					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P38					Dokumenttitel: **Politik for sikker kommunikation og multifaktorautentificering**						
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:						
X	Politik		Standard		Procedure		Formular		Register		Andet

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regulering

Standard/regulering	Klausul/artikel	Kommentar
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	
EU GDPR	Art. 32(1)(b)	
EU NIS2	Art. 21(2)(j)	
EU DORA	Art. 9(2)(d), Art. 11	
COBIT 2019	DSS05.04, DSS05.05, DSS05.	

1. Formål

1.1 At fastlægge krav til anvendelse af multifaktorautentificering eller løsninger til løbende autentificering ved systemadgang i overensstemmelse med NIS2 artikel 21, stk. 2, litra j.

1.2 At etablere kontroller for sikker tale-, video-, tekst- og nødkommunikation med henblik på at beskytte oplysningers fortrolighed og integritet.

2. Omfang

2.1 Denne politik gælder for alle autentificeringsmekanismer og kommunikationssystemer (taleopkald, videokonferencer, meddelelsestjenester og nødunderretningssystemer), som organisationen anvender.

2.2 Den omfatter alle medarbejdere, kontrahenter og eventuelle eksterne parter, der anvender organisationens kommunikationskanaler eller får adgang til dens netværks- og informationssystemer.

3. Mål

3.1 At sikre, at kun brugere med tilstrækkelig autentificering får adgang til systemer, og dermed reducere risikoen for uautoriseret adgang gennem implementering af multifaktorautentificering (MFA).

3.2 At sikre, at intern kommunikation og nødkommunikation overføres ved brug af sikre metoder (f.eks. krypterede kanaler), så aflytning eller manipulation forebygges.

3.3 At efterleve NIS2-krav til stærk autentificering og sikker kommunikation og dermed styrke den samlede cyberrobusthed.

4. Roller og ansvar

4.1 CISO/ISMS-ansvarlig/it-sikkerhed: Definerer og vedligeholder MFA-mekanismer og sikre kommunikationsværktøjer samt sikrer teknisk håndhævelse af denne politik.

4.2 It-administratorer: Implementerer MFA for relevante systemer, konfigurerer godkendte sikre kommunikationsplatforme og overvåger efterlevelse.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Overvågning og revision

9.1 It-sikkerhed skal løbende overvåge autentificeringsoptegnelser og logfiler for forsøg på login med kun én faktor eller unormale MFA-fejl. Logfiler fra sikre kommunikationssystemer skal, hvor det er relevant, overvåges for forsøg på uautoriseret adgang eller konfigurationsændringer.

9.2 Intern revision skal årligt gennemgå efterlevelsen af MFA-udrulning, herunder sikre, at alle kritiske systemer håndhæver MFA, og verificere, at godkendte sikre kanaler anvendes eksklusivt til følsom kommunikation. Konstateringer rapporteres til ledelsen med anbefalinger.

10. Gennemgang og vedligeholdelse

10.1 Denne politik gennemgås mindst årligt og ved enhver større sikkerhedshændelse eller nyidentificeret risiko relateret til autentificering eller kommunikation (f.eks. nye trusselsvektorer mod MFA eller konstateret brug af usikker kommunikation).

10.2 Revisioner af politikken gennemføres efter behov for at adressere teknologisk udvikling (f.eks. indførelse af mere robuste løsninger til løbende autentificering) eller for at efterleve opdateret regulatorisk vejledning (såsom fremtidige anbefalinger fra ENISA om sikker kommunikation).

11. Relaterede politikker og sammenhænge

11.1 P01 – Informationssikkerhedspolitik. Fastlægger virksomhedsdækkende sikkerhedsforanstaltninger for autentificering og kommunikation.

11.2 P04 – Politik for adgangskontrol. Etablerer adgangsstyring, som MFA i P38 håndhæver.

11.3 P11 – Politik for styring af brugerkonti og privilegier. Knytter MFA til livscyklusstyring af privilegeret adgang.

11.4 P18 – Politik for kryptografiske kontroller. Angiver godkendt kryptografi og nøglestyring for sikker kommunikation.

11.5 P21 – Politik for netværkssikkerhed. Sikrer transportkanaler anvendt til tale, video og meddelelsestjenester.

11.6 P22 – Lognings- og overvågningspolitik. Overvåger autentificeringshændelser og brug af sikre kanaler.

11.7 P32 – Politik for forretningskontinuitet og genopretning efter alvorlige hændelser. Sikrer nødkommunikation under kriser.

11.8 P08 – Politik for bevidsthed om informationssikkerhed og uddannelse. Træner brugere i MFA og sikker kanalhygiejne.

12. Referencer

12.1 NIS2-direktivet (EU 2022/2555), artikel 21, stk. 2, litra j (brug af multifaktorgodkendelse og sikker kommunikation)

12.2 Kommissionens gennemførelsesforordning (EU) 2024/2690, bilag afsnit 11 (krav til adgangsstyring, herunder MFA for privilegerede konti)

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