					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P38					Dokumenttitel: **Policy för säker kommunikation och multifaktorautentisering (MFA)**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Anpassning till standarder och regelverk

Standard/förordning	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:s GDPR	Art. 32(1)(b)	
EU:s NIS2-direktiv	Art. 21(2)(j)	
EU:s DORA-förordning	Art. 9(2)(d), Art. 11	
COBIT 2019	DSS05.04, DSS05.05, DSS05.	

1. Syfte

1.1 Fastställa krav för användning av multifaktorautentisering (MFA) eller lösningar för kontinuerlig autentisering vid åtkomst till system, i enlighet med artikel 21.2 j i EU:s NIS2-direktiv.

1.2 Fastställa kontroller för säker röst-, video-, text- och nödkommunikation för att skydda informationens konfidentialitet och riktighet.

2. Omfattning

2.1 Denna policy gäller för alla autentiseringsmekanismer och kommunikationssystem (röstsamtal, videokonferenser, meddelandetjänster och system för nödavisering) som används av organisationen.

2.2 Den omfattar alla anställda, entreprenörer och tredjepartsleverantörer samt andra externa parter som använder organisationens kommunikationskanaler eller får åtkomst till dess nätverks- och informationssystem.

3. Mål

3.1 Säkerställa att endast användare som har autentiserats på ett tillräckligt robust sätt får åtkomst till system, vilket minskar risken för obehörig åtkomst genom införande av multifaktorautentisering (MFA).

3.2 Säkerställa att intern kommunikation och nödkommunikation överförs med säkra metoder (t.ex. krypterade kanaler) för att förhindra avlyssning eller manipulation.

3.3 Uppfylla kraven i EU:s NIS2-direktiv avseende stark autentisering och säker kommunikation samt stärka den övergripande cyberresiliensen.

4. Roller och ansvar

4.1 Informationssäkerhetschef (CISO) / IT-säkerhetsfunktion: Ska fastställa och förvalta MFA-mekanismer och verktyg för säker kommunikation samt säkerställa tekniskt genomförande av denna policy.

4.2 IT-administratörer: Ska införa MFA för relevanta system, konfigurera godkända plattformar för säker kommunikation samt övervaka efterlevnaden.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Övervakning och revision

9.1 IT-säkerhetsfunktionen ska kontinuerligt övervaka autentiseringsloggar avseende försök till inloggning med enbart en faktor eller avvikande MFA-fel. Loggar från system för säker kommunikation

ska, där så är tillämpligt, övervakas med avseende på försök till obehörig åtkomst eller konfigurationsändringar.

9.2 Internrevisionen/funktionen för regelefterlevnad ska årligen granska efterlevnaden av införandet av MFA (för att säkerställa att alla kritiska system tillämpar MFA) och verifiera att endast godkända säkra kanaler används för känslig kommunikation. Resultaten ska rapporteras till ledningen tillsammans med rekommendationer.

10. Granskning och underhåll

10.1 Denna policy ska granskas minst årligen samt vid varje större säkerhetsincident eller nyidentifierad risk relaterad till autentisering eller kommunikation (t.ex. nya angreppsvektorer mot MFA eller upptäckt av osäker användning av kommunikationskanaler).

10.2 Revideringar ska göras vid behov för att hantera teknikutveckling (t.ex. införande av mer robusta lösningar för kontinuerlig autentisering) eller för att uppfylla uppdaterad regulatorisk vägledning (såsom framtida rekommendationer från ENISA om säker kommunikation).

11. Relaterade policyer och kopplingar

11.1 P01 – Informationssäkerhetspolicy. Fastställer organisationens övergripande skyddsåtgärder för autentisering och kommunikation.

11.2 P04 – Policy för åtkomstkontroll. Fastställer den behörighetsstyrning som MFA i P38 upprätthåller.

11.3 P11 – Policy för hantering av användarkonton och privilegier. Kopplar MFA till livscykelhantering för privilegierad åtkomst.

11.4 P18 – Policy för kryptografiska kontroller. Anger godkänd kryptografi och nyckelhantering för säker kommunikation.

11.5 P21 – Nätverkssäkerhetspolicy. Skyddar överföringskanaler som används för röst, video och meddelandetjänster.

11.6 P22 – Loggnings- och övervakningspolicy. Reglerar övervakning av autentiseringshändelser och användning av säkra kanaler.

11.7 P32 – Policy för verksamhetskontinuitet och katastrofåterställning. Säkerställer säker nödkommunikation under kriser.

11.8 P08 – Policy för informationssäkerhetsmedvetenhet och utbildning. Utbildar användare om MFA och säker användning av kommunikationskanaler.

12. Referenser

12.1 NIS2-direktivet (EU 2022/2555), artikel 21.2 j (användning av multifaktorautentisering (MFA) och säkerställd kommunikation)

12.2 Kommissionens genomförandeförordning (EU) 2024/2690, bilaga avsnitt 11 (krav för åtkomstkontroll, inklusive MFA för privilegierade konton)

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