					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P33S					Asiakirjan nimi: **Auditointi- ja vaatimustenmukaisuuden seurantapolitiikka**							
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/säädös	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	Lausekkeet 9.2, 10	Sisäiset auditoinnit, jatkuva parantaminen ja poikkeamien korjaaminen
ISO/IEC 27002:2022	Kontrollit 5.35, 5.37	Aikataulutetut sisäiset katselmoinnit, riippumattomat katselmoinnit ulkoistetuissa prosesseissa
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	Tietoturva-arvioinnit, jatkuva seuranta, auditointien katselmointi, analysointi ja raportointi
EU:n GDPR	Artiklat 24 ja 32	Teknisten ja organisatoristen toimenpiteiden auditointi, näyttö kontrollien tehokkuudesta
EU:n NIS2-direktiivi	Artikla 21(2)(f)	Ennakoiva katselmointi ja näyttöön perustuva vaatimustenmukaisuus
EU:n DORA-asetus	Artikla 10	ICT-riskien hallinta, seuranta ja raportointi
COBIT 2019	MEA01, MEA03	Seuranta ja vaatimustenmukaisuuden arviointi, vaatimustenmukaisuus, valmius kolmannen osapuolen katselmointeihin

1. Tarkoitus

1.1 Tämä politiikka määrittää organisaation menettelytavat sisäisten auditointien, tietoturvakontrollien tarkastusten ja vaatimustenmukaisuuden seurannan toteuttamiseksi. Se varmistaa, että kaikki kontrollit, politiikat, järjestelmät ja palveluntarjoajat kuuluvat säännöllisen ja rakenteisen katselmoinnin piiriin.

1.2 Tarkoituksena on havaita kontrollien pettäminen, ehkäistä vaatimustenvastaisuutta ja osoittaa huolellisuusvelvoitteen täyttyminen ISO/IEC 27001:n, EU:n GDPR:n ja niihin liittyvien viitekehysten mukaisesti.

1.3 Politiikka mahdollistaa sen, että pk-yritys voi ylläpitää operatiivista hallintaa ja auditointivalmiutta myös ilman erillistä vaatimustenmukaisuustoimintoa hyödyntämällä yksinkertaisia, toistettavia tarkistuslistoja ja riskiperusteisesti priorisoituja auditointihavaintoja.

2. Soveltamisala

2.1 Tämä politiikka koskee:

2.1.1 Kaikkia sisäisiä osastoja ja ulkoisia palveluntarjoajia, joilla on vastuita IT-järjestelmiin, henkilötietoihin ja liiketoimintakriittisiin palveluihin liittyen

2.1.2 Kaikkia tietoturvallisuuden hallintajärjestelmän (ISMS) soveltamisalaan kuuluvia kontrolleja ja järjestelmiä

2.1.3 Kaikkia sisäisiä auditointeja, tietoturvakontrollien katselmointeja ja vaatimustenmukaisuustarkastuksia riippumatta siitä, tehdäänkö ne sisäisesti vai ulkoisen konsultin, asiakkaan tai viranomaisen toimesta

2.2 Tämä politiikka koskee myös näytön keräämistä ja raportointia seuraavia varten:

2.2.1 ISO/IEC 27001 -sertifiointi- ja uudelleensertifiointiauditoinnit

2.2.2 EU:n GDPR:n tai sopimusehtojen mukaiset tietosuoja-auditoinnit

2.2.3 Asiakkaiden käynnistämät tietoturvakyselyt tai due diligence -arvioinnit

2.2.4 Mahdolliset EU:n NIS2-direktiivin tai DORA-asetuksen mukaiset viranomais- tai riippumattomat katselmoinnit soveltuvin osin

3. Tavoitteet

3.1 Varmistaa, että kaikki keskeiset kontrollit ja politiikat katselmoidaan säännöllisesti tehokkuuden ja vaatimustenmukaisuuden osalta.

3.2 Ylläpitää audit trailia ja korjaavien toimenpiteiden kirjauksia osoitusvelvollisuuden ja jatkuvan parantamisen osoittamiseksi.

3.3 Valmistautua sertifiointiin, uudelleensertifiointiin ja asiakkaiden varmennusohjelmiin (esim. ISO 27001, toimittajan käyttöönotto).

3.4 Tunnistaa puutteet varhaisessa vaiheessa, jotta korjaavat toimenpiteet voidaan toteuttaa viipymättä ennen kuin ongelmat eskaloituvat tai johtavat velvoitteiden rikkomiseen.

3.5 Mahdollistaa sen, että toimitusjohtaja ja IT-palveluntarjoaja voivat koordinoida katselmointeja mahdollisimman vähäisellä monimutkaisuudella varmistaen samalla puolustettavat lopputulokset.

4. Roolit ja vastuut

4.1 Toimitusjohtaja

4.1.1 Valvoo auditointiohjelmaa

4.1.2 Hyväksyy sisäiset katselmointisuunnitelmat ja auditointihavainnot

4.1.3 Osoittaa korjaavat toimenpiteet ja seuraa niiden toteutusta

4.1.4 Valtuuttaa ulkoisten auditoijien tai konsulttien käytön

4.2 IT-palveluntarjoaja / järjestelmänvalvoja

4.2.1 Toimittaa näytön sisäisten ja ulkoisten auditointien aikana (esim. lokit, konfiguraatiot, pääsynhallintatiedot)

4.2.2 Avustaa teknisissä tarkastuksissa (esim. varmuuskopioinnin tila, korjauspäivitysten vaatimustenmukaisuustila)

4.2.3 Ylläpitää auditointitietovarastoa

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Politiikan ja auditointisuunnitelman vuosittainen katselmointi

9.1.1 Toimitusjohtajan on katselmoitava tämä politiikka ja auditointiaikataulu vähintään kerran vuodessa.

9.1.2 Katselmoinnissa on arvioitava:

9.1.2.1 Auditointien tehokkuus puutteiden tunnistamisessa

9.1.2.2 Auditointien ja korjaavien toimenpiteiden valmistumisaste

9.1.2.3 Sovellettaviin lakisääteisiin, sääntelyyn liittyviin tai sertifiointivaatimuksiin tehdyt muutokset

9.2 Heräteperusteiset päivitykset

9.2.1 Politiikka on katselmoitava ja päivitettävä, kun:

9.2.2 Sertifiointi- tai valvontaauditointi johtaa merkittävään poikkeamaan

9.2.3 Oikeudelliset tai sääntelyyn liittyvät viitekehykset muuttuvat (esim. uusi EU:n GDPR-ohjeistus, EU:n NIS2-direktiivin kansallinen täytäntöönpano)

9.2.4 Liiketoiminnan muutokset vaikuttavat auditoinnin soveltamisalaan kuuluviin järjestelmiin, prosesseihin tai toimittajiin

9.2.5 Kriittinen poikkeama tai tietomurto paljastaa aiemmin havaitsemattomia kontrolliaukkoja

9.3 Päivitysten dokumentointi

9.3.1 Kaikkia muutoksia on seurattava politiikan versionhallintalokissa

9.3.2 Päivitykset on jaettava kaikille auditointeihin osallistuville tiimin jäsenille

9.3.3 Päivitetyn politiikan yhteyteen on liitettävä yhteenveto muutoksista ymmärtämisen varmistamiseksi

10. Liittyvät politiikat ja yhteydet

10.1 Tätä politiikkaa tukevat ja täydentävät useat muut pk-yrityksen politiikat:

10.1.1 P1S – Tietoturvapolitiikka: Määrittää kaikkien kontrolliodotusten perustason ja edellyttää niiden varmentamista auditointien avulla.

10.1.2 P2S – Hallintoroolien ja vastuiden politiikka: Määrittää vastuut auditoinnin suunnittelulle, toteutukselle ja korjaavien toimenpiteiden omistajuudelle.

10.1.3 P6S – Riskienhallintapolitiikka: Tunnistaa auditoinneissa havaitut kontrollipuutteet ja varmistaa, että auditointihavainnot dokumentoidaan riskirekisteriin.

10.1.4 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: Määrittää ne EU:n GDPR:n mukaiset kontrollit, jotka on auditoitava, mukaan lukien tietojen käsittely, tietoturvaloukkauksiin reagointi ja tietosuojailmoitukset.

10.1.5 P22S – Lokitus- ja valvontapolitiikka: Tuottaa lokit ja forensiset tiedot, joita käytetään vaatimustenmukaisuus- ja kontrollikatselmoinneissa.

10.1.6 P30S – Tietoturvapoikkeamien hallintapolitiikka: Edellyttää poikkeamatallenteiden ja tapahtuman jälkeisten katselmusten säännöllistä auditointia reagoinnin tehokkuuden varmentamiseksi.

10.1.7 P31S – Näytön keräämisen ja forensiikan politiikka: Määrittää menettelyt todennettavissa olevan, hallussapitoketjun säilyttävän näytön keräämiseksi auditointien aikana.

10.2 Yhdessä nämä politiikat muodostavat suljetun kontrolliympäristön, joka mahdollistaa sisäisen varmennuksen, ulkoisen varmentamisen ja standardien mukaisen hallinnan.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001:

11.1.1 Lauseke 9.2 – Edellyttää sisäisiä auditointeja ISMS:n suorituskyvyn ja vaatimustenmukaisuuden arvioimiseksi.

11.1.2 Lauseke 10.1 – Edellyttää jatkuvaa parantamista auditointitulosten ja poikkeamien korjaamisen perusteella.

11.2 ISO/IEC 27002:

11.2.1 Kontrolli 5.35 – Edellyttää kontrollien ja prosessien aikataulutettuja sisäisiä katselmointeja.

11.2.2 Kontrolli 5.37 – Korostaa riippumattomia katselmointeja erityisesti ulkoistetuissa prosesseissa.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Tietoturva-arvioinnit: Edellyttää toteutettujen kontrollien auditointia tehokkuuden varmentamiseksi.

11.3.2 CA-7 – Jatkuva seuranta: Korostaa kontrollipuutteiden ennakoivaa havaitsemista ja katselmointia.

11.3.3 AU-6 – Auditointien katselmointi, analysointi ja raportointi: Edellyttää auditointilokien ja auditointihavaintojen säännöllistä analysointia ja käsittelyä.

11.4 EU:n GDPR:

11.4.1 Artiklat 24 ja 32 – Edellyttävät teknisten ja organisatoristen toimenpiteiden toteutusta ja auditointia, mukaan lukien näyttö kontrollien tehokkuudesta ja ajan myötä tapahtuvasta parantamisesta.

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

11.5.1 Artiklat 20–21 – Edellyttävät ennakoivaa kontrollien katselmointia, näyttöön perustuvaa vaatimustenmukaisuutta ja auditoitavuutta keskeisille ja tärkeille toimijoille.

11.6 COBIT 2019:

11.6.1 MEA01 – Suorituskyvyn ja vaatimustenmukaisuuden seuranta, arviointi ja tarkastelu: Edellyttää prosessien ja kontrollien suorituskyvyn säännöllistä arviointia standardeja ja tavoitteita vasten.

11.6.2 MEA03 – Ulkoisten vaatimusten noudattamisen varmistaminen: Painottaa sisäistä seurantaa ja valmiutta kolmannen osapuolen auditointeihin sekä sääntelykatselmointeihin.