

Information Security Policy (CW)

Version	Date	Author	Description
1.0	Sep, 2022	IT Management	Initial version of Information Security Policy document covering purpose, scope, security objectives, ISMS framework, and exceptions/exemptions procedures.
1.1	September 2024	IT Management	Clarifications expanded on exemption items.

1. Purpose

1.1 The Information Security Policy states Slotbox's approach to protecting its information assets from all threats, whether internal or external, deliberate or accidental. Slotbox operates a risk-based approach to protecting information assets that identifies applicable vulnerabilities and threats, ensures compliance with legal, statutory, and regulatory requirements, and implements appropriate mitigating controls to preserve confidentiality, integrity, and availability.

Notes:

- Slotbox information is all information relating to Slotbox business, staff and customers including but not limited to all personal and commercial confidential information.
- An information asset (i.e information) is knowledge or data that has value to the individual or organisation that warrants protection to guard against loss of confidentiality, integrity or availability.

1.2 The Information Security policy is the overarching policy and sets requirements concerning:

- Information security objectives and how to achieve these objectives;
- Assignment of specific responsibilities for information security; and

- Processes for handling exceptions (i.e. unauthorised non-compliances) and requesting exemptions (i.e. authorised non-compliances).

1.3 The Information Security Policy is supported by Security guidance documents / Policies and at a lower level by procedures, standards and guidelines which further mandate the implementation of information security controls.

2. Scope

2.1 This policy is applicable to all Slotbox employees, contractors and suppliers (collectively referred to as Users) that have access to Slotbox information assets.

2.2 This policy is applicable to all information assets within Slotbox, and information processing facilities: offices and infrastructure in order to provide a consistent approach to protecting assets and, thereby, protecting the Slotbox brand.

2.3 This policy is also applicable to all process and system interactions with Group companies, offices and infrastructure.

2.4 Inappropriate use of information assets can damage Slotbox and its reputation. Breach of this policy may be dealt with under Slotbox disciplinary policy and in serious cases, could be treated as gross misconduct leading to summary dismissal.

2.5 This policy shall be communicated to the business and made available to interested parties, on request.

3. Information Security Objectives and Responsibilities

3.1 Information security essentially means to protect the confidentiality, integrity and availability of information assets.

- **Confidentiality** - Slotbox shall allow access to information only to authorized users, systems and processes to prevent unauthorised disclosure.
- **Integrity** - Slotbox shall prevent unauthorised changes to information to preserve accuracy and authenticity.
- **Availability** - Slotbox shall ensure that the information is accessible and usable when needed by authorized users and interested parties.

3.2 On a yearly basis, security objectives shall be defined based on technology objectives and aligned to Company business goals and values.

3.3 The security objectives shall take into account external and internal requirements and expectations (e.g derived from legislation, regulatory bodies, customers, suppliers internal operations). The security objectives shall be measurable (if practical).

3.4 Slotbox management shall ensure that the responsibilities and authorities for roles relevant to defining and achieving information security objectives are assigned and communicated.

3.5 Information shall be classified based in terms of legal requirements, value, criticality and sensitivity.

3.6 An information security risk management process shall be implemented to identify, assess and control risks associated with the loss of confidentiality, integrity and availability.

3.7 A security due-diligence process shall be implemented to address risks that derive from third-party products and services.

3.8 Physical, administrative and technical controls shall be implemented to achieve levels of protection derived from information classification and the risk management process.

3.9 The performance of security processes and controls in achieving the desired objective shall be measured periodically and actions shall be taken to improve it when necessary.

3.10 A formal incident management process shall be established and maintained to ensure a timely and effective response to security incidents, breaches, and threats.

3.11 Business continuity and disaster recovery plans shall be developed, implemented, and tested to ensure the availability of critical information systems and business operations in the event of a disruption.

3.12 All information security activities shall comply with applicable laws, regulations (including the specific requirements of the Curacao Gaming Board), and contractual obligations related to data protection and information security.

4. Information Security Management System (ISMS)

4.1 Slotbox shall use a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security. This framework, consisting of processes, roles, documentation, and controls shall be aligned to:

- ISO 27001 and related standards

4.2 Slotbox management shall utilise ISMS to:

- Formulate information security policy, objectives and management direction for information security governance;
- Identify information assets and application ownership;
- Identify, implement and measure effectiveness of information security controls

4.3 Internal assessments shall be performed periodically to ensure that processes and controls implemented to achieve the security objectives are adequate and effective.

4.4 The Managing Director shall have overall responsibility for the ISMS and shall demonstrate leadership and commitment by:

- Ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of Slotbox;
- Ensuring the integration of ISMS requirements into Slotbox processes;
- Ensuring that the resources needed for the ISMS are available;
- Ensuring that security awareness training is provided to all staff upon hire and at least annually;
- Communicating the importance of effective information security management and of conforming to the ISMS requirements;
- Ensuring that the ISMS achieves its intended outcomes;
- Directing and supporting persons to contribute to the effectiveness of ISMS;
- Promoting continual improvement; and

- Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.
- Ensuring that information security is aligned with and supports compliance with all applicable legal, statutory, regulatory, and contractual requirements;

4.5 Policy Review

This Information Security Policy shall be reviewed at least annually, or upon significant changes to the business, technology environment, or regulatory landscape, to ensure its ongoing suitability, adequacy, and effectiveness.

5. Exceptions and Exemptions (Risk Acceptance)

5.1 Definitions

5.1.1 Exceptions are unauthorised non-compliances of mandatory requirements. Exceptions are typically identified by compliance activities, management reviews, during software development, process engineering, procurement of services, or from information security incidents.

5.1.2 Exemptions are authorised non-compliances of mandatory requirements. The exemption request process formalises risk management decisions to accept an identified exception.

5.2 Exemption requests and risk acceptance

5.2.1 Exemptions from information security policies, procedures, standards and processes shall be requested by contacting the Security team.

5.2.2 Exemption requests shall state a justifiable business or operational reason why compliance cannot be achieved.

5.2.3 Security shall review exemption requests and respond accordingly to the requestor.

5.2.4 A condition of authorising an exemption request may specify the implementation of compensating controls or acceptance or ownership of a risk through a formal risk management process.

5.2.5 Authorised exemption requests (accepted risks) shall be recorded by the Security team.

5.3 Exceptions

5.3.1 Any identified non-compliance (an exception) with information security policies or standards must be reported to the Security team immediately.

5.3.2 Upon receipt, the Security team will log the exception and initiate a risk assessment. Based on the assessment, the exception will either be remediated to achieve compliance or be formally processed as an exemption request as defined in section 5.2.