					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P05S					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**

Standardien ja säädösten viitekehys

Standardi/säädös	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohdat 6.1, 8	
ISO/IEC 27002:2022	Kontrolli 8	
NIST SP 800-53 Rev. 5	CM-2–CM-5, CM-11	
EU:n NIS2-direktiivi	Artikla 21(2)(b)	
EU:n DORA-asetus	Artiklat 6(9), 8(4)(b)	
COBIT 2019	BAI06, DSS	

1. Tarkoitus

1.1 Tämän politiikan tarkoituksena on varmistaa, että kaikki IT-järjestelmiin, määrityksiin, liiketoimintasovelluksiin tai pilvipalveluihin kohdistuvat muutokset suunnitellaan, riskit arvioidaan, testataan ja hyväksytään ennen käyttöönottoa.

1.2 Tavoitteena on vähentää toiminnallisia häiriöitä, tietoturvariskejä ja palvelukatkoja määrittämällä yksinkertainen mutta velvoittava menettely, jota sovelletaan myös pienissä yrityksissä, joilla on rajalliset resurssit.

1.3 Tämä politiikka tukee ISO/IEC 27001:2022 -sertifiointia formalisoimalla teknisten ja operatiivisten muutosten hallinnan ja dokumentoinnin.

2. Soveltamisala

2.1 Tämä politiikka koskee:

2.1.1 työntekijöitä ja osastopäälliköitä, jotka ehdottavat tai toteuttavat muutoksia

2.1.2 ulkoisia IT-palveluntarjoajia, jotka hallinnoivat järjestelmiä tai ohjelmistoja

2.1.3 toimitusjohtajaa, jolla on kokonaisvastuu muutosten hyväksymisestä

2.2 Politiikka kattaa muutokset, jotka kohdistuvat:

2.2.1 ohjelmistoihin (päivitykset, tietoturvakorjaukset, uudet sovellukset)

2.2.2 laitteistoihin (vaihdot, päivitykset)

2.2.3 verkko- ja palomuurimäärityksiin

2.2.4 pilvipalveluihin, käyttäjien käyttöoikeuksiin tai toimittajaintegraatioihin

2.2.5 kriittisiin liiketoimintaprosessien muutoksiin, jotka liittyvät tietojärjestelmiin

2.3 Tämän politiikan soveltamisalaan kuuluvat sekä suunnitellut muutokset että hätämuutokset.

3. Tavoitteet

3.1 Varmistaa, että kaikki IT- ja liiketoimintajärjestelmiin kohdistuvat muutokset ovat hyväksyttyjä, dokumentoituja ja tarvittaessa peruutettavissa.

3.2 Estää hallitsemattomista muutoksista aiheutuvat suunnittelemattomat käyttökatkot, tietojen menetykset ja tietoturvapoikkeamat.

3.3 Määrittää yksinkertaiset ja toistettavat menettelyt muutospyyntöjen laatimiseen, hyväksyntään, testaukseen ja muutoksen peruuttamiseen.

3.4 Ylläpitää todennettavissa olevaa muutoslokia, joka tukee jäljitettävyyttä, vastuun osoittamista ja vaatimustenmukaisuutta.

3.5 Mahdollistaa riskiperusteisen päätöksenteon merkittävissä tai arkaluonteisissa muutoksissa.

4. Roolit ja vastuut

4.1 Toimitusjohtaja

4.1.1 Vastaa viime kädessä kaikista merkittävistä muutoksista.

4.1.2 Katselmoi ja hyväksyy muutokset, jotka eivät ole rutiininomaisia tai jotka ovat kriittisiä tai korkean riskin muutoksia.

4.1.3 Katselmoi muutoslokin neljännesvuosittain tai merkittävien poikkeamien jälkeen.

4.2 IT-tuki tai ulkoinen IT-palveluntarjoaja

4.2.1 Toteuttaa muutokset, mukaan lukien määrityspäivitykset, tietoturvakorjaukset ja järjestelmämigraatiot.

4.2.2 Ylläpitää perustason muutoslokia, johon kirjataan päivämäärät, muutostyypit, lopputulokset ja hyväksyjät.

4.2.3 Testaa muutokset ennen käyttöönottoa ja toteuttaa tarvittaessa muutoksen peruutustoimet.

4.2.4 Tiedottaa vaikutuksen piirissä oleville käyttäjille ennen merkittäviä muutoksia ja niiden jälkeen.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Vuosittainen katselmointi

9.1.1 Toimitusjohtajan tai nimetyn IT-yhteyshenkilön tulee katselmoida tämä politiikka vuosittain sen varmistamiseksi, että se vastaa nykyisiä järjestelmiä, työnkulkuja ja sääntelyvaatimuksia.

9.2 Katselmoinnit katselmointijaksojen välillä

9.2.1 Katselmointi on käynnistettävä myös seuraavissa tilanteissa:

9.2.1.1 tietoturvapoikkeamat, jotka johtuvat puutteellisesta muutoksenhallinnasta

9.2.1.2 uusien IT-järjestelmien käyttöönotto

9.2.1.3 muutokset asiaankuuluvissa standardeissa, kuten ISO-standardeissa, EU:n NIS2-direktiivissä tai EU:n DORA-asetuksessa

9.3 Päivitysten dokumentointi

9.3.1 Tähän politiikkaan tehtävät muutokset on hallittava versionhallinnalla ja hyväksytettävä toimitusjohtajalla. Jokaisesta versiosta on kirjattava päivämäärä, muutosten yhteenveto ja hyväksyjä.

9.4 Politiikasta viestiminen

9.4.1 Kaikista päivityksistä on tiedotettava kaikille vaikutuksen piirissä oleville työntekijöille ja ulkoisille palveluntarjoajille. Dokumentaatio on päivitettävä kaikkiin viitesijainteihin (esim. henkilöstöportaali, jaetut asemat).

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka liittyy läheisesti seuraaviin pk-yritysten politiikkoihin:

10.1.1 P2S – Hallinnointiroolien ja vastuiden politiikka: Määrittää muutosten hyväksyntävaltuudet.

10.1.2 P4S – Käyttöoikeuksien hallintapolitiikka: Varmistaa, että muutoksista johtuvat käyttöoikeusmuutokset dokumentoidaan ja toteutetaan asianmukaisesti.

10.1.3 P7S – Perehdytys- ja työsuhteen päättymispolitiikka: Yhteensovittaa roolimuutoksiin ja käyttöoikeuksien myöntämiseen liittyvät muutokset.

10.1.4 P15S – Varmuuskopiointi- ja palautuspolitiikka: Varmistaa, että muutoksen peruuttaminen ja palautuminen voidaan toteuttaa, jos muutos epäonnistuu.

10.1.5 P30S – Poikkeamien hallintapolitiikka: Määrittää, miten epäonnistuneita tai luvattomia muutoksia käsitellään tietoturvapoikkeamina.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Kohta 6.1 – Riskiperusteisen suunnittelun tulee kattaa myös muutostoimet.

11.1.2 Kohta 8.1 – Operatiivisia kontrolleja on sovellettava johdonmukaisesti muutoksiin liittyvissä toimissa palvelun eheyden varmistamiseksi.

11.2 ISO/IEC 27002

11.2.1 Kontrolli 8.32 – Antaa ohjeistusta turvallisiin muutoksenhallintaprosesseihin, mukaan lukien dokumentointi, testaus ja hyväksyntä.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-2 – Järjestelmien perusmääritys ennen muutosta.

11.3.2 CM-3 – Määritysmuutosten hallinta.

11.3.3 CM-4 – Tietoturvavaikutusten analyysi.

11.3.4 CM-5 – Muutosten hyväksyntä ja dokumentointi.

11.3.5 CM-11 – Muutosten auditointi ja seuranta.

11.4 EU:n NIS2-direktiivi

11.4.1 Artikla 21(2)(b) – Edellyttää muodollisia menettelyjä teknisille ja organisatorisille turvatoimille, mukaan lukien muutoksenhallinta.

11.5 EU:n DORA-asetus

11.5.1 Artiklat 6(9) ja 8(4)(b) – Edellyttävät, että finanssialan toimijat ylläpitävät ICT-järjestelmien muutoksenhallintaa ja määritysten hallintaa.

11.6 COBIT 2019

11.6.1 BAI06 – Muutosten hallinta: Korostaa suunnittelua, riskien arviointia ja muutoksen peruutuskyvykkyyttä.

11.6.2 DSS01 – Operaatioiden hallinta: Varmistaa operatiivisen eheyden teknisten siirtymien ja muutosten aikana.