SEAMOS
MARKETING

Information Security Policy

SEAMOS Marketing SL

Security

Classification: **Internal**

1 PURPOSE

The purpose of this policy is to define the high-level direction, principles, and objectives for Information Security at SEAMOS Marketing SL (SMSL). It demonstrates the commitment of Top Management to protect the confidentiality, integrity, and availability of information assets, particularly regarding our role as a specialized ICT provider for the **Byrom Group** and the **major sporting events** sector, as required by **ISO 27001:2022 Clause 5.2**.

2 SCOPE AND APPLICABILITY

This policy applies to all employees, contractors, and third parties operating within the scope defined in 4.3-Determining Scope Information Security Management System.

- **Primary Focus:** The logical security of the software development lifecycle (SDLC), the Azure DevOps environment, and consulting services.
- **Shared Responsibility:** We explicitly acknowledge our reliance on **Byrom PLC** for physical security and core network perimeter controls. This policy governs the assets under SMSL's direct control while ensuring alignment with Group-wide standards.

3 POLICY STATEMENT

3.1 Strategic Alignment

Information security is not an obstacle but a business enabler. Our strategy is based on improving the company security following the industry standards, with a contained cost and a path that provides us not only the security and monitoring tools we need but also the certifications that improves our business opportunities. Furthermore, aligned with the Byrom Group's commitment to **ISO 20121 (Event Sustainability Management)**, SMSL commits to a "Cloud-First" security strategy (Azure) that optimizes energy consumption and reduces physical hardware waste.

3.2 Core Security Principles

SMSL adopts the core security principles. All controls and procedures must adhere to:

- **Least Privilege**: Users and systems (including Azure Service Principals) are granted only the minimum access necessary to perform their function.
- **Segregation of Duties**: Critical tasks (e.g., coding vs. deploying to production) must be separated to prevent fraud or error (Ref: Clause 5.3).

- **Defence in Depth**: Security should be layered; reliance on a single control (e.g., passwords) is insufficient. Multifactor Authentication (MFA) is mandatory for all remote access.
- **Privacy by Design**: Security and data protection measures must be embedded into the software development lifecycle from the initial design phase.

3.3 Commitment to Satisfy Requirements

SMSL is committed to satisfying all applicable information security requirements, including:

- **Legal & Regulatory:** Full compliance with the **GDPR** and requirements from the **Spanish Data Protection Agency (AEPD)** regarding the processing of personal data.
- **Industry Standards (Payments):** In alignment with the Byrom Group policy and our activity regarding online ticket sales, SMSL commits to maintaining compliance with the **Payment Card Industry Data Security Standard (PCI-DSS)** for all systems processing, storing, or transmitting payment card information.
- **Sector Specific (Events):** SMSL acknowledges the high-profile nature of our clients (e.g., FIFA, UEFA) and commits to adhering to their specific **Data Protection Regulations** and "Clean Venue" IT policies when acting as a data processor for these entities.
- **Contractual:** Meeting the Service Level Agreements (SLAs) regarding uptime and data protection defined in our contracts with clients and the Byrom Group (Reference: 4.2-Understanding the Requirements of Interested Parties).
- **Internal:** Adherence to the **Byrom Group IT Security Principles**.

3.4 Commitment to Continual Improvement

SMSL commits to the continual improvement of the ISMS. We do not view security as a "one-off" project but as an iterative process driven by the **Plan-Do-Check-Act (PDCA)** cycle.

- **Mechanism:** Improvements are identified through **Scrum Retrospectives,** Internal Audits, and the monitoring of KPIs **(Reference: 10.1-Continuous Improvement).**

3.5 Principles of Acceptable Use

To ensure the protection of assets, SMSL establishes the following principles regarding acceptable behavior:

- **Business Use:** Corporate systems (Email, Azure DevOps, Teams) are provided for professional business purposes.
- **Unacceptable Behavior:** It is strictly prohibited to use SMSL assets for illegal activities, harassment, copyright infringement, or to bypass security controls (e.g., disabling antivirus).

- **Confidentiality:** Users must not disclose sensitive company data to unauthorized external parties or public AI tools without approval.

4 INFORMATION CLASSIFICATION

To ensure consistent protection across the Group, SMSL adopts the Byrom PLC Information Classification Scheme. All information assets must be labeled and handled according to the following levels:

1. **Public or Unrestricted:** Information intended for public release (e.g., Marketing materials).
2. **Internal:** Information for internal use only; unauthorized disclosure could cause minor embarrassment (e.g., Intranet news, Staff Policies).
3. **Confidential:** Sensitive information where disclosure could cause financial or reputational damage (e.g., Client Contracts, Architecture Diagrams, Source Code).
4. **Highly Confidential:** Highly sensitive information restricted to specific named individuals (e.g., Merger details, passwords)

5 FRAMEWORK FOR SETTING OBJECTIVES

Information security objectives are not arbitrary. They are established annually by the **Security Operations Team (SOT)** and approved by the IT Director. Objectives must be:

1. **Consistent with this Policy.**
2. **Measurable** (e.g., "Remove Windows 10 by Oct 2025").
3. **Risk-Based:** Derived from the Risk **Assessment (Reference: 6.1-Actions to Address Risks Opportunities**, prioritizing risks with high "Degradation" or "Probability" scores.
4. **Communicated:** Shared with relevant teams via the Intranet and Town Halls.

Current objectives are detailed in document: **6.2-Establishing Measurable Information Security Objectives**.

6 ROLES AND RESPONSIBILITIES

Detailed authorities are defined in **7.2-Skills**. A summary of high-level responsibilities for this policy includes:

- **IT Director:** Accountable for the ISMS and final approval of policies.

- **Security Operations Team (SOT):** Responsible for the operational implementation of this policy, reviewing security logs, and managing the Risk Register.
- **Data Protection Officer (DPO):** Responsible for ensuring alignment with GDPR and handling data subject requests.
- **All Employees:** Responsible for maintaining the confidentiality of information they process, adhering to the "Acceptable Use" principles, and reporting security incidents immediately to the SOT.

7 COMMUNICATION AND COMPLIANCE

7.1 Communication

The issues identified

- **Internal**: This policy is communicated to all employees upon induction. Proof of understanding is required via signature (Reference: **Statement of Applicability 2025** Control 5.1).
- **External**: This policy is available to interested parties (clients, auditors, regulators) upon request.
- **Plan**: Communication channels are further defined in the corporate-Communication Plan.

7.2 Non-Compliance

Compliance with this policy is mandatory. Violations may result in disciplinary action, up to and including termination of employment, in accordance with the Policy on Resources and local labour laws.

SMSL explicitly grants the Byrom PLC Internal Audit Team the authority to inspect SMSL systems and records to verify compliance with this policy.