					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P10					Asiakirjan nimi: **Puhtaan pöydän ja näytön käytäntö**							
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	Lauseke 6.1.3, lauseke 8	Riskienkäsittelysuunnitelma sekä operatiivinen suunnittelu ja hallinta turvallisten työtilojen varmistamiseksi
ISO/IEC 27002:2022	Kontrolli 7	Käyttäytymiseen ja fyysiseen ympäristöön liittyvät kontrollit valvomatta jätettyjen fyysisten tietojen suojaamiseksi
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	Fyysinen pääsy, ulkopuolisen henkilöstön turvallisuus, median hävittäminen, istunnon lukitus sekä konfiguraatio- ja tunnistautumiskontrollit
EU:n GDPR	Artiklat 5(1)(f), 32; johdanto-osan kappale 39	Tietojen eheys, luottamuksellisuus ja fyysiset tietosuojatoimenpiteet
EU:n NIS2-direktiivi	Artiklat 21(2)(d), 21(3)	Fyysistä turvallisuutta, käyttäytymistä ja tietovuotojen ehkäisyä koskevat politiikat
EU:n DORA-asetus	Artiklat 5, 8, 9	Sisäinen hallinto, ICT-riskien hallinta sekä fyysiseen turvallisuuteen liittyvien poikkeamien hallinta
COBIT 2019	DSS01, DSS05, MEA	Hallitut operaatiot, tietoturvapalvelut ja vaatimustenmukaisuuden seuranta

1. Tarkoitus

1.1 Tämä politiikka määrittää pakolliset kontrollit arkaluonteisten tietojen suojaamiseksi edellyttämällä fyysisten asiakirjojen, työasemien, näyttöjen ja siirrettävien tallennusvälineiden turvallista käsittelyä toimistoissa ja yhteiskäyttöisissä työtiloissa.

1.2 Se tukee ISO/IEC 27001:n liitteen A kontrollia 7.7 toimeenpanemalla käyttäytymiseen ja teknologiaan perustuvia käytäntöjä, joilla lievennetään valvomatta jätetyistä tai näkyville jääneistä tiedoista aiheutuvaa luvattoman paljastumisen, varkauden tai tietojen menetyksen riskiä.

1.3 Tämä politiikka vahvistaa fyysistä turvallisuutta ja tietoturvaa päivittäisessä toiminnassa sekä tukee sovellettavien lakisääteisten, sopimukseen perustuvien ja sääntelyyn perustuvien velvoitteiden noudattamista.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkea henkilöstöä, joka työskentelee fyysisissä työtiloissa tai käyttää niitä, mukaan lukien:

2.1.1 vakituiset ja määräaikaiset työntekijät

2.1.2 sopimuskumppanit, konsultit, toimittajat ja harjoittelijat

2.1.3 kolmannen osapuolen palveluntarjoajat ja paikan päällä vierailevat henkilöt, joilla on pääsy arkaluonteisiin tietoihin

2.2 Vaatimuksia sovelletaan seuraavissa ympäristöissä:

2.2.1 henkilökohtaiset toimistot, työpisteet ja avotoimistot

2.2.2 neuvotteluhuoneet ja yhteiset yhteistyötilat

2.2.3 tulostuspisteet, vastaanottotiskit ja kopiointihuoneet

2.2.4 alueet, joilla käytetään etätyöasemia tai yhteiskäyttöisiä päätelaitteita

2.3 Tämä politiikka koskee myös tilapäisiä tai hybridityöympäristöjä, kuten työpisteiden yhteiskäyttöä, sekä julkisia ympäristöjä, joissa on riski sivusta seuraamisesta tai valvomatta jätetyistä tiedoista.

3. Tavoitteet

3.1 Estää luottamuksellisten, arkaluonteisten tai sääntelyn alaisten tietojen luvaton käyttö, kun niitä jää näkyville fyysisessä tai digitaalisessa muodossa.

3.2 Edistää yhdenmukaista tietoturvan tasoa kaikissa työympäristöissä fyysisten suojatoimien, työasemamääritysten ja loppukäyttäjien toiminnan avulla.

3.3 Vähentää huolimattomuudesta tai valvonnan puutteesta aiheutuvien tietosuojaloukkausten, immateriaalioikeuksien menetyksen ja tietojen luvattoman siirtämisen riskiä.

3.4 Vakiinnuttaa puhtaan pöydän ja puhtaan näytön toimintatapa osaksi organisaatiokulttuuria tukemaan operatiivista kurinalaisuutta, todennettavuutta ja oikeudellista puolustettavuutta.

3.5 Tukea ISO/IEC 27001:n, GDPR:n artiklan 32, NIS2:n artiklan 15 ja muiden kriittisiin tietoihin tai henkilötietoihin liittyvien fyysisen turvallisuuden vaatimusten noudattamista.

4. Roolit ja vastuut

4.1 Ylin johto

4.1.1 Hyväksyy tämän politiikan ja edistää tietoturvatietoista kulttuuria kaikissa liiketoimintayksiköissä.

4.1.2 Osoittaa tarkoituksenmukaiset resurssit politiikan toimeenpanoon, tietoisuuskampanjoihin ja fyysisiin kontrollimekanismeihin.

4.2 Tietoturvajohtaja (CISO) / ISMS-päällikkö

4.2.1 Vastaa tästä politiikasta ja varmistaa sen yhdenmukaisuuden ISO/IEC 27001:2022:n, auditointivaatimusten ja riskienkäsittelystrategioiden kanssa.

4.2.2 Kehittää tietoisuusohjelmia ja kontrolleja johdonmukaisen toimeenpanon varmistamiseksi toimitiloissa ja hybridityöympäristöissä.

4.2.3 Koordinoi toimitilapalveluiden ja IT:n kanssa, jotta tarkoituksenmukaiset fyysiset suojatoimet ovat käytössä.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Politiikan katselmointiaikataulu

9.1.1 Tämä politiikka on katselmoitava:

9.1.1.1 vähintään vuosittain

9.1.1.2 työtiloihin tai näytön altistumiseen liittyvän auditointipoikkeaman jälkeen

9.1.1.3 fyysiseen turvallisuuteen tai ympäristöön liittyvän poikkeaman jälkeen, kuten laitteen varkauden, perässä kulkemisen tai valvontapoikkeaman yhteydessä

9.1.1.4 uuden toimistotilaratkaisun, toimitilapolitiikan tai työskentelymallin, kuten työpisteiden yhteiskäytön tai etätyöhubien, käyttöönoton yhteydessä

9.2 Vastuutahot

9.2.1 Politiikan omistaja on tietoturvajohtaja (CISO) tai nimetty ISMS-päällikkö.

9.2.2 Katselmointiprosessiin on osallistuttava:

9.2.2.1 toimitilapalveluiden ja yritysturvallisuuden tiimien

9.2.2.2 IT:n ja infrastruktuurin laitteisiin liittyvän toimeenpanon osalta

9.2.2.3 henkilöstöhallinnon sekä laki- ja compliance-toiminnon käyttäytymisen ohjauksen ja kurinpidollisen yhdenmukaisuuden osalta

9.2.3 Kaikkien politiikkapäivitysten on oltava versiohallittuja, ISMS-ohjausryhmän hyväksymiä ja jaettavia uudelleen siten, että uusi hyväksyntä pyydetään tarvittaessa.

9.3 Muutoksista viestiminen

9.3.1 Käyttäjille on ilmoitettava olennaisista päivityksistä seuraavien kanavien kautta:

9.3.1.1 intranetin politiikkakeskus tai portaali

9.3.1.2 kohdennetut sähköpostiviestit

9.3.1.3 perehdytyksen kertaukset ja neljännesvuosittaiset tiedotustilaisuudet

9.3.1.4 pakolliset hyväksyntäkehotteet kaikkien uusien kriittisten toimeenpanolausekkeiden osalta

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka on yhdenmukainen seuraavien politiikkojen kanssa ja tukee niitä:

10.1.1 P1 – Tietoturvapolitiikka: määrittää tähän politiikkaan liittyvät käyttäytymiseen ja fyysiseen turvallisuuteen kohdistuvat odotukset.

10.1.2 P3 – Hyväksyttävän käytön politiikka: käsittelee käyttäjän vastuuta tietojen ja järjestelmien suojaamisessa, mukaan lukien fyysiset ympäristöt.

10.1.3 P6 – Riskienhallintapolitiikka: sisällyttää fyysisiin työtiloihin liittyvät riskit osaksi koko organisaation tietoriskien analysointia.

10.1.4 P12 – Omaisuudenhallintapolitiikka: tukee työpöydille jätettyjen laitteiden ja tallennusvälineiden seurantaa ja turvallista käsittelyä.

10.1.5 P13 – Tiedon luokittelu- ja merkintäpolitiikka: kytkeytyy puhtaan pöydän vaatimuksiin, kun fyysiset asiakirjat on merkitty luottamuksellisiksi tai sisäisiksi.

10.1.6 P14 – Tietojen säilytys- ja hävityspolitiikka: ohjaa fyysisten asiakirjojen säilyttämistä, silppuamista ja hävitysastioiden käsittelyä.

10.1.7 P22 – Lokitus- ja valvontapolitiikka: voidaan käyttää työasemien lukitustilan, toimettomuusajan tai työtilojen kamerasyötteiden seurantaan, kun se on sallittua.

10.2 Nämä liittyvät politiikat muodostavat integroidun tietoturvakulttuurin, jossa yhdistyvät käyttäjätietoisuus, fyysiset suojatoimet ja vastuun osoitettavuus häiriönsietokykyisten työtilojen varmistamiseksi.

11. Viitestandardit ja viitekehykset

11.1 Tämä politiikka on yhdenmukainen maailmanlaajuisesti tunnustettujen standardien ja oikeudellisten vaatimusten kanssa, jotka edellyttävät arkaluonteisten tietojen suojaamista fyysisissä ympäristöissä ja käyttäytymisen avulla.

11.2 ISO/IEC 27001

11.2.1 Lauseke 6.1.3 – riskienkäsittelysuunnitelma: tukee kontrollien toteutusta fyysisten ja ympäristöön liittyvien riskien lieventämiseksi, mukaan lukien avotyötiloissa tapahtuvaan käyttäytymiseen liittyvät riskit.

11.2.2 Lauseke 8.1 – operatiivinen suunnittelu ja hallinta: määrittää operatiiviset suojatoimet turvallisten työtilojen ja laitteiden käytön hallitsemiseksi.

11.3 ISO/IEC 27002:2022 – kontrolli 7

11.3.1 Tämä kontrolli edellyttää käyttäytymiseen ja fyysiseen ympäristöön liittyviä suojatoimia, joilla estetään tietojen luvaton käyttö valvomatta jätettyjen tallennusvälineiden, näyttöjen tai tulostettujen aineistojen kautta. Tämä politiikka toimeenpanee fyysisten työtilojen järjestystä, näytön lukitusta ja arkaluonteisten asiakirjojen hävittämistä koskevat vaatimukset.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (fyysisen pääsyn valtuutukset): kytkeytyy työtilarajoituksiin ja lukitun säilytyksen vaatimuksiin korkean riskin ympäristöissä.

11.4.2 PS-7 (ulkopuolisen henkilöstön turvallisuus): toteutuu puhtaan pöydän ja puhtaan näytön vaatimuksilla, jotka ulotetaan sopimuskumppaneihin ja kolmannen osapuolen käyttäjiin.

11.4.3 MP-6 (median puhdistus) ja AC-11 (istunnon lukitus): toteutetaan turvallisilla hävitysmenettelyillä ja pakollisilla näytön lukitusajastimilla.

11.4.4 CM-6 (konfiguraatioasetukset) ja IA-5 (todentajien hallinta): tukevat näytön lukituksen ja istunnon hallinnan teknistä toteutusta päätelaitteissa.

11.5 EU:n GDPR (2016/679)

11.5.1 Artikla 5(1)(f): edellyttää henkilötietojen eheyttä ja luottamuksellisuutta, mukaan lukien suojaaminen fyysiseltä altistumiselta tai asiattomien henkilöiden nähtäville joutumiselta.

11.5.2 Artikla 32 – käsittelyn turvallisuus: edellyttää asianmukaisia fyysisiä ja organisatorisia toimenpiteitä henkilötietojen suojaamiseksi vahingossa tapahtuvalta tai lainvastaiselta tuhoutumiselta, häviämiseltä tai luvattomalta paljastumiselta, mikä toteutetaan työpöytä- ja näyttökontrolleilla.

11.5.3 Johdanto-osan kappale 39: edellyttää henkilötietoihin pääsyn rajaamista valtuutettuihin henkilöihin; tähän sisältyy myös tiedon suojaaminen fyysisessä muodossa silloin, kun se jätetään ilman valvontaa.

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

11.6.1 Artikla 21(2)(d): edellyttää fyysiseen turvallisuuteen ja ympäristöturvallisuuteen liittyviä politiikkoja ja menettelyjä, mukaan lukien työpaikkatason tietoturvan suojatoimet.

11.6.2 Artikla 21(3): edistää tietoturvakulttuuria, johon sisältyvät hyvä käyttäjätoiminta, tietoisuus ja tahattomien tietovuotojen ehkäisy; tätä tukevat tämän politiikan käyttäytymiseen liittyvät kontrollit.

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

11.7.1 Artikla 5 – sisäinen hallinto ja valvonta: edellyttää, että kaikkia ICT-riskejä, mukaan lukien inhimilliset ja ympäristöön liittyvät uhat, hallitaan toimeenpantavilla politiikoilla.

11.7.2 Artikla 8 – ICT-riskien hallinta: edellyttää suojatoimia sekä digitaalisissa että fyysisissä ympäristöissä varmistaen, etteivät etä-, toimipiste- tai omissa tiloissa työskentelevät käyttäjät aiheuta hallitsematonta altistumista.

11.7.3 Artikla 9 – poikkeamien hallinta: edellyttää, että ympäristöön tai käyttäytymiseen liittyvät puutteet, jotka johtavat tietojen altistumiseen, kirjataan lokiin, luokitellaan ja käsitellään asianmukaisilla korjaavilla toimenpiteillä.

11.8 COBIT 2019

11.8.1 DSS01 – hallitut operaatiot: varmistaa operatiivisen kurinalaisuuden fyysisten työtilojen ja järjestelmien suojaamisessa toistettavien kontrollien avulla.

11.8.2 DSS05 – hallitut tietoturvapalvelut: tukee tietojen, laitteiden ja päätepisteiden suojaamista käyttäytymiseen perustuvalla toimeenpanolla, kuten puhtaan pöydän käytännöillä.

11.8.3 MEA03 – vaatimustenmukaisuuden seuranta, arviointi ja tarkastelu: tukee fyysisten suojatoimien ja politiikan toimeenpanon auditointia päivittäisissä liiketoimintakäytännöissä.