

Novusbet Platform

Information Security Policy

Version	1.00	Date	2025-02-01
Recipient	N/A	Produced by	Softquo Schweiz

© 2019-2025 SoftQuo Schweiz GmbH. All rights reserved. The information in this document belongs to SoftQuo Schweiz GmbH and It may not be used, reproduced or disclosed without the written approval of SoftQuo Schweiz GmbH.

Notice of non-liability:

SoftQuo Schweiz GmbH is providing the information in this document to you "as-is" with all faults. SoftQuo Schweiz GmbH makes no warranties of any kind (whether express, implied or statutory) with respect to the information contained herein. SoftQuo Schweiz GmbH assumes no liability for damages (whether direct or indirect), caused by errors or omissions, or resulting from the use of this document or the information contained in this document or resulting from the application or use of the product or service described herein. In the event that SoftQuo Schweiz GmbH make changes to any information in this document the appropriate persons/entities will receive an updated version of this document.

Content

Content	3
1. Purpose and Scope	5
2. Information Security Management System (ISMS) Platform Audit	5
3. Information Security Policy Implementation	7
4. Policy Approval and Communication	7
5. Roles and Responsibilities	7
6. Security Responsibilities and Governance	10
7. Security Controls	10
8. Incident Management	11
9. Service Provider Evaluation	11
10. Change Management	11
11. Training and Awareness	12
12. Monitoring and Audit Evidence	12
13. Policy Exceptions and Non-Compliance	12
14. Review and Revision	12

1. Purpose and Scope

The Information Security Policy establishes a structured approach to managing information security risks across the entire lifecycle of the online betting platform as owned by SoftQuo Schweiz GmbH (“the Company”). It outlines strategic principles, operational responsibilities, and procedural controls designed to safeguard the platform's information assets from threats, vulnerabilities, and breaches. This policy serves as a cornerstone of the platform's broader commitment to regulatory compliance, risk management, and business continuity.

The key objectives of this policy are to ensure the following security principles are upheld:

- 1.1. Confidentiality:** Prevent unauthorized access to sensitive and critical information, ensuring that data is only accessible to those with the appropriate permissions.
- 1.2. Integrity:** Protect information from unauthorized modifications, deletions, or corruption to ensure its accuracy and trustworthiness.
- 1.3. Availability:** Guarantee the timely and reliable access to information and services required for business operations, ensuring that security measures do not impede the efficiency of platform functions.

2. Information Security Management System (ISMS) Platform Audit

A robust and recurring audit process forms a key element of the Information Security Management System (ISMS), providing continuous assurance that the platform's security posture meets both internal and external compliance requirements. The purpose of this audit process is to assess and verify that all information security controls are properly implemented, maintained, and effective in mitigating risks across the platform's infrastructure and services.

Audit Objectives

The ISMS platform audit aims to:

- 2.1. Verify the application and performance of security controls across platform components such as:
 - A. Information Security Services: Authentication, access control, encryption, and threat detection.
 - B. Cloud Services: Configuration management, data protection, and network security.
 - C. Payment Services: Security of financial transactions and compliance with payment standards (e.g., PCI DSS).
 - D. Live Gaming Services: Secure integration and real-time data flow management.
 - E. Other Critical Services: Any third-party services directly affecting platform operations or user data protection.
- 2.2. Detect and address vulnerabilities, misconfigurations, and other risk factors that may compromise the platform's security.

2.3. Ensure alignment with regulatory requirements and policies applicable to the jurisdictions where the platform operates.

2.4. Audit Frequency and Responsibility

A. The ISMS platform audit is conducted at least annually, though more frequent audits may be scheduled in response to:

- 1) Significant changes to the platform's architecture or risk profile.
- 2) Regulatory requests or updates to compliance frameworks.
- 3) Major security incidents or breaches.

B. Audits are performed by appropriately accredited entities, which may include:

- 1) Internal security audit teams with relevant expertise.
- 2) Third-party service providers that are certified in information security auditing standards (e.g., ISO/IEC 27001 Lead Auditors).

C. The Company may leverage audit results from previously completed assessments within the current audit period (e.g., the past 12 months) to streamline compliance efforts, provided those assessments were conducted by qualified and accredited providers.

2.5. Audit Scope

The audit shall cover all core components of the platform and assess their compliance with security policies and standards. Key areas of evaluation include:

A. Organizational Security Governance:

1. Review of security policies, roles, and responsibilities.
2. Assessment of security awareness and training programs.

B. Risk Management:

1. Analysis of risk assessments and the effectiveness of risk treatment plans.
2. Evaluation of risk acceptance criteria and controls for mitigating high-risk scenarios.

C. Access Controls:

1. Verification of access control policies, including multi-factor authentication (MFA), least privilege, and role-based access controls.
2. Assessment of physical and logical access logs and monitoring practices.

D. Asset Management:

1. Inventory of critical information assets and evaluation of their protection measures.
2. Assessment of data classification policies and the secure handling of sensitive information.

E. Operational Security:

1. Evaluation of incident response plans, procedures, and records.
2. Assessment of the implementation of business continuity and disaster recovery plans.
3. Review of security patching and vulnerability management processes.

F. Third-Party Service Provider Evaluation:

1. Verification that service providers meet contractual security obligations.
2. Review of external audit reports and certifications provided by service providers.

G. System and Application Security:

1. Assessment of security controls within software development and deployment pipelines.
2. Review of secure coding practices, vulnerability testing, and change management processes.

2.6. Audit Execution

The audit process involves multiple phases to ensure thorough coverage and documentation:

A. Planning:

1. Define the audit scope, objectives, and criteria.
2. Schedule the audit with input from key stakeholders (e.g., IT Security Officer, Compliance Officer).

B. Data Collection and Assessment:

1. Gather relevant documentation, including:
 - Security policies and procedures.
 - Access control and system activity logs.
 - Incident response records and audit trails.
2. Conduct interviews with key personnel (e.g., system administrators, compliance managers).

C. Testing and Evaluation:

1. Perform security testing, which may include vulnerability scans, penetration tests, and system performance reviews.
2. Assess compliance with audit criteria and identify deviations from security policies or standards.

D. Reporting:

1. Document audit findings, including:
 - Non-conformities or areas of non-compliance.
 - Recommendations for corrective actions.
2. Generate a formal Audit Report, which includes:
 - Executive summary.
 - Detailed findings.
 - Corrective action plan with deadlines.
3. Share the report with senior management and relevant stakeholders.

E. Follow-Up and Remediation:

1. Implement corrective actions to address audit findings.
2. Conduct a follow-up assessment to verify the effectiveness of remedial measures.
3. Maintain records of remediation activities as evidence for future audits.

2.7. Audit Evidence and Record-Keeping

To ensure transparency and readiness for future audits or regulatory inspections, the following evidence shall be generated and maintained:

A. Audit Planning Records:

- Scope and objectives of the audit.
- List of stakeholders involved in the audit process.

B. Documentation Collected:

- Security policies, access control logs, and vulnerability assessment reports.

C. Audit Report:

- Summary of findings, corrective actions, and audit conclusions.

- Detailed descriptions of any identified risks or non-compliances.

D. Corrective Action Plans:

- Records of corrective actions taken, including status updates and final outcomes.

E. Communication Logs:

- Emails and meeting notes demonstrating the communication of audit findings and recommendations.

2.9. Continuous Improvement

The ISMS platform audit process is part of an ongoing effort to improve the platform's security posture.

Audit results are used to inform:

- Updates to security policies and risk management strategies.
- Enhancements to security awareness programs.
- The prioritization of security investments and resources.

3. Information Security Policy Implementation

A. Policy Review and Updates

1) The Information Security Policy shall be reviewed at least annually or whenever significant changes to the platform or risk profile occur, such as:

- Changes to critical infrastructure, services, or technology.
- New regulatory requirements or audit findings.
- Significant security incidents or newly identified risks.

B. Reviews will be documented, including any updates made to the policy, and results will be communicated to senior management.

4. Policy Approval and Communication

A. The policy is formally approved by senior management and documented in organizational governance records.

B. Once approved, the policy is communicated to:

1. All employees through onboarding, security training, and annual updates.
2. Relevant third-party providers via contracts and service-level agreements (SLAs).

5. Roles and Responsibilities

Effective information security management requires a clear allocation of roles and responsibilities across all stakeholders. This section defines the responsibilities of internal staff, third-party providers, and senior management to ensure accountability and compliance with both the platform's security policies and regulatory requirements.

5.1. The Company's Responsibilities (Senior Management)

The Company's (senior management) holds ultimate accountability for the platform's information security and compliance with the country regulations, including. Their key responsibilities include:

- Developing, approving, and overseeing the implementation of the Information Security Policy.
- Establishing and supporting an Information Security Management System (ISMS) that complies with ISO/IEC 27001 or equivalent standards.
- Allocating sufficient resources (personnel, technology, and budget) to enable the effective management of security risks.
- Approving contracts with external service providers that require compliance with platform security standards.
- Periodically reviewing reports on ISMS performance, incidents, and audits.
- Convening and participating in the Security Forum (explained below).

5.2. Security Forum Responsibilities

The Security Forum is a formally established body composed of senior management, IT leadership, and compliance officers. It is responsible for ensuring the ISMS remains effective, adequate, and aligned with business and regulatory requirements.

Duties of the Security Forum:

- Meeting quarterly (or as required by MINCETUR) to review ISMS performance.
- Reviewing risk assessments, audit results, and significant incidents.
- Approving or recommending changes to security policies and procedures.
- Reviewing service provider evaluations and reports.

5.3. IT Security Officer Responsibilities

The IT Security Officer is appointed to oversee the implementation of technical security measures and incident response protocols.

Key Responsibilities:

- Managing security technologies (e.g., firewalls, access control systems, encryption tools).
- Ensuring compliance with access control policies, including multi-factor authentication and role-based permissions.
- Conducting internal audits and coordinating external security audits.
- Providing security training to employees and service providers.
- Leading the response to security incidents, including documentation and reporting.

5.4. Information Owners

Information Owners are responsible for safeguarding information assets under their control, ensuring that appropriate security measures are applied to their data.

Key Responsibilities:

- Classifying information assets according to their sensitivity (confidential, internal, public).
- Authorizing access to information and periodically reviewing access rights.
- Reporting incidents involving information assets promptly to the IT Security Officer.

5.5. Employees and Internal Users

All employees, contractors, and internal users are required to follow the platform's security policies and report any security incidents or suspicious activities.

Key Responsibilities:

- Understanding and complying with security policies and procedures.
- Protecting passwords, devices, and sensitive information from unauthorized access.
- Locking computer screens when leaving workstations unattended.
- Reporting security incidents to their direct manager or the IT Security Officer.

5.6. Third-Party Service Providers

Third-party service providers play a crucial role in the operation of the platform. Therefore, they are required to adhere to the platform's security policies and demonstrate ongoing compliance through audits and reporting.

Key Requirements for Service Providers:

- Signing contracts that include security obligations aligned with the platform's ISMS.
- Undergoing an initial security evaluation to verify compliance with ISO/IEC 27001 or an equivalent standard.
- Providing annual security reports or certifications to demonstrate continued compliance.
- Implementing adequate security measures for services such as cloud hosting, payment processing, and live gaming systems.
- Participating in security incident investigations if their services are involved in a breach.

5.6.1. Service providers are required to submit documentation such as security certifications (e.g., ISO 27001), internal audit results, or compliance reports via email.

A checklist-based service provider evaluation form is completed during onboarding and annually reviewed.

5.7. Compliance Officer Responsibilities

The Compliance Officer ensures that the platform adheres to regulatory obligations, including reporting to MINCETUR and other relevant authorities.

Key Responsibilities:

- Monitoring regulatory updates and ensuring the platform's policies remain compliant.
- Coordinating security audits and submitting required documentation to regulators.
- Preparing periodic compliance reports for senior management and regulatory authorities.

5.8. Security Awareness and Training Responsibilities

The training program is designed to ensure that all stakeholders understand their security responsibilities and are equipped to perform them.

Key Training Requirements:

- Initial security training upon joining the platform.
- Annual refresher training sessions for all employees.

- Specialized training for high-risk roles (e.g., IT administrators, compliance officers).

5.9. Assignment and Review of Responsibilities

Responsibilities defined in this policy are formally assigned and documented in role descriptions, contracts, and organizational charts.

An annual review of roles and responsibilities is conducted to ensure that they remain relevant and effective.

6. Security Responsibilities and Governance

6.1. Security Forum: A security forum composed of senior management and IT representatives is established to oversee ISMS performance.

Meetings are held quarterly or as required by MINCETUR regulations, with formal minutes maintained.

6.2. Security Management:

A. The Company is responsible for security strategies and action plans.

Responsibilities include:

Reviewing security processes for information, infrastructure, and game services.

Reporting security performance to senior management and the IT department.

Ensuring personnel have the necessary training and resources for risk management.

B. Security Policy Updates: The Company may recommend changes to security policies based on operational needs or regulatory updates.

7. Security Controls

7.1. Physical Security:

- Critical facilities (e.g., server rooms) are secured with restricted access, biometric controls, and video surveillance.
- Entry logs are maintained electronically and reviewed monthly.

7.2. Access Control:

- Access to information systems is restricted to authorized personnel.
- Multi-factor authentication (MFA) is enforced for administrative access to critical systems.

7.3. Data Protection:

- Data at rest and in transit is encrypted using industry-standard algorithms (e.g., AES-256).
- Regular backups are performed, stored securely, and periodically tested for recovery.

8. Incident Management

The management of information security incidents follows the guidelines set forth in the Company's **A. Security and Monitoring Procedure**. This separate procedure details comprehensive steps for security controls, real-time monitoring, incident detection, and incident response management. It ensures that security incidents are swiftly identified, analyzed, contained, and resolved to minimize risks to platform operations.

C. Key principles of incident management include:

1. Defining incidents as events that compromise the confidentiality, integrity, or availability of platform information.
2. Reporting incidents promptly through designated channels, as outlined in the Security and Monitoring Procedure.
3. Classifying incidents based on severity to prioritize response efforts.

9. Service Provider Evaluation

Initial and Ongoing Evaluations:

- A. Service providers are evaluated during onboarding and annually thereafter to ensure they meet security requirements.
- B. Evaluations focus on information security practices, including compliance with ISO/IEC 27001 or equivalent standards.

10. Change Management

The Company's approach to change management is guided by a separate **Change Management Procedure**, which outlines detailed steps for managing, monitoring, and maintaining the security and performance of the platform. This procedure aligns with ISMS best practices and supports regulatory compliance, ensuring that changes do not introduce vulnerabilities or disrupt operations.

11. Training and Awareness

11.1. Security Training: All employees undergo annual information security training. Training covers security best practices, incident reporting, and data protection responsibilities.

11.2. Awareness Programs: Periodic security awareness campaigns are conducted to reinforce policies and procedures.

12. Monitoring and Audit Evidence

12.1. System Monitoring: Security monitoring tools generate automated alerts for incidents, unauthorized access, and system anomalies. Notifications are sent to the IT and security teams for immediate action.

12.2. Audit Logs: Audit logs are maintained for critical systems, including access control, changes, and incident responses. Logs are reviewed quarterly to ensure compliance and readiness for regulatory audits.

13. Policy Exceptions and Non-Compliance

A. Exceptions: Any exceptions to this policy require formal approval from the security forum.

B. Non-Compliance: Non-compliance with this policy may result in disciplinary action, including termination of access privileges or employment.

14. Review and Revision

This policy will be reviewed annually or as required by changes in regulatory requirements, technology, or business processes.

Amendments to the policy will be documented and communicated to all stakeholders.