					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	Clauses 5.1, 5.2, 6.1, 8	Leadership, risk management, and operational control over external communications
ISO/IEC 27002:2022	Controls 5.10, 5.11	Acceptable use and information security in communications
NIST SP 800-53 Rev.5	PL-4, AU-7, IR-6, AC-22	Rules of behavior, audit, incident reporting, and management of publicly accessible content and access
EU GDPR	Articles 5, 32, 33	Data protection principles, security, and breach notification affecting public communications
EU NIS2	Article 21(2)(e), 21(2)(f)	Policies for system use and supply chain/public communications risk management
EU DORA	Article 14(4)	Communication obligations following incidents

1. Purpose

1.1. This policy establishes mandatory requirements for all public-facing communications, including social media use, press engagement, and external digital content, where such communications refer to the company, its personnel, clients, systems, or internal practices.

1.2. This policy supports the protection of the company's reputation, maintenance of legal and regulatory compliance, and reduction of the risk of information leakage, misinformation, or security incidents.

1.3. This policy enables staff and partners to participate in online discussions in a positive and responsible manner while avoiding accidental disclosure or misrepresentation.

1.4. This policy strengthens SME readiness for ISO/IEC 27001 certification by addressing control over information made available to the public or external stakeholders.

2. Scope

2.1. This policy applies to all individuals affiliated with the organization, including:

2.1.1. Employees and contractors

2.1.2. Freelancers, consultants, and third-party providers/vendors

2.1.3. Interns or part-time staff involved in client service delivery or system access

2.2. This policy applies to all forms of external communication that refer to the organization, including:

2.2.1. Social media posts (LinkedIn, Twitter/X, TikTok, Instagram, Facebook, etc.)

2.2.2. Blog posts, online forums, customer reviews, and discussion threads

2.2.3. Speaking engagements (e.g., conferences, webinars, podcasts)

2.2.4. Emails or messages sent to journalists, government representatives, or influencers

2.2.5. Publicly shared screenshots, photographs, or videos from work environments

2.3. This policy also applies where such communication is made:

2.3.1. From personal devices or accounts

2.3.2. Outside normal working hours

2.3.3. Without malicious intent; accidental or informal remarks are also in scope where they refer to the company

3. Objectives

3.1. Reputation Protection: Prevent damage to the company's image through unauthorized or inappropriate public communication

3.2. Data Security: Prevent the unintentional exposure of sensitive data, internal systems, or client information through social media or public channels

3.3. Legal and Regulatory Compliance: Ensure that all public content referring to the company complies with applicable data protection and business communication laws

3.4. Professional Conduct: Promote responsible participation in online discussions and media engagements, including through personal accounts

3.5. Incident Preparedness: Define clear and actionable steps in the event of accidental disclosure or policy violations

4. Roles and Responsibilities

4.1. General Manager (GM)

4.1.1. Owns and approves this policy

4.1.2. Reviews and authorizes public statements, press engagements, and media interviews

4.1.3. Ensures this policy is clearly communicated to all employees and third parties

4.1.4. Investigates and responds to violations of this policy in coordination with Incident Reporting and Management procedures

4.2. Designated Employee or Communications Lead (if assigned)

4.2.1. Supports the General Manager by reviewing content before external publication, such as blog posts or speaking topics

4.2.2. Maintains logs of approved media activity or high-risk social media posts

4.2.3. Monitors known company mentions online for reputational or security risks, as capacity permits

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

9. Review and Update Requirements

9.1. Annual Review

9.1.1. This policy must be reviewed at least annually by the General Manager (GM)

9.1.2. The review must ensure alignment with updated legal obligations, communication trends, and internal business changes

9.2. Trigger-Based Reviews

9.2.1. This policy must be updated immediately following:

9.2.1.1. A significant social media incident or reputational issue

9.2.1.2. A change in third-party vendors managing communications

9.2.1.3. New legislation or regulatory obligations relating to online communication, media, or branding

9.3. Documentation of Changes

9.3.1. All updates must be recorded, including the revision date, summary of changes, and approval by the General Manager

9.3.2. A version history must be maintained for audit and certification purposes

9.4. Distribution of Updates

9.4.1. All staff and contractors must be informed of any policy changes

9.4.2. Updated versions must be distributed by email or through internal portals

9.4.3. Any public communications vendor must acknowledge updated terms before continuing work

10. Related Policies and Linkages

10.1. This policy operates in coordination with the following SME policies:

10.1.1. P3S – Acceptable Use Policy: Defines acceptable behavior when using communication platforms, including social media access during working hours

10.1.2. P8S – Information Security Awareness and Training Policy: Ensures staff are trained to identify the risks of oversharing, phishing, or reputational threats online

10.1.3. P17S – Data Protection and Privacy Policy: Ensures personal and customer data is not shared in external communications, in alignment with GDPR and other legal requirements

10.1.4. P30S – Incident Response Policy: Governs the response to accidental public disclosure, online threats, or reputational attacks resulting from misuse of social media

10.1.5. P37S – Legal and Regulatory Compliance Policy: Establishes the organization's broader legal and contractual obligations when content is shared publicly

10.2. These policies must be applied together to maintain a secure, respectful, and legally compliant external presence.

11. Reference Standards and Frameworks

11.1. ISO/IEC 27001

11.1.1. Clause 5.1 – Leadership and Commitment: Requires leadership oversight of reputational and information risks

11.1.2. Clause 6.1 – Risk Management: Includes communication-related risk exposure

11.1.3. Clause 8.1 – Operational Control: Covers rules governing how information is communicated externally

11.2. ISO/IEC 27002

11.2.1. Control 5.10 – Acceptable Use of Information and Assets

11.2.2. Control 5.11 – Information Security in Communication

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Rules of Behavior: Governs appropriate conduct in the use of information resources

11.3.2. AU-7 – Audit Reduction and Report Generation: Supports monitoring of public system use

11.3.3. IR-6 – Incident Reporting: Requires response to reputational and communications breaches

11.3.4. AC-22 – Publicly Accessible Content: Ensures control over external publications and access

11.4. EU GDPR (2016/679)

11.4.1. Article 5 – Principles relating to the processing of personal data (accuracy, integrity, accountability)

11.4.2. Article 32 – Security of Processing: Requires safeguards around public sharing

11.4.3. Article 33 – Breach Notification: Applies where personal data is exposed through external communication

11.5. EU NIS2 Directive (2022/2555)

11.5.1. Article 21(2)(e) – Policies on information system use, including communication platforms

11.5.2. Article 21(2)(f) – Policies for handling cybersecurity risks in the supply chain and public platforms

11.6. EU DORA (2022/2554)

11.6.1. Article 14(4) – Communication obligations to customers, third parties, and authorities following operational incidents

11.7. COBIT 2019

11.7.1. APO09 – Manage Service Agreements: Covers oversight of vendors and communication-related third parties

11.7.2. DSS05 – Manage Security Services: Includes protection of public-facing digital assets

11.7.3. EDM03 – Ensure Risk Optimization: Emphasizes management of reputational and compliance risks related to communication