					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P10S					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	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohdat 7.2, 8	
ISO/IEC 27002:2022	Kontrolli 7	
NIST SP 800-53 Rev.5	PE-2, AC-11	
EU:n NIS2-direktiivi	Artikla 21(2)(d)	
EU:n DORA-asetus	Artikla 9(2)(f)	
COBIT 2019	DSS01.06, DSS05	
EU:n yleinen tietosuoja-asetus (GDPR)	Artikla 32	

1. Tarkoitus

1.1 Tällä käytännöllä vahvistetaan sitovat vaatimukset turvallisen työympäristön ylläpitämiseksi varmistamalla, että pöydillä, työasemilla ja näytöillä ei ole näkyvissä luottamuksellisia tietoja silloin, kun niitä ei valvota.

1.2 Käytännön ensisijaisena tarkoituksena on estää arkaluonteisten tietojen luvaton käyttö tilanteissa, joissa tulosteita jätetään valvomatta, näytöt jäävät lukitsematta tai siirrettävä tallennusväline on väärässä paikassa, sekä fyysisissä toimistoympäristöissä että etätyöpisteissä.

1.3 Tässä käytännössä määritellyt puhtaan pöydän ja näytön menettelyt vahvistavat organisaation kykyä täyttää ISO/IEC 27001 -sertifioinnin vaatimukset minimoimalla vältettävissä olevat altistumisriskit. Ne osoittavat myös asiakkaille, kumppaneille ja auditoijille, että suhtaudumme tietoturvaan vakavasti myös resurssirajoitteisissa ympäristöissä.

1.4 Tämä käytäntö tukee osoitusvelvollisuuden ja tietoturvatietoisuuden kulttuuria sekä varmistaa, että kaikki henkilöt roolista tai teknisestä osaamisesta riippumatta ymmärtävät vastuunsa suojata yrityksen ja asiakkaiden tiedot visuaaliselta altistumiselta, varkaudelta ja katoamiselta.

2. Soveltamisala

2.1 Tätä käytäntöä sovelletaan seuraaviin:

2.1.1 kaikkiin työntekijöihin, sopimuskumppaneihin, harjoittelijoihin ja määräaikaisiin työntekijöihin, jotka käyttävät yrityksen omistamia tai heille osoitettuja työasemia, työpöytiä tai mobiililaitteita

2.1.2 kaikkiin liiketoiminnassa käytettäviin fyysisiin sijainteihin, mukaan lukien erilliset toimistot, yhteiskäyttöiset työtilat sekä etä- ja kotityöpisteet

2.1.3 kaikkiin liiketoimintatarkoituksiin käytettäviin digitaalisiin laitteisiin, joissa on näyttö, mukaan lukien pöytätietokoneet, kannettavat tietokoneet, tabletit ja ulkoiset näytöt

2.2 Käytäntö koskee myös kaikkia fyysisiä tai digitaalisia omaisuuseriä, jotka voivat näyttää, sisältää tai välittää arkaluonteisia tietoja, mukaan lukien:

2.2.1 tulostetut asiakirjat tai käsinkirjoitetut muistiinpanot

2.2.2 USB-muistit, CD-levyt ja ulkoiset kiintolevyt

2.2.3 matkapuhelimet, joita käytetään liiketoimintaan liittyvään viestintään tai sähköpostiin

2.2.4 tietokonenäytöt ja projektorit, jotka on liitetty työjärjestelmiin

2.3 Tämä käytäntö on voimassa myös tavanomaisen työajan ulkopuolella ja poikkeuksellisissa toimintatilanteissa (esim. työajan jälkeinen ylläpito tai hätätilanteeseen liittyvä työ).

3. Tavoitteet

3.1 Toteuttaa käytännölliset ja yhdenmukaiset kontrollit, joilla varmistetaan, ettei arkaluonteisia tietoja jätetä näkyville pöydille, näytöille tai yhteiskäyttöisiin tiloihin.

3.2 Minimoida luvattoman pääsyn riski sekä sisäisistä lähteistä (esim. muiden työntekijöiden tahaton pääsy) että ulkoisista uhista (esim. vierailijat, siivoushenkilöstö tai sopimuskumppanit).

3.3 Tukea fyysisen pääsyn turvallisuutta ja loogisen pääsyn rajoituksia edellyttämällä, että henkilöstö suojaa aktiivisesti työmateriaalit ja lukitsee tietokoneet poistuessaan niiden ääreltä.

3.4 Vahvistaa henkilöstön tietoisuutta turvallisista työskentelykäytännöistä ja määrittää yksinkertaiset, velvoittavat säännöt päivittäiseen toimintaan työskentelypaikasta riippumatta.

3.5 Varmistaa yhdenmukaisuus ISO/IEC 27001:n liitteen A kontrollin 7.7 sekä ISO/IEC 27002:n puhdasta pöytää ja näyttöä koskevan soveltamisohjeistuksen kanssa.

3.6 Varmistaa, että organisaatio voi osoittaa asianmukaisen huolellisuuden ja auditointivalmiuden ilman enterprise-tason infrastruktuuria.

4. Roolit ja vastuut

4.1 toimitusjohtaja

4.1.1 Omistaa tämän käytännön ja varmistaa, että se viestitään asianmukaisesti sekä että kaikki työntekijät ja sopimuskumppanit ymmärtävät ja noudattavat sitä.

4.1.2 Vastaa poikkeusten hyväksymisestä, rikkomuksiin reagoimisesta ja turvallisiin työkäytäntöihin liittyvän koulutuksen valvonnasta.

4.1.3 Suorittaa tai delegoi säännölliset tarkastukset vähintään neljännesvuosittain sen varmistamiseksi, että fyysiset ja digitaaliset työtilat täyttävät tämän käytännön vaatimukset.

4.2 nimetty vastuuhenkilö (jos nimetty)

4.2.1 Hänelle voidaan osoittaa vastuu teknisten määritysten toteuttamisesta (esim. näytön aikakatkaisuasetukset) tai fyysisten säilytysratkaisujen (esim. lukittavat laatikot) järjestämisestä.

4.2.2 Tukee toimitusjohtajaa ilmoittamalla poikkeamista, muistuttamalla työtilojen turvallisuudesta ja seuraamalla korjaavia toimenpiteitä, kun ongelmia havaitaan.

4.2.3 Auttaa varmistamaan, että kaikilla työntekijöillä on mahdollisuuksien mukaan käytettävissään asianmukaiset lukitusmekanismit tai turvalliset säilytystilat.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Toimitusjohtajan on katselmoitava tämä käytäntö vähintään kerran vuodessa sekä minkä tahansa seuraavan tapahtuman jälkeen:

9.1.1 uusien toimistotilojen, laitteiden tai yhteiskäyttöisten järjestelmien käyttöönotto

9.1.2 sovellettaviin lakisääteisiin tai sertifiointivaatimuksiin tehdyt muutokset

9.1.3 auditointien, riskiarviointien tai tietoturvapoikkeamien havainnot

9.2 Väliaikaisista päivityksistä on tiedotettava kaikille työntekijöille sähköpostitse, ja niiden hyväksyminen on pakollista.

9.3 Tämän käytännön aiemmat versiot on säilytettävä turvallisesti ja todennettavasti, jotta voidaan osoittaa jatkuva yhdenmukaisuus ISO/IEC 27001:n ja siihen liittyvien viitekehysten kanssa.

10. Liittyvät käytännöt ja yhteydet

10.1 P2S – Hallinnointirooleja ja vastuita koskeva politiikka: Täsmentää toimitusjohtajan toimivallan fyysiseen ja digitaaliseen työtilakäyttäytymiseen liittyvässä valvonnassa ja auditoinnissa.

10.2 P4S – Pääsynhallintapolitiikka: Tukee näytön lukituksen ja turvallisten työasemakirjautumiskäytäntöjen teknistä toteutusta.

10.3 P8S – Tietoturvatietoisuus- ja koulutuspolitiikka: Vahvistaa käytännön noudattamisen edellyttämän käyttäytymiseen liittyvän koulutuksen.

10.4 P17S – Tietosuojan ja yksityisyyden politiikka: Määrittelee velvoitteet henkilötietojen ja arkaluonteisten tietojen käsittelyyn ja suojaamiseen EU:n yleisen tietosuoja-asetuksen (GDPR) mukaisesti.

10.5 P30S – Tietoturvapoikkeamien hallintapolitiikka: Määrittää eskalointi- ja reagointiviitekehyksen tilanteissa, joissa rikkomus johtaa tietojen altistumiseen tai tietomurtoon.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Kohta 7.2: Edellyttää, että koko henkilöstö on tietoinen tietoturvavastuistaan, mukaan lukien fyysiset suojatoimet.

11.1.2 Kohta 8.1: Operatiivisten kontrollien on varmistettava asianmukaiset fyysiset ja loogiset suojaukset.

11.2 ISO/IEC 27002

11.2.1 Kontrolli 7.7: Antaa yksityiskohtaiset ohjeet puhtaan pöydän ja näytön vaatimusten määrittämiseen, viestimiseen ja soveltamiseen.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: Määrittelee fyysisen pääsyn hallinnan odotukset, mukaan lukien henkilöstön käyttäytyminen turvallisissa ympäristöissä.

11.3.2 AC-11: Edellyttää työasemille istunnon lukitustoiminnallisuutta luvattoman katselun tai käytön estämiseksi.

11.4 EU:n yleinen tietosuoja-asetus (GDPR)

11.4.1 Artikla 32: Edellyttää organisaatioita suojaamaan henkilötietoja fyysisillä ja teknisillä suojatoimilla, mukaan lukien työasemat ja asiakirjat.

11.5 EU:n NIS2-direktiivi

11.5.1 Artikla 21(2)(d): Edellyttää organisaatioita ottamaan käyttöön riskiperusteiset fyysisen ja loogisen pääsyn käytännöt.

11.6 EU:n DORA-asetus

11.6.1 Artikla 9(2)(f): Edellyttää ICT-turvallisuuspolitiikkoja, mukaan lukien turvallinen työtilahygienia, finanssialan toimijoille ja niiden toimitusketjuille.

11.7 COBIT 2019

11.7.1 DSS01.06: Edellyttää omaisuuden suojauskäytäntöjä, mukaan lukien työtiloihin ja tallennusvälineisiin kohdistuvat fyysiset kontrollit.

11.7.2 DSS05.02: Tukee loppukäyttäjien tietoturvakäytäntöjen soveltamista eri toimintaympäristöissä.