					Insert Registered Legal Entity Name Here							
Document number: P36S					Document Title: **Social Media and External Communications 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	Clause 8	Defined processes and role-based training governance for managing public communications, ensuring accuracy, approval workflows, and incident escalation.
ISO/IEC 27002:2022	Controls 5.10, 5.11, 5.35, 5.36	Governs use, acceptable use, external contact/authority communication, and compliance monitoring.
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	Rules for system and communication use, user notifications, and audit record retention.
EU GDPR	Articles 5, 25, 32, 33	Principles of data processing, data protection by design, security of processing, and breach notification requirements.
EU NIS2	Article 21	Cybersecurity risk management measures, incident obligations, and risk-related public messaging.
EU DORA	Articles 9, 16	ICT risk management and communication strategy for critical providers.
COBIT 2019	APO09, DSS05	Service agreement and communication governance, and secure communication and incident management practices.

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 consistent with the organization's brand.

1.3 This policy is intended to minimize risks associated with reputational harm, regulatory non-compliance, intellectual property leakage, and unauthorized disclosures through public-facing channels.

1.4 It further promotes accountability and structured governance across all forms of digital communication involving or affecting the organization.

2. Scope

2.1 This policy applies to all employees, contractors, third-party service providers, 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, panel discussions, or recorded media appearances

2.2.5 Participation in online communities in which 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 such 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 ensure consistency in messaging across internal departments and external platforms.

3.4 To comply with applicable legal obligations relating to public statements, including but not limited to GDPR, NIS2, DORA, and sector-specific communications requirements.

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 Officer, Chief Communications Officer, or 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) / Information 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

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

9. Enforcement and Compliance

9.1 This policy is mandatory for all covered personnel and third parties. Failure to comply may result in:

9.1.1 Formal warnings

9.1.2 Temporary or permanent revocation of access to platforms or systems

9.1.3 Disciplinary action, including termination

9.1.4 Legal proceedings, if external communication results in reputational damage, a data breach, or regulatory non-compliance

9.2 Disciplinary Actions

9.2.1 Internal violations (e.g., leaking confidential data, defaming the organization) will trigger Human Resources involvement, a formal investigation, and documentation in the employee file.

9.2.2 Where applicable, Legal will pursue civil remedies or notify authorities of criminal activity (e.g., impersonation, insider trading leaks).

9.3 Compliance Monitoring

9.3.1 The Security and Communications teams must perform ongoing monitoring of:

9.3.1.1 Brand mentions across major platforms

9.3.1.2 Unofficial use of company imagery or trademarks

9.3.1.3 Known risks (e.g., disgruntled employees, impersonation attempts)

9.3.2 Monitoring must comply with employee privacy laws and regulations, and all flagged cases must be verified by a human reviewer.

9.4 Whistleblower and Misuse Reporting

9.4.1 Any employee who suspects a violation of this policy is encouraged to report it to the Information Security Team, Legal, or anonymously through the Whistleblower portal.

9.4.2 Retaliation against whistleblowers is strictly prohibited and will be subject to immediate disciplinary action.

10. Review and Update Requirements

10.1 This policy must be reviewed annually, or sooner if:

10.1.1 There are significant changes to regulatory requirements (e.g., new EU digital communications laws)

10.1.2 New social media platforms or communication channels are adopted

10.1.3 A significant incident occurs or repeated violations indicate process gaps

10.1.4 There is a structural or leadership change in PR, Legal, or Security functions

10.2 The review must be conducted jointly by:

10.2.1 The Head of Marketing / PR

10.2.2 The CISO or Security Risk Lead

10.2.3 Legal and Compliance Officers

10.3 Updates must be documented in the Policy Change Register and communicated through internal awareness channels. Where material changes occur, all affected personnel must reconfirm policy acknowledgment.

11. Related Policies and Linkages

11.1 This policy is supported by and interrelated with the following components of the organization's Information Security Management System (ISMS):

11.1.1 P1 – Information Security Policy: Establishes overarching principles for safeguarding information, including ensuring that communications do not result in unauthorized disclosure.

11.1.2 P3 – Acceptable Use Policy: Defines acceptable behaviors for digital platforms and technologies, which directly govern personal and professional use of social channels.

11.1.3 P6 – Risk Management Policy: Provides the risk framework for assessing threats related to public communication and reputational exposure.

11.1.4 P8 – Information Security Awareness and Training Policy: Mandates awareness programs that educate staff on secure communication practices and social engineering threats.

11.1.5 P13 – Data Classification and Labeling Policy: Guides personnel on what constitutes restricted or confidential information, which must not be disclosed externally.

11.1.6 P30 – Incident Response Policy: Defines how to handle public communication-related incidents, including data leaks, impersonation, and regulatory breaches.

11.1.7 P33 – Audit and Compliance Monitoring Policy: Governs the audit processes that validate social media controls, monitoring systems, and compliance with external communication policies.

12. Reference Standards and Frameworks

12.1 ISO/IEC 27001:

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

12.2 ISO/IEC 27002:2022:

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

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

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

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

12.3 NIST SP 800-53 Rev.5:

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

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

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

12.4 EU GDPR (2016/679):

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

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

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

12.4.4 Article 33 – Breach Notification: Mandates timely notification of personal data breaches involving public channels.

12.5 EU NIS2 Directive (2022/2555):

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

12.6 EU DORA (2022/2554):

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

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

12.7 COBIT 2019:

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

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