

PRIVACY POLICY

1. STATEMENT

BETSEN is committed to protecting the confidentiality, integrity, and availability of its information assets. This policy defines BETSEN's approach to safeguarding its gambling and business systems from unauthorized access, data breaches, and other security threats.

2. SCOPE AND PURPOSE

This policy applies to all employees, contractors, and third parties who access company information systems, as well as all data processed, stored, or transmitted within BETSEN's IT environment.

Purpose:

- Protect customer and company data against loss, theft, and unauthorized disclosure.
- Ensure compliance with GDPR, ISO/IEC 27001:2022, and CGA requirements.
- Establish a secure IT infrastructure and working environment for staff and authorized users.

3. PRINCIPLES

- Protect information assets from unauthorized access and misuse.
- Classify and handle data according to confidentiality and sensitivity.
- Ensure accountability and security awareness among all users.
- Apply the principle of least privilege to data and system access.
- Commit to ongoing risk assessment and continuous improvement.

4. LEGAL AND REGULATORY OBLIGATIONS

- General Data Protection Regulation (GDPR)
- ISO/IEC 27001:2022 and ISO/IEC 27002:2022 standards
- Curaçao Gaming Authority (CGA) information security requirements

5. INFORMATION SECURITY FRAMEWORK

5.1 Security Risk Assessment

- Annual evaluations to identify risks and implement mitigation measures.
- Regular reviews to align with evolving threats and technologies.

5.2 Access Control

- Role-based access controls (RBAC) and Two-Factor Authentication (2FA) for all critical systems.
- Restrict access to sensitive data to authorized users only.

5.3 Information Classification

- Confidential: High sensitivity; access limited to authorized personnel.
- Restricted: Controlled distribution to specific groups.
- Internal Use: Accessible within BETSEN as needed.
- Public: Openly shareable subject to legal and regulatory compliance.

5.4 Physical and Network Security

- Firewalls, VPNs, encryption, and endpoint protection (antivirus, antimalware).
- Regular patch management and system updates.

5.5 Remote Access and BYOD

- Remote access permitted via approved VPN with 2FA.
- Personal device use requires CISO approval and adherence to security protocols.
- Prohibit use of public or unsecured devices for accessing company systems.

5.6 Data Retention and Backup

- Retain critical data only as long as required by law.
- Backups encrypted and stored securely on/off-site.
- Disaster recovery procedures regularly tested.

6. INCIDENT HANDLING

- All security incidents must be reported immediately to the CISO.
- Incident response includes detection, analysis, containment, and remediation.

7. STAFF TRAINING AND AWARENESS

- Annual mandatory training on information security practices.
- Regular phishing simulations and awareness campaigns.

8. POLICY REVIEW AND DEVELOPMENT

- Policy reviewed annually and updated for legal, regulatory, or technical changes.

9. POLICY ENFORCEMENT

- Breaches may result in disciplinary action, termination, and possible legal proceedings.

By: Director of Great BDG Randon Entertainment N.V.

Name: (SMES) Solutions for Management and Employment Support N.V.

Date: 22/07/2025

Signature:

