					Insert Registered Legal Entity Name Here							
Document number: P38					Document Title: **Secure Communications and Multi-Factor Authentication (MFA) Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations

Standard/Regulation	Clause/Article	Comment
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. Purpose

1.1 Define requirements for the use of Multi-Factor Authentication (MFA) or continuous authentication solutions for system access, in line with NIS2 Article 21(2)(j).

1.2 Establish controls for secure voice, video, text, and emergency communications to protect the confidentiality, integrity, and availability of information.

2. Scope

2.1 This policy applies to all authentication mechanisms and communication systems (voice calls, video conferencing, messaging, and emergency notification systems) used by the organization.

2.2 It applies to all employees and contractors, as well as any external parties using the organization's communication channels or accessing its network and information systems.

3. Objectives

3.1 Ensure that only adequately authenticated users gain access to systems, thereby reducing the risk of unauthorized access through the implementation of Multi-Factor Authentication (MFA).

3.2 Ensure that internal and emergency communications are transmitted using secure methods (e.g., encrypted channels) to prevent interception or tampering.

3.3 Comply with NIS2 requirements for strong authentication and secure communications, thereby strengthening overall ICT resilience.

4. Roles and Responsibilities

4.1 CISO / Information Security: Define and maintain Multi-Factor Authentication (MFA) mechanisms and secure communication tools; ensure technical enforcement of this policy.

4.2 IT Administrators: Implement Multi-Factor Authentication (MFA) for relevant systems, configure approved secure communication platforms, and monitor compliance.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Monitoring and Audit

9.1 Information Security shall continuously monitor authentication logs for any single-factor login attempts or anomalous Multi-Factor Authentication (MFA) failures. Logs from secure communication systems, where applicable, shall be monitored for unauthorized access attempts or configuration changes.

9.2 The Internal Audit and Compliance function shall annually review adherence to Multi-Factor Authentication (MFA) deployment requirements, including confirmation that all critical systems enforce Multi-Factor Authentication (MFA), and verify that only approved secure channels are used for sensitive communications. Audit findings shall be reported to management together with recommendations.

10. Review and Maintenance

10.1 This policy shall be reviewed at least annually and following any major security incident or newly identified risk related to authentication or communications (e.g., new threat vectors targeting Multi-Factor Authentication (MFA) or the identification of insecure communications usage).

10.2 Revisions shall be made as necessary to address evolving technologies (e.g., adoption of more robust continuous authentication solutions) or to comply with updated regulatory guidance (such as future ENISA recommendations on secure communications).

11. Related Policies and Linkages

11.1 P01 – Information Security Policy. Establishes organization-wide safeguards for authentication and communications.

11.2 P04 – Access Control Policy. Establishes access governance that Multi-Factor Authentication (MFA) under P38 enforces.

11.3 P11 – User Account and Privilege Management Policy. Links Multi-Factor Authentication (MFA) to the privileged access lifecycle.

11.4 P18 – Cryptographic Controls Policy. Defines approved cryptographic controls and key management for secure communications.

11.5 P21 – Network Security Policy. Secures the transport channels used for voice, video, and messaging.

11.6 P22 – Logging and Monitoring Policy. Monitors authentication events and secure channel usage.

11.7 P32 – Business Continuity and Disaster Recovery Policy. Secures emergency communications during crises.

11.8 P08 – Information Security Awareness and Training Policy. Trains users on Multi-Factor Authentication (MFA) and secure channel hygiene.

12. References

12.1 NIS2 Directive (EU 2022/2555), Article 21(2), point (j) (use of Multi-Factor Authentication (MFA) and secure communications)

12.2 Commission Implementing Regulation (EU) 2024/2690, Annex Section 11 (access control requirements, including Multi-Factor Authentication (MFA) for privileged accounts)

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