					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P38					Dokumendi pealkiri: **Turvalise teabevahetuse ja mitmefaktorilise autentimise 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	5.30, 5.31, 8.24	
ISO/IEC 27002:2022	5.15, 5.17, 5.18, 8.24, 8.28	
NIST SP 800-53 Rev.5	IA-2, IA-3, IA-5, IA-8, SC-12, SC-13, SC-31	
ELi isikuandmete kaitse üldmäärus (GDPR)	Art. 32(1)(b)	
ELi NIS2 direktiiv	Art. 21(2)(j)	
ELi DORA määrus	Art. 9(2)(d), Art. 11	
COBIT 2019	DSS05.04, DSS05.05, DSS05.	

1. Eesmärk

1.1 Kehtestada nõuded mitmefaktorilise autentimise või pideva autentimise lahenduste kasutamiseks süsteemidele juurdepääsul kooskõlas NIS2 direktiivi artikli 21 lõike 2 punktiga j.

1.2 Kehtestada kontrollimeetmed turvalise kõne-, video-, teksti- ja hädaolukorra side jaoks, et kaitsta teabe konfidentsiaalsust ja terviklust.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõigi organisatsioonis kasutatavate autentimismehhanismide ja sidesüsteemide suhtes, sealhulgas häälkõnede, videokonverentside, sõnumside ja hädaolukorra teavitussüsteemide suhtes.

2.2 See hõlmab kõiki töötajaid, töövõtjaid ja kõiki väliseid osapooli, kes kasutavad organisatsiooni sidekanaleid või pääsevad ligi selle võrkudele ja infosüsteemidele.

3. Eesmärgid

3.1 Tagada, et süsteemidele pääsevad ligi üksnes nõuetekohaselt autentitud kasutajad, vähendades loata juurdepääsu riski mitmefaktorilise autentimise rakendamise kaudu.

3.2 Tagada, et sise- ja hädaolukorra side edastatakse turvaliste meetodite abil, näiteks krüpteeritud kanalite kaudu, vältides pealtkuulamist või kompromiteerimist.

3.3 Täita NIS2 nõuded tugeva autentimise ja turvalise side osas ning tugevdada organisatsiooni üldist küberkerksust.

4. Rollid ja vastutused

4.1 Infoturbejuht / IT-turbefunktsioon: määratleb ja haldab MFA mehhanisme ning turvalise side lahendusi; tagab käesoleva poliitika tehnilise rakendamise.

4.2 IT-administraatorid: rakendavad MFA asjakohastes süsteemides ja seadistavad heakskiidetud turvalise side platvormid; teostavad vastavusseiret.

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

9. Seire ja audit

9.1 IT-turbefunktsioon peab pidevalt seirama autentimislogisid, et tuvastada ühefaktorilise sisselogimise katsed või anomaalsed MFA tõrked. Turvaliste sidesüsteemide logisid tuleb asjakohasel juhul seirata loata juurdepääsukatsete või konfiguratsioonimuudatuste tuvastamiseks.

9.2 Siseaudit vaatab igal aastal üle MFA rakendamise järgimise, tagades, et kõik kriitilised süsteemid rakendavad MFA-d, ning kontrollib, et tundliku side jaoks kasutatakse üksnes heakskiidetud turvalisi kanaleid. Auditileiud esitatakse juhtkonnale koos soovitustega.

10. Läbivaatamine ja hooldus

10.1 Käesolev poliitika vaadatakse läbi vähemalt kord aastas ning pärast iga olulist turvaintsidenti või uue autentimise või sidega seotud riski tuvastamist, näiteks uute MFA vastu suunatud ründevektorite ilmnemisel või ebaturvaliste sidekanalite kasutamise avastamisel.

10.2 Vajaduse korral tehakse muudatusi, et arvestada arenevaid tehnoloogiaid, näiteks tugevamate pideva autentimise lahenduste kasutuselevõttu, või täita ajakohastatud regulatiivseid suuniseid, näiteks tulevasi ENISA soovitusi turvalise side kohta.

11. Seotud poliitikad ja seosed

11.1 P01 – Infoturbepoliitika. Määrab kogu ettevõttes kehtivad autentimise ja side kaitsemeetmed.

11.2 P04 – Juurdepääsukontrolli poliitika. Kehtestab juurdepääsuõiguste halduse, mida P38 MFA nõuded rakendavad.

11.3 P11 – Kasutajakontode ja õiguste haldamise poliitika. Seob MFA privilegeeritud juurdepääsu elutsükliga.

11.4 P18 – Krüptograafiliste kontrollimeetmete poliitika. Määrab turvalise side jaoks heakskiidetud krüptograafia ja võtmehalduse.

11.5 P21 – Võrguturbe poliitika. Kaitseb hääl-, video- ja sõnumside jaoks kasutatavaid transpordikanaleid.

11.6 P22 – Logimis- ja seirepoliitika. Seirab autentimissündmusi ja turvaliste kanalite kasutamist.

11.7 P32 – Talitluspidevuse ja katastroofitaaste poliitika. Tagab hädaolukorra side turvalisuse kriiside ajal.

11.8 P08 – Infoturbeteadlikkuse ja koolituse poliitika. Koolitab kasutajaid MFA ja turvaliste kanalite kasutamise hügieeni osas.

12. Viited

12.1 NIS2 direktiiv (EL 2022/2555), artikli 21 lõike 2 punkt j (mitmefaktorilise autentimise ja turvalise side kasutamine)

12.2 Komisjoni rakendusmäärus (EL) 2024/2690, lisa punkt 11 (juurdepääsukontrolli nõuded, sealhulgas MFA privilegeeritud kontode jaoks)

12.3 ISO/IEC 27001:2022 ja ISO/IEC 27002:2022