					[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: IT							
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	Clauses 5.1, 5.2, 6.1, 8.1	
ISO/IEC 27002:2022	Controls 5.10, 5.11	
NIST SP 800-53 Rev.5	PL-4, AU-7, IR-6, AC-22	
EU GDPR	Articles 5, 32, 33	
EU NIS2	Article 21(2)(e), 21(2)(f)	
EU DORA	Article 14(4)	

<table>
<tr><td colspan="3"></td><td colspan="9">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="3">Document number:
P36S</td><td colspan="9">Document Title:
Social Media and External Communications Policy</td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="2">Effective Date:
01.01.2025</td><td colspan="9">Document Owner:
IT</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

1. **Purpose**
   1.1. This policy establishes mandatory guidelines for all public-facing communication — including social media use, press engagement, and external digital content — when referencing the company, its personnel, clients, systems, or internal practices.
   1.2. The policy helps protect the company's reputation, maintain legal and regulatory compliance, and reduce the risk of information leaks, misinformation, or security incidents.
   1.3. It enables staff and partners to engage positively and responsibly in online discussions, while avoiding accidental disclosures or misrepresentation.
   1.4. The policy reinforces SME preparedness for ISO/IEC 27001 certification by addressing the control of 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 vendors
      2.1.3. Interns or part-time staff involved in client delivery or system access
   2.2. The policy applies to all forms of external communication that reference 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 to journalists, government representatives, or influencers
      2.2.5. Publicly shared screenshots, photos, or videos from work environments
   2.3. The policy also applies when 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 — even accidental or "offhand" remarks are in scope if they reference 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**: Avoid the unintentional exposure of sensitive data, internal systems, or client details through social media or public channels
   3.3. **Legal and Regulatory Compliance**: Ensure all public content referencing the company complies with relevant data protection and business communication laws
   3.4. **Professional Conduct**: Encourage responsible participation in online discussions and media engagements, even on personal accounts
   3.5. **Incident Preparedness**: Provide clear, actionable steps in case of accidental disclosures 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 any public-facing statements, press engagements, or media interviews

[……]

Reference Standards and Frameworks

ISO/IEC 27001:2022

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

Clause 6.1 – Risk Management: Includes communication-related risk exposures

Clause 8.1 – Operational Control: Covers rules for how information is communicated externally

ISO/IEC 27002:2022

Control 5.10 – Acceptable Use of Information and Assets

Control 5.11 – Information Security in Communication

NIST SP 800-53 Rev.5

PL-4 – Rules of Behavior: Governs appropriate conduct for use of information resources

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

IR-6 – Incident Reporting: Enforces response to reputational and communications breaches

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

EU GDPR (2016/679)

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

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

Article 33 – Breach Notification: Triggers if personal data is exposed via external communication

EU NIS2 Directive (2022/2555)

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

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

EU DORA (2022/2554)

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

COBIT 2019

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

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

EDM03 – Ensure Risk Optimization: Emphasizes managing reputational and compliance risks related to communication