					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P09					Dokumendi pealkiri: **kaugtööpoliitika**							
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**

1. Eesmärk

1.1 Käesolev poliitika kehtestab kohustuslikud nõuded kaugtöö turvaliseks tegemiseks, sealhulgas organisatsiooni süsteemide kasutamiseks, andmetele juurdepääsuks ja tööülesannete täitmiseks väljaspool ettevõtte ruume.

1.2 See tagab kaugjuurdepääsu kaudu kasutatavate teabevarade konfidentsiaalsuse, tervikluse ja käideldavuse ning kehtestab kontrollimeetmed hajutatud töökeskkondadega seotud riskide maandamiseks.

1.3 Poliitika täidab standardi ISO/IEC 27001:2022 lisa A kontrollimeetme 6.7 nõuded, rakendades kaugtöötingimustele kohandatud tehnilisi ja protseduurilisi kaitsemeetmeid.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kogu personalile, kellel on volitus teha kaugtööd, sealhulgas:

2.1.1 töötajad (täistööajaga, osalise tööajaga, lepingu alusel)

2.1.2 välised teenuseosutajad, konsultandid ja tarnijad

2.1.3 ajutised töötajad ja projektipõhine personal, kellel on heakskiidetud kaugjuurdepääs

2.2 Poliitika hõlmab:

2.2.1 juurdepääsu organisatsiooni süsteemidele VPNi või heakskiidetud kaugjuurdepääsuvahendite kaudu

2.2.2 tundliku ja reguleeritud teabe käitlemist väljaspool turvaalasid

2.2.3 organisatsioonile kuuluvate seadmete või isiklike seadmete kasutamist (BYOD)

2.2.4 füüsilisi ja loogilisi kaitsemeetmeid kaugtöö keskkondades

2.3 Poliitika kehtib kõigis geograafilistes asukohtades ja ajavööndites, kus organisatsioon lubab kaugtööd, sõltumata sellest, kas tegemist on püsiva, ajutise või talitluspidevuse sündmuse ajal tehtava tööga.

3. Eesmärgid

3.1 Tagada, et organisatsiooni sisevõrkudele, süsteemidele ja teabele saavad kaugjuurdepääsu ainult volitatud isikud.

3.2 Tagada krüpteerimise, mitmefaktorilise autentimise (MFA) ja lõppseadmete kaitse rakendamine kõigi kaugjuurdepääsu viiside puhul.

3.3 Säilitada turvaseisund ohtude vastu, nagu andmepüük, pahavara, andmete väljaviimine ja süsteemide lubamatu väline eksponeerimine.

3.4 Reguleerida tundlike andmete edastamist, salvestamist ja printimist väljaspool ettevõtte asukohti.

3.5 Rakendada füüsilise turbe meetmeid, mis vähendavad nähtavust ja loata jälgimist kaugsessioonide ajal.

3.6 Tagada vastavus rahvusvahelistele nõuetele, mis käsitlevad andmetele kaugjuurdepääsu, sealhulgas GDPR-i, NIS2 ja DORA nõuetele.

4. Rollid ja vastutused

4.1 Tippjuhtkond

4.1.1 Kiidab käesoleva poliitika heaks ning tagab selle rakendamiseks vajalike ressursside eraldamise ja lõimimise personali (HR), IT ja turbeoperatsioonidega.

4.1.2 Kinnitab organisatsiooni kaugtöö sobivuskriteeriumid ja äriüksuste kohaldatavuse.

4.2 Infoturbejuht / ISMS-i juht

4.2.1 Vastutab poliitika eest, hoiab selle ajakohasena ning tagab selle kooskõla riskipositsiooni ja regulatiivsete nõuetega.

4.2.2 Määratleb kaugjuurdepääsu turbekontrollid (nt krüpteerimine, lõppseadmete kaitse, seansi aegumine).

4.2.3 Kiidab heaks erandite käsitlemise ja seirab kontrollimeetmete tõhusust.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Läbivaatamise sagedus

9.1.1 Käesolev poliitika tuleb läbi vaadata kord aastas või sagedamini järgmistel juhtudel:

9.1.1.1 uute kaugjuurdepääsutehnoloogiate kasutuselevõtt

9.1.1.2 kaugtöö oluline laiendamine (nt hübriidtööjõu algatused)

9.1.1.3 uute ohtude, haavatavuste või kaugkeskkondadega seotud intsidentide ilmnemine

9.1.1.4 asjakohaste õiguslike või regulatiivsete raamistike muudatused

9.2 Omanik ja läbivaatamise protsess

9.2.1 Poliitika omanik on infoturbejuht. Läbivaatamine tuleb koordineerida järgmiste osapooltega:

9.2.1.1 IT-operatsioonid ja arhitektuur

9.2.1.2 personal (HR) ja haldusüksus (operatiivsete ja tööruumiga seotud mõjude osas)

9.2.1.3 andmekaitseametnik (andmekaitse ja piiriüleste andmete kontrollimeetmete osas)

9.2.2 Poliitikamuudatused peavad olema:

9.2.2.1 infoturbe juhtimissüsteemi juhtkomitee poolt heaks kiidetud

9.2.2.2 edastatud kõigile mõjutatud töötajatele ja töövõtjatele

9.2.2.3 lõimitud tööle asumise ja korduskoolituse materjalidesse

9.3 Dokumendihaldus ja levitamine

9.3.1 Poliitika peab sisaldama versioonihaldust, jõustumiskuupäeva ja versiooniajalugu.

9.3.2 Asendatud versioone tuleb säilitada vastavalt dokumendihalduse poliitikale (P14).

9.3.3 Muudetud versioonide avaldamisel tuleb kaugtööks volitatud kasutajatelt nõuda kohustuslikku uut tutvumiskinnitust.

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika toimib koos järgmiste dokumentidega:

10.1.1 P1 – Infoturbepoliitika: kehtestab varade turvalise käitlemise lähtealuse, mis kehtib kõigis töökeskkondades, sealhulgas kaugtöös.

10.1.2 P3 – IT-vahendite lubatud kasutuse poliitika: reguleerib organisatsiooni seadmete ja süsteemide asjakohast kasutamist kaugtööseansside ajal.

10.1.3 P4 – Juurdepääsukontrolli poliitika: tagab, et kaugjuurdepääsuõigused järgivad vähimate õiguste põhimõtet ja korrektseid autentimismehhanisme.

10.1.4 P6 – Riskijuhtimise poliitika: määratleb, kuidas kaugtöö riske ISMS-is tuvastatakse, käsitletakse ja seiratakse.

10.1.5 P12 – Varahalduse poliitika: nõuab kõigi kaugkasutuses olevate seadmete inventeerimist ja konfiguratsioonihaldust.

10.1.6 P22 – Logimis- ja seirepoliitika: tagab, et kaugsessioone seiratakse, auditeeritakse ja säilitatakse vastavalt vastavusnõuetele.

10.1.7 P14 – Andmete säilitamise ja kõrvaldamise poliitika: määratleb kaugtööga seotud andmekäitlusreeglid, sealhulgas teisaldatavad andmekandjad ja seadmete kasutuselt kõrvaldamise.

10.2 Need poliitikad koos tagavad, et kaugtöö on turvaline, nõuetele vastav ja rakendatav kõigis funktsioonides ning geograafilistes asukohtades.

11. Viitestandardid ja raamistikud

11.1 Käesolev poliitika on kooskõlas rahvusvaheliselt tunnustatud infoturbe, andmekaitse ja IKT-riskide juhtimise raamistikega, et tagada turvalised, jälgitavad ja nõuetele vastavad kaugtöö praktikad.

11.2 ISO/IEC 27001

11.2.1 Punkt 6.1.3 – riski käsitlemise planeerimine: käesolev poliitika toetab kaugjuurdepääsu ja hajutatud töökeskkondadega seotud riskide käsitlemist.

11.2.2 Punkt 8.1 – operatiivne planeerimine ja kontroll: nõuab kontrollimeetmete rakendamist süsteemidele, millele pääsetakse ligi väljaspool organisatsiooni ruume.

11.2.3 Lisa A kontrollimeede 6.7 – kaugtöö: käesolev poliitika käsitleb täielikult nõutavaid infoturbe kontrollimeetmeid ajaks, mil personal töötab väljaspool organisatsiooni ruume, sealhulgas füüsilisi ja loogilisi kaitsemeetmeid, juurdepääsuhaldust ning kasutajate käitumise seiret.

11.3 ISO/IEC 27002:2022 – Kontroll 6

11.3.1 See kontroll nõuab kaugtöö jaoks protseduurilisi ja tehnilisi kaitsemeetmeid. See hõlmab nõudeid seadmete turbele, juurdepääsumeetoditele, andmekäitlusele, keskkonnakaitsemeetmetele ja kolmandate osapoolte osalemise haldamisele, mida kõiki rakendatakse käesoleva poliitika kaudu.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (kaugjuurdepääs): otseselt toetatud VPN-kontrollimeetmete, MFA, seansside logimise ja kaugkasutajate rollipõhise juurdepääsu volitamise kaudu.

11.4.2 AC-2 (kontohaldus): kontrollib juurdepääsu sobivust, kaugõiguste määramist ja kontode deaktiveerimist.

11.4.3 SC-12 kuni SC-13 (krüptograafiline kaitse, krüptovõtmete loomine): rakendatud VPNide ja täisketta krüpteerimise kohustusliku kasutamise kaudu kaugkasutuses olevatel lõppseadmetel.

11.4.4 MP-5 (andmekandjate transpordi kaitse) ja PE-18 (infosüsteemi komponentide asukoht): kaugtöö juhised nõuavad transpordikaitset ja füüsilisi kaitsemeetmeid väljaspool ettevõtte asukohti.

11.4.5 AU-2, AU-6: kaugsessioonide logimine ja seire toetavad auditi- ja intsidendihalduse nõudeid.

11.5 EU GDPR (2016/679)

11.5.1 Artikkel 32 – töötlemise turvalisus: käesolev poliitika rakendab isikuandmete kaitseks vajalikud kaugjuurdepääsu turbe-, krüpteerimis- ja logimiskontrollid, kui andmetele pääsetakse ligi või neid töödeldakse kaugkeskkonnas.

11.5.2 Artikkel 5(1)(f): tagab, et väljaspool ettevõtte asukohti kasutatavad isikuandmed on kaitstud loata või õigusvastase töötlemise ja juhusliku kaotsimineku eest.

11.5.3 Põhjendus 39: rõhutab juurdepääsu piiramist, terviklust ja konfidentsiaalsust, mis on eriti oluline siis, kui seadmed viiakse turvalistest ruumidest välja.

11.6 EU NIS2 direktiiv (2022/2555)

11.6.1 Artikkel 21(2)(a, b, d): nõuab, et kaugjuurdepääs oleks kaitstud organisatsiooni IKT-riskide juhtimise raamistiku osana. Käesolev poliitika täidab nõude turvameetmete kohta, mis hõlmavad juurdepääsukontrolli, andmeturvet ja organisatsioonilisi poliitikaid kaugkeskkondade jaoks.

11.6.2 Artikkel 21(3): soodustab turbeteadlikkust ja poliitika järgimist töötajate seas, kes töötavad väljaspool keskseid ruume.

11.7 EU DORA (2022/2554)

11.7.1 Artikkel 5 – juhtimise ja sisekontrolli raamistik: käesolev poliitika toetab IKT-riskide kontrolli ootusi kõigis tegevusstsenaariumides, sealhulgas hübriid- ja kaugmudelites.

11.7.2 Artikkel 8 – IKT-riskijuhtimise raamistik: kaugjuurdepääsuga seotud riskid tuvastatakse, maandatakse ja juhitakse siin rakendatud tehniliste ja korralduslike meetmete kaudu.

11.7.3 Artikkel 9 – teabe jagamise korraldus: kaitseb digitaalse operatiivse toimepidevuse võrgustikes jagatavat teavet kauglekke eest.

11.8 COBIT 2019

11.8.1 DSS01 – hallatud operatsioonid: käesolev poliitika toetab äritegevuse turvalist järjepidevust sõltumata füüsilisest asukohast.

11.8.2 BAI06 – hallatud IT-muudatused ja BAI09 – hallatud varad: tagavad, et kaugtöö seadmeid jälgitakse, need on turvaliselt konfigureeritud ja neid käsitletakse kriitiliste varadena.

11.8.3 APO13 – hallatud turve: edendab kaugkeskkondade jaoks määratletud turbejuhtimise raamistikku.

11.8.4 MEA03 – vastavuse seire, hindamine ja auditeerimine: sätestab, et kaugtöö tegevused peavad olema logitud, läbi vaadatud ja auditeeritud.