					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P09S					Asiakirjan nimi: **Etätyöpolitiikka**							
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	Kohta 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontrolli 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
EU:n NIS2-direktiivi	Artikla 21(2)(b), 21(2)(h)	EU:n NIS2-direktiivi
EU:n DORA-asetus	Artikla 9	EU:n DORA-asetus
COBIT 2019	DSS05, APO13	COBIT 2019
EU:n GDPR	Artikla 32	EU:n GDPR

1. Tarkoitus

1.1 Tämä politiikka määrittää tietoturvavaatimukset työntekijöille ja sopimuskumppaneille, jotka työskentelevät etänä, mukaan lukien kotoa, yhteiskäyttöisissä työtiloissa tai matkustaessa.

1.2 Tämän politiikan tarkoituksena on suojata liiketoimintatietojen luottamuksellisuus, eheys ja saatavuus silloin, kun tietoja käsitellään yrityksen hallitsemien ympäristöjen ulkopuolella.

1.3 Tämä politiikka varmistaa vaatimustenmukaisuuden kansainvälisten standardien ja sääntelyvaatimusten kanssa sekä vähentää riskejä, kuten luvatonta pääsyä, tietojen menetystä ja palvelukatkoksia.

2. Soveltamisala

2.1 Tätä politiikkaa sovelletaan kaikkiin henkilöstöryhmiin (työntekijät, sopimuskumppanit, konsultit ja määräaikaiset työntekijät), jotka käyttävät yrityksen järjestelmiä, verkkoja tai tietoja työskennellessään yrityksen toimipaikkojen ulkopuolella.

2.2 Politiikka kattaa:

2.2.1 yrityksen tarjoamien ja henkilökohtaisten laitteiden käytön

2.2.2 pääsyn VPN-yhteyden, etätyöpöytäyhteyden tai pilvipalvelujen kautta

2.2.3 tietojen turvallisen käsittelyn yrityksen tilojen ulkopuolella

2.2.4 seurannan, poikkeusten käsittelyn ja soveltamisen

2.3 Tätä politiikkaa sovelletaan sekä kokoaikaisiin että osa-aikaisiin etätyöjärjestelyihin, mukaan lukien tilapäinen etäkäyttö.

3. Tavoitteet

3.1 Estää luvaton pääsy yrityksen järjestelmiin tai arkaluonteisiin tietoihin etätyön aikana.

3.2 Varmistaa, että toimiston ulkopuolella käytettävät laitteet ja tietoliikenneyhteydet täyttävät perustason tietoturvavaatimukset.

3.3 Ylläpitää etäkäyttöoikeuksien hallintaa ja seurantaa.

3.4 Antaa työntekijöille ja esihenkilöille selkeät ohjeet turvallisiin etätyökäytäntöihin.

3.5 Täyttää ISO-standardien, NIS2:n, GDPR:n, DORA:n ja COBITin etä- ja mobiilityötä koskevat vaatimukset.

4. Roolit ja vastuut

4.1 Toimitusjohtaja

4.1.1 Hyväksyy etätyöjärjestelyt ja valvoo politiikan noudattamista.

4.1.2 Eskaloi tietoturvapoikkeamat ja toistuvan noudattamatta jättämisen.

4.1.3 Katselmoi poikkeukset ja varmistaa korjaavien toimenpiteiden toteuttamisen.

4.2 IT-tukipalveluntarjoaja tai ulkoinen IT-palveluntarjoaja

4.2.1 Ottaa käyttöön turvallisen etäkäytön (esim. VPN, monivaiheinen todennus).

4.2.2 Toteuttaa päätelaitesuojauksen, salauksen ja laitemääritysten vaatimukset.

4.2.3 Tukee käyttäjiä ja selvittää tekniset tietoturvaongelmat.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Politiikan vuosittainen katselmointi

9.1.1 Toimitusjohtajan ja IT-tuen on katselmoitava tämä politiikka vuosittain, jotta se pysyy yhdenmukaisena teknologian, henkilöstön ja oikeudellisten vaatimusten muutosten kanssa.

9.2 Ennenaikaisen päivityksen käynnistävät tapahtumat

9.2.1 Välitön katselmointi vaaditaan seuraavien jälkeen:

9.2.1.1 merkittävä etätyöhön liittyvä tietoturvapoikkeama

9.2.1.2 muutokset NIS2:n, GDPR:n tai DORA:n vaatimuksissa

9.2.1.3 siirtyminen uuteen etäkäyttöteknologiaan (esim. eri VPN-alusta)

9.3 Versionhallinta ja arkistointi

9.3.1 Kaikkien tämän politiikan versioiden on oltava:

9.3.1.1 päivättyjä ja toimitusjohtajan hyväksymiä

9.3.1.2 versionumeroituja

9.3.1.3 arkistoituja vähintään kolmen vuoden ajaksi

9.4 Henkilöstöviestintä

9.4.1 Politiikkapäivityksistä on tiedotettava kaikille etäkäyttäjille. Merkittävistä muutoksista vaaditaan kuittaus.

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka liittyy seuraaviin politiikkoihin ja tukee niitä:

10.1.1 P2S – Hallintoroolien ja vastuiden politiikka: määrittää, kuka valtuuttaa etäkäytön ja vastaa sen valvonnasta

10.1.2 P4S – Pääsynhallintapolitiikka: määrittää turvallisen etäkäytön käyttöönoton ja käyttöoikeuksien poistamisen menettelyt

10.1.3 P6S – Riskienhallintapolitiikka: seuraa ja arvioi yrityksen toimipaikkojen ulkopuoliseen käyttöön liittyviä riskejä

10.1.4 P8S – Tietoturvatietoisuus- ja koulutuspolitiikka: kouluttaa käyttäjiä etätyön riskeistä ja parhaista käytännöistä

10.1.5 P30S – Tietoturvapoikkeamien hallintapolitiikka: ohjaa etäkäyttöön liittyviin poikkeamiin reagointia, kuten tunnistetietojen vuotamista tai laitteen katoamista

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Kohta 6.1 – Riskiperusteinen suunnittelu etäkäyttöskenaarioita varten

11.1.2 Kohta 6.2 – Käsittelee henkilöstöhallinnon vastuita mobiili- ja etätyöympäristöissä

11.1.3 Kohta 8.1 – Etäprosessien operatiivinen suunnittelu ja hallinta

11.2 ISO/IEC 27002

11.2.1 Kontrolli 6.7 – Antaa käytännön ohjeita etä- ja mobiilityön turvallisuudesta

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – Etäkäytön hallinta, istuntojen suojaus ja tietoturvan seuranta

11.3.2 AC-2 – Tilien hallinta yrityksen toimipaikkojen ulkopuolisille käyttäjille

11.4 EU:n GDPR

11.4.1 Artikla 32 – Edellyttää tietosuojaa suunnittelun ja oletusarvojen mukaisesti myös etäympäristöissä

11.5 EU:n NIS2-direktiivi

11.5.1 Artikla 21(2)(b) – Edellyttää verkko- ja tietojärjestelmien turvallista käyttöä

11.5.2 Artikla 21(2)(h) – Edellyttää henkilöstöön liittyviä tietoturvatoimenpiteitä, mukaan lukien toimipaikan ulkopuoliset kontrollit

11.6 EU:n DORA-asetus

11.6.1 Artikla 9 – Edellyttää, että finanssialan toimijat ylläpitävät ICT-häiriönsietokykyä kaikissa toimintamalleissa, mukaan lukien etäkäyttö

11.7 COBIT 2019

11.7.1 DSS05 – Tietoturvapalveluiden hallinta: sisältää päätelaitesuojauksen ja turvalliset etätyökäytännöt

11.7.2 APO13 – Hallittu tietoturva: varmistaa mobiili- ja etäkäytön turvallisen käyttöoikeuksien myöntämisen ja riskien valvonnan