

Information Security Policy

Version 1.0

Effective Date: July, 2025

Table of Contents

1. Introduction.....	3
2. Scope and Applicability	4
2.1. Purpose of the Policy	4
2.1.1. Strategic Security Objectives.....	4-5
2.2. Scope of Information.....	5
2.3. Scope of Information Systems.....	5-6
2.4. Third- Party and Outsourced Services.....	6
2.5. Users Covered by this Policy.....	6
3. Individual Responsibilities.....	6
3.1. All Employees, Contractors and Partners.....	6-7
3.2. System Users and Data Handlers.....	7
3.3. Information Governance & Data Protection Team	7
4. Compliance.....	8-9
4.1. Awareness and Training	9
4.2. Monitoring and Enforcement.....	9
5. Specific Security Objectives.....	11
6. Oversight and Governance.....	12

1. Introduction

OMEGA ENTERTAINMENT N.V., a limited liability company incorporated under the laws of Curaçao, with company registration number 145632, with its registered address at Dr. H. Fergusonweg 1, Curaçao, operates a range of online betting and gaming platforms under applicable eGaming licensing frameworks (hereinafter referred to as the "Operator" or "the Company").

This Information Security Policy (hereinafter the "Policy") outlines the formal rules, principles, responsibilities, and security controls adopted by OMEGA ENTERTAINMENT N.V. to protect the confidentiality, integrity, and availability of its data, systems, and services.

The Policy is designed to provide a robust framework for securing the Operator's information assets, managing risks related to information security, and ensuring compliance with applicable international standards and regulatory requirements, including but not limited to:

- ISO/IEC 27001:2022 – Information Security Management Systems (ISMS);
- ISO/IEC 27002:2022 – Code of practice for information security controls;
- General Data Protection Regulation (EU) 2016/679 (GDPR);
- Curacao eGaming regulations, including applicable AML/KYC compliance obligations;
- Applicable Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and responsible gaming legislation and guidance.

2. Scope and Applicability

2.1. Purpose of the Policy

2.1.1. The purpose of this Information Security Policy is to ensure that the information assets of the Company are protected in a manner that is consistent with internationally recognized best practices, applicable legislation, and the expectations of regulators, customers, and business partners.

This Policy is based on the fundamental security principles of:

1. Confidentiality – Access to data shall be restricted to individuals and systems with appropriate authorization, ensuring that sensitive information is not disclosed to unauthorized parties.
2. Integrity – All information assets shall remain accurate, reliable, and safeguarded against unauthorized or accidental modification. Systems and networks must function in accordance with their design and purpose.
3. Availability – Information and related services shall be accessible and usable when required, ensuring continuity of operations, customer service, and regulatory compliance.

In support of these principles, the Company is committed to achieving the following objectives:

2.1.1. Strategic Security Objectives

- Establish and communicate the Company's strategic and operational commitment to securing its digital assets, infrastructure, and information across all platforms and business functions.
- Define clear responsibilities and obligations for all personnel, contractors, vendors, and third parties who access, process, store, or manage Company information systems and data.
- Protect personal, operational, financial, and customer data from unauthorized access, disclosure, loss, alteration, or misuse, in accordance with GDPR and other applicable laws.
- Ensure data accuracy and system reliability, maintaining trust in betting systems, customer transactions, reporting, and decision-making.
- Provide structured guidance on the implementation of security controls, procedures, and practices that reduce information-related risks to acceptable levels.
- Support legal and regulatory compliance with all applicable laws, including those of Curaçao, the General Data Protection Regulation (GDPR), and industry-specific obligations (e.g., AML/KYC, responsible gaming).

- Promote a culture of information security awareness and accountability across the organization.
- Enable continuous improvement of the Company's Information Security Management System (ISMS), through ongoing monitoring, risk assessments, audits, and management reviews.

2.2. Scope of Information

This Information Security Policy applies to all forms of information processed or held by the Operator, whether digital or physical, and includes, but is not limited to:

- External Customer Information: All personal, financial, and behavioral data collected and processed in relation to player accounts and betting activities;
- Operational Documentation: Internal communications, operational plans, business strategies, audit reports, and meeting records;
- Financial, Legal, and Compliance Records: Company financial statements, tax filings, regulatory reports, and anti-money laundering (AML) documentation;
- Human Resources and Employee Records: Employment contracts, performance evaluations, health and safety records, and payroll information.

This also includes all information handled in accordance with applicable privacy, gaming, and financial regulations (e.g., GDPR, KYC/AML laws, Curacao eGaming requirements).

According to this Policy the Company shall achieve the following:

- systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts
- design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable in line with the Commission's Risk Appetite.
- adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis
- monitor the development of the Information Security Policy to ensure continual improvement.

2.3 Scope of Information Systems

The policy applies to all information processing facilities, including but not limited to:

- Data centers, servers, cloud environments, storage media;
- Workstations, laptops, and mobile devices used for Company business;
- Software platforms, databases, and network devices;
- Internal and external communication systems (e.g., email, VoIP, messaging tools).

2.4 Third-Party and Outsourced Services

This Policy also applies to all external entities (vendors, service providers, consultants, affiliates) that:

- Provide hosting, payment, marketing, customer support, or identity verification services;
- Have access to Company data or infrastructure;
- Process personal data on behalf of the Company under data processing agreements (DPAs) or contracts.

2.5 Users Covered by this Policy

The following categories of users are bound by this Policy:

- Full-time and part-time employees
- Independent contractors and consultants
- Temporary staff, interns, and agency workers
- Third-party service providers (with access to information assets or processing systems)

All users are collectively referred to as "**Users**" in this policy.

3. Individual Responsibilities

Information security forms a critical part of the Operator's risk management and compliance framework. This section outlines the roles and responsibilities of individuals and key stakeholders involved in protecting information assets and maintaining the integrity of the Operator's information security management system (ISMS).

All users—internal or external—who access or interact with the Operator's information or systems are expected to understand and fulfill their responsibilities as described below.

3.1 All Employees, Contractors, and Partners

All colleagues, contractors, consultants, and authorized third-party users are responsible for:

- Complying with this Information Security Policy and all related security, privacy, and compliance procedures;
- Protecting all Company information assets, including customer data, operational documents, and system credentials, from unauthorized access, disclosure, alteration, or destruction;
- Following secure usage practices for hardware, software, and communication platforms;
- Completing mandatory information security and data protection training during onboarding and annually thereafter;
- Promptly reporting any actual or suspected security incidents, data breaches, system misuse, or policy violations through the defined reporting channels (e.g., internal ticketing or directly to the Information Security Officer);
- Maintaining awareness of phishing threats, social engineering risks, and other cyberattack vectors.

3.2 System Users and Data Handlers

Any individual user—internal or external—who uses the Operator's systems or processes Company information, whether via internal platforms or through remote access, is responsible for:

- Complying with all applicable Company policies, regulatory obligations (e.g., GDPR, AML/KYC), and contractual terms relating to information security;
- Ensuring access credentials (e.g., usernames, passwords, API keys) are kept secure and never shared;
- Handling Company data only for authorized business purposes;

- Reporting unauthorized access, data loss, or any breach of this Policy through the established reporting procedures.

3.3 Information Governance & Data Protection Team

The Information Governance & Data Protection Team is responsible for the strategic oversight, management, and protection of the Company's information assets and data privacy obligations. This team encompasses key roles including the Senior Information Risk Owner (SIRO), Information Asset Owners (IAOs), and the Data Protection Officer (DPO), who work collaboratively to ensure the Company's information security and data protection frameworks align with business objectives, regulatory requirements, and industry best practices.).

Combined Responsibilities:

- Providing executive oversight of the Company's information security risk profile and ensuring strategic alignment with business goals and regulatory expectations.
- Identifying, assessing, and managing information security risks across all business functions, including the approval of security controls, investment decisions, and resource allocations.
- Maintaining an accurate and up-to-date Information Asset Register (IAR), ensuring all assets are properly classified, documented, and managed in accordance with internal policies and data sensitivity.
- Defining and enforcing access controls, usage restrictions, and data retention practices to protect information integrity, availability, and confidentiality.
- Ensuring compliance with the General Data Protection Regulation (GDPR) and other applicable privacy laws across all jurisdictions where the Company operates.
- Advising on Data Protection Impact Assessments (DPIAs), privacy-by-design principles, and lawful data processing activities.
- Facilitating incident response planning, business continuity strategies, and coordination of risk assessments related to information security and data privacy.
- Serving as the primary liaison with supervisory authorities, managing data subject rights requests, and addressing inquiries from external regulatory bodies.
- Promoting a culture of data protection awareness and accountability across the organization through ongoing collaboration with internal stakeholders.

4. Compliance

The Company ensures full compliance with all applicable laws, regulations, standards, and contractual obligations, including those imposed by Curacao eGaming, GDPR, and relevant AML/KYC legislation.

This Policy is intended to prevent violations of legal, regulatory, or contractual requirements by establishing a framework for information security governance.

All users of information systems operated or managed by the Company are required to observe and comply with the applicable laws and internal controls as outlined in this Policy and related procedures.

All employees, contractors, consultants, and third parties with access to the Operator's information systems or data are required to comply with this Policy in full. Non-compliance—whether intentional or due to negligence—may result in:

- Internal disciplinary action, up to and including termination of employment or contractual relationship;
- Regulatory reporting obligations;
- Legal action where applicable under data protection or gambling legislation.

To ensure effective compliance, the Company will:

- Provide ongoing training and awareness programs on information security, privacy, and acceptable use to all staff;
- Ensure that employees understand their individual responsibilities under this Policy, including how to identify and report potential threats, breaches, or vulnerabilities;
- Review training content regularly to reflect emerging risks, regulatory changes, and evolving best practices.

4.1. Awareness and Training

To ensure effective compliance, the Company will:

- Provide ongoing training and awareness programs on information security, privacy, and acceptable use to all staff;
- Ensure that employees understand their individual responsibilities under this Policy, including how to identify and report potential threats, breaches, or vulnerabilities;
- Review training content regularly to reflect emerging risks, regulatory changes, and evolving best practices.

4.2. Monitoring and Enforcement

Compliance with this Policy will be monitored through:

- Regular audits and system reviews;
- Ongoing risk assessments and control testing;
- Investigation of reported security incidents and suspected violations.

Where breaches are identified, appropriate corrective actions will be taken, and lessons learned will be used to inform future improvements.

5. Specific Security Objectives

To fulfill its obligations and manage risk effectively, the Company has adopted the following operational security objectives:

- **Controlled access:** Information is only accessible to authorized individuals, and only for as long as access is required for operational or regulatory purposes;
- **Delegated access rights:** Access levels are defined and enforced based on roles and responsibilities, through centralized identity and access management tools;
- **Confidentiality and integrity:** The Company ensures that data and systems remain accurate, consistent, and protected against unauthorized modification or disclosure;
- **Service availability:** All applications and services, including cloud-hosted platforms, are maintained according to their applicable Service Level Agreements (SLAs);
- **Business continuity:** Business continuity and disaster recovery policies are established, maintained, and tested to ensure resilience in the event of disruption;
- **Policy access:** All security and data protection policies are clearly documented and readily accessible to all staff and relevant third parties;
- **Incident management:** All information security breaches or suspected weaknesses are to be reported, logged, and investigated promptly, with appropriate remedial actions taken;
- **Audits and reviews:** Regular internal audits and risk reviews are conducted to ensure ongoing compliance, relevance, and improvement of the security framework;
- **Secure deployment:** All new systems, applications, and services are introduced in a controlled and secure manner, including formal risk assessments and approval processes;
- **Vulnerability management:** Systems are regularly audited and tested for vulnerabilities. Patch management is automated where possible, and identified vulnerabilities are addressed through a documented process including impact assessment, reporting, and remediation within defined timeframes.

6. Oversight and Governance

The Operator's Security Governance Group (or equivalent internal authority) is responsible for monitoring performance against these objectives. This group will:

- Review security objectives at least annually, or in response to regulatory or risk-based changes;
- Ensure alignment between the Operator's security posture and its risk management strategy;
- Monitor and evaluate risks related to confidentiality, service delivery, and the availability of information systems.



(SMES) Solutions for Management Employment Support N.V.

Managing Director

03.06.2026