					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P33					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/sääntely	Vaatimus/artikla	Kommentti
ISO/IEC 27001:2022	Vaatimukset 9.2, 9.3, 10	
ISO/IEC 27002:2022	Kontrollit 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
EU:n GDPR	Artiklat 24, 32, 33	
EU:n NIS2-direktiivi	Artikla 21(2)(g), 27	
EU:n DORA-asetus	Artiklat 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Tarkoitus

1.1 Tämän politiikan tarkoituksena on määrittää ja ohjata organisaation auditointi- ja vaatimustenmukaisuuden seurantaohjelmaa siten, että:

1.1.1 tietoturva- ja tietosuojakontrollien tehokkuus todennetaan

1.1.2 sovellettavien standardien, oikeudellisten viitekehysten ja sopimusvelvoitteiden noudattaminen varmistetaan

1.1.3 poikkeamat, tehottomuudet ja vaatimustenmukaisuusriskit tunnistetaan oikea-aikaisesti

1.1.4 jatkuvaa parantamista sekä valmiutta sertifiointeihin, arviointeihin ja sääntelytarkastuksiin tuetaan

1.2 Tämä politiikka tukee tietoturvallisuuden hallintajärjestelmän (ISMS) eheyttä ja kypsyystasoa sisällyttämällä siihen rakenteelliset, riskiperusteiset ja näyttöön perustuvat auditointi- ja seurantakäytännöt.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia seuraavia:

2.1.1 sisäisiä liiketoimintayksiköitä, toimintoja ja osastoja

2.1.2 fyysisiä toimitiloja, pilviympäristöjä, SaaS-ympäristöjä ja ulkoistettuja palveluja

2.1.3 tietojärjestelmiä, sovelluksia, infrastruktuuria ja tietovaroja, joita hallitaan ISMS:n puitteissa

2.1.4 työntekijöitä, toimeksisaajia ja kolmannen osapuolen palveluntarjoajia, joilla on auditointi- tai vaatimustenmukaisuusvelvoitteita

2.2 Politiikka kattaa seuraavat osa-alueet:

2.2.1 sisäinen tarkastus

2.2.2 ulkoiset auditoinnit ja sertifiointiauditoinnit

2.2.3 tekninen vaatimustenmukaisuuden seuranta

2.2.4 toimittaja- ja kolmannen osapuolen auditoinnit

2.2.5 korjaavat ja ennaltaehkäisevät toimenpiteet (CAPA)

2.2.6 mittarit, mittaristot ja raportointiprosessit

2.3 Tätä politiikkaa sovelletaan kaikkiin organisaatiota koskeviin viitekehyksiin, mukaan lukien ISO/IEC 27001, EU:n GDPR, EU:n NIS2-direktiivi, EU:n DORA-asetus ja SOC 2.

3. Tavoitteet

3.1 Varmistaa ISMS:ssä ja siihen liittyvissä ympäristöissä toteutettujen kontrollien, politiikkojen ja menettelyjen riittävyys ja tehokkuus.

3.2 Tunnistaa ja korjata puutteet, poikkeamat ja vaatimustenmukaisuusvajeet ennen kuin ne johtavat poikkeamiin tai rikkomuksiin.

3.3 Varmistaa jatkuva valmius sisäisiin hallinnon katselmointeihin, ulkoisiin auditointeihin ja riippumattomiin sertifiointeihin.

3.4 Tuottaa oikeudellisesti puolustettavaa näyttöä ja auditointijälkiä sääntelyyn liittyvien tiedustelujen, oikeudellisten menettelyjen tai asiakkaiden tai kumppaneiden varmennuspyyntöjen tueksi.

3.5 Kytkeä auditointitulokset organisaation laajempaan riskienhallintaan, tietoturvamittareihin ja jatkuvan parantamisen toimintoihin.

4. Roolit ja vastuut

4.1 Sisäisen tarkastuksen vastuuhenkilö / vaatimustenmukaisuuspäällikkö

4.1.1 Suunnittelee, aikatauluttaa ja toteuttaa sisäiset auditoinnit riskiprioriteettien perusteella.

4.1.2 Ylläpitää auditointirekisteriä, koordinoi auditointitoimintoja ja seuraa korjaavien toimenpiteiden toteutusta.

4.2 Tietoturvajohtaja (CISO)

4.2.1 Varmistaa, että auditoinnin soveltamisala kattaa kaikki asiaankuuluvat ISMS:n osa-alueet ja liitteen A kontrollit.

4.2.2 Valvoo CAPA-toimenpiteiden varmennusta ja integroi auditointitulokset tietoturvaohjelmaan.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Vaatimustenmukaisuuspäällikön ja tietoturvajohtajan (CISO) on katselmoitava tämä politiikka vähintään vuosittain tai aikaisemmin, jos jokin seuraavista toteutuu:

9.1.1 muutokset sääntelyssä, sopimuksissa tai sertifiointiviitekehyksissä

9.1.2 merkittävät auditointihavainnot tai toistuvat kontrollien pettämiset

9.1.3 organisaatiomuutokset tai GRC-järjestelmän muutokset

9.1.4 ulkoisen auditoijan suositukset tai viranomaispalaute

9.2 Katselmointiprosessissa on arvioitava:

9.2.1 auditoinnin suunnittelumenetelmä ja tiheys

9.2.2 muutokset ISMS:n soveltamisalassa tai infrastruktuurissa

9.2.3 kontrollikatalogin tai lakirekisterin päivitykset

9.2.4 auditointinäytön ja CAPA-prosessien yhdenmukaisuus ja laatu

9.3 Kaikki politiikkamuutokset on:

9.3.1 dokumentoitava versionhallittuun tietovarastoon

9.3.2 hyväksyttävä ylimmän johdon toimesta

9.3.3 viestittävä kaikille vaikutuksen piirissä oleville henkilöille ja sisällytettävä päivitettyihin menettelyihin ja tietoisuusohjelmiin

9.4 Katselmoinnin jälkeisessä varmennuksessa on vahvistettava, että päivitetyt vaatimukset näkyvät auditointirekisterissä, vaatimustenmukaisuustyökaluissa ja sisäisissä valvontanäkymissä.

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka on yhdenmukainen seuraavien organisaation politiikkojen kanssa:

10.1.1 P1 – Tietoturvapolitiikka: määrittää ISMS:n ja asettaa vastuut vaatimustenmukaisuudesta ja jatkuvasta parantamisesta

10.1.2 P5 – Muutoksenhallintapolitiikka: varmistaa auditointien näkyvyyden infrastruktuuri- ja konfiguraatiomuutoksiin, jotka vaikuttavat kontrolliympäristöihin

10.1.3 P6 – Riskienhallintapolitiikka: integroi auditointitulokset organisaation riskienarviointi- ja riskienkäsittelytoimiin

10.1.4 P14 – Tietojen säilytys- ja hävityspolitiikka: ohjaa auditointinäytön, lokien ja vaatimustenmukaisuustallenteiden säilytystä

10.1.5 P18 – Kryptografisten hallintakeinojen politiikka: tukee arkaluonteisten auditointitietojen turvallista säilytystä ja siirtoa

10.1.6 P26 – Kolmannen osapuolen ja toimittajien tietoturvapolitiikka: kattaa auditointioikeudet, varmennusdokumentaation ja toimittajien vaatimustenmukaisuuden valvonnan

10.1.7 P30 – Tietoturvapoikkeamien hallintapolitiikka: yhdenmukaistaa poikkeamien käsittelyprosessien auditoinnit ISMS:n varmennustavoitteiden kanssa

10.1.8 P32 – Liiketoiminnan jatkuvuus- ja katastrofipalautuspolitiikka: edellyttää jatkuvuustestauksen ja DRP-vaatimustenmukaisuuden varmennusta auditointijaksojen aikana

11. Viitestandardit ja viitekehykset

11.1 Tämä politiikka on yhdenmukainen kansainvälisten auditointia ja jatkuvaa vaatimustenmukaisuuden todentamista koskevien standardien ja oikeudellisten vaatimusten kanssa.

11.2 ISO/IEC 27001:

11.2.1 Vaatimus 9.2 – sisäinen tarkastus: edellyttää ISMS:n säännöllisiä, riskiperusteisia auditointeja tehokkuuden ja vaatimustenmukaisuuden arvioimiseksi.

11.2.2 Vaatimus 9.3 – johdon katselmus: auditointitulosten on tuettava strategista katselmointia ja parantamista.

11.2.3 Vaatimus 10.1 – poikkeama ja korjaava toimenpide: auditointihavainnot on käsiteltävä dokumentoitujen CAPA-menettelyjen kautta.

11.3 ISO/IEC 27002:2022 – kontrollit 5.35–5.37:

11.3.1 Liitteen A kontrollit 5.35–5.37: kattavat riippumattoman katselmoinnin, oikeudellisten ja sopimusvaatimusten noudattamisen sekä auditointilokituksen.

11.3.2 Ne antavat toteutusohjeita auditointi- ja vaatimustenmukaisuusohjelmien suunnitteluun, toteutukseen ja parantamiseen.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – kontrollien arvioinnit: edellyttää toteutettujen tietoturvakontrollien rutiininomaista arviointia.

11.4.2 CA-5 – toimenpidesuunnitelma ja virstanpylväät (POA&M): vastaa auditointihavaintojen seurantaa ja korjaamista.

11.4.3 CA-7 – jatkuva seuranta: tukee ennakoivia, automatisoituja vaatimustenmukaisuuden arviointeja.

11.5 EU:n GDPR (2016/679):

11.5.1 Artiklat 24 ja 32: edellyttävät näyttöä tietoturvakontrollien toteutuksesta ja tehokkuudesta asianmukaisten hallintorakenteiden avulla.

11.5.2 Artikla 33: tukee varmennettujen auditointijälkien tarvetta tietoturvaloukkausten käsittelyssä ja ilmoittamisessa.

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

11.6.1 Artikla 21(2)(g): edellyttää politiikkojen ja menettelyjen auditointia osana kyberturvallisuuden riskienhallinnan vähimmäistoimenpiteitä.

11.6.2 Artikla 27: kansalliset viranomaiset voivat suorittaa auditointeja tai edellyttää niitä keskeisiltä ja tärkeiltä toimijoilta.

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

11.7.1 Artikla 10(2)(e): yhteisöjen on suoritettava sisäisiä ja ulkoisia auditointeja ICT-riskien hallinnan käytännöistä.

11.7.2 Artikla 25 – auditointivaatimukset: edellyttää määräajoin tehtäviä auditointeja sisäisten tai riippumattomien ulkoisten auditoijien toimesta siten, että viranomaisnäkyvyys varmistetaan.

11.8 COBIT 2019:

11.8.1 MEA01 – suorituskyvyn ja vaatimustenmukaisuuden seuranta, arviointi ja arvioiminen: varmistaa, että kontrollien tehokkuus todennetaan ja raportoidaan hallintoelimille.

11.8.2 MEA03 – vaatimustenmukaisuuden seuranta, arviointi ja arvioiminen: edellyttää organisaation käytäntöjen yhdenmukaisuutta oikeudellisten, sopimukseen perustuvien ja standardipohjaisten vaatimusten kanssa.