

1. Definitions

- **Account Holder** – A person who holds a Player Account on the Website.
- **Back Up** – A regularly created duplicate copy of business or operational data.
- **Business Data** – Non-personal information processed by the Company in the course of its business operations.
- **Classified Information** – Information as defined under Article 4.3 of this Policy.
- **The Company** – Gleneagles B.V., a limited liability company duly incorporated under the laws of Curaçao and registered with the Chamber of Commerce and Industry under number 158256.
- **Computer System** – A combination of hardware and software components working together to perform defined tasks by receiving input, processing data, storing information, and generating output. The system is essential for the Company to provide its services effectively.
- **Confidential Business Information** – Business-related data which the Company considers undesirable to be disclosed to external parties.
- **Data Subject** – An identifiable natural person whose personal data is processed by the Company.
- **Employee** – Any person employed by or working for the Company.
- **Player** – An individual registered with the Company for the purpose of using the Services provided through the Website, for whom a Player Account with a unique identifier has been created.
- **Player Account** – An account established by the Company for a Player upon registration on the Website, required to participate in real-money gaming. Only one Player Account is permitted per person, household, IP address, and shared environment.
- **Personal Data** – Any information relating to an identifiable natural person who can be identified directly or indirectly by reference to details such as a name, identification number, location data, username, or factors specific to their physical, mental, economic, cultural, or social identity.
- **Sensitive Information** – Data that is considered confidential or sensitive and must be safeguarded against unauthorized access to protect the privacy and security of individuals or organizations.
- **Service** – The gaming and betting products offered online by the Company to Account Holders through the Website.
- **Website** – The online gaming platform operated and maintained by the Company.

2. Information Security Policy

2.1 Policy

To ensure the secure and efficient functioning of the Company, it is essential to maintain the availability, integrity, and confidentiality of all business information. Certain categories of information, identified as Sensitive Information, require additional protection due to legal, contractual, or shareholder obligations. This Policy establishes the principles and guidelines for safeguarding such

information and will be reviewed periodically to ensure compliance with applicable regulations and maintain trust in the Company's operations.

2.2 Objective

The purpose of this Policy is to protect the integrity, confidentiality, and availability of all information managed by the Company and to demonstrate management's ongoing commitment to maintaining high standards of information security.

2.3 Responsibilities

All Employees must conduct themselves ethically and responsibly, ensuring that:

- Information obtained improperly is never used;
- Any discovered system vulnerability is reported immediately and not exploited;
- Each Employee performs their duties diligently and is accountable for any misuse of Company information systems;
- Any known security breaches or weaknesses are reported to the appropriate security personnel or department.

3. Data

Sensitive information can exist in multiple forms. Under the applicable data protection legislation, including Curaçao Data Privacy and the GDPR, a distinction is made between Personal Data and Confidential Business Data.

3.1 Personal Data

Personal information collected or processed when using the Services includes, but is not limited to:

1. Information provided during account registration or other submissions through the Website, such as full name, date of birth, contact number, and email address;
2. Verification documents and data required to confirm a Player's identity, process deposits or withdrawals, and perform anti-fraud checks, including identification copies, payment confirmations, or bank statements;
3. Account-related data such as login credentials, IP address, device type, browser data, logs, and activity records;
4. Any communication exchanged with the Website, including messages, emails, and other correspondence;
5. Records of transactions, survey responses, or related participation data;
6. Feedback or survey responses collected through customer satisfaction assessments.

3.2 Confidential Business Data

The Company may process non-personal information for internal operational purposes. Such Business Data is considered confidential when it is not intended for disclosure outside the Company.

3.3 Classified Data

The Company may handle information that requires enhanced protection measures. Classified Information includes assets where disclosure could result in legal consequences or financial penalties. Payroll data, personnel files, sensitive player details, and financial information fall within this classification.

4. Security of Information

4.1 Security During Usage of Company's Systems

All Company hardware and software, whether fixed or mobile, must be used and maintained in accordance with manufacturer guidelines. The Company's IT staff are responsible for ensuring that security updates and software patches are installed promptly on all devices used to store or access sensitive data.

4.1.1 Password

All devices and storage media containing Sensitive Information must be secured with an access protection method such as a password, two-factor authentication, or encryption.

1. Passwords must meet the strength and renewal standards recommended by international cybersecurity guidelines.
2. If the Company requires the use of a password manager, Employees must utilize it for generating and maintaining secure passwords.

4.1.2 Security and Proprietary Information

Passwords and accounts must remain confidential. Employees must not share credentials or accounts. Authorized users are responsible for maintaining the security of their passwords. Caution must be exercised when opening email attachments from unknown sources, which may contain viruses or malicious code.

4.1.3 Acceptable Use Policy

Employees must exercise good judgment when using the internet or IT resources. Usage should be primarily for professional purposes. Information or content that could identify or negatively affect customers, colleagues, or the Company must not be posted on social networks or shared through any device, whether during or outside working hours.

4.1.4 Secrecy

Employees and third-party suppliers are bound by strict confidentiality regarding any sensitive information encountered in the course of their duties. This obligation continues even after the termination of employment or contractual relationships. Communication with media or government bodies is restricted to authorized Company representatives.

4.1.5 Remote Connections

Employees or third parties with remote access rights must ensure their login credentials remain secure and must not share them under any circumstances.

4.1.6 Remove Sensitive Information

Storing sensitive data involves inherent risks of loss, theft, or unauthorized access. Regular evaluations must be conducted to determine whether such data still needs to be retained. Information that is no longer required for business or legal purposes must be securely deleted or destroyed. Sensitive data may not be removed from Company premises unless necessary for official duties.

4.1.7 Retention Terms and Personal Data

The Company maintains relevant documentation in a secure database for a minimum of five years following the end of a business relationship. Records must allow investigating authorities to trace an adequate audit trail of transactions, including their type, currency, and amounts.

4.2 Secure Disposal and Destruction of Business Information and Devices After Use

Documents or devices containing business information must never be disposed of through public waste systems.

4.2.1 Devices

When an Employee's device (phone, computer, tablet, etc.) is no longer in use, it must be returned to the designated manager for secure handling.

4.2.2 Physical Documents

Non-electronic business information such as paper records must be securely destroyed, for example, by shredding or through a certified disposal service provider.

4.2.3 Destruction of Business Information

Information that is no longer required for Company operations must be formally marked for removal and securely destroyed. Periodic checks must ensure that:

1. Unused or decommissioned devices are securely wiped or destroyed;
2. Obsolete Company information, including backups, is permanently deleted or destroyed.

5. Security of the Computer System

5.1 Safeguarding of Applications

All systems connected to the internet, along with their operating software, must always be updated with the latest security patches.

5.2 Safeguarding of Networks

Wireless networks must be password protected and accessible only to authorized Company staff. Transfers of classified or confidential data must be strictly managed. Such information must never be copied, downloaded, printed, or left unattended.

5.3 Logs and Other Systems Security Tools

Systems handling sensitive or critical data must record all relevant security events, such as login attempts, password resets, privilege changes, and modifications to production or system software. If a security incident or network abuse is suspected, logs and related data must be securely stored offline until investigations are completed.

5.4 Measures Against Data Loss

The Company maintains secure backup facilities for storing regular copies of business information. Employees must minimize data storage on local devices and instead use network storage to prevent accidental or intentional data loss.

6. External Parties

6.1 Hiring of External Parties

Before engaging with external parties, the Company must confirm a legitimate business need for access to Sensitive Information. The Company must verify that the external party complies with this Policy and formalize those conditions in a written agreement signed prior to granting access. Any access provided to third parties, auditors, or consultants must be approved by Management and revoked once their assignment ends.

7. Physical Security of Buildings and the Surrounding Area

7.1 Clean Desk Policy

Employees must ensure that documents, devices, and data carriers are not left unattended. After working hours, all desks and work areas must be cleared and sensitive materials securely stored.

7.2 Employees Access

Employees are permitted to access only those areas of the Company's premises for which they have been authorized via key or access card. Any misuse of access rights may lead to disciplinary action.

7.3 Visitors

Visitors are not permitted in areas where sensitive data is accessible. They must be accompanied by a Company representative throughout their visit, who is responsible for escorting them to and from the premises.

8. Training

All Employees must attend training sessions or webinars on privacy and the protection of personal data. New Employees are also required to complete this training upon joining, and compliance checklists will be maintained to ensure all staff remain up to date.