					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P05					Asiakirjan nimi: **Muutoksenhallintapolitiikka**							
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**

Yhdenmukaistettu soveltuvin osin standardien ja säädösten kanssa

Standardi/säädös	Kohta/artikla	Huomio
ISO/IEC 27001:2022	Kohdat 6.1, 5.15	Kattaa riskeihin liittyvät toimenpiteet, pääsynhallinnan ja muutoksenhallinnan
ISO/IEC 27002:2022	Kontrolli 8	Toteuttaa jäsennellyn muutoksenhallintaprosessin
NIST SP 800-53 Rev.5	CM-2–CM-14	Konfiguraationhallinnan kontrollit
EU:n GDPR	Artiklat 32(1)(b–d), 25; johdanto-osan kappale 78	Järjestelmien ja tietojen turvallisuutta muutosten aikana koskevat tekniset ja organisatoriset toimenpiteet
EU:n NIS2-direktiivi	Artikla 21(2)(a, b, d, e)	Edellyttää ICT-muutoksiin liittyvien riskien hallintaa
EU:n DORA-asetus	Artiklat 5, 8, 12	Sääntelee operatiivisia riskejä, ICT-riskejä ja poikkeamien raportointia
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Jäsennelty IT-muutoksenhallinta, sen suorituskyky, vaatimustenmukaisuus ja vaatimukset

1. Tarkoitus

1.1. Tämä politiikka määrittää muodollisen viitekehyksen organisaation tietojärjestelmiin, infrastruktuuriin, sovelluksiin ja niihin liittyviin prosesseihin kohdistuvien muutosten käynnistämiselle, arvioinnille, hyväksynnälle, toteutukselle ja katselmoinnille.

1.2. Politiikka varmistaa, että kaikki muutokset toteutetaan hallitusti ja auditoitavasti siten, että käyttökatkosten, tietoturvan vaarantumisen ja vaatimustenvastaisuuden riski minimoidaan.

1.3. Se tukee ISO/IEC 27001:2022 -standardin liitteen A kontrollia 8.32 varmistamalla turvalliset, dokumentoidut ja riskienhallinnan kanssa yhdenmukaiset muutoksenhallintakäytännöt.

1.4. Politiikka varmistaa myös muutospäätösten jäljitettävyyden ja tukee toiminnallista resilienssiä suunniteltujen ja kiireellisten muutosten aikana.

2. Soveltamisala

2.1. Tämä politiikka koskee kaikkia ISMS:n soveltamisalaan kuuluvia järjestelmiin, tietoihin ja ympäristöihin vaikuttavia muutoksia, mukaan lukien:

2.1.1. IT-infrastruktuuri (omissa tiloissa, pilvi, hybridi)

2.1.2. Tuotanto-, esituotanto- ja katastrofipalautusympäristöt

2.1.3. Liiketoimintasovellukset, palvelut, ohjelmointirajapinnat ja integraatiot

2.1.4. Konfiguraatioasetukset, paikkaukset, ohjelmistojulkaisut ja järjestelmämigraatiot

2.1.5. Hätäkorjaukset sekä projektipohjaiset tai suunnitellut muutokset

2.2. Politiikka koskee muutoksia, jotka käynnistää:

2.2.1. Sisäinen henkilöstö (IT-operaatiot, kehittäjät, järjestelmäomistajat)

2.2.2. Ulkoiset toimittajat, hallinnoidut palveluntarjoajat (MSP:t) ja urakoitsijat

2.2.3. Projektitiimit järjestelmien käyttöönottojen, päivitysten tai palvelusiirtymien yhteydessä

2.3. Tämä politiikka ei koske:

2.3.1. Väliaikaisia testi- ja kehitysympäristöjä, joilla ei ole pääsyä tuotantotietoihin

2.3.2. Käyttäjien henkilökohtaisia asetuksia (katettu hyväksyttävän käytön politiikassa)

2.3.3. Organisaation hallintarajauksen ulkopuolisiin järjestelmiin kohdistuvia muutoksia, elleivät ne vaikuta integroituihin omaisuuseriin tai vaatimustenmukaisuusvelvoitteisiin

3. Tavoitteet

3.1. Varmistaa, että kaikki muutokset katselmoidaan, hyväksytään, testataan ja dokumentoidaan ennen toteutusta.

3.2. Ylläpitää järjestelmien saatavuutta, tietojen eheyttä ja palvelujen jatkuvuutta muutostoimien aikana ja niiden jälkeen.

3.3. Edellyttää määritettyjä muutosluokituksia, palautussuunnitelmia ja riskien arviointia kaikille muutostyypeille.

3.4. Mahdollistaa läpinäkyvän päätöksenteon ja eskaloinnin jäsennellyn hallintamallin kautta.

3.5. Tukea auditointivalmiutta jäljitettävien muutostallenteiden ja käyttöönoton jälkiarviointien avulla.

3.6. Varmistaa tehtävien eriyttämisen ja vähentää luvattomien tai ristiriitaisten muutosten riskiä kriittisissä järjestelmissä.

4. Roolit ja vastuut

4.1. Ylin johto

4.1.1. Hyväksyy muutoksenhallintapolitiikan ja varmistaa sen yhdenmukaisuuden strategisten tavoitteiden ja sääntelyvelvoitteiden kanssa.

4.1.2. Hyväksyy vaikutukseltaan merkittävät tai poikkitoiminnalliset muutosohjelmat osana hallinnollista valvontaa.

4.1.3. Osoittaa tarvittavat resurssit ja budjetin muutoksenhallinnan työkaluihin ja henkilöstön koulutukseen.

4.2. Muutosneuvosto

4.2.1. Katselmoi ja hyväksyy vakiomuutokset ja merkittävät muutokset sekä varmistaa riskien, vaikutusten ja riippuvuuksien asianmukaisen arvioinnin.

4.2.2. Validoi palautussuunnitelmat, testitulokset, sidosryhmäviestinnän ja aikataulutuksen.

4.2.3. Muutosneuvosto koostuu järjestelmäomistajien, tietoturvan, IT-operaatioiden, liiketoimintavastaavien ja vaatimustenmukaisuuden edustajista.

4.2.4. Se voi dokumentoiduin ehdoin delegoida päätöksiä matalan riskin tai kiireellisten muutosten osalta.

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

9. Katselmointi- ja päivitysvaatimukset

9.1. Katselmoinnin herätteet ja tiheys

9.1.1. Tämä politiikka on katselmoitava vuosittain tai seuraavissa tilanteissa:

9.1.1.1. Merkittävät IT- tai infrastruktuurimuutokset

9.1.1.2. Merkittävät epäonnistuneisiin tai luvattomiin muutoksiin liittyvät poikkeamat

9.1.1.3. Sääntelypäivitykset tai uudet muutoksiin liittyvät lakisääteiset velvoitteet

9.1.1.4. Uuden työkaluston tai uusien CMS-alustojen käyttöönotto

9.2. Muutoksenhallintapolitiikan katselmointiprosessi

9.2.1. Muutospäällikkö johtaa katselmointiprosessia yhteistyössä seuraavien kanssa:

9.2.1.1. IT, tietoturva ja operaatiot

9.2.1.2. Sisäinen tarkastus ja riskienhallinta

9.2.1.3. Muutosneuvoston edustajat

9.2.2. Päivitykset on katselmoitava ja hyväksyttävä ylimmässä johdossa sekä ISMS-ohjausryhmässä.

9.2.3. Uudelleen julkaistut versiot on kirjattava asiakirjarekisteriin, ja niistä on tiedotettava vaikutuksen kohteena oleville osapuolille sekä tarvittaessa pyydettävä uusi kuittaus.

9.3. Asiakirjahallinta ja versiointi

9.3.1. Kaikkien versioiden on sisällettävä:

9.3.1.1. Politiikan tunniste, nimi ja luokittelutaso

9.3.1.2. Omistaja ja muutoshistoria

9.3.1.3. Muutosloki ja voimaantulopäivä

9.3.1.4. Hyväksyntävaltuus

9.3.2. Arkistoidut versiot on säilytettävä asiakirjojen säilytyspolitiikan mukaisesti (vähintään 3 vuotta).

10. Liittyvät politiikat ja yhteydet

10.1. Tämä politiikka liittyy suoraan seuraaviin politiikkoihin ja tukee niiden soveltamista:

10.1.1. P1 – Tietoturvapolitiikka: Määrittää vaatimuksen muodollisille tietoturvakontrolleille ja prosessitason vastuiden osoitettavuudelle, mukaan lukien muutoksenhallinnan hallinta.

10.1.2. P2 – Hallinnointirooleja ja vastuita koskeva politiikka: Määrittää muutosten hyväksyntään ja valvontaan liittyvät hyväksyntävaltuudet ja tehtävien eriyttämisen.

10.1.3. P4 – Pääsynhallintapolitiikka: Varmistaa, että muutoksia toteuttavien ja katselmoivien tahojen käyttöoikeudet noudattavat vähimmän etuoikeuden periaatetta.

10.1.4. P6 – Riskienhallintapolitiikka: Varmistaa, että kaikkiin muutoksiin sovelletaan asianmukaista riskien arviointia ja lieventämisstrategioita.

10.1.5. P33 – Auditointi- ja vaatimustenmukaisuuden seurannan politiikka: Ohjaa muutoksenhallintatallenteiden ja rikkomusten validointia sekä auditointikatselmointia.

10.2. Nämä politiikat yhdessä mahdollistavat puolustettavan, jäljitettävän ja turvallisen muutoksenhallinnan elinkaaren ISMS-viitekehyksessä.

11. Viitestandardit ja viitekehykset

11.1. ISO/IEC 27001:2022

11.1.1. Kohta 6.1 – Toimenpiteet riskien ja mahdollisuuksien käsittelemiseksi: Tämä politiikka tukee muutoksiin liittyvien riskien tunnistamista, arviointia ja hallintaa.

11.1.2. Kohta 5.15 – Pääsynhallinta: Varmistaa, että muutosten aikana käyttöoikeuksia hallitaan ja ne ovat jäljitettävissä.

11.1.3. Liitteen A kontrolli 8.32 – Muutoksenhallinta: Tämä politiikka toteuttaa täysimääräisesti vaatimuksen hallita tietojenkäsittelylaitteistoihin ja järjestelmiin kohdistuvia muutoksia suunnitellusti ja hallitusti.

11.2. ISO/IEC 27002:2022 – Kontrolli 8

11.2.1. Vahvistaa jäsennellyn muutoksenhallintaprosessin toteutusta, mukaan lukien muutosten luokittelu, hyväksyntä, testaus, palautus ja dokumentointi.

11.3. NIST SP 800-53 Rev.5

11.3.1. CM-perhe (CM-1–CM-14): Tämä politiikka on tiiviisti yhdenmukainen konfiguraationhallinnan kontrollien kanssa, mukaan lukien perustason konfiguraatiot (CM-2),

konfiguraatiomuutosten hallinta (CM-3), tietoturvavaikutusten analyysi (CM-4) ja käyttöoikeusrajoitukset (CM-5).

11.3.2. AU-perhe (AU-2, AU-6, AU-12): Tässä politiikassa viitatut lokitus- ja auditointimekanismit tukevat tapahtumien jäljitettävyyttä ja muutoksiin liittyvän toiminnan vaatimustenmukaisuuden katselmointia.

11.3.3. RA-3, RA-5: Muutosten käynnistämät riskien arvioinnit ja haavoittuvuusskannaukset on sisällytetty muutosten arviointiprosessiin.

11.3.4. PM-11 (tehtävän/liiketoimintaprosessin määrittely): Varmistaa, että liiketoiminnan jatkuvuus ja operatiiviset tavoitteet säilyvät muutosten aikana.

11.4. EU:n GDPR (2016/679)

11.4.1. Artikla 32(1)(b–d): Tämä politiikka tukee vaatimusta asianmukaisista teknisistä ja organisatorisista toimenpiteistä tietojen turvallisuuden varmistamiseksi erityisesti järjestelmämuutosten aikana.

11.4.2. Artikla 25 – Sisäänrakennettu ja oletusarvoinen tietosuoja: Varmistaa, että henkilötietoihin vaikuttavat muutokset sisällyttävät tietosuojan ja tietoturvan suunnitteluun ja käyttöönottoon.

11.4.3. Johdanto-osan kappale 78: Edellyttää, että rekisterinpitäjät toteuttavat mekanismeja, kuten muutoksenhallintapolitiikkoja, käsittelyjärjestelmien jatkuvan luottamuksellisuuden, eheyden ja resilienssin varmistamiseksi.

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

11.5.1. Artikla 21(2)(a, b, d, e): Edellyttää teknisiä ja organisatorisia toimenpiteitä ICT-riskien hallintaan, mukaan lukien järjestelmämuutoksista, ohjelmistopäivityksistä ja infrastruktuurimuutoksista aiheutuvat riskit.

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

11.6.1. Artikla 5 – Hallinnointi- ja sisäisen valvonnan viitekehys: Tämä politiikka toimeenpanee operatiivisen riskienhallinnan periaatteita, jotka liittyvät ICT-muutoksiin ja päivityksiin.

11.6.2. Artikla 8 – ICT-riskienhallintaviitekehys: Edellyttää, että finanssialan toimijat hallitsevat kaikki ICT-järjestelmiin vaikuttavat muutokset jäsennellyissä muutoksenhallintaprosesseissa, mikä vastaa tämän politiikan luokittelu-, testaus-, palautus- ja dokumentointivaatimuksia.

11.6.3. Artikla 12 – Poikkeamien raportointi: Varmistaa, että ICT-häiriöihin johtaneet epäonnistuneet muutokset ovat jäljitettävissä, dokumentoituja ja tarvittaessa raportoitavia.

11.7. COBIT 2019

11.7.1. BAI06 – Managed IT Changes: Tämä politiikka täyttää suoraan BAI06-tavoitteet määrittämällä jäsennellyt työnkulut muutosten hyväksynnälle, vaikutusarvioinnille, viestinnälle ja testaukselle.

11.7.2. BAI02 – Managed Requirements Definition ja BAI03 – Managed Solutions Identification and Build: Varmistavat, että liiketoimintalähtöiset muutokset katselmoidaan ja toteutetaan turvallisesti.

11.7.3. DSS01 – Managed Operations: Tukee järjestelmien jatkuvaa eheyttä muutosten toteutuksen aikana.

11.7.4. MEA01 ja MEA03 – Monitor, Evaluate, and Assess Performance and Compliance: Mahdollistavat muutoksenhallintapolitiikan tehokkuuden ja soveltamisen jatkuvan valvonnan.