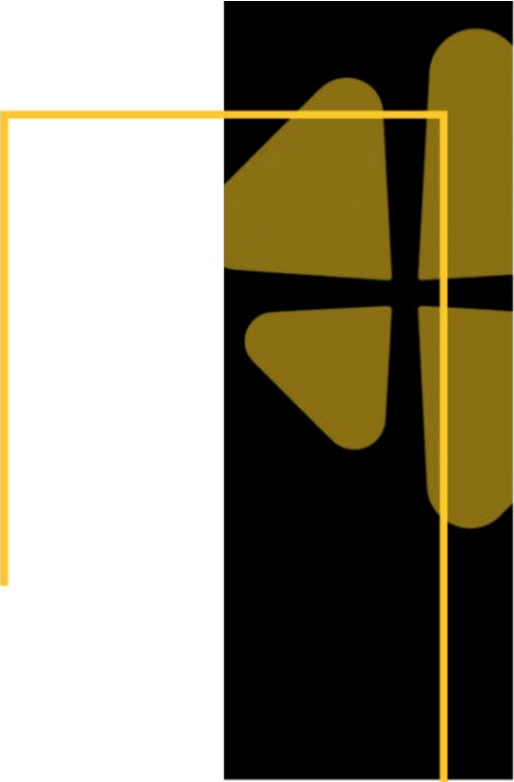




Information Security Policy 2025

MIC Group Entertainment N.V.

Index

I. Introduction	3
II. Objectives.....	3
III. Scope	3
IV. Justification.....	4
V. Definitions	4
VI. Principles of Security	5
VII. Information Security	6
VIII. Personal Data Protection	6
IX. Transaction Security	6
X. Fraud and Money Laundering Prevention	7
XI. Security Incident Response	7
XII. Access and Role Control.....	7
XIII. Technological Infrastructure Security	7
XIV. Gaming and Betting Security.....	8
XV. Training and Awareness	8
XVI. Policy Compliance and Updates.....	8

I. Introduction

micasino.com is committed to safeguarding information as a fundamental priority for its users, partners, and stakeholders. The company recognizes the importance of protecting personal data, financial transactions, and technological assets against evolving cyber threats and operational risks.

This Information Security Policy establishes the principles and controls designed to ensure the confidentiality, integrity, and availability of all information managed within the platform. It provides a framework for compliance with legal and regulatory obligations, alignment with international standards, and the promotion of secure and responsible gaming practices.

II. Objectives

- Protect the integrity, confidentiality, and availability of all platform data and systems.
- Maintain full adherence to relevant legal, regulatory, and industry requirements.
- Mitigate risks related to cyber threats, fraud, and money laundering.
- Promote business continuity through secure operations and recovery mechanisms.
- Foster user trust by safeguarding personal and financial information.

III. Scope

This Information Security Policy applies to all employees, contractors, suppliers, business partners, and users who interact with the platform of micasino.com. It covers all information, systems, applications, transactions, and technological infrastructure used to operate, manage, and deliver gaming and betting services.

The policy establishes guidelines for the protection of sensitive data, personal information, and financial transactions, ensuring confidentiality, integrity, and availability

across all processes. It also encompasses risk management related to cyber threats, fraud, money laundering, and internal or external security incidents.

IV. Justification

The implementation of this Information Security Policy at micasino.com is fundamental to protecting the integrity, confidentiality, systems, and transactions on the platform. As a digital gaming operator, micasino.com manages highly sensitive information, including personal user data, financial transactions, and operational records. Ensuring the security of these assets is crucial for maintaining user trust, achieving full compliance with applicable laws and regulatory standards, and effectively mitigating risks arising from cyber threats, fraud, and money laundering.

V. Definitions

- **Authentication.** The process of verifying the identity of a user, system, or entity before granting access to resources.
- **Authorization.** The process of granting or restricting access rights and permissions based on user roles or privileges.
- **Availability.** The assurance that information, systems, and services are accessible when needed by authorized users.
- **Business Continuity.** The capability of an organization to maintain essential operations and recover quickly in the event of disruptions or disasters.
- **Computer Security Incident Response Plan (CSIRP).** A documented approach for identifying, responding to, and mitigating the impact of security incidents.
- **Confidentiality.** The principle of ensuring that sensitive or personal information is accessible only to authorized individuals.
- **Cyber Threats.** Potential malicious actions or events, such as hacking, malware, phishing, or denial-of-service attacks, that could compromise information security.
- **Fraud.** Any intentional act of deception designed to secure an unfair or unlawful gain, including manipulation of financial transactions or gaming activity.

- **Information Security.** The practice of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and availability.
- **Integrity.** The protection of information and systems against unauthorized modification, corruption, or loss.
- **Money Laundering.** The process of concealing the origins of illegally obtained funds through financial transactions to make them appear legitimate.
- **Multi-Factor Authentication (MFA).** A security mechanism requiring two or more verification methods to grant access to systems or data.
- **Personal Data.** Any information relating to an identified or identifiable individual, including name, contact details, financial information, or gaming activity.
- **Random Number Generator (RNG).** A software algorithm used to ensure the fairness and unpredictability of gaming outcomes.
- **Regulatory Compliance.** Adherence to laws, regulations, and industry standards applicable to the operation of the online casino.
- **Risk Management.** The process of identifying, assessing, and mitigating potential threats to information, systems, and business operations.
- **Segregation of Duties (SoD).** The practice of dividing responsibilities among multiple personnel to prevent conflicts of interest and reduce the risk of errors or fraud.
- **Stakeholders.** Individuals or organizations with an interest or role in the platform, including users, employees, partners, and regulatory bodies.

VI. Principles of Security

- **Confidentiality:** Ensuring that sensitive information is accessible only to authorized users.
- **Integrity:** Safeguarding data and systems against unauthorized modifications or corruption.
- **Availability:** Guaranteeing continuous access to the platform through redundancy measures and disaster recovery mechanisms.

- **Authentication and Authorization:** Implementing robust identity verification and access control mechanisms.
- **Monitoring and Auditing:** Establishing processes for continuous supervision and periodic security reviews.

VII. Information Security

- a. Use of SSL/TLS encryption for all transactions and communications to protect user data.
- b. Implementation of firewalls and intrusion detection systems to prevent cyberattacks.
- c. Restriction of access to sensitive data through multi-factor authentication (MFA) and privilege segregation.
- d. Data backup and recovery mechanisms to ensure business continuity.
- e. Protection against internal threats through monitoring of access and suspicious activities.

VIII. Personal Data Protection

- a. Implementation of secure storage policies and data deletion when required.
- b. Obtaining explicit user consent for the use and processing of their data.
- c. Application of anonymization and pseudonymization techniques to safeguard privacy.
- d. Development of a privacy risk management system to prevent data breaches.

IX. Transaction Security

- a. Continuous monitoring of transactions to detect fraud and suspicious activities.
- b. Implementation of secure authentication protocols to verify user identity.
- c. Identity verification in fund withdrawal processes and changes to payment methods.
- d. Review of behavioral patterns to identify atypical or high-risk conduct.
- e. Periodic evaluation and certification of the payment methods used on the platform

X. Fraud and Money Laundering Prevention

- a. Compliance with UIF and CGA regulations for the prevention of money laundering:
 - i. Application of Know Your Customer (KYC) procedures for all users.
 - ii. Implementation of real-time transactional monitoring to identify suspicious activity.
 - iii. Mandatory reporting of unusual or suspicious transactions according to current regulations.
 - iv. Continuous training of personnel in fraud detection and prevention.
 - v. Generation of automated reports analyzing financial and reputational risks

XI. Security Incident Response

- a. Development of a Computer Security Incident Response Plan (CSIRP).
- b. Implementation of a system for recording and reporting security incidents.
- c. Immediate actions for containment, forensic analysis, and mitigation of incident impacts.
- d. Notification of relevant authorities in case of significant breaches.
- e. Periodic security evaluations and penetration testing to prevent attacks.
- f. Simulations and retrospective analyses to improve incident response.

XII. Access and Role Control

- a. Assignment of roles and permissions according to the principle of least privilege.
- b. Implementation of multi-factor authentication (MFA) for administrative access.
- c. Monitoring and auditing of access to critical information and internal systems.
- d. Activity and session logging for traceability and anomaly detection.
- e. Implementation of segregation of duties to avoid conflicts of interest in internal processes.

XIII. Technological Infrastructure Security

- a. Continuous platform maintenance with security patches and updates.
- b. Network segmentation to limit unauthorized access.
- c. Use of testing environments prior to implementing changes in production.
- d. Regular vulnerability assessments and penetration testing.

- e. Implementation of redundancies and disaster recovery systems to ensure business continuity.

XIV. Gaming and Betting Security

- a. Assurance of fairness in games through the use of software certified by regulatory authorities.
- b. Implementation of a periodically audited Random Number Generator (RNG).
- c. Control and verification of game integrity through regular testing.
- d. Prevention of collusion and manipulation in betting through real-time monitoring.
- e. Development of self-exclusion and betting limit mechanisms as responsible gaming measures.
- f. Security evaluations of software providers to ensure quality and reliability standards.

XV. Training and Awareness

- a. Ongoing training programs on information security and cybersecurity.
- b. Staff awareness of threats such as phishing, malware, and social engineering attacks.
- c. Periodic security incident drills to assess team preparedness.
- d. Internal campaigns on best practices in cybersecurity and information handling.

XVI. Policy Compliance and Updates

- a. Internal and external audits to verify adherence to the security policy.
- b. Periodic review and update of the policy in accordance with regulatory and technological changes.
- c. Disciplinary and/or legal sanctions in case of non-compliance with established provisions.
- d. Appointment of a security committee responsible for supervising the implementation of established measures.