

EDJOWA-GAMING N.V.

INFORMATION TECHNOLOGY / INFORMATION SECURITY POLICY

Document / Revision History

EDJOWA-GAMING N.V.	INFORMATION TECHNOLOGY / INFORMATION SECURITY POLICY
---------------------------	---

Change control

Revision #	Date	Written by/ Responsible Officer	Approved by	Description of Changes
V1.0	29.10.2025.	Director Dmitrijs VOLKS	Director Dmitrijs VOLKS	Initial document created.

CONTENTS

1. PURPOSE.....	4
2. OBJECTIVES.....	4
3. RESPONSIBILITIES.....	4
3.1. Director – Chief Technology Officer (“CTO”).....	4
3.2. Team Effort and Employee Responsibilities.....	4
4. IS POLICY	4
4.1. Safeguarding of Company Data	4
4.2. Data Classification.....	5
4.3. Safeguarding Applications and IT Assets	5
4.4. Data and Password Security.....	6
4.5. Network and System Security.....	7
4.6. Physical and Equipment Security.....	7
4.7. Remote Work and Mobile Device Policy.....	8
4.8. Media Handling and Disposal	8
4.9. Incident Management and Enforcement.....	9
5. BACKUP PROCEDURE	10
5.1. Purpose.....	10
5.2. Responsibilities.....	10
5.3. Backup Management.....	10
5.4. Backup Schedule.....	11
5.5. Backup Restoration and Testing.....	11
5.6. Security and Storage	11
6. BUSINESS CONTINUITY (“BC”) & DISASTER RECOVERY (“DR”)	11
6.1. Purpose.....	11
6.2. Objectives	12
6.3. Responsibilities.....	12
6.4. Scenarios and Mitigation Measures	12
6.5. Business Impact Analysis (“BIA”).....	13
6.6. Escalation and Regulatory Reporting	13
7. SYSTEM INFRASTRUCTURE & INFORMATION ASSETS.....	13
7.1. Purpose.....	13
7.2. Infrastructure Overview.....	14
7.3. Secure System Architecture.....	14
7.4. Hosting and Data Centres.....	14
7.5. Application and Platform Architecture.....	14
7.6. Information Assets.....	14
7.7. Redundancy and High Availability	15
7.8. Oversight and Compliance.....	15
7.9. Diagrammatic Representation.....	15
8. THE NETWORK INFRASTRUCTURE	15
8.1. Overview	15
8.2. Operator Access Security	15
8.3. Platform and Infrastructure Security.....	15
8.4. Monitoring and Performance Oversight.....	16
9. OVERSIGHT AND REVIEW	16
10. CONTACT INFORMATION.....	16

1. PURPOSE

This Information Technology (“IT”) and Information Security (“IS”) Policy (“**Policy**”) sets forth the principles, standards, and procedural framework governing the management, protection, and utilization of information technology resources and information assets within EDJOWA-GAMING N.V. (“**Company**”).

The purpose of this Policy is to articulate management’s guiding principles and to establish the necessary procedures that ensure the confidentiality, integrity, and availability of all Company information and business assets. This Policy also aims to promote responsible use of the Company’s IT and IS infrastructure, consistent with applicable laws, regulations, and internal governance standards.

2. OBJECTIVES

This Policy has been developed with the following objectives:

- To establish and maintain safeguards designed to protect information resources from theft, unauthorized access, abuse, misuse, loss, or any form of damage, and to assign clear responsibility and accountability for IS within the Company.
- To foster and maintain an appropriate level of awareness, knowledge, and technical proficiency among staff and management to effectively minimize the likelihood and impact of IS incidents.

This Policy should be read in conjunction with all other Company policies, procedures, and operational guidelines, which collectively form the framework for corporate governance, risk management, and compliance.

3. RESPONSIBILITIES

3.1. Director – Chief Technology Officer (“CTO”)

The Director, currently fulfilling the role of CTO, shall have overall responsibility for the development, implementation, and maintenance of this Policy. The Director–CTO is accountable for:

- Protecting and safeguarding all data and information assets belonging to the Company.
- Managing and mitigating IT and IS-related risks through appropriate controls and periodic assessments.
- Maintaining and updating this Policy to ensure its continued relevance and compliance with applicable standards.
- Overseeing the enforcement of this Policy, including ensuring that all employees receive appropriate training, guidance, and awareness on IS best practices and procedures.

3.2. Team Effort and Employee Responsibilities

IS is a shared responsibility. The effectiveness of this Policy depends on the collective participation, diligence, and cooperation of all employees, contractors, and third parties who access or manage Company information or information systems.

All personnel are required to:

- Understand and comply with this Policy and all related procedures.
- Exercise due care in handling Company data and technology resources.
- Promptly report any suspected or confirmed IS incidents or violations.
- Support the Company’s efforts to maintain a secure and resilient IT environment.

Through a collaborative and accountable approach, the Company aims to uphold the highest standards of information protection and operational integrity.

4. IS POLICY

4.1. Safeguarding of Company Data

Information is a vital asset of the Company, and all access to, use of, and processing of Company information must be consistent with applicable policies, standards, and regulatory requirements. Company information, as well as information entrusted to the Company by third parties, must be protected in a manner commensurate with its sensitivity, criticality, and classification. Appropriate security measures must be applied regardless of the medium on which information is stored, the systems that process it, or the methods by which it is transmitted, shared, or disposed of. Information must remain protected throughout its entire lifecycle — from origination and

storage to transmission, use, archival, and destruction — in accordance with its classification and applicable legal or regulatory obligations.

4.2. Data Classification

The Company has adopted an information classification framework that categorizes information into 4 distinct levels of sensitivity. All information under the Company's control, whether generated internally or obtained externally, falls within one of these classifications. All employees, contractors, and relevant third parties are required to familiarize themselves with these categories and apply the appropriate level of protection based on the information classification.

a. Public

This classification applies to information that has been specifically approved for public release. Unauthorized disclosure of such information will not cause harm to the Company, its customers, or business partners. Examples include marketing brochures, publicly distributed materials, and information posted on the Company's official website. Disclosure of information to the public requires that the information be explicitly designated as Public, or that prior management approval has been granted.

b. Internal Use Only

This classification applies to information intended solely for internal use within the Company and, where appropriate, with authorized business partners or affiliates. Unauthorized disclosure of this information may breach laws or regulations, or otherwise negatively impact on the Company, its customers, or its partners. Examples include internal policies and procedures, API and application architecture documentation, internal reports, marketing materials prior to public release, contracts, service level agreements, and internal communications such as departmental memos and intranet postings.

c. Confidential

This classification applies to information that is private or sensitive and must be restricted to individuals with a legitimate business need for access. Unauthorized disclosure may result in legal liability, financial loss, or reputational harm to the Company, its customers, or its business partners. Access to Confidential information must be explicitly authorized by the information owner and approved by management. Examples include customer account or transaction information, authentication data, payment details, employment contracts, performance evaluations, and correspondence with regulators, product providers, and business partners.

d. Secret

This classification applies to information of the highest sensitivity, the unauthorized disclosure of which could cause severe damage to the Company, its customers, or its partners. Access to Secret information is strictly controlled and limited to senior management or specifically authorized personnel. Examples include merger and acquisition plans, strategic initiatives, and legal communications protected under attorney–client privilege.

e. Default Classification

Any information not explicitly marked with one of the classifications above shall default to the Confidential category. Information categorized as Confidential or Secret is collectively referred to as Sensitive Information.

Unauthorized sharing, whether internal or external, of Secret or Confidential information is strictly prohibited. Access by third parties to such information shall only occur under a legally binding data sharing or confidentiality agreement signed by authorized representatives of both the Company and the third party. Any deliberate or negligent release, misuse, or unauthorized disclosure of sensitive information constitutes a violation of this Policy and may result in disciplinary action, up to and including termination of employment, and may also lead to civil or criminal legal consequences.

4.3. Safeguarding Applications and IT Assets

The integrity, confidentiality, and availability of the Company's IT environment depend on strict control of software, systems, and data-handling practices. All activities involving software, data, networks, and hardware must adhere to the following standards.

a. Software Source and Installation

Only approved, verified, and licensed software shall be used within the Company's IT infrastructure. Software must originate exclusively from trusted and authorized sources, including:

- Official business partners and approved vendors;
- Recognized systems security authorities;

- Reputable IT or network equipment vendors; or
- Commercial software vendors approved by the Company.

Software from unverified or public sources (e.g., freeware, shareware, bulletin boards, or public repositories) is strictly prohibited unless it has undergone formal testing and received written authorization from the Director – CTO.

Employees are prohibited from downloading, installing, or using unlicensed, illegal, or unapproved software on Company systems or networks.

b. Malware Protection and Screening

To protect against malicious software (malware), the following controls shall apply:

- All Company computers and devices used for business purposes must have approved antivirus software installed, configured for automatic updates and scheduled scans.
- Users must not disable or circumvent antivirus processes or system monitoring mechanisms.
- All incoming software, files, and removable media must be scanned for malware before opening or execution.
- Altering or disabling antivirus tools on Company systems is strictly prohibited.

c. Malware Detection and Response

If a device is suspected to be infected with malware:

- Immediately stop using the affected system and disconnect it from all Company networks.
- Notify the Director – CTO or designated IT representative without delay.
- Do not attempt self-repair. Virus removal must only be performed by authorized personnel under the direction of the Director – CTO.
- Any portable storage media used with the infected device must be quarantined until formally cleared.

d. User Security Responsibilities

All employees must practice vigilant cybersecurity hygiene:

- Do not open unsolicited email attachments, click unknown links, or interact with suspicious messages.
- Delete spam immediately; do not respond.
- Do not use Company devices for personal downloads, torrents, or media sharing.
- Do not disable or tamper with antivirus, firewall, or security controls.
- Keep all systems up to date with security patches and automated updates.

Failure to comply may result in disciplinary action up to and including termination and may also lead to civil or criminal liability.

4.4. Data and Password Security

The protection of data and authentication credentials is a fundamental component of the Company's IS program. All employees, contractors, and third parties are responsible for ensuring that information under their control is handled securely and that unauthorized disclosure or access is prevented at all times.

a. Data Protection in the Workplace

To maintain confidentiality and integrity of Company information, the following requirements apply:

- **Clean Desk Practice:** Confidential, Secret, or otherwise sensitive documents must not be left unattended on desks, printers, or in meeting rooms. All such materials must be stored securely in locked cabinets or drawers when not in use.
- **Document Disposal:** Sensitive information, whether in paper or electronic form, must be destroyed in a manner that prevents reconstruction or recovery. Printed documents must be shredded using approved shredders; digital files must be securely deleted following Company disposal procedures.
- **Display Security:** Computer monitors displaying sensitive information must be positioned to prevent unauthorized viewing by others.
- **Physical Access:** Access to areas where sensitive information is processed or stored must be restricted to authorized personnel only.

b. Password Requirements

Access to Company systems, networks, and applications must be protected by strong authentication measures. The following password requirements and best practices apply:

- **Uniqueness:** Passwords must be unique for each account. Reuse of passwords across multiple systems or between personal and business accounts is strictly prohibited.
- **Storage:** Passwords must never be written down, stored in plain-text files, spreadsheets, or unencrypted documents.
- **Password Managers:** Employees are encouraged to use Company-approved password management software (e.g., LastPass, KeePass) to securely store and manage credentials.
- **Change and Expiry:** Passwords must be changed immediately if compromise is suspected or when prompted by the system according to Company password lifecycle policies.
- **System Access:** Access to Company systems must automatically lock after a defined period of inactivity and require password re-entry to resume work.

Passwords are strictly personal and confidential. Employees must never share passwords or authentication credentials with anyone — including management, IT personnel, or colleagues. Any request to disclose a password must be reported immediately to the Director – CTO or IT security representative.

4.5. Network and System Security

The integrity, availability, and confidentiality of the Company's IT infrastructure rely on the continuous protection of its networks, servers, and systems. All components of the Company's IT environment must be safeguarded against unauthorized access, misuse, or compromise through appropriate technical and procedural controls.

a. Network Protection

To maintain a secure and reliable network environment, the following principles apply:

- **Intrusion Detection and Monitoring:** All Company servers, workstations, and network devices must include automated tools for intrusion detection, vulnerability monitoring, and log collection. These tools must be configured to identify and alert on any anomalous or suspicious activity.
- **Incident Reporting:** Any suspected or confirmed network intrusion, breach, or security anomaly must be reported immediately to the Director – CTO, who is responsible for coordinating investigation, response, and remediation activities.
- **Security Patching:** System administrators must apply relevant operating system and application security patches promptly after release from trusted sources such as official vendors or recognized security authorities. Unpatched systems present an unacceptable security risk and must not remain connected to Company networks.
- **Access Controls:** Network access must be limited to authorized users, devices, and systems, following the principle of least privilege. Access rights must be reviewed periodically to ensure continued appropriateness.
- **Network Segmentation:** Where feasible, the Company must implement network segmentation to isolate critical systems, sensitive data, and production environments from general user networks, thereby reducing potential exposure in the event of a security breach.
- **Encryption:** All sensitive data transmitted across Company networks or the internet must be encrypted using secure protocols (e.g., TLS/SSL, SSH, VPN). Unencrypted transmission of Confidential or Secret information is strictly prohibited.

4.6. Physical and Equipment Security

The Company shall maintain appropriate physical and environmental controls to protect its premises, equipment, and information assets from unauthorized access, damage, loss, or interference. Physical security measures form an integral part of the Company's overall Information Security framework and must be adhered to by all personnel.

a. Access Control

- Access to the Company's offices, data rooms, and other restricted areas shall be limited to authorized personnel only and managed through personal access cards or equivalent authentication mechanisms.
- Employees must immediately report the loss, theft, or suspected compromise of access cards, keys, or other physical security tokens to their supervisor or the Director – CTO.
- Office doors, equipment rooms, and storage areas must remain locked and secured when unattended.
- Visitors, contractors, or third parties must be escorted at all times and must not be left unsupervised within restricted areas.

b. Equipment Protection

- All critical equipment (e.g., servers, network hardware, and data storage devices) must be safeguarded against electrical, environmental, and physical risks by the use of Uninterruptible Power Supplies (“UPS”), surge protectors, and appropriate climate control systems.
- Equipment should be installed in designated secure environments that provide adequate protection against fire, flooding, humidity, overheating, and other natural or man-made hazards.
- Any movement, maintenance, or disposal of IT equipment containing sensitive data must be approved by the Director – CTO and performed under controlled conditions consistent with Company data disposal.

c. User Authentication and Accountability

- Each employee, contractor, or third-party user must access Company systems using unique, individually identifiable credentials.
- The use of generic, shared, or anonymous user accounts is strictly prohibited, except where explicitly authorized in writing by the Director – CTO for specific technical purposes.
- User credentials must not be shared or transferred under any circumstances. Unauthorized use or disclosure of authentication credentials constitutes a security violation and may result in disciplinary or legal action.

4.7. Remote Work and Mobile Device Policy

The Company recognizes that remote work and mobile connectivity are essential to modern business operations. However, such practices introduce additional security risks that must be effectively managed to ensure the protection of Company information and systems. This section establishes the requirements for secure remote work and mobile device usage.

a. Remote Work Requirements

- Employees working remotely must use Company-issued devices that are configured, secured, and maintained in accordance with Company IT and IS standards.
- Personal use of work devices is strictly prohibited. Work devices must not be used for non-business activities, personal email, or entertainment.
- Employees must not share their work devices with family members, friends, or any unauthorized persons.
- When working remotely, employees must ensure that screens are locked, and devices are secured whenever unattended.

b. Mobile Device Usage

- Only authorized and registered mobile devices may connect to the Company’s private Wi-Fi network or access internal systems.
- Mobile devices may be used for phone calls, secure messaging, and browsing in support of legitimate business functions.
- Storage or processing of Confidential or Secret information on mobile devices must be avoided unless encrypted and authorized by the Director – CTO.
- Lost or stolen mobile devices must be reported immediately to the Director – CTO to enable remote lock or data wipe functions.

c. Data Protection for Remote and Mobile Work

- Remote and mobile devices must have automatic locking, antivirus software, and system updates enabled at all times.
- Files containing Confidential or Secret information must only be accessed or transmitted using approved and encrypted Company channels.
- Sensitive data must not be stored locally on remote or mobile devices unless operationally necessary and explicitly approved.
- Employees are responsible for maintaining the confidentiality of all information accessed remotely, ensuring that it is not viewed, overheard, or accessed by unauthorized individuals.

4.8. Media Handling and Disposal

Proper handling and disposal of media are essential to prevent unauthorized disclosure, alteration, or loss of Company information. All forms of information storage media — including electronic, magnetic, optical, and physical formats — must be managed securely throughout their lifecycle.

a. Removable Media Usage

- Any removable media used within Company premises must be virus-scanned, encrypted, and used solely for legitimate business purposes.
- Transferring Confidential or Secret information via removable media must only occur with prior authorization from the Director – CTO and must be encrypted using approved encryption methods.

b. Media Storage and Transport

- Media containing Confidential or Secret information must be clearly labeled and securely stored in locked cabinets or designated secure areas.
- When physical transport of media is necessary, it must be carried by authorized personnel and protected from unauthorized access, loss, or environmental damage.

c. Secure Disposal Procedures

- Disposal of storage media (e.g., hard drives, SSDs, backup tapes, or other storage devices) must be carried out following secure data destruction procedures approved by the Director – CTO. This includes overwriting, degaussing, or physical destruction as appropriate to the media type.
- Paper documents containing Confidential or Secret information must be shredded using cross-cut shredders or disposed of via an approved secure document destruction service.
- Disposal or trade-in of IT assets (e.g., laptops, servers, mobile devices) requires the completion of relevant IS Management forms and submission via Jira for Director - CTO approval prior to any physical transfer or decommissioning.
- Verification of destruction or sanitization must be documented and retained for audit purposes.

4.9. Incident Management and Enforcement

The Company shall maintain a structured approach to the identification, reporting, management, and resolution of all IS or IT security incidents. Effective incident management ensures that security events are handled swiftly and appropriately to minimize potential damage and prevent recurrence.

a. Incident Reporting

- All employees, contractors, and third-party service providers are required to immediately report any suspected or actual security incident, including but not limited to data breaches, malware infections, unauthorized access, or loss of equipment, to the Director – CTO.
- Reports must be made through the designated reporting channel (e.g., Jira ticket or direct communication) and include all relevant details known at the time of detection.
- Delayed or non-reporting of incidents constitutes a violation of this Policy and may result in disciplinary action.

b. Investigation and Response

- The Director – CTO is responsible for the coordination, investigation, and remediation of all confirmed or suspected security incidents.
- Upon detection of a breach or unauthorized access, the following actions shall be initiated without delay:
 - Execution of a full system scan across affected devices and networks.
 - Reset of all potentially compromised passwords and credentials.
 - Review of audit logs and access records to determine the scope and source of compromise.
 - Isolation of affected systems to prevent further spread or data leakage.
- Where required, the Director – CTO shall coordinate with legal counsel, regulatory bodies, or external cybersecurity experts to ensure compliance with applicable laws and incident disclosure requirements.

c. Enforcement and Disciplinary Measures

- All employees must adhere strictly to this Policy and related IS/IT procedures.
- Any violation, negligence, or misconduct resulting in a security breach or compromise of Company systems or data shall be subject to disciplinary action, up to and including termination of employment.
- In cases involving deliberate misconduct, fraud, or unlawful activity, the Company reserves the right to pursue legal action and to refer the matter to the appropriate authorities.
- The Company reserves the right to monitor, audit, and inspect its systems and devices to ensure compliance with IS and IT standards.

5. BACKUP PROCEDURE

5.1. Purpose

This section establishes the formal Backup Procedure adopted by the Company to ensure the availability, integrity, and recoverability of its data and information systems. It defines the responsibilities, backup schedules, and testing procedures necessary to protect critical information assets in the event of data loss, corruption, or system failure.

This procedure applies to all internal systems, servers, and databases managed directly by the Company.

For externally hosted or platform-managed systems — such as the Company's Website, Customer Relationship Management ("CRM"), and Content Management System ("CMS") platforms — backup and recovery responsibilities are contractually assigned to third-party service providers under established Service Level Agreements ("SLAs"). In such cases, the third-party service providers' IT and IS policies govern the execution of backup activities, while the Director – CTO retains oversight to ensure compliance with contractual obligations, operational standards, and data protection requirements.

5.2. Responsibilities

a. Director – CTO Responsibilities

- Oversees and ensures the full implementation and ongoing effectiveness of the Company's data backup and restoration processes.
- Verifies that backups are executed in accordance with the defined schedule and that all backup media are securely stored and protected against unauthorized access, loss, or damage.
- Conducts periodic reviews and restoration tests to validate the integrity, completeness, and recoverability of backed-up data.
- Maintains detailed records, audit logs, and documentation of all backup, restoration, and testing activities.
- Coordinates with third-party service providers responsible for managing backups of hosted or platform-based systems, including the Company's website, CRM, and CMS platforms.
- Ensures that all third-party service providers comply with their contractual SLAs and maintain backup and recovery capabilities consistent with the Company's operational and regulatory requirements.

b. Third-Party Service Providers

- Are responsible for performing full and incremental backups of all data, configurations, and applications managed on behalf of the Company, in accordance with applicable SLAs.
- Must maintain redundancy, integrity, and recoverability of all data within the agreed Recovery Time Objectives ("RTOs") and Recovery Point Objectives ("RPOs").
- Conduct regular restoration testing and provide reports confirming successful completion to the Director – CTO.
- Ensure secure storage, encryption, and transmission of backup data, and promptly notify the Company of any incident that may compromise backup integrity or availability.
- Comply with all relevant legal, regulatory, and contractual data protection obligations.

5.3. Backup Management

a. Backup Process

- Master copies of critical software, system configurations, and essential data must be securely stored in restricted-access repositories (e.g., locked cabinets or encrypted storage).
- These master copies shall not be used for daily operations and are reserved exclusively for recovery in the event of data corruption, malware infection, or hardware failure.
- All internally managed backup activities must be conducted in accordance with the Company's established IT and IS procedures and controls.

b. File Naming Convention

- A standardized file naming convention must be applied to clearly distinguish between:
 - Production data
 - Test and training data
- Each file name must include appropriate timestamps and unique identifiers to ensure version control, traceability, and ease of restoration.

5.4. Backup Schedule

a. Internal Systems

- Full system backups include all data, configurations, and applications necessary to restore the Company's internal IT environment in the event of data loss, corruption, or hardware failure.
- Incremental backups of critical data—such as system configurations, application data, and operational logs—are performed at defined intervals in accordance with operational requirements.
- All internal backup activities are documented and monitored under the supervision of the Director – CTO, who verifies successful completion and adherence to approved procedures.

b. Third-Party Hosted Systems

- Customer, transactional, website, CRM, CMS, and platform data are hosted and maintained by authorized third-party service providers under formal SLAs.
- The third-party service providers are responsible for performing regular full and incremental backups, maintaining data integrity and availability, and ensuring recoverability in alignment with agreed operational and regulatory standards.
- Secure disaster recovery environments are maintained by the third-party service providers to support continuous data replication and off-site redundancy.
- The Director – CTO retains oversight of third-party service providers compliance, reviews periodic backup and restoration reports, and ensures relevant records are maintained for audit and regulatory review.

5.5. Backup Restoration and Testing

a. Internal Systems

- Restoration tests are performed in a controlled test environment at least once every 6 months to verify data integrity, completeness, and recoverability.
- Critical archives and software retained for long-term storage are subject to annual restoration testing to ensure continued accessibility and usability.
- The Director – CTO maintains detailed logs of all restoration tests, including test results, issues identified, and corrective actions implemented.

b. Third-Party Systems

- Restoration testing for third-party managed systems is conducted in accordance with each third-party service provider's established backup and recovery policies and procedures, as defined in the applicable SLA.
- The Director – CTO reviews and retains restoration reports provided by third-party service providers to confirm successful completion and continued compliance with contractual obligations.

5.6. Security and Storage

a. Internal Systems

- All backup media—whether physical or digital—must be encrypted, clearly labeled, and securely stored in accordance with the Company's data classification and access control procedures.
- Offsite backups must be transmitted via encrypted channels and stored in secure facilities that meet recognized IS standards (e.g., ISO 27001 or equivalent).
- Access to backup data is restricted to authorized personnel designated by the Director – CTO and monitored in line with the Company's IT and IS access control policies.

b. Third-Party Systems

- Backup media and data managed by third-party service providers are stored and protected in accordance with their established IS frameworks and contractual obligations under the applicable SLA.
- The Director – CTO ensures that third-party service providers maintain equivalent security controls, including encryption, restricted access, and compliance with relevant international security standards.

6. BUSINESS CONTINUITY (“BC”) & DISASTER RECOVERY (“DR”)

6.1. Purpose

To ensure that the Company can maintain or promptly resume critical operations in the event of significant IS or IT incidents, including system outages, data loss, or other service disruptions. This section establishes the framework for business continuity and disaster recovery planning, defines oversight responsibilities, and ensures alignment with the Company's operational, regulatory, and contractual obligations — including those managed through third-party service providers.

6.2. Objectives

This section aims to:

- Safeguard the availability, integrity, and continuity of the Company's business operations and information assets during disruptions.
- Minimize downtime and operational impact by ensuring timely recovery of critical systems and services.
- Maintain compliance with applicable legal, regulatory, and contractual obligations.

All critical business applications, infrastructure, and processes must have a defined and periodically tested continuity plan designed to enable recovery within 72 hours of a disruption.

Where continuity and recovery rely on third-party service providers (e.g. platform, CRM, CMS, or hosting services), the third-party service providers' internal BC/DR policies and procedures apply as defined in the applicable SLAs. The Company retains oversight to ensure ongoing contractual and regulatory compliance.

6.3. Responsibilities

a. Director – CTO

- Oversees the Company's BC/DR framework and ensures that internal continuity procedures are properly defined, documented, and periodically tested.
- Maintains oversight of third-party service providers' BC/DR arrangements and ensures that their SLAs include adequate continuity and recovery provisions, including RTOs and RPOs.
- Reviews periodic BC/DR reports, incident summaries, and test results provided by third-party service providers.
- Ensures that internal personnel receive appropriate awareness and training on continuity and recovery procedures.

b. Senior Management

- The Board of Directors is responsible for making strategic decisions related to major incidents, resource allocation, and service restoration priorities.

c. Third-Party Service Providers

- Execute BC/DR procedures in accordance with their internal policies and the SLAs established with the Company.
- Maintain redundancy, data protection, and recovery capabilities consistent with contractual and industry requirements.
- Notify the Company promptly of any incident that may affect service continuity or data integrity.
- Provide periodic reports confirming successful completion of BC/DR testing and recovery verification, as required under the SLA.

6.4. Scenarios and Mitigation Measures

a. Power Failure

- The Company's office and data centre environments are equipped with UPS systems and basic generator support to sustain short-term outages.
- In the event of prolonged power loss, the Director – CTO coordinates with facility management and relevant third-party service providers to restore service or relocate essential operations.

b. Network or Internet Failure

- Network connectivity supporting the Company's operations is maintained under third-party SLAs.
- In the event of service interruption, traffic may be redirected to alternate or redundant sites managed by the third-party service providers.
- The Company monitors the situation and coordinates communication with affected stakeholders until service is fully restored.

c. Data, Server, or Firewall Failure

- The Company's critical systems and databases are hosted and maintained by authorized third-party service providers under formal SLAs.
- Third-party service providers are responsible for maintaining redundancy and performing recovery in accordance with their documented failover and backup procedures.
- The Director – CTO verifies incident resolution and ensures that recovery meets the agreed RTO and RPO parameters.

d. Unauthorized Access or Security Breach

- In the event of suspected unauthorized access or data compromise, the IS and IT functions coordinate an immediate investigation with the affected third-party service providers.
- Initial response actions include system containment, credential resets, data integrity validation, and review of relevant audit and security logs.
- The Director – CTO ensures that a post-incident analysis is conducted and that corrective and preventive actions are implemented.
- Incident reporting to regulatory or supervisory authorities is carried out in accordance with applicable legal and licensing obligations.

e. Major Disaster Resulting in Loss of Office Space

- In the event of loss of office space, employees may be instructed to operate from alternate secure locations, as coordinated by the Director – CTO.
- Access to systems and communication tools is maintained through secure, cloud-based environments managed under third-party SLAs.
- Operations are resumed from temporary or alternate premises as soon as practicable.

f. Major Disaster Resulting in Loss of Data Centre or Platform

- In the event of data centre or platform unavailability, third-party service providers initiate disaster recovery procedures in accordance with their internal BC/DR policies and SLAs.
- Redundancy and failover mechanisms are maintained by third-party service providers under the same agreements.
- The Director – CTO maintains oversight, ensures timely communication, and validates recovery status through reports provided by the third-party service providers.

6.5. Business Impact Analysis (“BIA”)

The Company conducts a BIA to identify critical business processes, recovery priorities, and potential operational, financial, and regulatory impacts resulting from service disruptions.

For systems or services managed by third-party service providers, the Company's BIA relies on the continuity and recovery assurances defined in the applicable SLAs. These are reviewed periodically by the Director – CTO to ensure they remain sufficient to meet the Company's operational and regulatory requirements.

6.6. Escalation and Regulatory Reporting

- The Director – CTO must be immediately notified of any incident or event that significantly disrupts business operations or affects system availability.
- Board of Directors must be informed in cases involving substantial operational, financial, or regulatory impact.
- Where required under applicable gaming or regulatory frameworks, the Director – CTO shall report material incidents, downtime, or service failures to the relevant Gaming Authority.
- Escalation procedures and contact details are maintained and communicated internally to ensure timely response and coordination during incidents.

7. SYSTEM INFRASTRUCTURE & INFORMATION ASSETS**7.1. Purpose**

This section outlines the Company's technical infrastructure and major information system assets, including both internal and third-party managed components. It defines how the Company ensures security, availability, and continuity of core systems supporting its operational and regulatory obligations.

7.2. Infrastructure Overview

The Company's core gaming platform, website, CRM, and CMS environments are hosted and maintained by approved third-party service providers under defined SLAs. These third-party service providers are responsible for ensuring the availability, security, and performance of production systems in accordance with agreed RTOs and RPOs.

Internal systems supporting day-to-day operations (e.g., productivity tools, local network infrastructure, endpoint devices, and internal backups) are managed and secured by the Company under the supervision of the Director – CTO.

7.3. Secure System Architecture

The Company maintains a layered security architecture combining internal controls with those implemented by third-party service providers. Security measures include:

- Network segmentation separating administrative, operational, and public-facing environments.
- Use of firewalls, intrusion detection/prevention systems (IDS/IPS), and secure VPN access.
- IP-based restrictions and access whitelisting for administrative interfaces.
- Multi-factor authentication and least-privilege access management.
- Encryption of data in transit and at rest using industry-standard protocols.
- Continuous monitoring and logging of critical systems.

Third-party service providers maintain their own secure infrastructure configurations, reviewed periodically by the Company to verify compliance with contractual and regulatory requirements.

7.4. Hosting and Data Centres

All production systems, databases, and platform components are hosted in data centres operated by third-party service providers certified under ISO 27001 or equivalent standards.

These facilities maintain redundancy for power, connectivity, and environmental controls to ensure business continuity.

Where applicable, off-site backup and disaster recovery environments are also managed by these third-party service providers under their internal BC/DR policies.

7.5. Application and Platform Architecture

The Company's iGaming platform and supporting applications are developed and maintained by third-party service providers. These include:

- CMS
- CRM platform
- Game management engine
- Payment gateway and transaction processing
- Back-office application
- Master and slave databases
- Business intelligence and reporting tools

Each system is integrated under a unified operational environment, ensuring secure data flow, centralized administration, and consistent player experience across brands and jurisdictions. Third-party service providers are required to:

- Maintain system redundancy and scalability.
- Conduct regular security and performance testing.
- Apply patches and updates under approved change-management processes.
- Report significant incidents or outages within agreed SLA timeframes.

7.6. Information Assets

Information assets managed by or on behalf of the Company include:

- Player and transaction data
- CRM

- Financial and payment information
- Operational and audit logs
- Vendor and partner data (limited to internal systems)

All information assets are protected in accordance with their sensitivity and business criticality to ensure appropriate levels of security, access control, and confidentiality. Third-party service providers managing systems or data on behalf of the Company are contractually required to maintain equivalent or stronger protection measures, consistent with their SLAs and all applicable regulatory and data protection obligations.

7.7. Redundancy and High Availability

To ensure high availability and fault tolerance:

- Third-party service providers implement redundancy across network, database, and application layers.
- Virtualized environments support failovers between primary and secondary systems.
- Backups and replications are performed and tested in line with defined RTOs and RPOs.

The Director – CTO retains oversight of continuity testing reports and reviews third-party service providers performance as part of SLA management.

7.8. Oversight and Compliance

The Director – CTO is responsible for maintaining oversight of all infrastructure and system assets to ensure:

- Compliance with data protection and gaming regulatory requirements.
- Periodic review of third-party service providers compliance reports and certifications.
- Validation of internal and third-party controls related to security, availability, and recoverability.

7.9. Diagrammatic Representation

Architecture and network diagrams of the production environment are maintained by the respective third-party service providers and made available to the Company upon request for audit or regulatory review.

8. THE NETWORK INFRASTRUCTURE

8.1. Overview

The Company's production and support environments are hosted and managed by approved third-party service providers under defined contractual and SLA arrangements.

The infrastructure is designed to ensure security, scalability, availability, and regulatory compliance, supporting the Company's online gaming operations and associated systems.

Network architecture maintains logical and physical segregation between customer-facing services, operational systems, and administrative environments to minimize risk and prevent unauthorized access.

8.2. Operator Access Security

Access for authorized Company personnel and administrative users ("operators") is restricted to designated CRM and Back-Office environments. Security controls include:

- Encrypted access via SSL/TLS
- HTML5 geo-location checks (within the application)
- Hardware hash authorization (e.g., Chrome-based extension)
- Multi-factor authentication (username/password + PIN or token)
- Platform-level Access Control Lists (ACLs)
- Role-based access through panel management
- IP whitelisting and device restrictions

8.3. Platform and Infrastructure Security

The Company's gaming platform, hosting, and supporting infrastructure are maintained by authorized third-party service providers under formal SLAs. These third-party service providers are responsible for implementing and

maintaining security, redundancy, and environmental controls in line with recognized industry standards (e.g., ISO 27001, PCI DSS, or equivalent).

Network segmentation ensures clear separation between public-facing, application, and database environments.

System hardening, patch management, and integrity verification are performed in accordance with the third-party service providers' internal policies.

The Director – CTO maintains oversight of third-party service providers security measures and reviews available compliance attestations or audit reports to verify ongoing adherence to contractual and regulatory obligations.

8.4. Monitoring and Performance Oversight

Performance and availability of systems supporting the Company's operations are continuously monitored by third-party service providers under their internal procedures and SLAs.

The Company receives periodic performance and incident reports to verify service levels and operational compliance.

Any service degradation or outage reported by third-party service providers is reviewed by the Director – CTO to assess operational impact and ensure timely remediation.

9. OVERSIGHT AND REVIEW

This Policy shall be reviewed at least annually, or sooner where required by changes in law, regulatory guidance, contractual obligations, or internal operational developments.

The review process shall be coordinated by the Director – CTO in consultation with Senior Management and other relevant departments (e.g., Compliance, Legal, and IS).

All relevant staff shall receive periodic awareness training covering business continuity, information security, and third-party management practices applicable to their roles.

The Company may perform internal audits or assessments to verify adherence to this Policy, evaluate control effectiveness, and identify improvement opportunities.

Third-party service providers' compliance with contractual IS/IT obligations may be reviewed periodically through reports, attestations, or independent audits, as made available under their SLAs.

10. CONTACT INFORMATION

The contact person for matters relating to the Policy is:

Name, surname: Dmitrijs VOLKS

Email: legal@planbet.com

Any questions, requests for clarification, or concerns regarding this procedure should be directed to the contact person(s) listed above.