					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P10S					Dokumendi pealkiri: **Puhta töölaua ja ekraani poliitika**							
Versioon: 1.0		Jõustumiskuupäev: 01.01.2025			Dokumendi omanik:							
X	Poliitika		Standard		Protseduur		Vorm		Register		Muu	

Muudatuste ajalugu				
Muudatuse number	**Muudatuse kuupäev**	**Muudatused**	**Läbi vaadanud**	**Protsessi omanik**

Kinnitused			
Nimi	**Ametikoht**	**Kuupäev**	**Allkiri**

Kooskõla standardite ja regulatsioonidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 7.2, 8	
ISO/IEC 27002:2022	Kontroll 7	
NIST SP 800-53 Rev.5	PE-2, AC-11	
EL NIS2	Artikkel 21(2)(d)	
EL DORA	Artikkel 9(2)(f)	
COBIT 2019	DSS01.06, DSS05	
EL GDPR	Artikkel 32	

1. Eesmärk

1.1 Käesolev poliitika kehtestab siduvad nõuded turvalise töökeskkonna säilitamiseks, tagades, et järelevalveta töölaudadel, tööjaamades ega kuvaritel ei ole nähtaval konfidentsiaalset teavet.

1.2 Poliitika peamine eesmärk on vältida loata juurdepääsu tundlikule teabele järelevalveta jäetud väljatrükkide, lukustamata ekraanide või nõuetevastaselt jäetud eemaldatavate andmekandjate kaudu nii füüsilistes kontorites kui ka kaugtöö- ja kodukontori asukohtades.

1.3 Käesolevas poliitikas sätestatud puhta töölaua ja puhta ekraani põhimõtted tugevdavad organisatsiooni võimekust täita ISO/IEC 27001 sertifitseerimise nõudeid, vähendades välditavaid teabe avalikuks tuleku riske. Need põhimõtted annavad klientidele, partneritele ja audiitoritele kinnituse, et käsitleme infoturvet tõsiselt ka piiratud ressurssidega keskkonnas.

1.4 Käesolev poliitika toetab vastutuse ja teadlikkuse kultuuri, tagades, et kogu personal mõistab oma rollist või tehnilisest pädevusest sõltumata vastutust kaitsta ettevõtte ja klientide teavet visuaalse avalikuks tuleku, varguse või kaotsimineku eest.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub järgmistele isikutele ja olukordadele:

2.1.1 kõigile töötajatele, töövõtjatele, praktikantidele ja ajutistele töötajatele, kes kasutavad ettevõttele kuuluvaid või neile isiklikult määratud tööjaamu, töölaudu või mobiilseadmeid

2.1.2 kõigile füüsilistele asukohtadele, kus toimub äritegevus, sealhulgas püsikontoritele, ühiskontoritele ning kaug- või kodutöö tegemise kohtadele

2.1.3 kõigile ärilistel eesmärkidel kasutatavatele kuvafunktsiooniga digiseadmetele, sealhulgas lauaarvutitele, sülearvutitele, tahvelarvutitele ja välistele monitoridele

2.2 Poliitika laieneb kõigile füüsilistele ja digitaalsetele varadele, mis võivad kuvada, sisaldada või edastada tundlikku teavet, sealhulgas:

2.2.1 trükitud dokumendid või käsitsi kirjutatud märkmed

2.2.2 USB-mäluseadmed, CD-d ja välised kõvakettad

2.2.3 mobiiltelefonid, mida kasutatakse tööalaseks sõnumivahetuseks või e-postiks

2.2.4 arvutimonitorid ja projektorid, mis on ühendatud tööks kasutatavate süsteemidega

2.3 Käesolev poliitika kehtib ka väljaspool tavapärast tööaega ning mittestandardsete tegevuste ajal (nt töövälisel ajal tehtav hooldus või erakorraline reageerimine).

3. Eesmärgid

3.1 Rakendada praktilised ja ühtsed kontrollimeetmed, mis tagavad, et töölaudadele, ekraanidele ega ühiskasutatavatesse ruumidesse ei jää tundlikku teavet nähtavale.

3.2 Minimeerida loata juurdepääsu riski nii sisemistest allikatest (nt teiste töötajate tahtmatu juurdepääs) kui ka välistest ohtudest (nt külastajad, koristustöötajad või töövõtjad) tulenevalt.

3.3 Toetada füüsilise ja loogilise juurdepääsu piiranguid, nõudes töötajatelt töömaterjalide aktiivset kaitsmist ja arvutite lukustamist nende järelevalveta jätmisel.

3.4 Suurendada töötajate teadlikkust turvalistest töövõtetest ning kehtestada lihtsad ja siduvad reeglid, mida saab igapäevatöös rakendada sõltumata töö tegemise asukohast.

3.5 Tagada kooskõla ISO/IEC 27001 lisa A kontrollimeetmega 7.7 ja selle ISO/IEC 27002 rakendusjuhistega puhta töölaua ja puhta ekraani nõuete osas.

3.6 Tagada, et organisatsioon suudab tõendada hoolsuskohustuse täitmist ja auditivalmidust ka ilma ettevõtte taseme taristuta.

4. Rollid ja vastutused

4.1 Tegevjuht

4.1.1 Vastutab käesoleva poliitika eest ning tagab, et see on kõigile töötajatele ja töövõtjatele nõuetekohaselt teatavaks tehtud, arusaadav ja järgitav.

4.1.2 Vastutab erandite heakskiitmise, rikkumistele reageerimise ning turvaliste töövõtete alase koolituse järelevalve eest.

4.1.3 Peab tegema või delegeerima regulaarsed kontrollid vähemalt kord kvartalis, et kinnitada füüsiliste ja digitaalsete tööruumide vastavust käesoleva poliitika nõuetele.

4.2 Määratud töötaja (kui on määratud)

4.2.1 Talle võib määrata vastutuse tehniliste seadistuste rakendamise eest (nt ekraani ajalõpu seaded) või füüsiliste hoiustamisvahendite (nt lukustatavad sahtlid) väljastamise eest.

4.2.2 Toetab tegevjuhti mittevastavuste raporteerimisel, tööruumi turvalisust puudutavate meeldetuletuste korraldamisel ja parandusmeetmete jälgimisel probleemide tuvastamise korral.

4.2.3 Aitab tagada, et kõigil töötajatel on võimaluse korral juurdepääs sobivatele lukustusmehhanismidele või turvalistele hoiukohtadele.

[... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ...]

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Tegevjuht peab käesoleva poliitika läbi vaatama vähemalt üks kord aastas ning pärast mis tahes järgmist sündmust:

9.1.1 uute kontoriruumide, seadmete või ühissüsteemide kasutuselevõtt

9.1.2 kohaldatavate õiguslike või sertifitseerimisnõuete muudatused

9.1.3 auditite, riskihindamiste või turbeintsidentide tulemused

9.2 Vahepealsed ajakohastused tuleb kõigile töötajatele edastada e-posti teel ning nõuda nende kinnitamist.

9.3 Käesoleva poliitika varasemad versioonid tuleb hoiustada turvaliselt ja auditikõlblikul viisil, et tõendada pidevat kooskõla standardiga ISO/IEC 27001 ja seotud raamistikega.

10. Seotud poliitikad ja seosed

10.1 P2S – Juhtimisrollide ja vastutuste poliitika: täpsustab tegevjuhi volitusi füüsilise ja digitaalse tööruumi käitumisreeglite rakendamiseks ja auditeerimiseks.

10.2 P4S – Juurdepääsukontrolli poliitika: toetab ekraanilukustuse ja tööjaama turvalise sisselogimise tavade tehnilist rakendamist.

10.3 P8S – Infoturbeteadlikkuse koolituse poliitika: tugevdab poliitika järgimiseks vajalikku käitumuslikku koolitust.

10.4 P17S – Andmekaitse ja privaatsuse poliitika: määratleb GDPR-iga kooskõlas kohustused isikuandmete ja tundlike andmete käsitlemiseks ning kaitsmiseks.

10.5 P30S – Intsidentidele reageerimise poliitika (P30): sätestab eskaleerimise ja reageerimise raamistiku olukorraks, kus rikkumise tagajärjel toimub andmete nähtavale sattumine või turvanõuete rikkumine.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 7.2: nõuab, et kõik töötajad oleksid teadlikud oma turbekohustustest, sealhulgas füüsilistest kaitsemeetmetest.

11.1.2 Punkt 8.1: tegevuskontrollid peavad tagama asjakohased füüsilised ja loogilised kaitsemeetmed.

11.2 ISO/IEC 27002

11.2.1 Kontroll 7.7: annab üksikasjalikud juhised puhta töölaua ja puhta ekraani nõuete kehtestamiseks, teavitamiseks ja rakendamiseks.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: kehtestab füüsilise juurdepääsu kontrolli ootused, sealhulgas personali käitumise turvalistes keskkondades.

11.3.2 AC-11: nõuab tööjaamade seansilukustuse funktsionaalsust, et vältida loata vaatamist või kasutamist.

11.4 EL GDPR

11.4.1 Artikkel 32: nõuab, et organisatsioonid kaitseksid isikuandmeid füüsiliste ja tehniliste kaitsemeetmetega, sealhulgas tööjaamade ja dokumentide puhul.

11.5 EL NIS2 direktiiv

11.5.1 Artikkel 21(2)(d): nõuab, et organisatsioonid rakendaksid riskipõhiseid füüsilise ja loogilise juurdepääsu poliitikaid.

11.6 EL DORA

11.6.1 Artikkel 9(2)(f): nõuab finantssektori osalejatelt ja nende tarneahelatelt IKT-turbepoliitikaid, sealhulgas turvalise tööruumi hügieeni nõudeid.

11.7 COBIT 2019

11.7.1 DSS01.06: nõuab varade kaitse tavasid, sealhulgas füüsilisi kontrollimeetmeid tööruumide ja andmekandjate üle.

11.7.2 DSS05.02: toetab lõppkasutajate turbepraktikate rakendamist erinevates tegevuskeskkondades.