

iMoon B.V.

Information Security Policy

Software Development

Version 2.0

1.0 Purpose and Benefits

This policy defines the mandatory minimum information security requirements for iMoon B.V. ("iMoon" or "the Company"), a business-to-business (B2B) game provider. Any entity may, based on its individual business needs and specific legal and regulatory requirements, exceed the security requirements put forth in this document, but must, at a minimum, achieve the security levels required by this policy.

This policy acts as an umbrella document to all other security policies and associated standards. This policy defines the responsibility to:

- protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets;
- manage the risk of security exposure or compromise;
- assure a secure and stable information technology (IT) environment;
- identify and respond to events involving information asset misuse, loss or unauthorized disclosure;
- monitor systems for anomalies that might indicate compromise;
- promote and increase the awareness of information security;
- ensure compliance with applicable regulations and licensing requirements; and
- protect the integrity of software, random number generation and fair outcomes.

Failure to secure and protect the confidentiality, integrity and availability of information assets in today's highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions and vital government functions; compromise data; result in legal and regulatory non-compliance; undermine customer trust; and threaten licenses.

This policy benefits the Company by defining a framework that will assure appropriate measures are in place to protect the confidentiality, integrity and availability of data; protect software and systems integrity; ensure compliance with regulations; and assure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures and practices and know how to protect information.

2.0 Authority

This Information Security Policy is issued under the authority of the CEO of iMoon B.V. The Chief Technical Officer (CTO) is responsible for the development, implementation, and maintenance of this policy and associated standards.

3.0 Scope

This policy encompasses all systems, automated and manual, for which the Company has administrative responsibility.

Specific scope includes:

- All software development environments (including testing, staging and production);
- Random number generation (RNG) systems and related infrastructure;

- Servers, application programming interfaces (APIs), and integration platforms;
- Customer data management systems (where applicable under B2B arrangements);
- Financial transaction systems and payment processing interfaces;
- Source code repositories and intellectual property management systems;
- Analytics, monitoring and reporting systems;
- Business partner integration systems and operator platforms;
- Administrative and corporate IT infrastructure; and
- All systems subject to regulatory and testing requirements.

4.0 Information Statement

Organizational Security

- a. Information security requires both an information risk management function and an information technology security function. Depending on the structure of the Company, an individual or group can serve in both roles or a separate individual or group can be designated for each role. It is recommended that these functions be performed by a high-level executive or a group that includes high level executives.
 - i. The Company must designate an individual to be responsible for the risk management function assuring that:
 - (a) risk-related considerations for information assets and individual information systems, including authorization decisions, are viewed as an enterprise with regard to the overall strategic goals and objectives of carrying out its core missions and business functions; and
 - (b) the management of information assets and information system-related security risks is consistent, reflects the risk tolerance, and is considered along with other types of risks, to ensure mission/business success.
 - ii. The Company must designate an individual or group to be responsible for the technical information security function. For purposes of clarity and readability, this policy will refer to the individual, or group, designated as the Information Security Officer designated security representative. This function will be responsible for evaluating and advising on information security risks.
- b. Information security risk decisions must be made through consultation with both function areas described in (a) above.
- c. Although the technical information security function may be outsourced to third parties, the Company retains overall responsibility for the security of the information that it owns.

Functional Responsibilities

Executive management is responsible for:

1. evaluating and accepting risk on behalf of the Company;
2. identifying information security responsibilities and goals and integrating them;
3. supporting consistent implementation of information security policies and standards;
4. supporting security through commitment to appropriate resources;
5. promoting awareness of information security best practices;
6. implementing the process for determining information classification and categorization, based on industry recommended practices, organization directives, regulations, and legal and regulatory requirements, to determine the appropriate levels of protection;
7. implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization;

8. determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity and availability of the data;
9. participating in the response to security incidents;
10. complying with notification requirements in the event of a breach of private information;
11. adhering to specific legal and regulatory requirements related to information security;
12. communicating requirements to the designated security representative;
13. communicating requirements of this policy and the related standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements;
14. ensuring software integrity and compliance with regulatory testing requirements; and
15. maintaining relationships with regulators.

The designated security representative is responsible for:

1. maintaining familiarity with business functions and requirements;
2. maintaining an adequate level of current knowledge and proficiency in information security;
3. assessing compliance with information security policies both legal and regulatory;
4. understanding information security risks and how to appropriately manage those risks;
5. representing and assuring security architecture considerations are addressed;
6. advising on security issues related to procurement of products and services;
7. escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;
8. disseminating threat information to appropriate parties;
9. participating in the response to potential security incidents;
10. participating in the development of enterprise policies and standards that considers the Company's needs; and
11. promoting information security awareness.

IT management is responsible for:

1. supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners;
2. providing resources to maintain information security control consistent with this policy;
3. identifying and implementing all processes, policies and controls relative to security requirements defined by the business and this policy;
4. implementing the proper controls for information;
5. providing training to appropriate technical staff on secure operations;
6. fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting and implementing appropriate and cost-effective security controls and procedures; and
7. implementing business continuity and recovery plans.

The workforce is responsible for:

1. understanding the baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted;
2. protecting information and resources from unauthorized use or disclosure;
3. protecting personal, private, sensitive information from unauthorized use or disclosure;
4. reporting suspected information security incidents or weaknesses to the appropriate manager and designated security representative.

The CTO is responsible for:

1. providing in-house expertise as security consultants as needed;
2. developing the security program and strategy, including measures of effectiveness;

3. establishing and maintaining enterprise information security policy and standards;
4. assessing compliance with security policies and standards;
5. advising on secure system engineering;
6. providing incident response coordination and expertise;
7. monitoring networks for anomalies;
8. monitoring external sources for indications of data breaches, defacements, etc.;
9. maintaining ongoing contact with security groups/associations and relevant authorities;
10. providing timely notification of current threats and vulnerabilities; and
11. providing awareness materials and training resources.

Separation of Duties

- d. To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.
- e. Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities and management supervision.
- f. The approval of security controls must always remain independent and segregated from the implementation of security controls.

Information Risk Management

- g. Any system or process that supports business functions must be appropriately managed for information risk and undergo information risk assessments, at a minimum annually, as part of a secure system development life cycle.
- h. Information security risk assessments are required for new projects, implementations of new technologies, significant changes to the operating environment, or in response to the discovery of a significant vulnerability.
- i. The Company is responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies.
- j. Risk assessment results, and the decisions made based on these results, must be documented.

Associated Standard: Information Security Risk Management Standard; Secure System Development Lifecycle (SSDLC) Standard

Software-Specific Security Requirements

k. Random Number Generation (RNG) Security:

All RNG systems must be certified by approved testing laboratories (e.g., iTech Labs, eCOGRA, GLI, BMM Testlabs) and comply with the technical standards of applicable jurisdictions. RNG implementations must:

- iii. utilize cryptographically secure pseudo-random number generators;
- iv. implement proper seeding mechanisms using entropy sources that cannot be predicted or manipulated;
- v. be isolated from external influence and protected by access controls limiting modification to authorized personnel only;
- vi. maintain complete record keeping for all RNG system changes, configurations, and access;
- vii. undergo periodic testing to verify randomness, unpredictability, and absence of patterns;
- viii. be subject to version control with all changes requiring documented approval; and
- ix. maintain certification documentation and make available for regulatory inspection upon request.

I. Software Integrity:

All software must maintain demonstrable integrity throughout its lifecycle:

- x. source code must be maintained in secure version control systems with access restricted to authorized developers;
- xi. all code changes must undergo peer review and approval before integration;
- xii. compiled game executables must be cryptographically signed and verified before deployment;
- xiii. game logic, payout percentages (RTP), and mathematical models must be protected from unauthorized modification;
- xiv. integrity verification mechanisms (e.g., checksums, digital signatures) must be implemented for all deployed game files;
- xv. any modification to certified game software must trigger recertification requirements;
- xvi. game software must include anti-tampering mechanisms to detect unauthorized modifications; and
- xvii. backup copies of certified game software must be maintained in secure, tamper-evident storage.

m. Customer Data Protection (B2B Context):

While iMoon operates as a B2B provider, customer data may be processed in specific contexts. When customer data is accessible:

- xviii. all customer data must be encrypted both in transit and at rest;
- xix. access to customer data must be strictly limited to authorized personnel with documented business need;
- xx. customer data must be anonymized or pseudonymized wherever technically feasible;
- xxi. data retention periods must comply with applicable regulations;
- xxii. all access to customer data must be logged;
- xxiii. data processing agreements must clearly define responsibilities and liabilities;
- xxiv. mechanisms for data subject rights must be established; and
- xxv. customer data must not be used for purposes other than those specified in agreements with operators.

n. Transaction Integrity and Financial Controls:

For systems processing or facilitating financial transactions:

- xxvi. all transaction records must be immutable and maintained;
- xxvii. transaction data must be encrypted and cryptographically verified for integrity;
- xxviii. reconciliation processes must be implemented to detect discrepancies;
- xxix. financial transaction systems must implement strong authentication and authorization;
- xxx. transaction logs must be retained in accordance with regulations and financial reporting requirements;
- xxxi. fraud detection and prevention mechanisms must be implemented and regularly reviewed; and
- xxxii. suspicious transaction patterns must be detected, logged and investigated.

o. Anti-Money Laundering (AML) and Fraud Prevention:

The Company must implement technical controls to support AML and fraud prevention:

- xxxiii. systems must facilitate detection of suspicious behavioral patterns;
- xxxiv. transaction monitoring capabilities must be provided to operators;
- xxxv. data necessary for AML compliance must be captured and made available to operators;
- xxxvi. fraud detection algorithms and rules must be regularly updated;

- xxxvii. systems must support real-time alerts for high-risk activities;
- xxxviii. integration with third-party fraud prevention services must be secured; and
- xxxix. fraud detection and prevention activities must be maintained.

p. Responsible Software Controls:

Where applicable, the Company must support responsible requirements:

- xl. systems must support implementation of customer limits;
- xli. self-exclusion capabilities must be supported at the platform level;
- xlii. reality check and session reminder mechanisms must be implementable;
- xliii. data necessary for responsible monitoring must be captured and accessible; and
- xliv. software design must consider responsible principles and avoid features that exploit vulnerable customers.

q. Regulatory Compliance:

The Company must maintain systems and processes to support regulatory compliance:

- xliv. all systems subject to regulatory oversight must maintain comprehensive logs;
- xlvi. documentation of system designs, security controls and operational procedures must be maintained;
- xlvi. systems must facilitate data extraction and reporting;
- xlvi. changes to regulated systems must be documented and, where required, submitted for regulatory approval; and
- xlix. incident reports must be maintained.

r. API Security and Integration Controls:

All APIs exposed to operators or third parties must implement:

- i. strong authentication mechanisms;
- ii. rate limiting and throttling to prevent abuse;
- iii. input validation and sanitization to prevent injection attacks;
- liii. comprehensive logging of all API requests and responses;
- liv. encryption of all API communications;
- lv. API versioning and deprecation policies;
- lvi. security testing before deployment;
- lvii. IP whitelisting where technically feasible;
- lviii. monitoring for anomalous API usage patterns; and
- lix. contractual obligations defining security responsibilities between parties.

Associated Standard: Software Security Standard; RNG Security Standard; API Security Standard

Information Classification and Handling

- a. All information, which is created, acquired or used in support of business activities, must only be used for its intended business purpose.
- b. Information assets must have an owner established within the lines of business.
- c. Information must be properly managed from creation, authorized use and disposal.
- d. All information must be classified on an ongoing basis based on its confidentiality, integrity and availability characteristics.
- e. An information asset must be classified based on the highest level necessitated by its individual data elements.
- f. If the Company is unable to determine the confidentiality classification of information or the information is personal identifying information (**PII**) the information must have a high confidentiality classification.

- g. Merging of information which creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new classification of the merged data is warranted.
- h. All reproductions of information in its entirety must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.
- i. Each classification has an approved set of baseline controls designed to protect these classifications and these controls must be followed.
- j. The Company must communicate the requirements for secure handling of information to its workforce.
- k. A written or electronic inventory of all information assets must be maintained.
- l. Content made available to the general public must be reviewed according to a process that will be defined and approved by the Company. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.
- m. PII must not be made available without appropriate safeguards.
- n. For non-public information to be released outside the Company or shared between other entities, a process must be established that, at a minimum:
 - 1. evaluates and documents the sensitivity of the information to be released;
 - 2. identifies the responsibilities of each party for protecting the information;
 - 3. defines the minimum controls required to transmit and use the information;
 - 4. records the measures that each party has in place to protect the information;
 - 5. defines a method for compliance measurement;
 - 6. provides a signoff procedure for each party to accept responsibilities; and
 - 7. establishes a schedule and procedure for reviewing the controls.

Associated Standards: Information Classification Standard; Sanitization/Secure Disposal Standard

IT Asset Management

- s. All IT hardware and software assets must be assigned to a designated business unit or individual.
- t. The Company is required to maintain an inventory of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. This inventory must be automated where technically feasible.
- u. Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.

Associated Standard: Secure Configuration Standard

Personnel Security

- v. The workforce must receive general security awareness training, to include recognizing and reporting insider threats, within 30 days of hire. Additional training on specific security procedures, if required, must be completed before access is provided to specific Company sensitive information not covered in the general security training. All security training must be reinforced at least annually and must be tracked by the Company.

- w. The Company must require its workforce to abide by the Acceptable Use of Information Technology Resources Policy, and a process must be in place for users to acknowledge that they agree to abide by the policy's requirements.
- x. All job positions must be evaluated by the Company to determine whether they require access to sensitive information and/or sensitive information technology assets.
- y. For those job positions requiring access to sensitive information and sensitive information technology assets, the Company must conduct workforce suitability determinations, unless prohibited from doing so by law, regulation or contract. Depending on the risk level, suitability determinations may include, as appropriate and permissible, evaluation of criminal history record information or other reports from federal, state and private sources that maintain public and non-public records. The suitability determination must provide reasonable grounds for the Company to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to the Company.
- z. A process must be established within the Company to repeat or review suitability determinations periodically and upon change of job duties or position.
- aa. The Company is responsible for ensuring all issued property is returned prior to an employee's separation and accounts are disabled and access is removed immediately upon separation.

Associated Standard: Account Management/Access Control Standard

Cyber Incident Management

- bb. The Company must have an incident response plan, consistent with applicable standards, to effectively respond to security incidents.
- cc. All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the designated security representative as quickly as possible. If a member of the workforce feels that cyber security concerns are not being appropriately addressed, they may confidentially contact the CTO.
- dd. iMoon Support must be notified of any cyber incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to follow proper incident response procedures and guarantee coordination and oversight.
- ee. **Software-Specific Incident Reporting:**

The Company must maintain procedures for incident reporting that address:

- lx. immediate notification to affected operators of incidents impacting their services;
- lxi. regulatory notification requirements within jurisdictional timeframes;
- lxii. documentation of incidents affecting software integrity, RNG systems or customer data;
- lxiii. root cause analysis for incidents affecting regulated systems;
- lxiv. corrective action plans with timelines; and
- lxv. post-incident review and lessons learned documentation.

Associated Standard: Cyber Incident Response Standard

Physical and Environmental Security

- ff. Information processing and storage facilities must have a defined security perimeter and appropriate security barriers and access controls.

- gg. A periodic risk assessment must be performed for information processing and storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary.
- hh. All information technology equipment and information media must be secured to prevent compromise of confidentiality, integrity or availability in accordance with the classification of information contained therein.
- ii. Visitors to information processing and storage facilities, including maintenance personnel, must be escorted at all times.

Associated Standard: Information Security Risk Management Standard

Intellectual Property Protection

As a software developer, intellectual property represents core business value. The Company must implement comprehensive IP protection measures:

jj. Source Code Protection:

- lxvi. All proprietary source code must be maintained securely;
- lxvii. Code access must be restricted to need-to-know basis and role-based access;
- lxviii. All code commits should be attributed to the responsible developer;
- lxix. Code repositories must implement multi-factor authentication;
- lxx. Automated scanning for secrets, credentials and sensitive data in code must be implemented;
- lxxi. Source code must be encrypted at rest and in transit;
- lxxii. Offline backups of source code should be maintained in secure, geographically diverse locations; and
- lxxiii. Source code must never be stored on unsecured or personal devices.

kk. Confidentiality Agreements:

- lxxiv. All employees with access to proprietary information must sign comprehensive non-disclosure agreements (NDAs);
- lxxv. Employment contracts must include IP assignment clauses ensuring Company ownership of work product;
- lxxvi. Contractors and third parties must execute appropriate confidentiality and IP protection agreements;
- lxxvii. Enforcement mechanisms and remedies must be clearly defined.

ll. Trade Secret Protection:

- lxxviii. Proprietary algorithms, game mechanics and mathematical models must be classified as trade secrets;
- lxxix. Reasonable secrecy measures must be maintained and implemented;
- lxxx. Employees must be trained on trade secret identification and protection;
- lxxxi. Access to trade secret information must be logged and monitored; and
- lxxxii. Trade secret misappropriation must be promptly investigated and remediated.

mm. Third-Party Code Management:

- lxxxiii. All third-party libraries, frameworks and components must be inventoried;
- lxxxiv. Licensing compliance must be verified for all third-party code;
- lxxxv. Open source licenses must be reviewed ensuring compatibility with business model;
- lxxxvi. Third-party code must be scanned for security vulnerabilities; and
- lxxxvii. Software composition analysis tools must be utilized to track dependencies.

Associated Standard: Intellectual Property Protection Standard; Source Code Management Standard

5.0 Compliance

This policy takes effect upon approval of CEO. Compliance is expected with all company policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, the Company can request an exception through the Chief Technical Officer's exception process.

Violations of this policy may result in:

- Disciplinary action up to and including termination of employment;
- Suspension or revocation of system access privileges;
- Referral to law enforcement authorities for criminal prosecution;
- Civil liability for damages resulting from policy violations;
- Notification to regulators where required; and
- Impact on license status or renewal.

6.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at: support@imoon.com.

For security incidents or concerns requiring immediate attention, contact support at: support@imoon.com or via the designated incident reporting hotline.

7.0 Document Control

- **Document Owner:** Head of Legal
- **Approval Authority:** CEO
- **Effective Date:** 1 January 2023
- **Review Frequency:** Annual or as required by regulatory changes
- **Version History:** Version 2.0 -
- **Classification:** Internal Use - Confidential