					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P09					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**

1. Tarkoitus

1.1 Tämä politiikka määrittää pakolliset vaatimukset etätyön turvalliselle toteuttamiselle, mukaan lukien organisaation järjestelmien käyttö, tietojen käyttö ja työtehtävien suorittaminen organisaation toimitilojen ulkopuolella.

1.2 Politiikka varmistaa etäkäytössä olevien tietovarojen luottamuksellisuuden, eheyden ja saatavuuden toteutumisen sekä määrittää kontrollit hajautettuihin työympäristöihin liittyvien riskien lieventämiseksi.

1.3 Tämä politiikka täyttää ISO/IEC 27001:2022 -standardin liitteen A kontrollin 6.7 vaatimukset ottamalla käyttöön etätyöolosuhteisiin sovitetut tekniset ja menettelylliset suojatoimet.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkea henkilöstöä, jolla on valtuutus tehdä etätyötä, mukaan lukien:

2.1.1 työntekijät (vakituinen, osa-aikainen, sopimussuhteinen)

2.1.2 ulkoiset palveluntarjoajat, konsultit ja toimittajat

2.1.3 määräaikaiset työntekijät ja projektikohtainen henkilöstö, joilla on hyväksytty etäkäyttö

2.2 Politiikka kattaa:

2.2.1 pääsyn organisaation järjestelmiin VPN-yhteyden tai hyväksyttyjen etäkäyttötyökalujen kautta

2.2.2 arkaluonteisten ja sääntelyn alaisten tietojen käsittelyn turvallisten tilojen ulkopuolella

2.2.3 organisaation omistamien laitteiden tai omien laitteiden käytön (BYOD)

2.2.4 fyysiset ja loogiset suojaustoimenpiteet etäympäristöissä

2.3 Tätä politiikkaa sovelletaan kaikilla maantieteellisillä alueilla ja aikavyöhykkeillä, joilla organisaatio sallii etätyön, riippumatta siitä, onko kyse säännöllisestä, tilapäisestä vai liiketoiminnan jatkuvuuteen liittyvästä etätyöstä.

3. Tavoitteet

3.1 Varmistaa, että vain valtuutetut henkilöt voivat käyttää sisäisiä järjestelmiä ja tietoja etänä.

3.2 Varmistaa salauksen, monivaiheisen tunnistautumisen (MFA) ja päätelaitesuojausten soveltaminen kaikissa etäkäytön yhteyksissä.

3.3 Ylläpitää turvallista tietoturvatasoa tietojenkalastelun, haittaohjelmien, tietojen luvattoman siirron ja järjestelmien luvattoman altistumisen kaltaisia uhkia vastaan.

3.4 Määrittää, miten arkaluonteisia tietoja siirretään, säilytetään ja tulostetaan organisaation toimipaikan ulkopuolisissa ympäristöissä.

3.5 Ottaa käyttöön fyysiset suojatoimet, jotka vähentävät näkyvyyttä ja luvatonta havainnointia etäistuntojen aikana.

3.6 Varmistaa kansainvälisten etätietojen käyttöä koskevien sääntelyvaatimusten noudattamisen, mukaan lukien EU:n GDPR, EU:n NIS2-direktiivi ja EU:n DORA-asetus.

4. Roolit ja vastuut

4.1 Ylin johto

4.1.1 hyväksyy tämän politiikan ja varmistaa, että sen toteuttamiseen on osoitettu riittävät resurssit ja että se on integroitu henkilöstöhallinnon, IT:n ja tietoturvaoperaatioiden toimintaan.

4.1.2 hyväksyy organisaation etätyökelpoisuuden kriteerit ja liiketoimintayksikkökohtaisen soveltamisen.

4.2 Tietoturvajohtaja (CISO) / ISMS-päällikkö

4.2.1 vastaa politiikasta ja sen ylläpidosta sekä varmistaa sen yhdenmukaisuuden riskitason ja sääntelyvaatimusten kanssa.

4.2.2 määrittää etäkäyttöä koskevat tietoturvakontrollit (esimerkiksi salaus, päätelaitesuojaus ja istunnon aikakatkaisut).

4.2.3 hyväksyy poikkeustenhallintamenettelyn ja seuraa kontrollien tehokkuutta.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Katselmointitiheys

9.1.1 Tämä politiikka on katselmoitava vuosittain tai useammin, jos jokin seuraavista toteutuu:

9.1.1.1 uusien etäkäyttöteknologioiden käyttöönotto

9.1.1.2 etätyön merkittävä laajentaminen (esimerkiksi hybridityötä koskevat aloitteet)

9.1.1.3 uusien etäympäristöihin liittyvien uhkien, haavoittuvuuksien tai poikkeamien ilmeneminen

9.1.1.4 muutokset sovellettavissa oikeudellisissa tai sääntelyyn liittyvissä viitekehyksissä

9.2 Omistajuus ja katselmointiprosessi

9.2.1 Politiikan omistaja on tietoturvajohtaja (CISO). Katselmointi on koordinoitava seuraavien kanssa:

9.2.1.1 IT-operaatiot ja arkkitehtuuri

9.2.1.2 henkilöstöhallinto ja toimitilojen hallinta (operatiivisten ja työtilaan liittyvien vaikutusten osalta)

9.2.1.3 tietosuojavastaava (yksityisyydensuojan ja rajat ylittävien tietokontrollien osalta)

9.2.2 Politiikkapäivitysten on oltava:

9.2.2.1 ISMS-ohjausryhmän hyväksymiä

9.2.2.2 viestittyjä kaikille vaikutuksen piirissä oleville työntekijöille ja sopimuskumppaneille

9.2.2.3 sisällytettyjä perehdytys- ja kertauskoulutusmateriaaleihin

9.3 Asiakirjahallinta ja jakelu

9.3.1 Politiikan on sisällettävä versionhallinta, voimaantulopäivä ja muutoshistoria.

9.3.2 Korvatut versiot on säilytettävä asiakirjahallintapolitiikan (P14) mukaisesti.

9.3.3 Tarkistetut versiot on otettava käyttöön siten, että etätyöhön oikeutettujen käyttäjien pakollinen uudelleenhyväksyntä käynnistyy.

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka toimii yhdessä seuraavien kanssa:

10.1.1 P1 – Tietoturvapolitiikka: määrittää omaisuuserien turvallisen käsittelyn perustason, jota sovelletaan kaikkiin työympäristöihin, myös etätyöhön.

10.1.2 P3 – Hyväksyttävän käytön politiikka: määrittää organisaation laitteiden ja järjestelmien asianmukaisen käytön etätyöistuntojen aikana.

10.1.3 P4 – Pääsynhallintapolitiikka: varmistaa, että etäkäyttöoikeudet noudattavat vähimmän oikeuden periaatetta ja asianmukaisia tunnistautumismekanismeja.

10.1.4 P6 – Riskienhallintapolitiikka: määrittää, miten etätyöhön liittyvät riskit tunnistetaan, käsitellään ja niitä seurataan ISMS:ssä.

10.1.5 P12 – Omaisuudenhallintapolitiikka: edellyttää kaikkien etäkäytössä käytettävien laitteiden inventointia ja konfiguraationhallintaa.

10.1.6 P22 – Lokitus- ja valvontapolitiikka: varmistaa, että etäistuntoja valvotaan, auditoidaan ja säilytetään vaatimustenmukaisuusvaatimusten mukaisesti.

10.1.7 P14 – Tietojen säilytys- ja hävityspolitiikka: määrittää etätyöhön liittyvät tietojen käsittelysäännöt, mukaan lukien siirrettävät tietovälineet ja laitteiden hävittäminen.

10.2 Nämä politiikat yhdessä varmistavat, että etätyö on turvallista, vaatimustenmukaista ja sovellettavissa kaikissa toiminnoissa ja kaikilla maantieteellisillä alueilla.

11. Viitestandardit ja viitekehykset

11.1 Tämä politiikka on yhdenmukainen kansainvälisesti tunnustettujen tietoturvan, tietosuojan ja ICT-riskien hallinnan viitekehysten kanssa, jotta etätyökäytännöt ovat turvallisia, jäljitettäviä ja vaatimustenmukaisia.

11.2 ISO/IEC 27001

11.2.1 Kohta 6.1.3 – Riskienkäsittelyn suunnittelu: tämä politiikka tukee etäkäyttöön ja hajautettuihin työympäristöihin liittyvien riskien käsittelyä.

11.2.2 Kohta 8.1 – Operatiivinen suunnittelu ja ohjaus: edellyttää kontrollien toteutusta järjestelmille, joita käytetään organisaation toimitilojen ulkopuolella.

11.2.3 Liite A, kontrolli 6.7 – Etätyö: tämä politiikka kattaa täysimääräisesti vaaditut tietoturvakontrollit tilanteissa, joissa henkilöstö työskentelee organisaation toimitilojen ulkopuolella, mukaan lukien fyysiset ja loogiset suojaustoimenpiteet, pääsyn hallinta ja käyttäjien toiminnan seuranta.

11.3 ISO/IEC 27002:2022 – Kontrolli 6

11.3.1 Tämä kontrolli edellyttää menettelyllisiä ja teknisiä suojatoimia etätyöhön. Se sisältää vaatimuksia laitteiden turvallisuudesta, pääsymenetelmistä, tietojen käsittelystä, ympäristöön liittyvistä suojatoimista ja kolmansien osapuolten osallistujien hallinnasta, jotka kaikki toteutetaan tämän politiikan kautta.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (Remote Access): toteutetaan suoraan VPN-kontrollien, MFA:n, istuntolokituksen ja etäkäyttäjien roolipohjaisen käyttöoikeuksien myöntämisen avulla.

11.4.2 AC-2 (Account Management): ohjaa käyttökelpoisuuden, etäkäyttöoikeuksien myöntämisen ja tilien poistamisen hallintaa.

11.4.3 SC-12–SC-13 (Cryptographic Protection, Cryptographic Key Establishment): toteutetaan pakollisella VPN-yhteyksien ja koko levyn salauksen käytöllä etäpäätelaitteissa.

11.4.4 MP-5 (Media Transport Protection) ja PE-18 (Location of Information System Components): etätyöohjeistus edellyttää siirron suojaamista ja fyysisiä suojatoimia organisaation toimipaikan ulkopuolisissa ympäristöissä.

11.4.5 AU-2, AU-6: etäistuntojen lokitus ja seuranta tukevat auditointi- ja tietoturvapoikkeamiin reagoinnin vaatimuksia.

11.5 EU:n GDPR (2016/679)

11.5.1 Artikla 32 – Käsittelyn turvallisuus: tämä politiikka ottaa käyttöön etäkäytön tietoturvan, salauksen ja lokituksen kontrollit, jotka ovat tarpeen etänä käytettävien tai käsiteltävien henkilötietojen suojaamiseksi.

11.5.2 Artikla 5(1)(f): varmistaa, että organisaation toimipaikan ulkopuolella käytettävät henkilötiedot suojataan luvattomalta tai lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta menettämiseltä.

11.5.3 Johdanto-osan kappale 39: korostaa pääsyn rajoittamista, eheyttä ja luottamuksellisuutta, mikä on erityisen olennaista, kun laitteet poistuvat turvallisista tiloista.

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

11.6.1 Artikla 21(2)(a, b, d): edellyttää etäkäytön suojaamista osana organisaation ICT-riskienhallinnan viitekehystä. Tämä politiikka täyttää vaatimuksen tietoturvatoimenpiteistä, jotka kattavat pääsynhallinnan, tietoturvan ja etäympäristöjä koskevat organisatoriset politiikat.

11.6.2 Artikla 21(3): edistää tietoturvatietoisuutta ja politiikan soveltamista keskitettyjen toimitilojen ulkopuolella työskentelevän henkilöstön keskuudessa.

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

11.7.1 Artikla 5 – Hallinnointi ja sisäisen valvonnan viitekehys: tämä politiikka tukee ICT-riskien hallintaa koskevia odotuksia kaikissa operatiivisissa tilanteissa, mukaan lukien hybridi- ja etätoimintamallit.

11.7.2 Artikla 8 – ICT-riskienhallinnan viitekehys: etäkäyttöön liittyvät riskit tunnistetaan, niitä lievennetään ja hallinnoidaan tässä määritettyjen teknisten ja organisatoristen kontrollien avulla.

11.7.3 Artikla 9 – Tietojenvaihtojärjestelyt: suojaa digitaalisen operatiivisen häiriönsietokyvyn verkostoissa jaettavia tietoja etäympäristöistä aiheutuvalta vuotamiselta.

11.8 COBIT 2019

11.8.1 DSS01 – Managed Operations: tämä politiikka tukee liiketoiminnan jatkuvuuden turvallista toteutumista fyysisestä sijainnista riippumatta.

11.8.2 BAI06 – Managed IT Changes ja BAI09 – Managed Assets: varmistavat, että etätyölaitteita seurataan, ne konfiguroidaan turvallisesti ja niitä käsitellään kriittisinä omaisuuserinä.

11.8.3 APO13 – Managed Security: edistää määriteltyä tietoturvan hallinnan viitekehystä etäympäristöille.

11.8.4 MEA03 – Monitor, Evaluate, and Assess Compliance: määrittää, että etätyötoiminta on lokitettava, katselmoitava ja auditoitava.