					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P38					Documenttitel: **Beleid inzake beveiligde communicatie en multifactorauthenticatie**						
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:						
X	Beleid		Standaard		Procedure		Formulier		Register		Overig

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Afstemming op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
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	
AVG	Art. 32(1)(b)	
NIS2-richtlijn	Art. 21(2)(j)	
DORA	Art. 9(2)(d), Art. 11	
COBIT 2019	DSS05.04, DSS05.05, DSS05.	

1. Doel

1.1 Het vaststellen van vereisten voor het gebruik van multifactorauthenticatie of continue authenticatie voor systeemtoegang, in lijn met artikel 21(2)(j) van de NIS2-richtlijn.

1.2 Het vaststellen van beheersmaatregelen voor beveiligde spraak-, video-, tekst- en noodcommunicatie ter bescherming van de vertrouwelijkheid en integriteit van informatie.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle authenticatiemechanismen en communicatiesystemen (spraakoproepen, videoconferenties, berichtenverkeer en noodmeldingssystemen) die door de organisatie worden gebruikt.

2.2 Dit beleid geldt voor alle medewerkers, opdrachtnemers en externe partijen die gebruikmaken van de communicatiekanalen van de organisatie of toegang hebben tot haar netwerk- en informatiesystemen.

3. Doelstellingen

3.1 Waarborgen dat uitsluitend adequaat geauthenticeerde gebruikers toegang krijgen tot systemen, om het risico op ongeautoriseerde toegang te verminderen door de implementatie van MFA.

3.2 Waarborgen dat interne communicatie en noodcommunicatie via beveiligde methoden worden verzonden (bijvoorbeeld versleutelde kanalen), zodat afluisteren of manipulatie wordt voorkomen.

3.3 Voldoen aan de NIS2-vereisten voor sterke authenticatie en beveiligde communicatie en daarmee de algehele cyberweerbaarheid versterken.

4. Rollen en verantwoordelijkheden

4.1 CISO / informatiebeveiligingsfunctie: het definiëren en onderhouden van MFA-mechanismen en middelen voor beveiligde communicatie, en het borgen van de technische handhaving van dit beleid.

4.2 IT-beheerders: het implementeren van MFA voor relevante systemen, het configureren van goedgekeurde platforms voor beveiligde communicatie en het toezien op naleving.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Monitoring en audit

9.1 De informatiebeveiligingsfunctie moet authenticatielogboeken continu monitoren op pogingen tot aanmelding met één factor of afwijkende MFA-faalpatronen. Logboeken van systemen voor beveiligde

communicatie moeten, waar van toepassing, worden gemonitord op pogingen tot ongeautoriseerde toegang of configuratiewijzigingen.

9.2 De interne audit- en compliancefunctie beoordeelt jaarlijks de naleving van de uitrol van MFA, waarbij wordt vastgesteld dat alle kritieke systemen MFA afdwingen, en verifieert dat goedgekeurde beveiligde kanalen exclusief worden gebruikt voor gevoelige communicatie. Bevindingen worden met aanbevelingen gerapporteerd aan het management.

10. Herziening en onderhoud

10.1 Dit beleid wordt ten minste jaarlijks beoordeeld en daarnaast na elk ernstig beveiligingsincident of nieuw geïdentificeerd risico met betrekking tot authenticatie of communicatie (zoals nieuwe dreigingsvectoren tegen MFA of vastgesteld onveilig gebruik van communicatiekanalen).

10.2 Herzieningen worden waar nodig doorgevoerd om in te spelen op technologische ontwikkelingen (zoals de invoering van robuustere oplossingen voor continue authenticatie) of om te voldoen aan geactualiseerde wettelijke richtsnoeren (zoals toekomstige ENISA-aanbevelingen over beveiligde communicatie).

11. Gerelateerde beleidslijnen en samenhang

11.1 P01 – Informatiebeveiligingsbeleid. Stelt organisatiebrede waarborgen voor authenticatie en communicatie vast.

11.2 P04 – Beleid inzake toegangscontrole. Legt de governance voor toegang vast die door MFA in P38 wordt afgedwongen.

11.3 P11 – Beleid inzake beheer van gebruikersaccounts en privileges. Verbindt MFA met de levenscyclus van geprivilegieerde toegang.

11.4 P18 – Beleid inzake cryptografische beheersmaatregelen. Biedt goedgekeurd crypto- en sleutelbeheer voor beveiligde communicatie.

11.5 P21 – Beleid inzake netwerkbeveiliging. Beveiligt transportkanalen die worden gebruikt voor spraak, video en berichtenverkeer.

11.6 P22 – Logging- en monitoringbeleid. Monitort authenticatiegebeurtenissen en het gebruik van beveiligde kanalen.

11.7 P32 – Beleid inzake bedrijfscontinuïteit en herstel na verstoringen. Beveiligt noodcommunicatie tijdens crisissituaties.

11.8 P08 – Beleid inzake bewustwording en opleiding op het gebied van informatiebeveiliging. Traindt gebruikers in MFA en veilig gebruik van communicatiekanalen.

12. Referenties

12.1 NIS2-richtlijn (EU 2022/2555), artikel 21(2), punt (j) (gebruik van multifactorauthenticatie en beveiligde communicatie)

12.2 Uitvoeringsverordening (EU) 2024/2690 van de Commissie, bijlage, sectie 11 (vereisten inzake toegangscontrole, waaronder MFA voor geprivilegieerde accounts)

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