					[Insert Registered Legal Entity Name Here]									
Document number: P38					Document Title: Secure Communications and Multi-Factor Authentication 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 where applicable		
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, DSS05.07	

NOTE:

P38 Secure Communications and MFA Policy: This policy was introduced to fulfill NIS2 Article 21(2)(j), which explicitly requires the use of multi-factor authentication and secured communications (voice, video, text, and emergency systems) where appropriate. The Commission's Implementing Regulation annex on access control underscores strong authentication (MFA) for privileged and regular user access, so P38 extends those controls organization-wide. It also sets requirements for encrypted communication platforms, addressing the lack of a secure communications framework in the base policies. By defining how to securely handle emergency communications and requiring encryption for voice/video calls, P38 closes the gap in protecting sensitive communications channels. P38 ensures compliance with NIS2's authentication and communications security clause and aligns with ENISA guidance that stresses using state-of-the-art security for internal communications and user access

1. **Purpose**
   1.1 Define the requirements for using multi-factor or continuous authentication solutions for system access, in line with NIS2 Article 21(2)(j).
   1.2 Establish controls for secured voice, video, text, and emergency communications to protect confidentiality and integrity 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 covers all employees, contractors, and any external parties using the organization's communication channels or accessing its network and information systems.
3. **Objectives**
   3.1 Ensure only adequately authenticated users gain access to systems, reducing risk of unauthorized access through MFA implementation.
   3.2 Guarantee that internal and emergency communications are transmitted using secure methods (e.g., encrypted channels), preventing eavesdropping or tampering.
   3.3 Comply with NIS2 requirements for strong authentication and secure communications, enhancing overall cyber resilience.
4. **Roles and Responsibilities**
   4.1 CISO / IT Security: Define and maintain MFA mechanisms and secure communication tools; ensure technical enforcement of this policy.
   4.2 IT Administrators: Implement MFA for relevant systems and configure approved secure communication platforms; monitor compliance.
   4.3 All Employees and Contractors: Use the designated MFA methods and secure channels as mandated; report any issues or exceptions to IT Security.
   4.4 Emergency Response Coordinator: Ensure emergency communication systems are secure and accessible during crises; conduct periodic drills using secure channels.

   […….

   …….

   …….

   …….

   …….]

10. **Review and Maintenance**
    10.1 This policy will be reviewed at least annually, and upon any major security incident or newly identified risk related to authentication or communications (e.g., new threat vectors against MFA, discovery of insecure comms usage).
    10.2 Revisions will be made as needed 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. Mandates enterprise-wide authentication and communications safeguards.
    11.2 **P04** – Access Control Policy. Establishes access governance that MFA in P38 enforces.
    11.3 **P11** – User Account and Privilege Management Policy. Ties MFA to privileged access lifecycle.
    11.4 **P18** – Cryptographic Controls Policy. Provides approved crypto/key management for secure comms.

11.5 **P21** – Network Security Policy. Secures transport channels used by voice/video/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 MFA and channel hygiene.

12. References

12.1 NIS2 Directive (EU 2022/2555), Article 21(2), point (j) (use of multi-factor authentication and secured communications)
12.2 Commission Implementing Regulation (EU) 2024/2690, Annex Section 11 (Access control requirements, including MFA for privileged accounts)
12.3 ISO/IEC 27001:2022 and ISO/IEC 27002:2022