

Bet Play B.V.

# IT Security Policy

## CONFIDENTIALITY STATEMENT

*This is a confidential document for Bet Play B.V. It contains confidential and/or proprietary information that may not be disclosed or discussed with anyone outside the organization without written approval of Bet Play B.V.*

## Disclaimer

NO PART OF THIS DOCUMENT MAY BE REPRODUCED, TRANSMITTED OR IN ANY OTHER WAY DISTRIBUTED WITHOUT THE PRIOR WRITTEN PERMISSION OF BET PLAY B.V. ALL TECHNOLOGIES, DESIGNS, IMPLEMENTATIONS, TRADE SECRETS AND BUSINESS MODELS DESCRIBED HEREIN IS THE INTELLECTUAL PROPERTY OF BET PLAY B.V AND/OR IT'S PARTNERS AND IS PROVIDED FOR INFORMATION PURPOSES ONLY.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY CONCERNING ITS ACCURACY OR QUALITY. IN NO EVENT WILL BET PLAY B.V BE LIABLE FOR DIRECT OR INDIRECT DAMAGES RESULTING FROM INCIDENTAL DEFECTS OR INACCURACIES IN THIS DOCUMENT.

BET PLAY B.V RESERVE THE RIGHT TO REVIEW AND MODIFY DIGITAL COPIES OF THIS DOCUMENT AT ANY TIME WITHOUT PRIOR NOTICE.

THE BET PLAY B.V NAMES, THE BET PLAY B.V LOGOTYPES, GAME BRANDS, SERVICES AND PRODUCT NAMES ARE REGISTERED TRADEMARKS AND/OR SERVICE MARKS OF BET PLAY B.V

Property of BetPlay B.V

## Document Version Control

| Version | Date       | Author        | Purpose                        |
|---------|------------|---------------|--------------------------------|
| 1.0     | 10-10-2025 | Bet Play B.V. | Creation of IT Security Policy |

Property of BetPlay B.V.

## Table of contents

|                                                        |    |
|--------------------------------------------------------|----|
| 1. Purpose and scope.....                              | 5  |
| 2. Security principles and objectives.....             | 5  |
| 3. Access control .....                                | 5  |
| 3.1 User access management .....                       | 5  |
| 3.2 Privileged access control .....                    | 5  |
| 4. Data protection and privacy .....                   | 5  |
| 4.1 Data classification and handling .....             | 5  |
| 4.2 Personal data protection .....                     | 6  |
| 5. Network security .....                              | 6  |
| 5.1 Firewalls and intrusion detection.....             | 6  |
| 6. System security .....                               | 6  |
| 6.1 Patch management .....                             | 6  |
| 6.2 Antivirus and Malware protection .....             | 6  |
| 7. Application security .....                          | 6  |
| 7.1 Secure Software Development Lifecycle (SDLC) ..... | 6  |
| 7.2 Third-party software and integrations.....         | 7  |
| 8. Incident response and management .....              | 7  |
| 8.1 Incident Response Team (IRT) .....                 | 7  |
| 8.2 Incident reporting and documentation .....         | 7  |
| 8.3 Communication with CGA .....                       | 7  |
| 9. Security awareness and training .....               | 7  |
| 10. Compliance and audit.....                          | 7  |
| 10.1 Internal audits.....                              | 7  |
| 10.2 Penalties for non-compliance.....                 | 8  |
| 11. Policy review and updates.....                     | 8  |
| 12. Business Continuity Plan .....                     | 8  |
| 13. Signatory page .....                               | 10 |

## 1. Purpose and scope

The purpose of this IT Security Policy is to protect Bet Play B. V's or "The Company" information systems, ensure the confidentiality and security of customer data, and maintain compliance with the requirements set forth by the Curacao Gaming Authority. This policy applies to all employees, contractors, and third-party suppliers who access or manage the Company's information technology resources.

## 2. Security principles and objectives

Bet Play B.V is committed to:

- **Confidentiality:** Protecting customer data and proprietary information from unauthorized access.
- **Integrity:** Ensuring data accuracy and consistency across all platforms and systems.
- **Availability:** Providing reliable access to IT systems and data for authorized users.
- **Compliance:** Adhering to Curacao Gaming Authority regulations, industry best practices, and international standards (e.g., GDPR, ISO 27001).

## 3. Access control

### 3.1 User access management

- **Role-Based Access Control (RBAC):** Access to systems and data is based on employees' job roles and responsibilities. Privileged access is restricted to necessary personnel only.
- **Authentication:** Multi-factor authentication (MFA) is required for accessing critical systems, with strong password policies enforced across all accounts.
- **User access reviews:** Access rights are reviewed annually to ensure permissions are current and align with employees' roles.

### 3.2 Privileged access control

- **Administrator controls:** System administrators and privileged users have additional security checks, including activity monitoring and strict authentication measures.
- **Least privilege principle:** Access is limited to the minimum permissions necessary to perform job functions, reducing the risk of unauthorized data exposure or manipulation.

## 4. Data protection and privacy

### 4.1 Data classification and handling

- **Data classification:** All data is classified according to sensitivity (e.g., public, internal, confidential, and restricted). This classification dictates the data's storage, handling, and access requirements.
- **Encryption:** All sensitive and restricted data, including customer data and financial records, is encrypted at rest and in transit using strong encryption protocols.
- **Data masking:** Sensitive customer information is masked when displayed in internal systems to prevent unauthorized access.

## 4.2 Personal data protection

- **GDPR compliance:** Personal data is handled in accordance with GDPR standards, with customer consent obtained before data collection and strict limitations on data retention.
- **Data minimization:** Only necessary personal data is collected and only if it is needed, and data that is no longer needed is securely deleted or anonymized in line with data retention policies.
- **Breach notification:** In the event of a data breach involving personal information, customers and regulatory bodies are notified as per GDPR and CGA requirements.

## 5. Network security

### 5.1 Firewalls and intrusion detection

- **Firewall protection:** Network firewalls are configured to restrict access to company resources based on IP addresses and other parameters. Regular firewall rule reviews ensure effective protection.
- **Intrusion Detection and Prevention Systems (IDPS):** IDPS continuously monitors network traffic to detect and block unauthorized or suspicious activity.

## 6. System security

### 6.1 Patch management

- **Regular updates:** All software, hardware, and firmware are updated regularly to protect against known vulnerabilities. Critical patches are applied within 48 hours of release.
- **Patch testing:** New patches are tested in a controlled environment before being deployed to production systems to prevent compatibility issues.

### 6.2 Antivirus and Malware protection

- **Antivirus software:** Company-approved antivirus software is installed on all endpoint devices and servers, with real-time scanning and automatic updates enabled.
- **Malware scanning:** Regular malware scans are conducted on all systems, with any detected threats immediately isolated and removed.

## 7. Application security

### 7.1 Secure Software Development Lifecycle (SDLC)

- **Secure coding standards:** Developers follow secure coding practices, such as input validation, authentication, and session management, to minimize vulnerabilities.
- **Code reviews:** All code undergoes peer reviews to identify potential security issues before deployment.
- **Application testing:** Security testing, including penetration tests and vulnerability assessments, is conducted on new applications before they go live.

## 7.2 Third-party software and integrations

- **Supplier Security Assessment:** All third-party software and services are evaluated for security risks before integration, with priority given to CGA-compliant suppliers.
- **API security:** Secure API practices, such as encryption and access controls, are implemented to protect data shared with third-party systems.

## 8. Incident response and management

### 8.1 Incident Response Team (IRT)

- **Team composition:** An Incident Response Team, comprising IT, Compliance, and Legal representatives, is responsible for managing security incidents.
- **Incident triage:** All reported incidents are triaged by the IRT to determine their severity and impact on company operations and customer data.

### 8.2 Incident reporting and documentation

- **Internal reporting:** Employees are required to report any suspected security incidents immediately to the IT security team.
- **Documentation:** All incidents are documented, including the nature, resolution steps, and lessons learned, to improve future response efforts.

### 8.3 Communication with CGA

- **Regulatory notification:** Security incidents involving data breaches or system compromise are reported to the CGA as per regulatory guidelines.
- **Customer notification:** Affected customers are notified in compliance with CGA and data protection requirements, with transparent communication regarding incident details and mitigation steps.

## 9. Security awareness and training

- **Mandatory training:** All employees receive annual security training covering data protection, phishing awareness, password security, and incident reporting protocols.
- **Simulated phishing tests:** Regular phishing simulations help employees recognize and report suspicious emails, reducing the risk of social engineering attacks.
- **Compliance and policy updates:** Employees are informed of updates to security policies and regulatory requirements, ensuring ongoing awareness of best practices.

## 10. Compliance and audit

### 10.1 Internal audits

- **Regular audits:** Annual IT security audits are conducted to assess policy compliance, identify vulnerabilities, and verify controls are effectively implemented.
- **CGA compliance review:** The audit includes a review of CGA-specific requirements to ensure continued licensing compliance and adherence to gaming security standards.

## 10.2 Penalties for non-compliance

- **Disciplinary actions:** Employees found in violation of IT security policies may face disciplinary action, including warnings, suspension, or termination, depending on the severity of the violation.
- **Policy violations reporting:** All non-compliance incidents are documented, and, when necessary, reported to the CGA as per regulatory guidelines.

## 11. Policy review and updates

- **Policy revisions:** This IT Security Policy is reviewed annually by the IT Security and Compliance teams to ensure alignment with the latest CGA guidelines, industry standards, and emerging security threats.
- **Employee notification:** Major policy updates are communicated to all employees, with training provided on new procedures and security controls.
- **Feedback and continuous improvement:** Employees can provide feedback on the policy, which is considered in the review process to foster a practical and responsive security culture.

## 12. Business Continuity Plan

### 12.1 Objectives of Business Continuity Plan

- Maintain uninterrupted service to clients and partners.
- Minimize the impact of operational, technical, or security incidents.
- Protect and recover critical data, assets, and systems.
- Ensure compliance with regulatory, contractual, and data protection obligations (e.g., GDPR, ISO 27001, CGA requirements).

### 12.2 Incident Classification, Response and Continuity Procedures

#### 12.2.1 Classification of Reported Faults

##### Priority 1: Critical Gameplay Impact

The Reported Fault results in a total or near-total failure of the Services, such as all or most games being unavailable, API failure, or severe errors affecting the core functionality of games. These issues have an immediate and significant impact on player experience and the Licensee's revenue, and must be treated as urgent.

Examples:

- Aggregation API completely inaccessible
- All or major group of games unavailable
- Gameplay errors resulting in incorrect player balances
- Jackpot system failures (value not updating, won jackpot not recorded)

- Widespread crash or error across multiple games/studios
- Game returns invalid win/loss value

### **Priority 2: Significant Player or Revenue Impact**

The Reported Fault affects one or more key functionalities or games, significantly degrading player experience or affecting a substantial portion of the player base. These issues are serious but do not constitute a complete outage.

Examples:

- Game or group of games unavailable for large group of players
- Bonus or feature not triggering in one or more popular games
- New game released but unavailable to players
- Player session timeout
- Game causing problems on the Licensee's side (losing money)
- A VIP player is having problems with the games
- One of the games is not Available for all players
- A new issue blocking the gameplay was reported in the game, which blocks gameplay for multiple players
- A player won a high stakes win and the Company should validate if the win is valid

### **Priority 3: Low or Individual Impact**

The Reported Fault impacts individual players, games, or non-core functionalities. These issues are minor, cosmetic, or administrative in nature and do not significantly affect player experience or system performance.

Examples:

- Player reports missing bonus spins or rewards
- A single game fails to launch for an individual player
- Game unavailable in one geo/market
- Game thumbnail, name, or category mismatch
- Whitelist/blacklist request for a specific game or studio
- Operational problems of individual players
- A player is blocked and cannot play a game.
- A player cannot open a game.

## **12.2.2 Incidents SLAs**

- **Priority 1 (Critical Gameplay Impact):** 2-hour resolution, hourly updates.
- **Priority 2 (Significant Impact):** 24-hour resolution, 4-hour updates.
- **Priority 3 (Low Impact):** 48-hour resolution, daily updates.

If resolution targets are not met, escalation to the Account Manager or Incident Manager occurs. Repeated SLA breaches trigger an Improvement Plan.

### 12.3 Communication Plan

During disruptions, the Customer Support team coordinates communications with Licensees, with updates per SLA.

Post-incident reports are provided within 48 hours of resolution.

### 12.4 Improvement Plan

If the Company fails to meet the agreed service levels for two (2) consecutive months, it shall promptly develop and implement an Improvement Plan to restore performance to the agreed standards.

The Improvement Plan shall:

- Identify the root causes of the performance deficiencies
- Define corrective actions and timelines to prevent recurrence
- Assign responsibilities and establish clear performance metrics and
- Include a report detailing findings and proposed improvements, to be submitted to the Licensee for review and approval prior to implementation.

If the Company fails to achieve the required service levels for three (3) consecutive months, despite the implementation of the Improvement Plan, the Licensee reserves the right to terminate the Agreement immediately by providing written notice to the Company.

## 13. Signatory page



Mark Cauchi  
Compliance Officer