

**INFORMATION
SECURITY POLICY
SUNSTAR IMPACT N.V.**

1. Definitions

Business Continuity	The capability of the Company to maintain or quickly resume critical operations following a disruption
Confidential Information	Any non-public information belonging to the Company, its players, or its partners, including commercial, financial, technical, or operational data.
Data	Information which: • It is being processed by means of equipment operating automatically in response to instructions given for that purpose. • It is recorded with intention that it should be processed by means of such equipment. • It is recorded as part of filing system.
Data protection laws	• National ordinance on data protection (NODP) (Landsverordening bescherming persoonsgegevens, National Gazette 2010, Consolidated text no. 84) – regulates the processing of personal data by both public and private entities in Curaçao. • General Data Protection Regulation (the GDPR) – regulation of the European Union, which has implication for a data controller/ data processor as the extra-territorial reach of the GDPR is not only relevant to business established in the European Union but also to international businesses established in Curaçao which offer goods or services to individuals in the European Union or monitor their behavior in the European Union.
Data Subject	The natural person to whom personal data relates (e.g., players, employees, contractors)
DPO	Data Protection Officer
Encryption	The process of converting data into a coded form to prevent unauthorized access, using industry-standard algorithms.
Incident	Any actual or suspected event that compromises the confidentiality, integrity, or availability of the Company information or systems (e.g., data breach, cyberattack, fraud attempt)
Information Asset	Any data, system, software, or infrastructure that supports the Company's operations and requires

	protection against unauthorized access, alteration, loss, or disclosure.
Multi-Factor Authentication (MFA)	A security mechanism requiring two or more independent credentials (e.g., password and mobile verification) before granting access.
National data protection authority	• NODP – The Personal Data Protection Committee as referred to in article 42 of the National Ordinance Personal Data Protection. • GDPR – An independent public authority established by a member state pursuant to article 51 of the GDPR (Article 4(21), GDPR). The authority is responsible for monitoring the application of the GDPR to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the European Union.
Personal Data	Any information that identifies or can reasonably identify a natural person, directly or indirectly (e.g., name, ID number, IP address, location data, financial information).
Personal Data Protection Board (CBP Curaçao)	Curaçao's supervisory authority established to oversee compliance with the NODP (as of November 2025, the CBP has been formally established but is not yet fully operational).
Processing	Any activity performed on personal data, including collection, storage, retrieval, use, disclosure, alignment, alteration, restriction, erasure, or destruction.
Processor	A natural or legal person which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority.
Relevant Filing System	Any structured set of personal data accessible according to specific criteria, whether centralized, decentralized, or dispersed.
Sensitive Personal Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, genetic data, biometric data, or information about a person's sex life or sexual orientation. Where applicable, the GDPR definition applies only to EU-based players.

Vendor/ Third Party	An external organization or service provider that processes or has access to the Company data and must comply with contractual and regulatory requirements.
---------------------	---

2.Introduction

This Information Security Policy (“the Policy”) establishes the framework by which Sunstar Impact N.V. (“the Company”), a licensed online gaming operator in Curaçao, protects the confidentiality, integrity, and availability of its information assets. The Policy applies company-wide and covers personal data, financial information, gaming records, and all related systems and processes.

The Policy ensures that the Company’s handling of information is lawful, secure and transparent in line with:

- The National Ordinance on the Protection of Personal Data (NODP) of Curaçao.
- The General Data Protection Regulation (GDPR) were applicable to EU players.
- The National Ordinance on Games of Chance (NOGC) and Curaçao Gaming Authority (CGA) license conditions.
- ISO/ IEC 27001 (Information Security Management Systems), as the baseline framework for security governance.
- PCI DSS (Payment Card Industry Data Security Standard), for secure handling of cardholder data, and
- Other relevant AML/ CFT, Responsible Gaming and gaming compliance regulations.

The objectives of this Policy are to:

- Safeguard customer, employee, and company information against unauthorized access, misuse, loss or corruption.
- Support compliance with regulatory requirements, including AML/ CFT unusual transaction monitoring and Responsible Gaming obligations.
- Ensure resilience of gaming operations through robust technical, organizational, and cybersecurity measures, and
- Build trust with regulators, players, and business partners by demonstrating accountability, transparency, and strong governance.

This Policy applies to all employees, contractors, and third-party providers handling information on behalf of the Company. Compliance with the Policy is mandatory and subject to continuous monitoring, periodic audits and annual review.

3. Information Security Objectives and Principles

Sunstar Impact N.V. is committed to maintaining the confidentiality, integrity, and availability of information assets. The Company's objectives are to:

- Protect player and company data from unauthorized access or disclosure
- Ensure resilience of gaming platforms, systems, and services
- Comply with all applicable laws and regulatory requirements, including the NODP, GDPR (where applicable), the National Ordinance on Games of Chance, and CGA license conditions.
- Maintain stakeholder trust through robust cybersecurity and data privacy practices.

4. Access Control and Authentication

Access to player personal data and gaming records is strictly limited to authorized personnel whose duties require such access. Access to systems and data shall be granted on a "need-to-know" and "least privilege" basis. Only the Company-approved devices that meet defined security standards may be used to access systems containing player data, gaming records, or financial information. The use of personal or unmanaged devices for such access is prohibited unless expressly authorized and subject to equivalent security controls.

All Company-approved endpoints used to access sensitive systems shall be subject to the following minimum-security requirements:

- **Encryption:** Devices must use full-disk encryption or equivalent safeguards to protect data at rest and in transit.
- **Secure Configuration:** Endpoints shall be configured in accordance with Company security standards, including timely installation of operating system and application security updates and the disabling of unnecessary services and software.

- **Antivirus/ Endpoint Detection and Response:** Approved antivirus and/ or EDR solutions must be installed, active, and regularly updated on all endpoints accessing the Company systems.
- **Remote Access Controls:** Remote access to Company systems shall only be permitted through approved secure channels and is subject to strong authentication controls, including multi-factor authentication (MFA).
- **Prohibited Uses:** Endpoints used for Company operations must not be used for unauthorized software installation, insecure file sharing, or activities that may compromise the confidentiality, integrity, or availability of Company data.

Role-based access control shall be implemented for all systems handling player or financial data. MFA is mandatory for all privileged accounts and remote access. Privileged accounts must be separately monitored, logged, and reviewed quarterly by the Compliance Officer and IT teams.

Access rights must be revoked promptly upon termination of employment or engagement. Accounts of termination users shall be disabled within 24 hours of departure or immediately where risk is identified.

The Company shall further:

- Maintain access logs of all staff interactions with personal data and critical gaming and financial systems.
- Require confidentiality agreements and data protection obligations for all employees and contractors with access to sensitive information.
- Prohibit disclosure of personal data to third parties except:
 - As required for regulatory compliance (e.g., CGA, AML/ CFT reporting)
 - or
 - Where mandated by law, with proper documentation.

Any suspected compromise of an endpoint or unauthorized access to systems shall be treated as a security incident and handled in accordance with the Company incident Response Plan.

5. Data Protection Principles

The Data Protection Principles sets out principles which the Company adheres to in relation to the Processing of Personal Data.

The Company also engages Processors to process Personal Data on its behalf, such Processors must, pursuant to the agreement entered by both parties, comply with the principles in their processing of Personal Data on behalf of the Company.

When processing personal data, the Company follows the principles established under the Data Protection Principles and the NODP. External processors engaged by the Company must comply with these same principles under contractual agreements.

The seven key principles are:

1. **Lawfulness, Fairness, and Transparency:** Data must be processed on a valid legal basis, handled fairly, and explained to individuals in clear terms.
2. **Purpose Limitation:** Data is collected only for defined, legitimate business purposes (e.g., account creation, fraud prevention, payment, regulatory compliance) and not reused for incompatible purposes.
3. **Data Minimization:** Only the minimum personal data necessary for each purpose is collected and retained.
4. **Accuracy:** Personal data must be correct and updated when necessary; inaccurate data is corrected or deleted promptly.
5. **Storage Limitation:** Data is kept no longer than required for business or legal purposes, unless archived securely for public interest, research, or statistical use.
6. **Integrity and Confidentiality:** Data must be secured against unauthorized or unlawful use, loss, or damage with appropriate technical and organizational measures.
7. **Accountability:** The Company is responsible for compliance and must be able to demonstrate it.

5.1 Lawful Processing

Processing of personal data must always be based on valid legal grounds. Depending on the circumstances, this may include:

1. **Consent:** The player has given explicit agreement for their data to be processed for a stated purpose.
2. **Contractual necessity:** Data must be processed to provide services under a contract with the player (e.g., account management, processing wagers).
3. **Legal obligation:** Data is processed to comply with legal or regulatory requirements (e.g., AML/ CFT laws, tax reporting)
4. **Vital interests:** Data is processed to protect a person's life or safety in exceptional cases.
5. **Public task:** Processing is necessary for duties in the public interest or under regulatory authority.
6. **Legitimate interests:** Processing is necessary for the Company's legitimate business purposes (e.g., fraud detection, service improvement), provided players' rights are not overridden.

The Company shall consider the applicable legal basis for Processing Personal Data and apply each basis where relevant.

5.2 Sensitive Personal Data

Special categories of Personal Data, such as health information or political views are subject to stricter protection. These may only be processed if:

- The player has given explicit consent.
- The processing is required by law (e.g., employment obligations).
- It is necessary to protect the player's vital interests.
- The data has been made public by the player.
- It is required for legal claims, public health, or other specific grounds permitted by Data Protection Principles.

5.3 Personal Data Lifecycle Management

The Company applies a structured lifecycle approach to the handling of Personal Data, covering its collection, processing, storage, access, transfer, archival, and destruction. This lifecycle model ensures that Personal Data is protected throughout its entire existence and processed only for legitimate purposes and documented purposes. The Company remains responsible for

ensuring that Personal Data is managed in accordance with this lifecycle model.

Lifecycle Stage	Requirements
Collection	Personal Data shall be collected only where necessary for clearly defined and lawful purposes, including player account registration and verification, provision of gaming services, fraud prevention, and regulatory compliance (including AML/ CFT and responsible gaming obligations). At the point of collecting, the Company shall inform individuals of the purpose and legal basis for processing, collect only the minimum data required for stated purpose, and avoid the collection of special categories of data unless a lawful exception applies.
Processing	Personal Data shall be stored in secure systems protected by appropriate technical and organizational measures, including access controls, encryption where applicable, and logging. Data shall be retained only for as long as necessary to fulfill business and legal obligations in accordance with defined retention periods and protected against unauthorized access, loss, or alteration.
Access	Access to Personal Data is restricted to authorized personnel whose job responsibilities require such access and is governed by the principles of least privilege and need-to-know. Access rights shall be reviewed periodically, privileged access shall be monitored and logged, and confidentiality obligations apply to all staff and contractors with access to Personal Data.
Transfer and Disclosure	Personal Data may be transferred internally or disclosed to external parties only where a lawful basis exists and appropriate contractual and security safeguards are in place, including Data Processing Agreements where applicable. Transfers outside Curaçao or the European Union shall be subject to additional safeguards in accordance with GDPR and NODP requirements. Personal Data shall not be shared for incompatible or unauthorized purposes.
Archival	Where Personal Data must be retained beyond its primary operational use for legal, regulatory, or audit purposes, it shall be archived securely. Archived data shall be segregated from active systems, subject to restricted access controls, protected against unauthorized

	modification or deletion, and retained only for as long as legally required.
Destruction and Deletion	When Persona; Data is no longer required for its original purpose and applicable retention periods have expired, it shall be securely destroyed or anonymized. Destruction methods should prevent reconstruction or recovery and apply to both electronic and physical records. Data destruction shall also occur upon termination of a contractual relationship with a processor, subject to legal and regulatory retention obligations.

5.4 Consent

Consent must be freely given, specifically informed and unambiguous. It requires clear affirmative action, not silence or pre-ticked boxes. The Company must record when and how consent was given.

Players can withdraw consent at any time, and the Company must stop processing for that purpose once consent is withdrawn.

5.5 Rights of the Data Subject

Players (data subjects) have several rights regarding their personal data:

1. **Right to be informed:** Players must be told how their data is collected, used, shared, and retained in a clear and accessible way.
2. **Right of access:** Players can request a copy of their personal data. Responses must be provided free of charge (except in abusive cases) and within one month.
3. **Right to rectification:** Incorrect or incomplete data must be corrected promptly.
4. **Right to erasure (“right to be forgotten”):** In certain circumstances, players can request deletion of their data.
5. **Right to restrict processing:** Players can request that their data be stored but not actively processed.
6. **Right to data portability:** Players can request their data in a commonly used, machine-readable format.
7. **Right to object:** Players may object to processing based on legitimate interests or direct marketing.
8. **Rights related to automated decision making:** Players have the right not to subject to decisions made solely by automated processes without human oversight, except where allowed by law or explicit consent.

5.6 Communication Channels for Data Subjects

The Company shall ensure that clear and accessible communication channels are available for players and other data subjects to contact the DPO regarding data protection matters.

These channels shall include:

- Contact details published in the Company's Privacy Notice.
- A dedicated email address or other appropriate means of communication.
- Procedures for handling and responding to data subject requests and complaints in a timely manner.

The DPO shall oversee the handling of data subject requests, including requests for access rectification, erasure, restriction, or objection to processing.

6.Accountability and Governance

The Company ensures compliance with data protection and information security obligations by:

- Maintaining internal records of all personal data processing activities (Processing Register)
- Conducting Data Protection Impact Assessments (DPIAs) when new technologies or high-risk processing activities are introduced.
- Providing all employees with initial and annual refresher training on data protection, confidentiality and breach reporting.
- Requiring employees to acknowledge and sign confidentiality and data protection undertakings.

The Company shall ensure that all employees are involved in processing personal data:

- Receive initial and annual refresher training in data protection, breach reporting and confidentiality.
- Understand their responsibilities under GDPR, NODP and the National Ordinance on Games of Chance; and
- Acknowledge and sign confidentiality and data protection undertakings as part of their employment.

6.1 Data Protection Officer (DPO)

The Company appoints a Data Protection Officer (DPO) where required under the GDPR or were deemed appropriate based on the nature and scale of Personal Data processing activities.

The Data Protection Officer is responsible for:

- Informing and advising the Company and its employees of their obligations under GDPR, NODP and this Policy.
- Monitoring compliance with data protection laws, internal policies and related procedures.
- Providing guidance on data protection impact assessments (DPIAs) were required.
- Advising on data protection risks associated with new projects, systems or processing activities.
- Cooperating with and acting as primary contact point for the competent supervisory authorities.
- Supporting investigations and audits relating to Personal Data processing.
- Promoting awareness and training of staff involved in Personal Data processing.

The Data Protection Officer shall report directly to senior management and were applicable to the Board of Directors or equivalent governing body. The DPO shall have the authority to escalate material data protection risks, breaches or compliance concerns directly to senior management without undue delay.

6.2 Records Keeping and Retention

The Company maintains complete records of:

- Player registration and KYC documentation.
- All gaming and financial transactions.
- Communications related to gaming activities and complaints.

These records are retained for at least five (5) years after the last transaction, in line with Curaçao AML/ CFT and gaming laws. After this period, data will be securely deleted or anonymized unless required for ongoing investigations or legal obligations.

Unless a longer period is required for ongoing investigations, regulatory inquiries, litigation, fraud prevention, or to meet statutory obligations, the following minimum retention periods apply:

Category	Details	Retention Period
Player Identification and KYC Documentation	KYC files, identity verification data, due diligence records and supporting documents related to player onboarding and monitoring.	At least five (5) years following the player's last transaction or the closure of the player's account.
Gaming and Transaction Records	All records relating to wagers, bets, game results, account balances, deposits, withdrawals, session logs, gameplay history and system-generated gaming data.	Five (5) years.
Financial, accounting and Tax Records	Financial statements, accounting ledgers, transaction records, payment processor statements and statutory tax-related documents.	Five (5) years or any longer period mandated by applicable financial or tax laws.
Player Communications and Complaints Records	Records of customer support interactions, internal complaint logs, dispute correspondence and related supporting documentation.	Five (5) years.
Security, System and Access Logs	System access logs, authentication logs, incident logs and security monitoring records.	At least one (1) year, unless otherwise required for operational continuity, forensics or regulatory investigation. Where logs from part of gaming system audits, they shall be retained for five (5) years.
Responsible Gaming and Player Protection Records	Records relating to self-exclusion, Responsible Gaming interventions, affordability assessments	Five (5) years

	and monitoring of player behavior.	
Vendor and Third-Party Processing Records	Contracts, due diligence reports and data processing agreements	For the duration of the relationship and for five (5) years thereafter.

6.3 Data Protection Impact Assessments

Data Protection Impact Assessments are tools which the Company uses to assist when identifying the most effective way to comply with the GDPR and to meet individuals' expectations of privacy. The Company requires a data protection impact assessment to be undertaken when:

- Using new technologies; and
- The Processing of Personal Data is likely to result in a high risk to the rights and freedoms of individuals.
- Processing that is likely to result in high risk includes, but is not limited to:
- Systematic and extensive Processing activities, including profiling and where decisions that have legal effects – or similarly negative effects – on individuals.
- Large scale processing of special categories of Personal Data in relation to criminal convictions or offences.

6.4 Transfer of Data

Personal data may only be transferred outside the European Union if adequate protections are in place:

- Transfers to countries approved by the European Commission as “adequate” are permitted.
- Transfers to other countries require additional safeguards such as standard contractual clauses, binding corporate rules or explicit player consent.

The Company may also transfer Personal Data where the organization receiving the Personal Data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

6.5 Data Storage and Server Location

Sunstar Impact N.V. shall ensure that all critical digital records, including players' personal data, gaming transaction data and financial records are stored on a Tier-IV certified data center located in Curaçao, in compliance with the Curaçao NOGC and the Curaçao Gaming Authority License Conditions.

To reduce the risk of data loss and ensure continuity of operations:

- Backups shall be stored in a secure and segregated environment separate from production systems.
- At least one copy of critical backups shall be maintained in an offsite or geographically separate location.
- Redundancy mechanisms shall be implemented to protect against single points of failure.

Where cloud-based backup services are used, they must meet the Company's security and regulatory requirements and be subject to appropriate contractual safeguards.

These records shall always be accessible to the Curaçao Gaming Authority upon request for audit, inspection or investigation purposes.

In addition, the Company maintains technical and organizational measures to protect stored data against unauthorized access, accidental loss or damage.

6.6 Backups and Recovery Controls

Backups shall be performed in accordance with the criticality of the data and systems involved.

- Critical systems and data (including player accounts, transaction records, gaming data and compliance records) shall be backed up at least daily.
- System configurations and application code repositories shall be backed up following material changes and at least weekly.
- Backup schedules shall be documented and reviewed periodically.

All backups containing personal data, gaming records or sensitive system information shall be protected through appropriate encryption or equivalent safeguards.

- Backup data shall be encrypted both in transit and at rest where technically feasible.
- Access to backup repositories shall be restricted to authorized personnel only and logged.

6.7 Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

The Company shall define and maintain appropriate recovery objectives based on system criticality:

- **Recovery Time Objective (RTO):** The maximum acceptable time to restore critical systems following a disruption shall be defined and aligned with business and regulatory needs. For core gaming and player account systems, the target RTO shall be within a commercially reasonable timeframe (e.g., with 24 hours or less, subject to system classification).
- **Recovery Point Objective (RPO):** The maximum acceptable data loss in the event of an incident shall be defined and minimized for critical systems. For player and transaction data, the target RPO shall not exceed one business day and shall reflect the frequency of backups performed.

RTO and RPO targets shall be reviewed periodically and tested as part of the disaster recovery and restoration exercises.

6.8 Encryption and Data Security

All player personal data, financial information and gaming records shall be encrypted. Encryption keys shall be managed securely with restricted access and regular rotation. Applications and systems are subject to secure coding standards, vulnerability scanning and periodic penetration testing.

7. Third Party and Vendor Risk Management

All third-party service providers handling company data must undergo security due diligence before onboarding.

Data Processing Agreements must explicitly require compliance with GDPR, NODP and Curaçao Gaming Authority security standards.

Critical vendors (e.g., payment processors, hosting providers) must provide annual certifications (e.g., ISO 27001, PCI DSS). Vendors' performance and compliance shall be reviewed annually.

8. Data Breach Notification

All data breaches must be reported internally to the Board and the Compliance Officer as soon as possible.

Breaches affecting personal data will be reported to the Curaçao Gaming Authority within 24 hours, with a full incident report including: nature of the breach, data affected, immediate actions taken and planned corrective measures. Where required by GDPR, affected players will also be notified.

All breaches are logged and followed up with corrective actions.

8.1 Incident Response Plan

The Company shall maintain a documented Incident Response Plan covering:

- **Detection:** All staff must immediately report suspected security incidents.
- **Assessment:** The Incident Response Team (IRT) shall classify incidents by severity.
- **Containment and Eradication:** Immediate measures must be taken to prevent further damage.
- **Notification:** Regulatory reporting obligations (e.g., CGA, FIU, affected players) must be fulfilled within prescribed timelines.
- **Recovery:** Systems must be restored from secure backups.
- **Post-Incident Review:** Root cause analysis and corrective actions shall be documented.

Regular incident response drills shall be conducted to test readiness.

9. Policy Review

This Policy is reviewed annually or sooner if required by significant changes in laws or regulations, major security incidents or updates to technology or business operations.