					[Insert Registered Legal Entity Name Here]										
Document number: P36					Document Title: **Social Media and External Communications Policy**										
Version: 1.0		Effective Date: 01.01.2025			Document Owner: IT										
	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	Clause 8.1	
ISO/IEC 27002:2022	Controls 5.10,5.11, 5.35,5.36	
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	
EU GDPR	Articles 5, 25, 32, 33	
EU NIS2	Article 21	
EU DORA	Articles 9, 16	
COBIT 2019	APO09, DSS05	

					[Insert Registered Legal Entity Name Here]									
Document number: P36					Document Title: **Social Media and External Communications Policy**									
Version: 1.0		Effective Date: 01.01.2025			Document Owner: IT									
	Policy		Standard		Procedure		Form		Register		Other			

1. **Purpose**
   1.1. This policy establishes mandatory rules and responsibilities governing the use of social media and all forms of external communication by personnel affiliated with the organization.
   1.2. It ensures that public messaging—whether planned or spontaneous—is accurate, respectful, secure, legally compliant, and brand-consistent.
   1.3. The policy aims to minimize risks associated with reputational harm, regulatory breach, intellectual property leakage, and unauthorized disclosures via public-facing channels.
   1.4. It further promotes accountability and structured governance in all forms of digital communication involving or affecting the organization.
2. **Scope**
   2.1. This policy applies to all employees, contractors, interns, and third-party representatives who:
      2.1.1. Communicate on behalf of the organization, whether officially or informally
      2.1.2. Reference or imply affiliation with the organization in a public setting
      2.1.3. Use personal or corporate accounts to engage in public discussions involving the organization
   2.2. Covered communication channels include, but are not limited to:
      2.2.1. Social media platforms (e.g., LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook)
      2.2.2. Blogs, wikis, forums, and public discussion boards
      2.2.3. Email or direct messaging to external parties (e.g., clients, regulators, media)
      2.2.4. Press interviews, speaking panels, or recorded media appearances
      2.2.5. Participation in online communities where the organization is referenced
   2.3. This policy governs both real-time and pre-scheduled content and applies to all devices and accounts (personal or corporate) used to disseminate the communication.
3. **Objectives**
   3.1. To prevent the accidental or intentional disclosure of confidential, sensitive, or regulated information through external communication channels.
   3.2. To ensure that official public statements and social media content are accurate, authorized, and aligned with corporate branding, ethics, and strategic messaging.
   3.3. To prevent reputational damage and enforce consistency in messaging across internal departments and external platforms.
   3.4. To comply with applicable legal obligations related to public statements, including but not limited to GDPR, NIS2, DORA, and sector-specific communications rules.
   3.5. To define clear responsibilities, permissible use cases, and enforcement protocols for all personnel engaged in public-facing activities.
4. **Roles and Responsibilities**
   4.1. **Chief Marketing or Communications Officer / PR Lead**
      4.1.1. Approves all official company messaging for external publication
      4.1.2. Maintains social media content schedules and guidelines for brand consistency
      4.1.3. Monitors online mentions and media exposure involving the organization
   4.2. **Chief Information Security Officer (CISO) / Security Team**

4.2.1. Monitors digital platforms for indicators of data leakage, impersonation, or phishing attempts

4.2.2. Coordinates with incident response teams in the event of social media-based attacks or breaches

4.3. **Legal and Compliance Function**

[.....]

11. Reference Standards and Frameworks

This policy aligns with internationally recognized standards and regulatory requirements to ensure secure, lawful, and brand-consistent public communications.

ISO/IEC 27001:2022

Clause 8.1 – Operational Planning and Control: Requires defined processes and role-based governance for managing public communications, ensuring accuracy, approval workflows, and escalation of incidents involving data or reputation risk.

ISO/IEC 27002:2022 – Controls 5.10–5.11, 5.35–5.36

Control 5.10 – Use of Information: Governs the authorized and ethical dissemination of internal or external communications.

Control 5.11 – Acceptable Use of Information and Assets: Reinforces acceptable practices for sharing content using corporate assets or personal accounts.

Control 5.35 – Contact with Authorities: Requires structured and authorized external communication with regulatory bodies and public agencies.

Control 5.36 – Compliance with Policies and Standards: Enforces consistent application of internal policies in all communication scenarios.

NIST SP 800-53 Rev.5

PL-4 – Rules of Behavior: Requires formal rules for system and communication usage, including public disclosure standards.

AC-8 – System Use Notification: Supports mandatory disclaimers and content warnings on external-facing platforms.

AU-12 – Audit Record Retention: Applies to the preservation of logs and communications history for incident review and audit purposes.

EU GDPR (2016/679)

Article 5 – Principles of Data Processing: Prohibits unauthorized sharing of personal data through public communication.

Article 25 – Data Protection by Design and by Default: Requires privacy safeguards in communication tools and content workflows.

Article 32 – Security of Processing: Applies encryption, access control, and content approval processes.

Article 33 – Breach Notification: Mandates timely disclosure of personal data leaks via public channels.

EU NIS2 Directive (2022/2555)

Article 21 – Cybersecurity Risk Management Measures: Includes communication protocols and obligations during incidents and public messaging around risk.

EU DORA (2022/2554)

Article 9 – ICT Risk Management: Applies to externally triggered communication risks such as impersonation, misinformation, and reputational disruption.

Article 16 – Communications Strategy: Requires that critical financial or service providers manage communication risks and responses in crisis scenarios.

COBIT 2019

APO09 – Managed Service Agreements and Communication: Requires structured governance over internal and external communications.

DSS05 – Manage Security Services: Ensures that communication activities do not introduce additional risk or undermine incident handling processes.