					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P01S					Asiakirjan nimi: **Tietoturvapolitiikka**							
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	Kohta/artikla	Huomio
ISO/IEC 27001:2022	Kohdat 5.1, 5.2, 5.3, 6.1, 6.2, 8	Määrittää johdon sitoutumisen, politiikkavaatimukset, roolien osoittamisen, riskien arvioinnin ja operatiivisen ohjauksen
ISO/IEC 27002:2022	Kontrollit 5.1–5.5	Määrittää dokumentoitujen tietoturvapolitiikkojen laatimisen, roolien osoittamisen, tehtävien eriyttämisen ja johdon vastuut
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Asettaa vaatimukset tietoturvaohjelman suunnitelmalle, tietoturvasuunnittelun politiikalle, arviointi- ja valtuutusmenettelyille sekä pääsynhallinnalle
EU:n GDPR (2016/679)	Artikla 5(2), artikla 32	Osoitusvelvollisuusperiaate ja käsittelyn turvallisuutta koskevat toimenpiteet, erityisesti dokumentoitujen roolien osalta
EU:n NIS2-direktiivi (2022/2555)	Artikla 21(2)(a)	Edellyttää kyberturvallisuusriskien hallintatoimenpiteitä sekä roolien ja vastuiden määrittämistä
EU:n DORA-asetus (2022/2554)	Artikla 9, artikla 10	Edellyttää roolien osoittamista tieto- ja viestintätekniikkariskien hallintaan ja liiketoiminnan jatkuvuuden varmistamiseen
COBIT 2019	EDM03, APO13, DSS05	Varmistaa riskien optimoinnin, tietoturvan hallinnan ja tietoturvapalvelujen hallinnan selkeän vastuunjaon avulla

1. Tarkoitus

1.1 Tämä politiikka osoittaa organisaatiomme sitoutumisen asiakas- ja liiketoimintatietojen suojaamiseen määrittämällä vastuut ja käytännön turvatoimet selkeästi tavalla, joka soveltuu organisaatioille, joilla ei ole erillistä IT-tiimiä.

1.2 Tämä politiikka varmistaa, että kaikki työntekijät, alihankkijat ja palveluntarjoajat noudattavat velvoittavia sääntöjä, mikä mahdollistaa ISO/IEC 27001 -sertifioinnin vaatimusten täysimääräisen noudattamisen.

1.3 Tämä politiikka auttaa organisaatiotamme rakentamaan asiakkaiden luottamusta osoittamalla selkeästi, miten suojaamme heidän tietojaan määriteltyjen vastuiden, jäsenneltyjen prosessien ja selkeän vastuunjaon avulla.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia henkilöitä, jotka käsittelevät tai hallinnoivat organisaation tietoja ja järjestelmiä, mukaan lukien:

2.1.1 liiketoiminnan omistajat ja toimitusjohtaja

2.1.2 työntekijät, alihankkijat ja harjoittelijat

2.1.3 ulkoiset IT-palveluntarjoajat tai konsultit

2.2 Tämä politiikka kattaa kaikki tiedot, järjestelmät ja palvelut, mukaan lukien:

2.2.1 liiketoiminnan tallenteet, asiakastiedot, salasanat ja sähköpostit

2.2.2 IT-laitteet, kuten kannettavat tietokoneet ja puhelimet

2.2.3 pilvipalvelut, joita käytetään tiedostojen tallentamiseen, viestintään tai taloushallintoon

2.2.4 toimipaikoissa säilytettävät fyysiset asiakirjat

2.3 Tätä politiikkaa sovelletaan kaikissa työympäristöissä — toimistossa, etätyössä ja pilviympäristöissä — ja se kattaa kaikki laitteet ja ohjelmistot, joita käytetään liiketoimintatietojen käsittelyyn tai tallentamiseen.

3. Tavoitteet

3.1 Selkeä vastuunjako: Varmistetaan, että tietoturvalle on aina nimetty vastuuhenkilö. Tämä on tyypillisesti toimitusjohtaja tai hänen virallisesti nimeämänsä henkilö.

3.2 Asiakas- ja liiketoimintatietojen suojaaminen: Toteutetaan luotettavat ja yhdenmukaiset suojatoimet, joilla estetään arkaluonteisten tietojen, mukaan lukien asiakas- ja taloustietojen, väärinkäyttö, häviäminen tai anastaminen.

3.3 ISO/IEC 27001 -sertifioinnin tukeminen: Mahdollistetaan, että organisaatio voi osoittaa ISO/IEC 27001 -vaatimusten täysimääräisen noudattamisen ja ylläpitää auditointivalmiutta ilman monimutkaista infrastruktuuria.

3.4 Tietoturvan sisällyttäminen liiketoimintaan: Sisällytetään tietoturva osaksi organisaation päivittäistä toimintaa ja päätöksentekoa.

3.5 Tietoturvatietoisuuden ja -kulttuurin vahvistaminen: Varmistetaan, että jokainen työntekijä ymmärtää ja noudattaa tietoturvakäytäntöjä, kuten vahvojen salasanojen käyttöä ja epäilyttävän toiminnan ilmoittamista.

4. Roolit ja vastuut

4.1 Toimitusjohtaja tai liiketoiminnan omistaja

4.1.1 Vastaa tietoturvasta kokonaisuudessaan.

4.1.2 Hyväksyy tämän politiikan ja vastaa sen ylläpidosta.

4.1.3 Varmistaa, että kaikki keskeiset tietoturvatehtävät hoidetaan joko suoraan tai delegoidaan kirjallisesti.

4.1.4 Varmistaa, että mahdolliset delegoidut tietoturvatehtävät, kuten käyttöoikeuksien hallinta tai poikkeamiin reagointi, toteutetaan tehokkaasti.

4.1.5 Toimii ensisijaisena yhteyshenkilönä kaikissa sisäisissä ja ulkoisissa tietoturva-asioissa, mukaan lukien auditoinnit ja asiakaskyselyt.

4.1.6 Seuraa tavoitteiden toteutumista vuosittaisen katselmoinnin yhteydessä. Tavoitteiden on oltava mahdollisuuksien mukaan mitattavia (esim. koulutettujen työntekijöiden osuus, raportoitujen poikkeamien määrä), ja niitä on päivitettävä tietoturvahavaintojen ja riskimuutosten perusteella.

4.2 Nimetty työntekijä (tarvittaessa)

4.2.1 Voi tukea toimitusjohtajaa päivittäisten tehtävien hoidossa, kuten käyttäjätunnusten luomisessa, käyttöoikeuksien poistamisessa työsuhteen päättyessä tai yhteistyössä IT-palveluntarjoajan kanssa.

4.2.2 Hänet on nimettävä virallisesti, ja hänellä on oltava riittävä toimivalta sekä tarvittavat työvälineet tehtäviensä hoitamiseen.

4.2.3 Raportoi havaitut ongelmat toimitusjohtajalle.

[... 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 on katselmoitava tämä politiikka vähintään kerran vuodessa varmistaakseen ISO/IEC 27001 -sertifioinnin vaatimusten jatkuvan noudattamisen, sääntelymuutosten (kuten EU:n GDPR:n, EU:n NIS2-direktiivin ja EU:n DORA-asetuksen) huomioimisen sekä liiketoiminnan muuttuvat tarpeet.

9.2 Välikatselmoinnit

9.2.1 Lisäkatselmointeja on tehtävä aina, kun tapahtuu merkittäviä muutoksia, kuten:

9.2.1.1 merkittäviä tietoturvapoikkeamia tai tietomurtoja

9.2.1.2 uusien liiketoimintaprosessien tai teknologioiden käyttöönotto (esim. uudet ohjelmistot, etätyöalustat tai pilvipalvelut)

9.2.1.3 tietojen käsittelyyn vaikuttavat oikeudellisten tai sääntelyvaatimusten muutokset

9.3 Muutosten dokumentointi

9.3.1 Kaikki politiikan katselmoinnit ja muutokset on dokumentoitava virallisesti siten, että päivämäärä, muutosten sisältö ja toimitusjohtajan hyväksyntä käyvät selkeästi ilmi.

9.3.2 Politiikkaversioiden historiatiedot on säilytettävä turvallisesti, jotta politiikan kehittyminen ja vaatimustenmukaisuus voidaan osoittaa auditoinneissa.

9.4 Päivitysten viestintä

9.4.1 Kaikista tähän politiikkaan tehdyistä muutoksista on tiedotettava viipymättä kaikille työntekijöille, alihankkijoille ja asiaankuuluville kolmansille osapuolille.

9.4.2 Päivitettyjen politiikkaversioiden on oltava helposti saatavilla kaikille henkilöille, joita politiikka koskee (esim. sähköisesti jaettuna tai fyysisesti työpaikalla nähtävillä).

10. Liitännäiset politiikat ja yhteydet

10.1 Tämä politiikka liittyy läheisesti organisaation pk-yrityksille tarkoitettuun politiikkakokonaisuuteen, erityisesti seuraaviin politiikkoihin:

10.1.1 P2S – Hallintoroolien ja vastuiden politiikka: Täsmentää tietoturvatehtävien ja vastuiden osoittamista.

10.1.2 P4S – Pääsynhallintapolitiikka: Määrittää organisaation tietoihin kohdistuvan pääsyn turvallisen hallinnan.

10.1.3 P8S – Tietoturvatietoisuuden ja koulutuksen politiikka: Sisältää henkilöstön koulutusta ja tietoisuutta koskevat keskeiset ohjeet.

10.1.4 P17S – Tietosuojan ja yksityisyydensuojan politiikka: Varmistaa EU:n GDPR:n ja muun tietosuojalainsäädännön noudattamisen.

10.1.5 P30S – Poikkeamien hallintapolitiikka: Kuvaa yksityiskohtaiset toimenpiteet, joita tietoturvapoikkeamiin reagointi edellyttää.

10.2 Nämä liitännäiset politiikat antavat selkeää operatiivista ohjausta, ja ne on toteutettava kokonaisuutena, jotta ISO/IEC 27001 -sertifioinnin vaatimusten täysimääräinen noudattaminen voidaan saavuttaa.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Kohta 5.1 – Johtajuus ja sitoutuminen: Edellyttää ylimmän johdon sitoutumista ja vastuuta tietoturvan vaikuttavuudesta organisaatiossa.

11.1.2 Kohta 5.2 – Tietoturvapolitiikka: Edellyttää selkeitä, dokumentoituja politiikkoja, jotka ovat linjassa organisaation strategian ja vaatimustenmukaisuusvaatimusten kanssa.

11.1.3 Kohta 5.3 – Organisaation roolit ja vastuut: Määrittää tietoturvavastuiden selkeän osoittamisen koko organisaatiossa, mikä on olennaista tehokkaan hallinnan ja auditointien kannalta.

11.1.4 Kohta 6.1 – Toimet riskien ja mahdollisuuksien käsittelemiseksi: Varmistaa, että tietoturvariskit tunnistetaan, arvioidaan ja käsitellään järjestelmällisesti.

11.1.5 Kohta 8.1 – Operatiivinen suunnittelu ja ohjaus: Edellyttää, että organisaatio suunnittelee ja toteuttaa prosessit, joita tarvitaan tietoturvatavoitteiden saavuttamiseksi ja niihin liittyvien riskien tehokkaaksi hallitsemiseksi.

11.2 ISO/IEC 27002:2022 kontrollit 5.1–5.5

11.2.1 Liite A:n kontrolli 5.1 – Tietoturvapolitiikat: Määrittää dokumentoitujen tietoturvapolitiikkojen laatimisen ja viestimisen.

11.2.2 Liite A:n kontrolli 5.2 – Tietoturvaroolit: Täsmentää ja osoittaa virallisesti tietoturvaroolit ja -vastuut asiaankuuluville osapuolille.

11.2.3 Liite A:n kontrolli 5.3 – Tehtävien eriyttäminen: Edellyttää tehtävien selkeää eriyttämistä eturistiriitojen ja petosriskien vähentämiseksi arkaluonteisten tietojen hallinnassa.

11.2.4 Liite A:n kontrolli 5.4 – Johdon vastuut: Edellyttää, että johto osoittaa sitoutumisensa tietoturvaan aktiivisen valvonnan ja resurssien osoittamisen avulla.

11.2.5 Liite A:n kontrolli 5.5 – Yhteydenpito viranomaisiin: Korostaa tarvetta määrittää asianmukaiset yhteydenpitomenettelyt viranomaisten kanssa tarvittaessa.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Tietoturvaohjelman suunnitelma: Edellyttää dokumentoituja tietoturvan hallintastrategioita ja politiikkoja, jotka muodostavat viitekehyksen johdonmukaiselle toteutukselle ja hallinnalle.

11.3.2 PL-1 – Tietoturvasuunnittelun politiikka: Edellyttää koko organisaation kattavaa tietoturvasuunnittelun politiikkaa turvallisen toiminnan ja tietoturvatoimintojen strategisen yhdenmukaisuuden ohjaamiseksi.

11.3.3 CA-1 – Tietoturvan arviointi- ja valtuutuspolitiikka: Edellyttää selkeästi määriteltyjä arviointi- ja valtuutusrooleja tietoturvavaatimusten jatkuvan tehokkuuden ja noudattamisen varmistamiseksi.

11.3.4 AC-1 – Pääsynhallintapolitiikka: Edellyttää, että organisaatiot määrittävät, dokumentoivat ja toimeenpanevat pääsynhallinnan käytännöt ja vastuut selkeästi.

11.4 EU:n GDPR (2016/679)

11.4.1 Artikla 5(2) – Osoitusvelvollisuusperiaate: Edellyttää, että organisaatiot voivat osoittaa noudattavansa tietosuojaperiaatteita, mukaan lukien tietosuojavastuiden dokumentoidut roolit ja politiikat.

11.4.2 Artikla 32 – Käsittelyn turvallisuus: Edellyttää asianmukaisten teknisten ja organisatoristen toimenpiteiden toteuttamista, mukaan lukien selkeät tietoturvavastuut, henkilötietojen suojaamiseksi tietoturvaloukkauksilta ja luvattomalta pääsyltä.

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

11.5.1 Artikla 21(2)(a) – Riskienhallintatoimenpiteet: Edellyttää selkeitä hallintajärjestelyjä, mukaan lukien määritellyt tietoturvaroolit ja -vastuut, jotka ovat olennaisia kyberturvallisuusriskien tehokkaassa hallinnassa.

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

11.6.1 Artikla 9 – Tieto- ja viestintätekniikkariskien hallinta: Edellyttää, että organisaatiot osoittavat selkeästi tieto- ja viestintätekniikkariskien hallintaan liittyvät roolit ja vastuut sekä vahvistavat häiriönsietokykyä ja jatkuvuusvalmiutta.

11.6.2 Artikla 10 – Tieto- ja viestintätekniikan liiketoiminnan jatkuvuus: Edellyttää selkeää vastuunjakoa ja jäsenneltyjä rooleja tieto- ja viestintätekniikan häiriönsietokyvyn ja jatkuvuuden ylläpitämiseksi, jotta organisaatiot voivat reagoida häiriöihin luotettavasti.

11.7 COBIT 2019

11.7.1 EDM03 – Varmista riskien optimointi: Korostaa selkeästi määriteltyä vastuuta ja rooleja organisaation riskienhallinnassa sekä tukee vahvaa hallintaa ja tehokasta tietoturvariskien valvontaa.

11.7.2 APO13 – Hallitse tietoturvaa: Edellyttää, että organisaatiot määrittävät ja viestivät tietoturvan hallinnan vastuut selkeästi varmistaen yhdenmukaisuuden liiketoimintatavoitteiden ja sääntelyvaatimusten kanssa.

11.7.3 DSS05 – Hallitse tietoturvapalveluja: Edellyttää jäsenneltyjä rooleja ja selkeitä vastuita tietoturvapalvelujen hallinnassa, mikä mahdollistaa johdonmukaisen toteutuksen ja vaatimustenmukaisuuden todentamisen.