					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P15					Asiakirjan nimi: **Varmuuskopiointi- ja palautuspolitiikka**							
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	Lausekkeet 6.1.3, 8.1	Riskienkäsittely, suunnittelu ja varmuuskopiointia koskevat operatiiviset kontrollit
ISO/IEC 27002:2022	Kontrollit 8.13, 5.28, 5.29	Varmuuskopioiden hallinta, turvallinen hävittäminen ja häiriönsietokyky
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	Järjestelmien varmuuskopiointia, palautumista ja tallennusvälineiden turvallista puhdistamista koskevat vaatimukset
EU:n GDPR	Artikla 32, johdanto-osan kappale 49	Henkilötietojen palautettavuus ja saatavuus sekä liiketoiminnan jatkuvuus
EU:n NIS2-direktiivi	Artikla 21(2)(c-e)	Häiriönsietokykyä tukevat varmuuskopiointi- ja jatkuvuuskontrollit
EU:n DORA-asetus	Artiklat 10, 11	Finanssisektorin varmuuskopiointia, palautumista ja testausta koskevat vaatimukset
COBIT 2019	DSS01, DSS04, MEA03	Varmuuskopiointitoiminnot, jatkuvuus ja vaatimustenmukaisuuden seuranta

1. Tarkoitus

1.1 Tämän politiikan tarkoituksena on määrittää pakolliset vaatimukset tietojen, järjestelmien ja sovellusten varmuuskopioinnille ja palauttamiselle toiminnallisen häiriönsietokyvyn, tiedon eheyden ja liiketoiminnan jatkuvuuden tukemiseksi.

1.2 Tämä politiikka määrittää standardoidun viitekehyksen seuraaviin tarkoituksiin:

1.2.1 Organisaation tietojen suojaaminen menetykseltä, jonka syynä on poistaminen, korruptoituminen, vikaantuminen tai kyberhyökkäys

1.2.2 Palautumista koskevien odotusten määrittäminen selkeillä RTO- (Recovery Time Objective) ja RPO-parametreilla (Recovery Point Objective)

1.2.3 Varmuuskopiointitoimintojen integrointi laajempaan tietoturvallisuuden hallintajärjestelmään (ISMS) sekä liiketoiminnan jatkuvuus- ja palautumissuunnitelmiin (BCP/DRP)

1.2.4 Sovellettavien lakien ja toimialakohtaisten sääntelyvaatimusten noudattamisen varmistaminen saatavuuden ja palautettavuuden osalta

1.3 Tämä politiikka toimeenpanee ISO/IEC 27001:2022 -standardin kontrollit, jotka liittyvät laitteiden turvalliseen hävittämiseen tai uudelleenkäyttöön (5.28), tietoturvallisuuteen häiriötilanteiden aikana (5.29) ja tiedon varmuuskopiointiin (8.13), ja se vastaa ISO/IEC 27002:2022:n, NIST SP 800-53 Rev.5:n, EU:n GDPR:n, DORA-asetuksen ja EU:n NIS2-direktiivin hyviä käytäntöjä.

2. Soveltamisala

2.1 Tämä politiikka koskee:

2.1.1 Kaikkia liiketoimintakriittisiä ja operatiivisia järjestelmiä, jotka kuuluvat ISMS:n soveltamisalaan

2.1.2 Kaikkea rakenteista ja rakenteetonta dataa, mukaan lukien tietokannat, tiedostot, sähköpostit ja konfiguraatiot

2.1.3 Kaikkia ympäristöjä — paikallinen infrastruktuuri, pilviympäristöt, hybridiympäristöt sekä etä- ja muualla sijaitseva tallennus

2.1.4 Kaikkea henkilöstöä, joka vastaa varmuuskopiointiprosessien hallinnasta, toteutuksesta, varmistamisesta tai palauttamisesta

2.2 Politiikka koskee myös:

2.2.1 Varmuuskopiointivälineitä ja -infrastruktuuria, mukaan lukien fyysiset nauhat, virtuaaliset laitteet, levytilannevedokset ja pilvipohjaiset varmuuskopiointiratkaisut

2.2.2 Kolmannen osapuolen palveluntarjoajia, joiden kanssa on sovittu organisaation varmuuskopioiden isännöinnistä, hallinnasta tai käsittelystä

2.2.3 Lokien, konfiguraatioiden, auditointijäljen ja jatkuvuuden kannalta kriittisen operatiivisen dokumentaation varmuuskopiointia

2.3 Järjestelmät, jotka on nimenomaisesti rajattu varmuuskopioinnin ulkopuolelle, on dokumentoitava, niille on tehtävä riskienarviointi, ja tietoturvajohtajan sekä järjestelmäomistajan on hyväksyttävä ne muodollisesti.

3. Tavoitteet

3.1 Varmistaa, että kaikki kriittiset järjestelmät ja tiedot varmuuskopioidaan luotettavasti riittävällä tiheydellä, redundanssilla ja tietoturvakontrolleilla.

3.2 Tarjota palautusmekanismit, jotka täyttävät määritetyt RTO- ja RPO-vaatimukset liiketoimintavaikutusten arviointien mukaisesti.

3.3 Ylläpitää täydellistä dokumentaatiota varmuuskopiointimenettelyistä, säilytysaikatauluista, rooleista ja teknologioista.

3.4 Varmistaa varmuuskopiointitoimintojen tehokkuus järjestelmällisellä palautustestauksella, epäonnistumisten lokituksella ja korjaavien toimenpiteiden seurannalla.

3.5 Suojata varmuuskopioidut tiedot luvattomalta pääsyltä, muuttamiselta tai tuhoamiselta koko niiden elinkaaren ajan.

3.6 Mahdollistaa seuraavien vaatimusten noudattaminen:

3.6.1 ISO/IEC 27001 -standardin operatiivisia kontrolleja ja jatkuvuutta koskevat vaatimukset

3.6.2 NIST SP 800-53:n CP- ja MP-kontrolliperheet varmuuskopioinnin ja turvallisen puhdistamisen osalta

3.6.3 EU:n GDPR:n artikla 32 ja johdanto-osan kappale 49 henkilötietoihin pääsyn palauttamisen osalta

3.6.4 DORA-asetuksen artikla 10 ja EU:n NIS2-direktiivin artikla 21 ICT-jatkuvuuden ja häiriönsietokyvyn osalta

3.7 Varmistaa, että kolmannen osapuolen varmuuskopiointipalvelut täyttävät sopimukselliset ja sääntelyyn perustuvat tietoturvavelvoitteet, mukaan lukien salaus, hävittäminen ja ilmoitusmenettelyt.

4. Roolit ja vastuut

4.1 Ylin johto

4.1.1 Hyväksyy tämän politiikan ja varmistaa, että liiketoimintakriittiset järjestelmät suojataan asianmukaisesti hyväksytyillä varmuuskopiointi- ja palautuskäytännöillä.

4.1.2 Varmistaa, että varmuuskopiointitoimintoihin osoitetaan riittävät resurssit ja että niitä katselmoidaan säännöllisesti sääntelyvaatimusten noudattamisen varmistamiseksi.

4.2 Tietoturvajohtaja (CISO)

4.2.1 Omistaa tämän politiikan ja varmistaa sen yhdenmukaisuuden laajemman tietoturvallisuuden, riskienhallinnan ja jatkuvuuden viitekehyksen kanssa.

4.2.2 Valvoo varmuuskopiointimenettelyjen integrointia BCP/DRP-suunnitelmiin, poikkeamien käsittelyyn ja häiriönsietokyvyn suunnitteluun.

4.2.3 Katselmoi varmuuskopiointia koskevat poikkeukset ja arvioi kriittisten järjestelmien poissulkemisiin liittyvät riskin hyväksyntäesitykset.

[... 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 kerran vuodessa tai aiemmin, jos jokin seuraavista käynnistää katselmoinnin:

9.1.1 Muutokset liiketoiminnan jatkuvuuden tai katastrofipalautuksen strategiassa

9.1.2 Uudet sääntelyyn tai lainsäädäntöön perustuvat velvoitteet, jotka vaikuttavat varmuuskopiointitiheyteen tai tietojen säilytykseen

9.1.3 Muutokset järjestelmäarkkitehtuurissa, varmuuskopiointityökaluissa tai palveluntarjoajissa

9.1.4 Merkittävät poikkeamat tai auditointihavainnot, jotka liittyvät tietojen menetykseen tai palautumisen epäonnistumiseen

9.2 Katselmoinnin koordinoinnista vastaa tietoturvajohtaja (CISO) yhteistyössä seuraavien kanssa:

9.2.1 IT-infrastruktuuri ja IT-käyttö

9.2.2 Sisäinen tarkastus

9.2.3 Tietosuojavastaava (DPO)

9.2.4 Liiketoiminnan jatkuvuuden ja katastrofipalautuksen tiimit

9.3 Varmuuskopiointiaikataulut, järjestelmien sisällyttämisluettelot, palautusdokumentaatio ja poikkeuslokit on katselmoitava rinnakkain sen varmistamiseksi, että:

9.3.1 Varmuuskopioinnin kattavuus kaikille kriittisille omaisuuserille on oikein määritetty

9.3.2 RTO-/RPO- ja säilytysvaatimuksia noudatetaan

9.3.3 Testauslokit ja poikkeamaraportit ovat täydellisiä

9.3.4 Aiemmin tunnistetut kontrolliaukot on korjattu

9.4 Kaikkien päivitysten tulee:

9.4.1 Olla versiohallittuja ja säilytettyjä ISMS:n dokumenttirekisterissä

9.4.2 Sisältää yhteenveto muutoksista ja niiden perusteluista

9.4.3 Tulla ylimmän johdon hyväksymiksi

9.4.4 Tulla viestityiksi kaikille vaikutuksen piirissä oleville teknisille ja liiketoiminnan henkilöstöryhmille

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka tukee suoraan seuraavia asiakirjoja ja liittyy niihin:

10.1.1 P6 - Riskienhallintapolitiikka: Määrittää järjestelmien ja palvelujen varmuuskopiointisuojauksen riskiperusteisen priorisoinnin.

10.1.2 P12 - Omaisuudenhallintapolitiikka: Varmistaa, että varmuuskopiointikelpoiset järjestelmät sisältyvät omaisuusluetteloon ja että ne on sidottu elinkaaren seurantaan ja luokitteluun.

10.1.3 P13 - Tiedon luokittelu- ja merkintäpolitiikka: Ohjaa, mitkä tietoluokat on varmuuskopioitava, mukaan lukien priorisointia tukevat merkintämetatiedot.

10.1.4 P14 - Tietojen säilytys- ja hävityspolitiikka: Yhteensovittaa varmuuskopioiden säilytyksen sääntelyyn perustuviin säilytysrajoihin ja vanhentuneiden tallennusvälineiden asianmukaiseen hävittämiseen.

10.1.5 P16 - Tietojen peittämis- ja pseudonymisointipolitiikka: Tukee minimointia arkaluonteisia tietoaineistoja varmuuskopioitaessa.

10.1.6 P30 - Tietoturvapoikkeamien hallintapolitiikka: Aktivoidaan varmuuskopioinnin epäonnistumisten, palautusongelmien tai varmuuskopioiden tietovarastojen vaarantumisen yhteydessä.

10.2 Nämä toisiinsa liittyvät politiikat muodostavat yhtenäisen viitekehyksen, jolla varmistetaan, että varmuuskopioinnin hallinta on sisällytetty organisaation laajempaan ISMS:ään ja toiminnallisen häiriönsietokyvyn strategiaan.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001:

11.1.1 Lauseke 6.1.3 - riskienkäsittelysuunnitelma: Tukee varmuuskopioinnin riskiperusteista priorisointia ja palautumisen suunnittelua.

11.1.2 Lauseke 8.1 - operatiivinen suunnittelu ja ohjaus: Integroi palautumis- ja jatkuvuuskontrollit osaksi operatiivisia suojatoimia.

11.1.3 Liite A kontrolli 5.28 - laitteiden turvallinen hävittäminen tai uudelleenkäyttö: Kattaa varmuuskopiointivälineiden turvallisen puhdistamisen.

11.1.4 Liite A kontrolli 5.29 - tietoturvallisuus häiriötilanteiden aikana: Varmistaa palautusvalmiudet poikkeamien tai katastrofien aikana.

11.1.5 Liite A kontrolli 8.13 - tiedon varmuuskopiointi: Toteutuu suoraan aikataulutetuilla, testatuilla ja turvallisilla varmuuskopiointitoiminnoilla.

11.2 ISO/IEC 27002:2022 - kontrollit 8.13, 5.28, 5.29: Nämä kontrollit vahvistavat vaatimuksen säännöllisestä varmuuskopioinnista, eheyden validoinnista ja palautumisen suunnittelusta kaikissa IT-ympäristöissä.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - järjestelmän varmuuskopiointi: Määrittää kattavat varmuuskopiointimenettelyt, mukaan lukien muualla sijaitseva säilytys ja palautustestaus.

11.3.2 CP-10 - järjestelmän palautuminen ja palauttaminen: Edellyttää validoituja menettelyjä täydelliseen tai osittaiseen palauttamiseen palautumistavoitteiden mukaisesti.

11.3.3 MP-6 - tallennusvälineiden turvallinen puhdistaminen: Varmistaa käytöstä poistettujen varmuuskopiointivälineiden turvallisen käsittelyn.

11.3.4 SI-12 - tietojen käsittelymenettelyt: Vahvistaa varmuuskopiointiin ja palautumiseen liittyvät vastuut arkaluonteisten tietojen osalta.

11.4 EU:n GDPR (2016/679):

11.4.1 Artikla 32 - käsittelyn turvallisuus: Edellyttää palautusvalmiuksia ja tietojen saatavuuden suojatoimia erityisesti henkilötietojen osalta.

11.4.2 Johdanto-osan kappale 49: Tukee liiketoiminnan jatkuvuus- ja katastrofipalautustoimenpiteitä, mukaan lukien turvallinen varmuuskopiointi osana organisaation häiriönsietokykyä.

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

11.5.1 Artikla 21(2)(c-e): Edellyttää teknisiä ja organisatorisia toimenpiteitä, mukaan lukien varmuuskopiointi- ja jatkuvuuskontrollit, palvelujen häiriönsietokyvyn varmistamiseksi.

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

11.6.1 Artikla 10 - ICT-liiketoiminnan jatkuvuus: Edellyttää finanssialan toimijoilta kattavaa tietojen varmuuskopiointia, palautumista ja jatkuvuussuunnittelua.

11.6.2 Artikla 11 - ICT-liiketoiminnan jatkuvuussuunnitelmien testaus: Korostaa palautumiskyvykkyyden validointia säännöllisen testauksen avulla.

11.7 COBIT 2019:

11.7.1 DSS01 - hallitut operaatiot: Tukee palvelujen luotettavaa toimittamista suojatun tietojen saatavuuden avulla.

11.7.2 DSS04 - hallittu jatkuvuus: Määrittää strategiset ja operatiiviset jatkuvuuskontrollit, mukaan lukien varmennetut varmuuskopiot.

11.7.3 MEA03 - vaatimustenmukaisuuden seuranta, arviointi ja tarkastelu: Edellyttää jatkuvuustoimenpiteiden, mukaan lukien varmuuskopiointikontrollien tehokkuuden, säännöllistä arviointia.