					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P10					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 õigusaktidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 6.1.3, punkt 8	riskikäsitlusplaan, operatiivne planeerimine ja kontroll turvaliste tööruumide tagamiseks
ISO/IEC 27002:2022	Kontroll 7	käitumuslikud ja keskkondlikud kontrollimeetmed järelevalveta füüsilise teabe kaitseks
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	füüsiline juurdepääs, töövõtjate turvalisus, andmekandjate hävitamine, seansi lukustamine, konfiguratsiooni- ja autentimistunnuste kontrollimeetmed
ELi isikuandmete kaitse üldmäärus (GDPR)	Artiklid 5(1)(f), 32; põhjendus 39	andmete terviklus, konfidentsiaalsus ja andmete füüsilised kaitsemeetmed
ELi NIS2	Artiklid 21(2)(d), 21(3)	füüsilise turbe, kasutajakäitumise ja andmelekkete vältimise poliitikad
ELi DORA	Artiklid 5, 8, 9	sisemine juhtimine, IKT- ja füüsilist turvet hõlmav intsidendihaldus
COBIT 2019	DSS01, DSS05, MEA	hallatud operatsioonid, turvateenused ja vastavuse seire

1. Eesmärk

1.1 Käesoleva poliitikaga kehtestatakse kohustuslikud kontrollimeetmed tundliku teabe kaitseks, nõudes füüsiliste dokumentide, tööjaamade, ekraanide ja eemaldatavate andmekandjate turvalist käsitlemist nii kontorikeskkonnas kui ka ühiskasutatavates tööruumides.

1.2 Käesolev poliitika toetab standardi ISO/IEC 27001 lisa A kontrolli 7.7, rakendades käitumuslikke ja tehnilisi meetmeid, mis maandavad loata avalikustamise, varguse või andmekao riski, mis tuleneb järelevalveta või nähtavale jäetud teabest.

1.3 Käesolev poliitika tugevdab füüsilist turvet ja infoturvet igapäevases tegevuses ning toetab kohaldatavate õiguslike, lepinguliste ja regulatiivsete kohustuste täitmist.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõigile füüsilistes tööruumides tegutsevatele või neile juurdepääsu omavatele isikutele, sealhulgas:

2.1.1 alalised ja ajutised töötajad

2.1.2 töövõtjad, konsultandid, tarnijad ja praktikandid

2.1.3 kolmandatest osapooltest teenuseosutajad ja kohapealsed külastajad, kellel on juurdepääs tundlikule teabele

2.2 Nõuded kehtivad järgmistes kohtades:

2.2.1 eraldi kontorid, boksid ja avatud planeeringuga tööalad

2.2.2 koosolekuruumid ja ühised koostööalad

2.2.3 printerialad, vastuvõtulauad ja koopiaruumid

2.2.4 alad, kus kasutatakse kaugjuurdepääsuga tööjaamu või ühiskasutatavaid kioskeid

2.3 Käesolev poliitika kehtib ka ajutistes või hübriidsetes töökeskkondades (nt jagatud töölaudade kasutamisel) ning avalikes keskkondades, kus esineb üle õla vaatamise või järelevalveta andmete risk.

3. Eesmärgid

3.1 Vältida loata juurdepääsu konfidentsiaalsele, tundlikule või reguleeritud teabele, mis on jäetud nähtavale füüsilisel või digitaalsel kujul.

3.2 Tagada kõigis töökeskkondades ühtne turbetase füüsiliste kontrollimeetmete, tööjaamade konfiguratsiooni ja lõppkasutajate käitumise kaudu.

3.3 Vähendada hooletusest või ebapiisavast järelevalvest tingitud andmekaitserikkumiste, intellektuaalomandi kao ja andmete väljaviimise riski.

3.4 Kinnistada puhta töölaua ja tühja ekraani käitumisnõuded organisatsiooni kultuuri osana, toetades operatiivset distsipliini, auditeeritavust ja regulatiivset kaitstavust.

3.5 Toetada vastavust standardile ISO/IEC 27001, GDPR artiklile 32, NIS2 artiklile 15 ning muudele füüsilise turbe nõuetele, mis on asjakohased kriitiliste või isikuandmete kaitseks.

4. Rollid ja vastutused

4.1 Tippjuhtkond

4.1.1 Kinnitab käesoleva poliitika ja edendab turvateadlikku kultuuri kõigis äriüksustes.

4.1.2 Eraldab poliitika rakendamiseks, teadlikkuse tõstmise tegevusteks ja füüsiliste kontrollimeetmete kasutuselevõtuks vajalikud ressursid.

4.2 Infoturbejuht / ISMS-i juht

4.2.1 Vastutab käesoleva poliitika eest ning tagab selle kooskõla standardiga ISO/IEC 27001:2022, auditi nõuete ja riskikäsitlusstrateegiatega.

4.2.2 Kujundab teadlikkuse tõstmise programmid ja kontrollimeetmed, et tagada järjepidev rakendamine kõigis asukohtades ja hübriidsetes töökeskkondades.

4.2.3 Koordineerib halduse ja IT-ga, et tagada asjakohaste füüsiliste kontrollimeetmete olemasolu.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Poliitika läbivaatamise ajakava

9.1.1 Käesolev poliitika tuleb läbi vaadata:

9.1.1.1 vähemalt kord aastas

9.1.1.2 pärast mis tahes tööruumi või ekraani nähtavusega seotud auditi mittevastavust

9.1.1.3 pärast füüsilist või keskkonnaga seotud intsidenti (nt seadme vargus, sabasisenemine, jälgimine)

9.1.1.4 uue kontorilahenduse, halduspoliitikate või tööruumi mudelite (nt jagatud töölauad, kaugkontorite keskused) kasutuselevõtul

9.2 Vastutavad omanikud

9.2.1 Poliitika omanik on infoturbejuht või määratud ISMS-i juht.

9.2.2 Läbivaatamise protsessi tuleb kaasata:

9.2.2.1 haldus- ja ettevõtte turbe meeskonnad

9.2.2.2 IT ja taristu seadmetega seotud rakendamise tagamiseks

9.2.2.3 personaliüksus (HR) ning õigus ja vastavus käitumisnõuete rakendamise ja distsiplinaarse kooskõla tagamiseks

9.2.3 Kõik poliitikamuudatused peavad olema versioonihalduse all, heaks kiidetud infoturbe juhtimissüsteemi juhtkomitee poolt ning vajaduse korral uuesti kinnitamiseks edasi saadetud.

9.3 Muudatustest teavitamine

9.3.1 Kasutajaid tuleb olulistest muudatustest teavitada järgmiste kanalite kaudu:

9.3.1.1 intraneti poliitikakeskus või portaal

9.3.1.2 sihitud e-posti teavitused

9.3.1.3 tööle asumise korduskoolitused ja kvartalibriifingud

9.3.1.4 kohustuslikud kinnitustaotlused mis tahes uute kriitiliste rakendussätete puhul

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika on kooskõlas järgmiste poliitikatega ja toetab neid:

10.1.1 P1 – Infoturbepoliitika: kehtestab kasutajate käitumise ja füüsilise turbe ootused, mis on käesoleva poliitika aluseks.

10.1.2 P3 – IT-vahendite lubatud kasutuse poliitika: käsitleb kasutaja vastutust andmete ja süsteemide, sealhulgas füüsilise keskkonna kaitsmisel.

10.1.3 P6 – Riskijuhtimise poliitika: hõlmab füüsiliste tööruumide riske organisatsiooniülese teaberiskide analüüsi osana.

10.1.4 P12 – Varahalduse poliitika: toetab töölauale jäetud seadmete ja andmekandjate jälgimist ning turvalist käsitlemist.

10.1.5 P13 – Andmete klassifitseerimise ja märgistamise poliitika: seob puhta töölaua nõuete rakendamise konfidentsiaalsete või organisatsioonisiseste füüsiliste dokumentidega.

10.1.6 P14 – Andmete säilitamise ja hävitamise poliitika: suunab füüsiliste dokumentide säilitamist, hävitamist ja hävituskonteinerite kasutamist.

10.1.7 P22 – Logimise ja seire poliitika: seda võib kasutada tööjaama lukustuse oleku, jõudeoleku aja või tööruumide kaamerapildi seireks, kui see on lubatud.

10.2 Need seotud poliitikad loovad integreeritud turvakultuuri, ühendades kasutajate teadlikkuse, füüsilised kontrollimeetmed ja vastutuse, et tagada toimepidevad tööruumid.

11. Viitestandardid ja raamistikud

11.1 Käesolev poliitika on kooskõlas rahvusvaheliselt tunnustatud standardite ja õiguslike nõuetega, mis nõuavad tundliku teabe kaitset füüsilises keskkonnas ja kasutajakäitumise kaudu.

11.2 ISO/IEC 27001

11.2.1 Punkt 6.1.3 – riskikäsitlusplaan: toetab kontrollimeetmete rakendamist füüsiliste ja keskkonnariskide maandamiseks, sealhulgas avatud tööruumides kasutajakäitumisega seotud riskide puhul.

11.2.2 Punkt 8.1 – operatiivne planeerimine ja kontroll: kehtestab operatiivsed kontrollimeetmed turvaliste tööruumide ja seadmete kasutuse haldamiseks.

11.3 ISO/IEC 27002:2022 – kontroll 7

11.3.1 See kontroll nõuab käitumuslikke ja keskkondlikke kaitsemeetmeid, et vältida loata juurdepääsu teabele järelevalveta andmekandjate, ekraanide või trükitud materjalide kaudu. Käesolev poliitika nõuab tööruumi korrashoidu, ekraanilukustuse kasutamist ja tundlike dokumentide turvalist hävitamist.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (füüsilise juurdepääsu volitused): seotud tööruumide piirangute ja lukustatud hoiustamise nõuete rakendamisega kõrge riskiga keskkondades.

11.4.2 PS-7 (välise personali turvalisus): rakendatud puhta töölaua ja tühja ekraani nõuete kaudu, mis laienevad töövõtjatele ja kolmandate osapoolte kasutajatele.

11.4.3 MP-6 (andmekandjate puhastamine) ja AC-11 (seansi lukustamine): rakendatud turvalise hävitamise protseduuride ja kohustuslike ekraanilukustuse taimerite kaudu.

11.4.4 CM-6 (konfiguratsiooniseaded) ja IA-5 (autentimistunnuste haldus): toetavad ekraanilukustuse ja seansikontrolli tehnilist rakendamist lõppseadmetes.

11.5 ELi isikuandmete kaitse üldmäärus (GDPR) (2016/679)

11.5.1 Artikkel 5(1)(f): nõuab isikuandmete tervikluse ja konfidentsiaalsuse tagamist, sealhulgas kaitset füüsilise avalikustumise või loata isikute vaatamise eest.

11.5.2 Artikkel 32 – töötlemise turvalisus: nõuab asjakohaseid füüsilisi ja organisatsioonilisi meetmeid isikuandmete kaitsmiseks juhusliku või õigusvastase hävimise, kaotsimineku või loata avalikustamise eest; see saavutatakse töölauda ja ekraani käsitlevate kontrollimeetmetega.

11.5.3 Põhjendus 39: nõuab isikuandmetele juurdepääsu piiramist volitatud isikutega; see hõlmab ka nende kaitsmist füüsilisel kujul ajal, mil need on järelevalveta.

11.6 ELi NIS2 direktiiv (2022/2555)

11.6.1 Artikkel 21(2)(d): nõuab füüsilise ja keskkonnaturbega seotud poliitikaid ja protseduure, sealhulgas töökoha tasandi infoturbe kontrollimeetmeid.

11.6.2 Artikkel 21(3): soodustab turvakultuuri, mis hõlmab head kasutajakäitumist, teadlikkust ja tahtmatute andmelekkete vältimist; seda toetavad käesoleva poliitika käitumuslikud kontrollimeetmed.

11.7 ELi DORA (2022/2554)

11.7.1 Artikkel 5 – sisemine juhtimine ja kontroll: nõuab, et kõiki IKT-ga seotud riske, sealhulgas inim- ja keskkonnaohte, juhitaks rakendatavate poliitikate kaudu.

11.7.2 Artikkel 8 – IKT-riskide juhtimine: nõuab kontrollimeetmeid nii digitaalses kui ka füüsilises kontekstis, tagades, et kaug-, harukontori- ja kohapealsed kasutajad ei tekita juhtimata riskipositsiooni.

11.7.3 Artikkel 9 – intsidendihaldus: nõuab, et keskkonna- või käitumisalased puudused, mis põhjustavad andmete avalikustumist, logitaks, klassifitseeritaks ja käsitletaks asjakohaste parandusmeetmetega.

11.8 COBIT 2019

11.8.1 DSS01 – hallatud operatsioonid: tagab operatiivse distsipliini füüsiliste tööruumide ja süsteemide kaitsmisel korduvkasutatavate kontrollimeetmete abil.

11.8.2 DSS05 – hallatud turvateenused: toetab andmete, seadmete ja juurdepääsulõpp-punktide kaitset käitumuspõhise rakendamise kaudu, näiteks puhta töölaua tavadega.

11.8.3 MEA03 – vastavuse seire, hindamine ja auditeerimine: soodustab füüsiliste kontrollimeetmete ja poliitika rakendamise auditeerimist igapäevases äritegevuses.