					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P09S					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**

Kooskõla standardite ja regulatsioonidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontroll 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
EL NIS2	Artikkel 21(2)(b), 21(2)(h)	EL NIS2
EL DORA	Artikkel 9	EL DORA
COBIT 2019	DSS05, APO13	COBIT 2019
EL GDPR	Artikkel 32	EL GDPR

1. Eesmärk

1.1 Käesolev poliitika kehtestab turbenõuded töötajatele ja töövõtjatele, kes teevad kaugtööd, sealhulgas kodust, jagatud tööruumidest või reisil viibides.

1.2 Poliitika eesmärk on kaitsta ettevõtte kontrolli alt väljaspool asuvates keskkondades kasutatava äriteabe konfidentsiaalsust, terviklust ja käideldavust.

1.3 Käesolev poliitika tagab vastavuse rahvusvahelistele standarditele ning vähendab selliseid riske nagu volitamata juurdepääs, andmekadu ja teenusekatkestused.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõikidele töötajatele (sh töötajatele, töövõtjatele, konsultantidele ja ajutistele töötajatele), kes kasutavad ettevõtte süsteeme, võrke või andmeid väljaspool ettevõtte asukohta töötades.

2.2 Poliitika hõlmab järgmist:

2.2.1 ettevõtte väljastatud ja isiklike seadmete kasutamine

2.2.2 juurdepääs VPN-i, kaugtöölaua või pilveteenuste kaudu

2.2.3 teabe turvaline käitlemine väljaspool ettevõtte ruume

2.2.4 seire, erandite haldamine ja poliitika rakendamine

2.3 Poliitika kehtib nii täis- kui osalise ajaga kaugtöökorraldusele, sealhulgas juhuslikule kaugjuurdepääsule.

3. Eesmärgid

3.1 Tõkestada ettevõtte süsteemidele või tundlikele andmetele volitamatu juurdepääs kaugtöö käigus.

3.2 Tagada, et kontoriväliselt kasutatavad seadmed ja sideühendused vastavad infoturbe miinimumnõuetele.

3.3 Säilitada kontroll kaugjuurdepääsuõiguste ja seire üle.

3.4 Anda töötajatele ja juhtidele selged suunised turvaliseks kaugtööks.

3.5 Täita ISO, NIS2, GDPR-i, DORA ja COBIT-i nõudeid seoses kaug- ja mobiiltööga.

4. Rollid ja vastutused

4.1 Tegevjuht

4.1.1 Kiidab heaks kaugtöökorralduse ja jälgib nõuete täitmist.

4.1.2 Eskaleerib turvaintsidendid või korduva mittevastavuse.

4.1.3 Vaatab läbi erandid ja tagab intsidendijärgsete tegevuste elluviimise.

4.2 IT-tugi või väline IT-teenuse osutaja

4.2.1 Seadistab turvalise kaugjuurdepääsu (nt VPN, MFA).

4.2.2 Rakendab lõppseadmete turvet, krüpteerimist ja seadistuspoliitikaid.

4.2.3 Toetab kasutajaid ja uurib tehnilisi turbeprobleeme.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Iga-aastane poliitika läbivaatamine

9.1.1 Tegevjuht ja IT-tugi peavad selle poliitika kord aastas läbi vaatama, et viia see kooskõlla tehnoloogia, töökorralduse ja õiguslike muudatustega.

9.2 Varasema ajakohastamise käivitajad

9.2.1 Viivitamatu läbivaatamine on nõutav pärast järgmist:

9.2.1.1 olulist kaugtööga seotud turvaintsidenti

9.2.1.2 muudatusi NIS2, GDPR-i või DORA nõuetes

9.2.1.3 üleminekut uuele kaugjuurdepääsu tehnoloogiale (nt teisele VPN-platvormile)

9.3 Versioonihaldus ja arhiveerimine

9.3.1 Kõik selle poliitika versioonid peavad olema:

9.3.1.1 kuupäevastatud ja tegevjuhi poolt heaks kiidetud

9.3.1.2 versiooninumbriga tähistatud

9.3.1.3 arhiveeritud vähemalt kolmeks aastaks

9.4 Töötajate teavitamine

9.4.1 Poliitikamuudatustest tuleb teavitada kõiki kaugtöötajaid. Iga olulise muudatuse korral on nõutav kinnituse andmine.

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika on seotud järgmiste dokumentidega ja toetab neid:

10.1.1 P2S – Juhtimisrollide ja vastutuste poliitika: määratleb, kes annab kaugjuurdepääsule volituse ja teeb selle üle järelevalvet

10.1.2 P4S – Juurdepääsukontrolli poliitika: kehtestab turvalise kaugjuurdepääsu seadistamise ja juurdepääsuõiguste tühistamise protseduurid

10.1.3 P6S – Riskijuhtimise poliitika: jälgib ja hindab kontorivälise juurdepääsuga seotud riske

10.1.4 P8S – Infoturbeteadlikkuse ja koolituse poliitika: koolitab kasutajaid kaugtöö riskide ja heade tavade osas

10.1.5 P30S – Intsidentidele reageerimise poliitika (P30): käsitleb kaugjuurdepääsuga seotud intsidente, nagu autentimistunnuste lekked või seadmete kadumine

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 6.1 – riskipõhine planeerimine kaugjuurdepääsu stsenaariumide jaoks

11.1.2 Punkt 6.2 – käsitleb personaliosakonna vastutust mobiilse ja kaugtöö kontekstis

11.1.3 Punkt 8.1 – kaugprotsesside operatiivne planeerimine ja kontroll

11.2 ISO/IEC 27002

11.2.1 Kontroll 6.7 – annab praktilised suunised kaug- ja mobiiltöö turbe kohta

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – kaugjuurdepääsu kontroll, sessioonikaitse ja turvaseire

11.3.2 AC-2 – kontohaldus kontoriväliste kasutajate jaoks

11.4 EL GDPR

11.4.1 Artikkel 32 – nõuab andmekaitset lõimituna ja vaikimisi, sealhulgas kaugtöö keskkonnas

11.5 EL NIS2 direktiiv

11.5.1 Artikkel 21(2)(b) – nõuab võrgu- ja infosüsteemide turvalist kasutamist

11.5.2 Artikkel 21(2)(h) – nõuab personaliga seotud turvameetmeid, sealhulgas kontoriväliseid kontrollimeetmeid

11.6 EL DORA

11.6.1 Artikkel 9 – nõuab finantssektori üksustelt IKT toimepidevuse tagamist kõigis töörežiimides, sealhulgas kaugjuurdepääsu korral

11.7 COBIT 2019

11.7.1 DSS05 – turvateenuste haldamine: hõlmab lõppseadmete kaitset ja turvalise kaugtöö praktikaid

11.7.2 APO13 – turbe haldamine: tagab mobiilse ja kaugjuurdepääsu puhul juurdepääsuõiguste turvalise andmise ning riskide järelevalve