

Osmila N.V.

INFORMATION SECURITY POLICY

Table of Contents

REVISION HISTORY	3
1. DEFINITIONS	5
2. INFORMATION SECURITY POLICY	7
2.1 POLICY	7
2.2 OBJECTIVE	7
2.3 RESPONSIBILITIES	7
3. DATA	8
3.1 PERSONAL DATA	8
3.2 CONFIDENTIAL BUSINESS DATA	8
3.3 CLASSIFIED DATA	8
4. SECURITY OF INFORMATION	9
4.1 SECURITY DURING USAGE OF COMPANY'S SYSTEMS	9
4.1.1 Password	9
4.1.2 Security and Proprietary Information	9
4.1.3 Acceptable Use Policy	9
4.1.4 Secrecy	10
4.1.5 Remote Connections	10
4.1.6 Remove Sensitive Information	10
4.1.7 Retention Terms and Personal Data	10
4.2 SECURE DISPOSAL AND DESTRUCTION OF BUSINESS INFORMATION AND DEVICES AFTER USE	10
4.2.1 Devices	10
4.2.2 Physical documents	10
4.2.3 Destruction of business information	10
5. SECURITY OF THE COMPUTER SYSTEM	11
5.1 SAFEGUARDING OF APPLICATIONS	11
5.2 SAFEGUARDING OF NETWORKS	11
5.3 LOGS AND OTHER SYSTEMS SECURITY TOOLS	11
5.4 MEASURES AGAINST DATA LOSS	11
6. EXTERNAL PARTIES	11
6.1 HIRING OF EXTERNAL PARTIES	11
7. PHYSICAL SECURITY OF BUILDINGS AND THE SURROUNDING AREA	12
7.1 CLEAN DESK POLICY	12
7.2 EMPLOYEES ACCESS	12
7.3 VISITORS	12
8. TRAINING	13

REVISION HISTORY

Version #	Effective Date	Approving Official	Responsible Office	Next Review Date	Comments
1.0	Oct 31, 2025	eMoore N.V.	Compliance function	Oct 31, 2026	-
1.1	Oct 31, 2025	eMoore N.V.	Compliance function	Oct 31, 2026	Major update: ISMS scope, risk mgmt, IR/BCDR, IAM/MFA, crypto, logging, vendor risk, privacy/GDPR, change mgmt

1. Definitions

Account Holder	An individual who has a Player Account on the Website.
Back Up	Periodic spare copy of business information or other data.
Business data	Information other than personal data, that is processed within the Company for business processes.
Classified information	Information as mentioned under article 4.3
the Company	Osmila N.V., a limited liability company duly organized under Curaçao law registered with the Chamber of Commerce and Industry in Curaçao under number 102267.
Computer System	Combination of hardware and software that work together to perform specific tasks by accepting input, processing data, storing information, and producing output. The system is essential for the Company to deliver its services effectively.
Confidential business information	The business data of which it is deemed undesirable that these become known to parties outside of Company.
Data subject	identified or identifiable natural person
Employee	Any person working for the Company.
Player	Individual who has registered with the Company for the purpose of making use of the Services offered on the Website and for which a Player Account has been opened providing him/her with a unique code.
Player Account	An account granted to an individual after registration on the Website. The Player Account is created and issued by the Company and is required for wagering with real money. Only one Player Account is permitted per person, per IP address, per family and per Shared Environment.

Personal Data	Information relating to an identified or identifiable natural person who can be identified, directly or indirectly, on the basis of data such as name, ID number, location, user name, or factors such as physical, psychological, genetic, mental, economic, cultural or social identity connected to a natural person.
Sensitive Information	Sensitive or confidential data that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization.
Service	the gaming and betting offers provided by the internet gateway operated by the Company to the Account Holder, through the Website.
Website	the online gaming platform offering online gaming services operated by the Company.
Information Security Officer (ISO)	Appointed by the Board of Directors, responsible for establishing and maintaining the Company's Information Security Management System (ISMS), aligned with ISO/IEC 27001. The ISO oversees risk assessments, audits, awareness programs, and regulatory reporting to the Gaming Control Board (GCB) and the Financial Intelligence Unit (FIU Curaçao).
RPO/RTO	Recovery Point Objective and Recovery Time Objective — parameters defining backup frequency and service restoration time in business continuity planning
Money Laundering Reporting Officer (MLRO)	The designated officer responsible for AML/CFT oversight, evaluation of suspicious activity, and submission of Suspicious Transaction Reports (STR/SAR) to FIU Curaçao.

2. Information Security Policy

2.1 Policy

To ensure the smooth and secure operation of the Company, it is critical to maintain the availability, integrity, and confidentiality of all business information. Certain information, classified as Sensitive Information, requires enhanced protection due to legal obligations, contractual commitments, or shareholder requirements. This policy establishes the principles and guidelines for safeguarding Sensitive information, and will be reviewed periodically, ensuring compliance with applicable laws and maintaining trust in the operations by establishing a framework of management measures that work together to keep all company information secure, including sensitive data.

Osmila N.V. commits to maintaining compliance with the Curaçao Gaming Control Board's B2C license conditions and the FIU Curaçao's AML/CFT requirements.

This Policy is designed according to ISO/IEC 27001 principles and GDPR Article 32 to ensure continuous protection of all data handled by the Company.

The appointed Information Security Officer (ISO) reports quarterly to the Board of Directors on risk posture, incidents, and control effectiveness.

All information assets are classified and protected according to their sensitivity level, and an annual review of this policy shall be performed following any material incident.

Incident notifications impacting confidentiality, integrity, or availability of data shall be reported to:

- GCB and FIU Curaçao within 72 hours of detection, and
- affected data subjects (where applicable) under GDPR Article 33.

Encryption standards shall include AES-256 for data at rest and TLS 1.3 for data in transit. All administrative access must enforce multi-factor authentication (MFA) and password management through a company-approved password manager.

2.2 Objective

The objective of this policy is to safeguard the integrity, confidentiality and availability of all the information handled by the Company by making sure that the Information Security Policy shows that management is prepared to support an on-going commitment to information security.

2.3 Responsibilities

All employees have a responsibility to conduct themselves in an ethical manner, in particular:

- Data/information obtained inappropriately should not be used;
- Finding a system weakness should be reported immediately and should not be taken advantage of;
- Every user has a responsibility to carry out his/her work diligently and will be held accountable for misuse of the company's information system;
- Report any known violation or system weakness to the person or persons responsible for security.

3. Data

Sensitive information has many forms. From the legal perspective of the most applicable legislation, such as Curaçao Data Privacy as well as GDPR, we distinguish personal data and confidential business data.

3.1 Personal Data

The Personal information requested and or collected to use and process when using the Services, are without limitation:

- a. Information provided when completing Account Opening forms, or any other data further submitted to the Website in relation to the Account holder e.g. first and last name, date of birth, telephone number, email address;
- b. Documents and any other information to verify a player's account, facilitate deposits or withdrawals, and perform anti-fraud checks, either proactively or as required by law including but not limited to passport copies, payment receipts, and bank statements.
- c. Player Account related information such as login information, GeoIP location data, traffic data, browser and device information, weblogs, activity logs and any other related details;
- d. Any type of communication with the Website including but not limited: website messages, email, or other means of communication;
- e. All player transaction history including completed surveys;
- f. Survey participations or any other customer assessments that we may carry out from time to time.

3.2 Confidential Business data

The Company might process information, other than personal data, for business processes. This Business data can be regarded as confidential specifically if this is data which is not meant nor desired to be shared with parties outside of the Company.

3.3 Classified data

The company might also deal with information subject to stricter security measures. This Classified information are information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Payroll, personnel, sensitive player details, and financial information are also in this class, because of privacy requirements.

All personal data processed by Osmila N.V. shall comply with the Curaçao Data Privacy Framework and GDPR principles (lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity/confidentiality).

Data categories shall include:

- **Player personal data** collected under KYC/AML obligations.
- **Transaction and betting history** retained for audit and AML investigation.
- **Responsible Gaming Data** supporting risk behavior analysis.

Data Retention:

In accordance with **FIU Curaçao and AMLD requirements**, player and transaction records must be retained for **a minimum of five (5) years** following the end of the player relationship.

Upon expiry, data shall be securely erased or anonymized, except when retention is required for ongoing investigations.

Data Transfer and Hosting:

Cross-Border Transfers & Safeguards: When hosting or processing data offshore, Osmila ensures equivalent protection through;

- Encryption at rest/in transit, (ii) vendor due-diligence and security testing, and (iii) appropriate transfer mechanisms (e.g., adequacy decisions or Standard Contractual Clauses (SCCs) with supplementary measures as needed). A Data Protection Impact Assessment (DPIA) is performed when processing poses high risk to individuals' rights and freedoms.

4. Security of Information

4.1 Security during usage of Company's systems

All equipment (fixed and mobile) is set up, used and maintained in accordance with the manufacturer's instructions. The IT staff of Company ensures that software updates regarding device and software security will be installed on all devices used for the storage or access to sensitive information as quickly as possible.

4.1.1 Password

All equipment (fixed and mobile) and all mobile data carriers containing Sensitive Information that can be used for access to Sensitive Information is accommodated with a form of access security (for example: a password, two-factor authentication or encryption).

1. Passwords must at least meet the criteria in terms of **power** and **repetition** as advised by international standards of cybersecurity.
2. If the Company requires the use of a password manager, employees will use this password manager in their daily work to generate and replace passwords.

4.1.2 Security and Proprietary Information

Passwords are kept secure and employees must not share accounts. Authorized users are responsible for the security of their passwords and accounts.

Employees must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code.

4.1.3 Acceptable Use Policy

Employees are to take personal responsibility when exercising good judgement regarding reasonable personal use.

Internet access and its usage must be for professional purposes and should not be used for any other motive. Any work related issue or material that could identify an individual who is a customer/client or work colleague, which could adversely affect the Company a customer/client or our relationship with any customer/ client must not be placed on a social networking site either during or outside of working hours and includes access via any computer equipment, mobile phone or device.

4.1.4 Secrecy

Employees and suppliers of the Company are required to strict secrecy of sensitive information that comes to their attention related to their function, or what comes into their knowledge by virtue of their agreement with the Organization. This confidentiality obligation shall continue also after termination of the agreement. Contact with government agencies and Media shall be made exclusively through the persons appointed by Company.

4.1.5 Remote Connections

Any employee or third party that receives the right of remote access, must keep their security credentials secure, confirming that one will not share this information with anyone under any circumstances.

4.1.6 Remove Sensitive Information

Storing sensitive information always brings a risk of loss, theft or unauthorized access. That is why it is important to regularly assess whether the storage of specific kinds of sensitive information is still needed. For example for serving Company's clients or when it is required by law to store specific kinds of information. If this is not the case the information concerned should be removed and destroyed.

It is not allowed to take Sensitive information outside of the organization unless this is required for the exercise of the function.

4.1.7 Retention Terms and Personal Data

The Company maintains a record of all relevant documentation on a separate database for at least five years after ending a business relationship. The Company is obliged to retain files in a way that enables investigating authorities to identify a satisfactory audit trail for individual transactions including the amounts, currencies and type of transactions.

4.2 Secure disposal and destruction of business information and devices after use

In no case may documents or devices with business information be disposed in public waste processing.

4.2.1 Devices

When a device of the Organization (phone, laptop, tablet, PC, etc.) that was used by an Employee is no longer being used, the device is returned to the applicable manager.

4.2.2 Physical documents

Non-electronic business information, such as paper documents must be disposed of in a safe manner, for example by shredding and/or discharge by a reliable service provider that is certified for this type of procedure.

4.2.3 Destruction of business information

Company information that is no longer necessary for the conduct of business must be classified as such by Company and carefully removed. It is important that we periodically verify that:

1. Devices that are no longer used are erased or destroyed;

2. Company information that is no longer necessary erased or destroyed (including backups).

5. Security of the Computer System

5.1 Safeguarding of Applications

If a system is connected to the Internet, both it as well as the underlying operating system have the latest security patches installed.

5.2 Safeguarding of Networks

Wireless networks shall be password protected and used solely by staff of the Company.

Downloaded and uploaded classified and confidential information between systems must be strictly controlled. Classified and confidential Information must be stored in a manner inaccessible to unauthorized individuals. Classified information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise.

5.3 Logs and other Systems Security Tools

To the extent that systems software permits, computer and communications systems handling sensitive, valuable, or critical information must securely log all significant security relevant events such as Players switching user IDs during an online session, attempts to guess passwords, attempts to use privileges that have not been authorized, modifications to production application software and data, modifications to system software and data, changes to Player privileges, and changes to logging system configurations.

Certain information must be captured whenever it is suspected that computer or network related crime or abuse has taken place. The relevant information must be securely stored offline until such time as it is determined that the Company will not pursue legal action or otherwise use the information. The information to be immediately collected includes the system logs, application audit trails, other indications of the current system states, and copies of all potentially involved files.

5.4 Measures against data loss

Company has backup facilities where periodic backups of business information (hereinafter referred to as "**Backup**") are stored. Employees must in addition itself act adequately to prevent that (locally stored) data is lost or becomes inaccessible, either by accident or on purpose. Information should be stored on the network as much as possible and not on the hard disk of the computer

6. External Parties

6.1 Hiring of external parties

Before entering into any agreement with an external party, they shall not be given access to Sensitive Information unless determined that they have a legitimate business need. The Company shall verify that the external party meets the requirements under this policy. These requirements, along with the conditions governing the handling, protection, and use of Sensitive Information, shall be incorporated into the agreement with this Supplier ("Agreement"). The external party shall confirm its understanding and acceptance of these conditions by signing the Agreement prior to receiving any Sensitive Information.

Access given to third parties, auditors and consultants must only be given after confirmation by Management and shall only be given for the duration of the assignment. Access through profiles or accounts given to third parties will be revoked as soon as the assignment has ended.

All suppliers, partners, and third-party processors must undergo **security due diligence** before engagement.

Each contract shall include:

- Confidentiality and Non-Disclosure Agreement (NDA).
- Data Protection Addendum ensuring compliance with Curaçao Data Protection and GDPR.
- Termination clauses requiring secure data return or destruction.

The ISO maintains a **Supplier Risk Register** documenting risk scores, review frequency, and compliance status.

Third-party access credentials are time-limited and monitored. After project completion, all access is revoked and audited.

7. Physical security of buildings and the surrounding area

7.1 Clean desk policy

All Employees must ensure that devices, documents and data carriers will not be left unattended. Outside of regular working hours, all workers must clean their desks and working areas such that all sensitive or valuable data is properly secured.

7.2 Employees Access

Employees only have access to those parts of the buildings of the organization that are for general use or to which access to them by means of a key or access card is granted. In the event of misuse of the key or the access pass disciplinary measures can be taken.

7.3 Visitors

Visitors are not allowed in those parts of Company's buildings where sensitive information is stored or accessible. During the whole stay of the visitor is accompanied by a Company employee. The Employee is responsible for the visitor during the visit and is responsible to guide the visitor after the visit to the front door.

7.4 Datacenter

Datacenters shall employ 24/7 CCTV monitoring with recordings retained for 90 days. Access control must use smart cards or biometrics. Entry logs are maintained for a minimum of 1 year for auditability. Environmental controls (UPS, fire suppression, HVAC) must be periodically tested. Critical infrastructure rooms shall have dual-factor access control and alarm monitoring.

8. Training

All Employees will be required to follow a webinar about dealing with privacy and personal data. This also applies to new Employees, and checklists will be maintained to ensure that all Employees are up to speed.

All employees must complete **annual information security and AML/KYC awareness training**, including modules on:

- Data protection and privacy
- Responsible gaming obligations
- Phishing and social engineering prevention

Training completion is logged and verified by Compliance.

New hires must complete onboarding training within their first 30 days of employment.

9. Business Continuity and Backup

Osmila N.V. maintains a **Business Continuity Plan (BCP)** ensuring continuity of operations under disruption.

All systems must comply with defined recovery metrics:

- **RPO (Recovery Point Objective):** 1 hour
- **RTO (Recovery Time Objective):** 4 hours

Off-site backups are encrypted and stored in a Disaster Recovery Center that geographically different location from the primary site.

Annually, restoration tests shall validate recovery procedures.

Incident reviews feed back into risk assessments and security controls.

10. Governance and Audit

The ISO shall conduct internal security audits at least annually, or upon significant system changes.

Audit results are reviewed by the Compliance Function, and corrective actions are tracked to closure.

Independent third-party audits may be commissioned to validate alignment with ISO/IEC 27001 and Curaçao GCB requirements.

All reports are retained for a minimum of 5 years for regulatory inspection.

11. Policy Maintenance and Review

This policy is reviewed annually or following any major incident.

The ISO, together with Compliance and IT, ensures continuous improvement through lessons learned, control testing, and regulatory feedback.

All updates are approved by the Board of Directors and logged in the Revision History.