					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P37					Asiakirjan nimi: **Laki- ja sääntelyvaatimusten noudattamisen politiikka**							
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**

1. Tarkoitus

1.1 Tämä politiikka määrittää pakollisen viitekehyksen kaikkien organisaation tietoturvaan, tietosuojaan ja operatiiviseen toimintaan liittyvien lakisääteisten, sääntelyyn perustuvien ja sopimuksellisten velvoitteiden tunnistamiselle, hallinnalle ja noudattamiselle.

1.2 Tavoitteena on estää vaatimustenvastaisuus, joka voi johtaa seuraamuksiin, oikeudelliseen vastuuseen, liiketoiminnan häiriöihin, mainehaittaan tai viranomaistoimenpiteisiin.

1.3 Tämä politiikka tukee vaatimustenmukaisuusvelvoitteiden integroimista hallintoon, riskienhallintaan, operatiivisiin työnkulkuihin, projektien elinkaariin ja järjestelmäsuunnitteluun.

1.4 Tällä politiikalla varmistetaan, että kaikki merkitykselliset velvoitteet eri lainkäyttöalueilla, toimialoilla ja sääntelyn soveltamisaloilla dokumentoidaan, arvioidaan, seurataan ja toimeenpannaan organisaatiossa johdonmukaisesti.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia osastoja, toimintoja, liiketoimintayksiköitä ja henkilöitä, jotka toimivat organisaation puolesta, mukaan lukien:

2.1.1 Vakituiset ja määräaikaiset työntekijät

2.1.2 Sopimuskumppanit, konsultit ja harjoittelijat

2.1.3 Kolmannet osapuolet, henkilötietojen käsittelijät tai kumppanit, jotka käsittelevät organisaation tietoja, järjestelmiä tai sääntelyyn liittyviä vastuita

2.1.4 Kaikki liiketoimintaprosessit, projektit tai aloitteet, joihin kohdistuu lakisääteistä tai sääntelyyn perustuvaa ohjausta

2.2 Tämän politiikan kattamiin vaatimustenmukaisuusalueisiin kuuluvat muun muassa:

2.2.1 Tietoturvaa ja kyberturvallisuutta koskevat velvoitteet (esim. ISO/IEC 27001, NIS2, DORA)

2.2.2 Tietosuojaa ja yksityisyyden suojaa koskeva lainsäädäntö (esim. GDPR, toimialakohtaiset tietosuojalait)

2.2.3 Toimialakohtainen sääntely (esim. rahoitusala, terveydenhuolto, autoteollisuus, puolustusteollisuus)

2.2.4 Sopimukselliset velvoitteet, jotka perustuvat salassapitosopimuksiin (NDA), palvelutasosopimuksiin (SLA) tai kolmannen osapuolen käsittelysopimuksiin

2.2.5 Oikeudelliset vaatimukset, jotka liittyvät poikkeamien ilmoittamiseen, yhteistyöhön lainvalvontaviranomaisten kanssa ja kansainvälisiin tiedonsiirtoihin

3. Tavoitteet

3.1 Varmistaa, että kaikki sovellettavat lait, säädökset, standardit ja sopimukselliset velvoitteet tunnistetaan, dokumentoidaan, tulkitaan ja toimeenpannaan koko organisaatiossa.

3.2 Integroida laki- ja sääntelyvaatimukset organisaation tietoturvallisuuden hallintajärjestelmään (ISMS), riskienhallintaprosesseihin, toimittajasopimuksiin sekä tuotteiden ja palvelujen suunnitteluun.

3.3 Tarjota mekanismi sääntelymuutosten ennakoivaan seurantaan sekä kontrollien ja dokumentaation päivittämiseen niiden mukaisesti.

3.4 Määrittää selkeä vastuunjako vaatimustenmukaisuuden valvonnalle, rikkomusten eskaloinnille, poikkeusten käsittelylle ja ulkoiselle raportoinnille.

3.5 Varmistaa organisaation laki- ja sääntelyaseman todennettavuus ja puolustettavuus auditointien, tutkintojen tai sertifiointikatselmusten yhteydessä.

4. Roolit ja vastuut

4.1 Ylin johto

4.1.1 Vastaa strategisella tasolla laki- ja sääntelyvaatimusten noudattamisesta koko organisaatiossa.

4.1.2 Katselmoi ja hyväksyy korkean riskin vaatimustenmukaisuuspäätökset, mukaan lukien riskin hyväksynnät ja oikeudelliset riidat.

4.2 Laki- ja vaatimustenmukaisuusvastaava / lakiasiainjohtaja / oikeudellinen neuvonantaja

4.2.1 Ylläpitää vaatimustenmukaisuusvelvoitteiden rekisteriä, johon kirjataan kaikki sovellettavat lait, standardit, sertifioinnit ja sopimuslausekkeet.

4.2.2 Toteuttaa oikeudellisten vaikutusten arvioinnit uusille palveluille, markkinoille tai tietovirroille.

4.2.3 Antaa organisaation käyttöön lakien ja standardien sitovat tulkinnat.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Vuosittainen politiikan katselmointi

9.1.1 Tämä politiikka on katselmoitava vähintään kerran kalenterivuodessa, jotta voidaan:

9.1.1.1 Varmistaa jatkuva yhdenmukaisuus päivitettyjen lakien, toimialastandardien ja sääntelykehysten kanssa

9.1.1.2 Varmistaa operatiivinen tehokkuus auditointihavaintojen ja poikkeamahistorian perusteella

9.1.1.3 Huomioida organisaatiomuutokset (esim. uudet lainkäyttöalueet, järjestelmät tai liiketoiminta-alueet)

9.2 Heräteperusteiset katselmukset

9.2.1 Väliaikaiset katselmukset on käynnistettävä, kun:

9.2.2 Uusi lakisääteinen tai sääntelyyn perustuva vaatimus tulee voimaan tai sitä päivitetään

9.2.3 Vaatimustenmukaisuuspoikkeama tai auditointi paljastaa politiikan puutteita

9.2.4 Organisaatio siirtyy uudelle markkinalle tai uuteen palvelukategoriaan, johon sovelletaan erillisiä vaatimustenmukaisuuskehyksiä

9.2.5 Valvontatrendit tai viranomaisohjeistus osoittavat muutoksia riskitasossa

9.3 Omistajuus ja hyväksyntä

9.3.1 Lakiosasto ja laki- ja vaatimustenmukaisuusvastaava vastaavat yhdessä katselmointiprosessin koordinoinnista.

9.3.2 Politiikan lopulliset muutokset on hyväksyttävä ylimmässä johdossa ja kirjattava politiikkamuutosrekisteriin sekä liitettävä niihin muutoksenhallinnan viittaukset ja viestintäsuunnitelmat.

9.4 Versionhallinta ja viestintä

9.4.1 Tämän politiikan jokaisen päivitetyn version on:

9.4.1.1 Sisällettävä yhteenveto keskeisistä muutoksista

9.4.1.2 Oltava jaettu uudelleen virallisten kanavien kautta (esim. politiikkaportaali, LMS, sisäiset uutiskirjeet)

9.4.1.3 Edellytettävä hyväksyntä vaikutuksen alaiselta henkilöstöltä, erityisesti laki-, operatiivisissa, tietoturva- ja toimittajahallinnan rooleissa toimivilta henkilöiltä

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka toimii yhdessä seuraavien organisaation tietoturvallisuuden hallintajärjestelmän (ISMS) politiikkojen kanssa ja vahvistaa niitä:

10.1.1 P1 – Tietoturvapolitiikka: Määrittää hallinnan perusperiaatteet, joilla varmistetaan, että kaikki tietoturvapolitiikat, mukaan lukien vaatimustenmukaisuutta koskevat politiikat, ovat yhdenmukaisia strategisten liiketoiminta- ja sääntelyvaatimusten kanssa.

10.1.2 P2 – Hallintoroolien ja vastuiden politiikka: Määrittää päätöksentekovaltuudet, mukaan lukien laki- ja vaatimustenmukaisuusroolit, jotka vastaavat sääntelyyn liittyvästä valvonnasta ja osoitusvelvollisuudesta.

10.1.3 P6 – Riskienhallintapolitiikka: Tukee lakisääteisten ja sääntelyyn liittyvien vaatimustenmukaisuusriskien arviointia, omistajuutta ja lieventämistä koko organisaatiossa.

10.1.4 P8 – Tietoturvatietoisuus- ja koulutuspolitiikka: Varmistaa, että koko henkilöstö tuntee vaatimustenmukaisuuteen liittyvät vastuunsa ja saa roolilleen soveltuvan koulutuksen.

10.1.5 P12 – Omaisuudenhallintapolitiikka: Vahvistaa lakisääteisiä velvoitteita säänneltyjen tai sopimukseen perustuvien omaisuuserien hallinnassa ja suojaamisessa, mukaan lukien henkilötietoihin ja kriittiseen infrastruktuuriin liittyvät omaisuuserät.

10.1.6 P30 – Tietoturvapoikkeamien hallintapolitiikka: Ohjaa pakollisia lakisääteisiä ilmoituksia (esim. GDPR:n artikla 33) ja eskalointimenettelyjä vaatimustenmukaisuusrikkomuksen tai sääntelyyn liittyvän tapahtuman yhteydessä.

10.1.7 P33 – Auditointi- ja vaatimustenmukaisuuden seurantapolitiikka: Tarjoaa jäsennellyt varmistustoimet, mukaan lukien kontrollien testaus ja näytön kerääminen, joita tarvitaan sisäiseen ja ulkoiseen vaatimustenmukaisuuden varmentamiseen.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Kohta 4.2 – Asiaankuuluvien osapuolten tarpeiden ja odotusten ymmärtäminen: Edellyttää lakisääteisten ja sääntelyyn perustuvien vaatimusten tunnistamista ja integroimista tietoturvallisuuden hallintajärjestelmään (ISMS).

11.1.2 Kohta 5.1 – Johtajuus ja sitoutuminen: Edellyttää ylimmän johdon vastuunottoa organisaation lakisääteisen vaatimustenmukaisuuden luomisesta ja ylläpidosta.

11.1.3 Kohta 5.3 – Organisaation roolit, vastuut ja valtuudet: Varmistaa roolien selkeyden oikeudellisessa valvonnassa ja sääntelyvaatimusten noudattamisessa.

11.1.4 Liite A, kontrolli 5.36 – Laki- ja sopimusvaatimusten noudattaminen: Määrittää vaatimuksen tunnistaa ja täyttää laeista, säädöksistä ja sopimuksista johtuvat velvoitteet.

11.2 ISO/IEC 27002

11.2.1 Kontrolli 5.36: Kuvaa toteutusohjeet vaatimustenmukaisuusvelvoitteiden rekisterin ylläpitämiselle, sääntelyvaatimusten varmentamiselle ja jäsennellyn näytön säilyttämisen varmistamiselle.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PL-1 – Tietoturvasuunnittelun politiikka ja menettelyt: Edellyttää, että vaatimustenmukaisuusvelvoitteet sisällytetään hallintorakenteisiin ja dokumentaatioon.

11.3.2 PM-1 – Tietoturvaohjelman suunnitelma: Edellyttää sääntelykontrollien sisällyttämistä osaksi laajempaa tietoturvaohjelmaa.

11.3.3 CA-7 – Jatkuva seuranta: Tukee kontrollien tehokkuuden valvontaa lakisääteisten ja politiikkavaatimusten täyttämisessä.

11.3.4 AU-9 – Auditointitietojen suojaus: Varmistaa, että vaatimustenmukaisuuteen liittyvät auditointilokit ja tallenteet on suojattu ja saatavilla tarkastuksia varten.

11.4 EU:n GDPR (2016/679)

11.4.1 Artikla 5 – Henkilötietojen käsittelyä koskevat periaatteet: Edellyttää lainmukaista käsittelyä, läpinäkyvyyttä ja osoitusvelvollisuutta.

11.4.2 Artikla 6 – Käsittelyn lainmukaisuus: Edellyttää asianmukaisia oikeusperusteita kaikelle tietojen käsittelylle.

11.4.3 Artikla 24 – Rekisterinpitäjän vastuu: Määrittää suoran vastuun sääntelyvaatimusten noudattamisen varmistamisesta.

11.4.4 Artikla 32 – Käsittelyn turvallisuus: Edellyttää asianmukaisten teknisten ja organisatoristen kontrollien toteuttamista.

11.4.5 Artikla 33 – Tietoturvaloukkauksesta ilmoittaminen: Edellyttää, että henkilötietojen tietoturvaloukkaus ilmoitetaan toimivaltaisille viranomaisille 72 tunnin kuluessa.

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

11.5.1 Artiklat 20–21: Edellyttävät, että keskeiset ja tärkeät toimijat toteuttavat dokumentoidun hallinnan, lakisääteisen vaatimustenmukaisuuden strategiat ja oikeudellisten riskien jatkuvan katselmoinnin.

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

11.6.1 Artikla 5(2) – ICT-riskien hallinnan viitekehys: Edellyttää lakisääteisen vaatimustenmukaisuuden integroimista laajempiin riskienhallinta- ja valvontatoimintoihin.

11.6.2 Artikla 19 – ICT-kolmannen osapuolen riski: Asettaa erityisiä oikeudellisia vaatimuksia ulkoisiin toimittajiin ja alustoihin liittyvien sopimuksellisten ja sääntelyvelvoitteiden hallinnalle.

11.7 COBIT 2019

11.7.1 APO12 – Riskien hallinta: Sisällyttää lakisääteisen ja sääntelyyn liittyvän vaatimustenmukaisuuden keskeiseksi osaksi organisaation riskienhallintaa.

11.7.2 MEA03 – Ulkoisten vaatimusten noudattamisen seuranta: Määrittää jatkuvan seurannan, poikkeusten käsittelyn ja auditointivalmiuden kaikille sääntelyvelvoitteiden muodoille.