					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P38					Dokumenta nosaukums: **Drošas saziņas un daudzfaktoru autentifikācijas politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņots ar piemērojamajiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
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	
ES VDAR	32. panta 1. punkta b) apakšpunkts	
ES NIS2	21. panta 2. punkta j) apakšpunkts	
ES DORA	9. panta 2. punkta d) apakšpunkts, 11. pants	
COBIT 2019	DSS05.04, DSS05.05, DSS05.	

1. Mērķis

1.1 Noteikt prasības daudzfaktoru autentifikācijas vai nepārtrauktās autentifikācijas risinājumu izmantošanai piekļuvei sistēmām atbilstoši NIS2 direktīvas 21. panta 2. punkta j) apakšpunktam.

1.2 Noteikt kontroles pasākumus aizsargātai balss, video, teksta un ārkārtas saziņai, lai aizsargātu informācijas konfidencialitāti un integritāti.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visiem autentifikācijas mehānismiem un saziņas sistēmām (balss zvaniem, videokonferencēm, ziņapmaiņu un ārkārtas paziņošanas sistēmām), ko izmanto organizācija.

2.2 Tā attiecas uz visiem darbiniekiem, līgumslēdzējiem un jebkurām ārējām pusēm, kas izmanto organizācijas saziņas kanālus vai piekļūst tās tīklam un informācijas sistēmām.

3. Mērķi

3.1 Nodrošināt, ka piekļuve sistēmām tiek piešķirta tikai pienācīgi autentificētiem lietotājiem, samazinot nesankcionētas piekļuves risku, ieviešot daudzfaktoru autentifikāciju (MFA).

3.2 Nodrošināt, ka iekšējā un ārkārtas saziņa tiek pārraidīta, izmantojot drošas metodes (piemēram, šifrētus kanālus), novēršot noklausīšanos vai manipulācijas.

3.3 Nodrošināt atbilstību NIS2 prasībām attiecībā uz stingru autentifikāciju un drošu saziņu, stiprinot kopējo kiberdrošības noturību.

4. Lomas un pienākumi

4.1 Galvenais informācijas drošības vadītājs (CISO) / IT drošības funkcija: nosaka un uztur MFA mehānismus un drošas saziņas rīkus; nodrošina šīs politikas tehnisko izpildi.

4.2 IT administratori: ievieš MFA attiecīgajās sistēmās un konfigurē apstiprinātās drošās saziņas platformas; uzrauga atbilstību.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Uzraudzība un audits

9.1 IT drošības funkcijai nepārtraukti jāuzrauga autentifikācijas žurnāli, lai identificētu jebkādus vienfaktora pieteikšanās mēģinājumus vai anomālas MFA atteices. Drošo saziņas sistēmu žurnāli (ja

piemērojams) jāuzrauga, lai identificētu nesankcionētas piekļuves mēģinājumus vai konfigurācijas izmaiņas.

9.2 Iekšējais audits reizi gadā pārskata atbilstību MFA ieviešanai (nodrošinot, ka visās kritiskajās sistēmās tiek piemērota MFA) un pārbauda, vai sensitīvai saziņai tiek izmantoti tikai apstiprināti drošie kanāli. Konstatējumi un rekomendācijas tiek ziņoti vadībai.

10. Pārskatīšana un uzturēšana

10.1 Šī politika jāpārskata vismaz reizi gadā, kā arī pēc jebkura būtiska drošības incidenta vai jaunatklāta riska, kas saistīts ar autentifikāciju vai saziņu (piemēram, jauniem apdraudējuma vektoriem pret MFA vai nedrošu saziņas risinājumu izmantošanas atklāšanas).

10.2 Grozījumi jāveic pēc nepieciešamības, lai ņemtu vērā tehnoloģiju attīstību (piemēram, noturīgāku nepārtrauktās autentifikācijas risinājumu ieviešanu) vai nodrošinātu atbilstību aktualizētajām regulatīvajām vadlīnijām (piemēram, turpmākām ENISA rekomendācijām par drošu saziņu).

11. Saistītās politikas un sasaiste

11.1 P01 – Informācijas drošības politika. Nosaka visā organizācijā piemērojamos autentifikācijas un saziņas aizsardzības pasākumus.

11.2 P04 – Piekļuves kontroles politika. Nosaka piekļuves pārvaldību, kuras īstenošanu P38 ietvaros nodrošina MFA.

11.3 P11 – Lietotāju kontu un privilēģiju pārvaldības politika. Saista MFA ar priviliģētas piekļuves dzīves ciklu.

11.4 P18 – Kriptogrāfisko kontroles pasākumu politika. Nosaka apstiprināto kriptogrāfiju un atslēgu pārvaldību drošai saziņai.

11.5 P21 – Tīkla drošības politika. Aizsargā pārraides kanālus, kas tiek izmantoti balss, video un ziņapmaiņas saziņai.

11.6 P22 – Žurnālfiksēšanas un uzraudzības politika. Nodrošina autentifikācijas notikumu un drošo kanālu izmantošanas uzraudzību.

11.7 P32 – Darbības nepārtrauktības un avārijas seku novēršanas politika. Nodrošina ārkārtas saziņas aizsardzību krīzes situācijās.

11.8 P08 – Informācijas drošības informētības un apmācības politika. Apmāca lietotājus par MFA un saziņas kanālu drošas lietošanas praksi.

12. Atsauces

12.1 NIS2 direktīva (ES 2022/2555), 21. panta 2. punkta j) apakšpunkts (daudzfaktoru autentifikācijas un drošas saziņas izmantošana)

12.2 Komisijas Īstenošanas regula (ES) 2024/2690, pielikuma 11. sadaļa (piekļuves kontroles prasības, tostarp MFA priviliģētiem kontiem)

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