa

9.2 Laukaisuperusteiset päivitykset

9.2.1 Tämä politiikka tulee päivittää myös seuraavien perusteella:

9.2.1.1 merkittävät poikkeamat tai häiriöt, erityisesti jos tavoitteita ei saavutettu

9.2.1.2 uudet lakisääteiset tai sääntelyyn liittyvät velvoitteet (esim. DORA-asetuksen muutokset)

9.2.1.3 muutokset kriittisissä järjestelmissä, pilvialustoissa tai henkilöstössä

9.2.1.4 vuosittaisten BCP-/DR-testien havainnot

9.3 Muutoksenhallintaprosessi

9.3.1 Toimitusjohtajan tulee hyväksyä kaikki muutokset.

9.3.2 Versiohistorialokia tulee ylläpitää siten, että siitä käyvät ilmi päivämäärä, muutoksen kuvaus ja hyväksyjä.

9.3.3 Päivitetty politiikka tulee jakaa uudelleen kaikille asiaankuuluville henkilöille, mukaan lukien IT-palveluntarjoaja ja osastopäälliköt.

9.4 Opittujen asioiden dokumentointi

9.4.1 Testien tai todellisten häiriöiden jälkeen dokumentoidut opit tulee huomioida tulevissa päivityksissä.

9.4.2 Näihin katselmointeihin tulee sisällyttää myös toimittajien suorituskyvyn arvioinnit ja reagoinnin riittävyyden tarkastukset.

10. Liittyvät politiikat ja riippuvuudet

10.1 Tämä politiikka on tiiviisti integroitu seuraaviin SME-politiikkoihin:

10.1.1 P1S – Tietoturvapolitiikka: määrittää korkean tason tietoturvatavoitteet, joita jatkuvuus- ja palautumiskäytäntöjen tulee tukea.

10.1.2 P4S – Pääsynhallintapolitiikka: mahdollistaa käyttöoikeuksien hätäperuutuksen tai palauttamisen liiketoimintahäiriötilanteissa.

10.1.3 P6S – Riskienhallintapolitiikka: muodostaa perustan jatkuvuuteen liittyvien riskien tunnistamiselle, arvioinnille ja priorisoinnille.

10.1.4 P8S – Tietoturvatietoisuus- ja koulutuspolitiikka: varmistaa, että työntekijät ovat valmiita toimimaan häiriötilanteissa ja ymmärtävät liiketoiminnan jatkuvuussuunnitelman (BCP).

10.1.5 P15S – Varmuuskopiointi- ja palautuspolitiikka: määrittää yksityiskohtaiset tekniset menettelyt tietojen saatavuuden ja palautettavuuden turvaamiseksi.

10.1.6 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: varmistaa, että jatkuvuussuunnittelu suojaa henkilötietoja ja noudattaa EU:n GDPR:ää poikkeamien aikana ja niiden jälkeen.

10.1.7 P22S – Lokitus- ja valvontapolitiikka: tukee sellaisten tapahtumien havaitsemista, jotka voivat käynnistää BC/DR-prosessit, ja tuottaa forensiset audit trail -tiedot häiriöiden jälkeen.

10.1.8 P30S – Tietoturvapoikkeamien hallintapolitiikka: käynnistää suoraan palautusprosessin kyber- tai operatiivisissa poikkeamissa.

10.1.9 P31S – Todisteiden keruun ja forensiikan politiikka: varmistaa, että digitaalinen todistusaineisto kerätään jatkuvuustilanteissa vaatimustenmukaisuuden, vakuutusten tai tutkinnan tarpeisiin.

10.2 Nämä politiikat muodostavat yhtenäisen, auditointivalmiutta tukevan viitekehyksen häiriönsietokyvylle, vastuun osoitettavuudelle ja kontrollien jatkuvuudelle kaikissa pk-yrityksen toiminnoissa.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001:

11.1.1 Kohta 6.1 – edellyttää riskiperusteista suunnittelua ja käsittelyä, mukaan lukien liiketoiminnan jatkuvuus ja palautuminen.

11.1.2 Kohta 6.3 – korostaa jatkuvaa parantamista häiriöiden jälkeen.

11.1.3 Kohta 8.1 – edellyttää operatiivisia kontrolleja, joihin sisältyvät dokumentoidut jatkuvuustoimenpiteet.

11.2 ISO/IEC 27002:

11.2.1 Kontrolli 5.29 – edellyttää liiketoiminnan jatkuvuusjärjestelyjen määrittämistä ja ylläpitoa.

11.2.2 Kontrolli 5.30 – edellyttää näiden järjestelyjen testausta ja katselmointia.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-2 – määrittää varautumissuunnittelun vaatimukset.

11.3.2 CP-4 – edellyttää organisaation henkilöstölle varautumiskoulutusta.

11.3.3 CP-6 – kattaa vaihtoehtoista säilytyspaikkaa koskevat vaatimukset.

11.3.4 CP-7 – ohjaa vaihtoehtoista käsittelypaikkaa koskevia odotuksia.

11.4 EU:n GDPR:

11.4.1 Artikla 32 – edellyttää toimenpiteitä, joilla varmistetaan käsittelyjärjestelmien ja palvelujen jatkuva saatavuus ja häiriönsietokyky.

11.4.2 Artikla 33 – käynnistää ilmoitusvelvoitteet tilanteissa, joissa jatkuvuuden epäonnistuminen johtaa henkilötietojen vaarantumiseen.

11.5 EU:n NIS2-direktiivi (2022/2555):

11.5.1 Artikla 21(2)(f) – edellyttää jatkuvuussuunnittelua ja kriisinhallintakyvykkyyttä osana kyberriskivalmiutta.

11.6 EU:n DORA-asetus (2022/2554):

11.6.1 Artikla 10 – edellyttää digitaalisen operatiivisen häiriönsietokyvyn testausta ja palautumiskyvykkyyksien toteutusta erityisesti finanssialan pk-yrityksissä.

11.7 COBIT 2019:

11.7.1 DSS04 – Manage Continuity: tarjoaa organisaatiotason hallintaohjeistuksen operatiivisen häiriönsietokyvyn ylläpitämiseen ja validointiin, mukaan lukien omistajuus, testaus, toimittajaintegraatio ja poikkeaman jälkeiset katselmoinnit.