					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P37S					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**

Yhdenmukaisuus standardien ja sääntelyvaatimusten kanssa

Standardi/sääntely	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	Lausekkeet 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontrolli 5	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
EU:n GDPR	Artiklat 5, 6, 32, 33	
EU:n NIS2-direktiivi	Artiklat 21(2)(a), 21(2)(f), 23	
EU:n DORA-asetus	Artiklat 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Tarkoitus

1.1 Tämä politiikka määrittää organisaation toimintatavan lakisääteisten, sääntelyyn perustuvien ja sopimusperusteisten velvoitteiden tunnistamiseen, noudattamiseen ja noudattamisen osoittamiseen.

1.2 Politiikka määrittää selkeät vastuut ja käytännön toimenpiteet, joiden avulla liiketoiminta täyttää vaatimustenmukaisuusvelvoitteensa, mukaan lukien tietosuojalainsäädäntö, kyberturvallisuuden viitekehykset, asiakassopimukset ja sertifiointivaatimukset.

1.3 Politiikalla varmistetaan, että liiketoiminta voi myös ilman erillistä vaatimustenmukaisuustiimiä ylläpitää oikeudellisesti kestävää toimintaa, reagoida asianmukaisesti poikkeamiin ja säilyttää auditointivalmiuden.

1.4 Tämä politiikka on olennainen ISO/IEC 27001:2022 -sertifioinnin mahdollistamiseksi sekä asiakkaiden, viranomaisten ja kumppaneiden ulkoisten odotusten täyttämiseksi.

2. Soveltamisala

2.1 Tätä politiikkaa sovelletaan seuraaviin:

2.1.1 kaikkiin työntekijöihin, urakoitsijoihin, freelancereihin ja kolmansiin osapuoliin

2.1.2 kaikkiin palveluihin, toimintoihin, järjestelmiin ja tietojenkäsittelytoimiin, joissa organisaation on täytettävä lakisääteisiä tai sopimusperusteisia vaatimuksia

2.1.3 kaikkiin sijainteihin ja laitteisiin, joita käytetään liiketoimintatietojen käsittelyyn riippumatta siitä, tapahtuuko käsittely toimistossa, etänä vai pilvipalveluissa

2.2 Politiikka kattaa seuraavat osa-alueet:

2.2.1 tietosuojalainsäädäntö, kuten EU:n GDPR

2.2.2 kyberturvallisuutta koskeva sääntely, kuten EU:n NIS2-direktiivi

2.2.3 toimialakohtaiset velvoitteet soveltuvin osin

2.2.4 asiakassopimukset, salassapitosopimusten (NDA) ehdot ja auditointilausekkeet

2.2.5 vapaaehtoiset sertifioinnit (esim. ISO 27001) ja sisäiset politiikat, joita sovelletaan vaatimustenmukaisuuden varmistamiseksi

3. Tavoitteet

3.1 Vastuun selkeys: Määritetään selkeä vastuu lakisääteisten, sääntelyyn perustuvien ja sopimusperusteisten velvoitteiden seurannasta, päivittämisestä ja soveltamisesta.

3.2 Liiketoiminnan suojaaminen: Minimoidaan lainrikkomusten, seuraamusmaksujen, tietomurtojen ja mainehaittojen riski.

3.3 Auditointivalmius: Ylläpidetään todennettavat tallenteet siitä, miten organisaatio täyttää vaatimustenmukaisuusvelvoitteensa.

3.4 Politiikkojen yhteensovittamisen tukeminen: Varmistetaan, että lakisääteisiä ja sääntelyyn perustuvia velvoitteita sovelletaan johdonmukaisesti kaikissa politiikoissa ja prosesseissa.

3.5 Poikkeusten läpinäkyvä hallinta: Varmistetaan, että kaikki vaatimustenmukaisuuteen liittyvät poikkeukset dokumentoidaan, perustellaan ja hyväksytään vastuuriskien välttämiseksi.

4. Roolit ja vastuut

4.1 Toimitusjohtaja

4.1.1 Vastaa kokonaisuudessaan organisaation laki- ja sääntelyvaatimusten noudattamisesta.

4.1.2 Ylläpitää vaatimustenmukaisuusrekisteriä ja varmistaa, että se on ajan tasalla.

4.1.3 Katselmoi asiakassopimukset ja varmistaa, että erityisiä velvoitteita seurataan ja sovelletaan.

4.1.4 Hyväksyy poikkeukset vaatimustenmukaisuusvelvoitteista vain silloin, kun ne ovat oikeudellisesti perusteltavissa ja niille on määritetty korvaavat kontrollit.

4.2 Ulkoiset neuvonantajat (esim. oikeudelliset, IT- tai vaatimustenmukaisuusasiantuntijat)

4.2.1 Tukevat toimitusjohtajaa sovellettavien lakien, sertifiointien ja velvoitteiden tunnistamisessa (esim. GDPR, NIS2, ISO 27001).

4.2.2 Antavat ohjeistusta uusien säädösten tai voimassa olevan lainsäädännön muutosten tulkintaan.

4.2.3 Voivat avustaa politiikkapäivityksissä, auditoinneissa tai tietoturvaloukkausten käsittelyssä, kun asiaan liittyy oikeudellista riskiä.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Säännöllinen vuosittainen katselmointi

9.1.1 Toimitusjohtajan on katselmoitava tämä politiikka 12 kuukauden välein.

9.1.2 Katselmoinnissa on varmistettava:

9.1.2.1 politiikan ajantasaisuus suhteessa voimassa olevaan oikeudelliseen ja sopimusperusteiseen toimintaympäristöön

9.1.2.2 asiakassopimusten ja palveluvelvoitteiden asianmukainen huomiointi

9.1.2.3 yhdenmukaisuus vaatimustenmukaisuusrekisterin ja muiden politiikkojen kanssa

9.2 Tapahtumaperusteiset päivitykset

9.2.1 Välitön katselmointi on tehtävä, jos:

9.2.1.1 uusi laki tai sääntelyvaatimus tulee sovellettavaksi (esim. uusi tietosuojasääntö)

9.2.1.2 asiakas lisää sopimukseensa monimutkaisia vaatimustenmukaisuusehtoja

9.2.1.3 tapahtuu rikkomus tai vaatimustenvastaisuuteen liittyvä poikkeama

9.2.1.4 yritys laajenee säännellylle markkinalle tai toimialalle

9.3 Päivitysten hyväksyntä ja versionhallinta

9.3.1 Kaikki päivitykset on dokumentoitava, versioitava ja toimitusjohtajan hyväksyttävä.

9.3.2 Historialliset versiot on säilytettävä auditointi- ja oikeudellisia tarkoituksia varten.

9.4 Muutoksista tiedottaminen

9.4.1 Henkilöstölle ja urakoitsijoille on tiedotettava politiikkamuutoksista viiden työpäivän kuluessa hyväksynnästä.

9.4.2 Kaikkien vaikutuksen piirissä olevien toimittajien on myös kuitattava päivitetyt ehdot ennen palvelun tuottamisen jatkamista.

10. Liittyvät politiikat ja yhteydet

10.1 Tätä politiikkaa tukevat ja toimeenpanevat seuraavat pk-yrityksen politiikat:

10.1.1 P3S – hyväksyttävän käytön politiikka: ehkäisee toimintaa, joka voi rikkoa lakisääteisiä tai sopimusperusteisia ehtoja (esim. luvaton tiedostojen jakaminen)

10.1.2 P8S – tietoturvatietoisuus- ja koulutuspolitiikka: kouluttaa henkilöstöä vaatimustenmukaisuusvelvoitteista ja rikkomusten välttämisestä

10.1.3 P14S – Tietojen säilytys- ja hävityspolitiikka: varmistaa lainmukaiset tietojenkäsittelykäytännöt koko tiedon elinkaaren ajan

10.1.4 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: täyttää GDPR:n ja asiakkaiden tietojenkäsittelyä koskevat vaatimukset

10.1.5 P30S – Tietoturvapoikkeamien hallintapolitiikka: määrittää toimintatavan henkilötietojen tietoturvaloukkauksiin tai vaatimustenmukaisuuden laiminlyönteihin reagoinnissa, mukaan lukien ilmoitusmääräajat

10.1.6 P36S – Sosiaalisen median ja ulkoisen viestinnän politiikka: varmistaa, että julkinen viestintä ei riko lakisääteisiä tai sääntelyyn perustuvia velvoitteita

10.2 Kukin linkitetty politiikka toteuttaa osan laki- ja sääntelyvaatimusten noudattamisen viitekehyksestä, ja niitä on sovellettava yhdessä.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Lauseke 6.1 – Toimenpiteet riskien ja mahdollisuuksien käsittelemiseksi: sisältää vaatimustenmukaisuusriskit

11.1.2 Lauseke 8.1 – Toiminnan suunnittelu ja ohjaus: edellyttää sellaisten prosessien toteuttamista, jotka täyttävät lakisääteiset ja sopimusperusteiset vaatimukset

11.2 ISO/IEC 27002

11.2.1 Kontrolli 5.36 – ohjaa organisaatiota velvoitteita koskevien tallenteiden ylläpitämisessä ja asianmukaisen reagoinnin varmistamisessa laki- ja sääntelyvaatimuksiin

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Policy and Procedures: edellyttää muodollisia vaatimustenmukaisuuspolitiikkoja

11.3.2 PM-1 – Information Security Program Plan: edellyttää laki- ja sääntelyvaatimusten integrointia tietoturvan suunnitteluun

11.3.3 CA-1 – Assessment, Authorization, and Monitoring

11.3.4 AU-1 – Audit Policy: edellyttää vaatimustenmukaisuusnäytön ylläpitämistä

11.4 EU:n GDPR

11.4.1 Artikla 5 – henkilötietojen käsittelyn periaatteet, mukaan lukien osoitusvelvollisuus

11.4.2 Artikla 6 – käsittelyn oikeusperuste

11.4.3 Artikla 32 – käsittelyn turvallisuus

11.4.4 Artikla 33 – henkilötietojen tietoturvaloukkauksesta ilmoittaminen 72 tunnin kuluessa

11.5 EU:n NIS2-direktiivi

11.5.1 Artikla 21(2)(a) ja (f) – sisäiset politiikat riskien ja sääntelyyn liittyvän hallinnan tueksi

11.5.2 Artikla 23 – vaatimustenvastaisuuteen liittyvä valvonta ja seuraamukset

11.6 EU:n DORA-asetus

11.6.1 Artikla 5(2) – ICT-riskien hallinnan valvonta

11.6.2 Artikla 9(1) – vaatimustenmukaisuuden sisäinen hallinta

11.6.3 Artikla 17 – sopimusjärjestelyt ICT-palveluntarjoajien kanssa

11.7 COBIT 2019

11.7.1 APO12 – Managed Risk: varmistaa, että vaatimustenmukaisuusriskit tunnistetaan ja niitä käsitellään

11.7.2 APO13 – Managed Security: kattaa sääntely- ja sopimusvaatimusten riskiperusteisen soveltamisen

11.7.3 DSS01 – Managed Operations: edellyttää operatiivista valmiutta lakisääteisten velvoitteiden täyttämiseksi