

Information Security Policy

1 Document Information

1.1 Introduction

Storage of any data on computers and transfer across the network eases use and expands our functionality. Commensurate with that expansion is the need for the appropriate security measures.

The Information Security Policy recognizes that not all business functions within the Company are the same and that data are used differently by various units.

The Policy is written to incorporate current technological advances. Instances of non-compliance must be reviewed and followed up by the Information Security Manager.

The Company shall be responsible for recommending security policies and changes.

1.2 For use by

This Information Security Policy should be disseminated to all users including vendors, contractors, and business partners. This information security policy should be reviewed and updated at least yearly. All employees must sign an agreement verifying they have read and understood this document.

1.3 Permeable

Should positions within the Company, referred to within policies and procedures, be vacant, the responsible Key Person is vested with all the applicable responsibilities. The Responsible Key Person is authorised to engage consultants and experts in meeting his responsibilities relating to technical, legal and similar issues.

2 Purpose, Objective and Scope

By information security we mean protection of the Company's data, applications, networks, and computer systems from unauthorised access, alteration, or destruction.

The purpose and objective of this Information Security Policy is to protect the Company's information assets, including data printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or video, spoken in conversation, from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage.

The purpose of the information security policy is:

- a. To establish an operation-wide approach to information security.
- b. To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of data, applications, networks and computer systems.
- c. To define mechanisms that protect the reputation of the Company and allow the same to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
- d. To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.

The Company recognises the importance of regular testing.

This policy underlines that annual technical security tests must be conducted in the production environment to ensure there are no vulnerabilities that could compromise the security and operation of the Technological Platforms. These tests must follow a security assessment method simulating third-party attacks, using a recognized methodology. Vulnerability analysis must include identification and quantification of potential platform risks, which may include:

- UDP/TCP port scanning.
- Stack fingerprinting and TCP sequence prediction to identify operating systems and services.
- Appropriation of public service announcements.
- Web scanning using HTTP and HTTPS vulnerability scanners.
- Router scanning using BGP (Border Gateway Protocol), BGMP (Border Gateway Multicast Protocol), and SNMP (Simple Network Management Protocol) protocols.

Changes in security levels (amongst others) must be recorded, stored, and a backup of significant event information must be maintained. The information must be available to the regulator.

3 Responsibility

3.1. Information Security Internal Management

The Company has established an internal information security management team composed of key personnel from IT, security, and operations departments. This team is responsible for responding to and managing any identified malfunctions or security incidents:

The Information Security Manager is responsible for the regular updating, review, approval, publishing and implementation of the Information Security policy, management of information security and to provide advice and guidance on information security.

Google Cloud is not applicable to the physical access restriction. For the Maltese server, it is located in the Maltese office with strict security measures, only Anatoly Zhupanov and Sergey Logvinov have access to the server.

The Information Security Manager must ascertain that appropriate training is provided to data

owners, data custodians, network and system administrators, and users.

Managers / Directors are directly responsible for implementing the Information Security Policy within their business areas.

3.2 Incident Response Procedure

The Company has its own Incident Response Procedure in place, details procedures for assessing, containing, eradicating, and recovering from incidents. It includes steps for:

- 1) protection of the system / operation;
- 2) identification and analysis of the problem;
- 3) containment of the problem in line with mitigation plan;
- 4) eradication of the problem in line with mitigation plan;
- 5) recovering from the incident and the follow-up analysis;
- 6) Closure & Follow-Up

3.3 Control of Key Personnel

- 1) Roles and Responsibilities: CIO Anatoly Zhupanov and lead DevOps engineer Sergey Logvinov (key personnel) make up the security department. All key personnel involved in the gaming system's operation are clearly defined, with specific roles and responsibilities documented in our internal policies. This includes system administrators, security professionals, game integrity analysts, and customer support staff.
- 2) Training and Awareness: Regular training sessions are conducted to ensure that key personnel are aware of their responsibilities, the latest security practices, and incident response procedures. This training includes identifying information security weaknesses via the internal platform BambooHR.
- 3) Performance Monitoring: The performance of key personnel is monitored through regular reviews and audits. This includes evaluating adherence to security protocols, incident response times, and overall contribution to the gaming system's integrity.
- 4) Access Control: Access to sensitive systems and data is strictly controlled and limited to authorised personnel only. Access rights are based on the principle of least privilege, ensuring individuals have only the access necessary to perform their duties.
- 5) Security Forum: CIO, lead DevOps engineer organises the security forum every three months.

3.4 Competency Process

- 1) Recruitment and Selection: During the hiring process, all candidates for security roles undergo a thorough assessment of their qualifications and relevant experience. Each candidate is evaluated against a predefined set of competency criteria that reflect the technical skills, knowledge, and behavioural attributes required for the role.
- 2) Competency Assessments: Staff members undergo periodic competency assessments, including:

- Technical skills: Ability to manage, assess, and mitigate security risks.
- Problem-solving abilities: Effectiveness in identifying, analysing, and responding to security threats.
- Understanding of policies and procedures: Adherence to internal security policies and regulatory requirements.
- Communication skills: Ability to communicate and collaborate with other departments to ensure security policies are consistently applied.

3) Performance Reviews: Performance reviews are conducted annually to measure each staff member's competence in key areas of their role. Specific objectives and KPIs are used to ensure that employees are meeting the expectations of their role. Staff members in the Security Department are also evaluated based on their ability to proactively manage security risks, respond to incidents, and work effectively with technical teams.

4 General Policy

The Company adopts a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the operation's data, network and system resources. Vulnerability and risk assessment tests of external network connections are conducted on a regular basis.

5 Policies

Information must be protected from a loss of confidentiality, integrity and availability.

Regulatory and legislative requirements must be met.

Business continuity plans must be produced, maintained and regularly tested.

Security reviews of servers, firewalls, routers and monitoring platforms must be conducted on a regular basis. These reviews must include monitoring access logs and results of intrusion detection software, where it has been installed.

The audit logs which record staff members user activities, exceptions, and information security events are kept for a minimum of five years.

Education and training must be provided to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. This must be tailored to the role of the individual network administrator, system administrator, data custodian, and users.

All breaches of information security, actual or suspected, must be reported to, and investigated by, the Information Security Manager. The appropriate Incident Reporting

procedures must be followed.

Other guidance and procedures (such as system access control and backup procedures) within the company procedures manual support this policy.

It is the responsibility of each employee to adhere to the Information Security Policy. All

employees have a responsibility to conduct themselves in an ethical manner.

Non-compliance with this Policy will be subject to Management review and action in conformance with the Company's disciplinary procedures.

5.1 Data Classification Policy

It is essential that all data be protected. There are however gradations that require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance.

The Company ensures secure storage and processing of data in the production environment of the Technological Platform, including:

- Adopting methods for correct data processing, input validation, and rejection of corrupt data.
- Limiting access to workstations accessing critical applications or databases.
- Encryption, password protection, or equivalent measures for files and directories containing sensitive data. Alternatively, restriction of content visibility and log accesses.
- Avoiding options or mechanisms that could compromise data on the equipment.
- Avoiding mechanisms that automatically erase data in error.
- Ensuring no equipment allows data deletion from memory without transferring to secure components of the Technological Platform.
- Storing personal and sensitive information in encrypted server areas protected against unauthorised internal and external access.
- Separating production databases on a network apart from any player interface.
- Adjustments to the gaming account can only be made with authorization.
- Maintaining data availability regardless of server power supply.
- Storing data to prevent loss during replacement of parts or modules during maintenance.

The user account and registration data is retained during the validity period of the user account, starting from the authorization granted by the regulator to the Holder and continuing for five (5) years after its cancellation or annulment.

To start with, the Company identifies three (3) classes of data :

5.1.1 High Risk

Information assets over which there are legal requirements for preventing disclosure. Data covered by local and international legislation are in this class. Payroll, personnel, gaming, player and financial information are also in this class because of privacy requirements. This policy recognizes that other data may need to be treated as high risk because it would cause severe damage to the Company if disclosed or modified. The data owner should make this determination. Access to High Risk data must be controlled from creation to destruction, and will be granted only to those persons who require such access in order to perform their job ("need-to-know"). Access to High Risk data must be individually requested and then authorised by the Data Owner who is responsible for the data. In addition, the dissemination of such information with third parties is prohibited from doing so without the express confirmation in writing by a member of the Executive Team and preferably the right of the third party to receive such information should be prescribed in a contract.

5.1.2 Confidential

Data that would not expose the Company to loss if disclosed, but that the data owner feels should be protected to prevent unauthorised disclosure. Access to such data shall be by default given solely to employees who maintain a managerial role within the company. Access to other employees may be given on a 'need to know' basis. The dissemination of such information requires the express confirmation by a member of the Executive Team.

5.1.3 Public

Information that may be freely disseminated. Access to such information need not be controlled although specific guidelines may be issued by the Executive Team if they perceive the dissemination of such information to be harmful to the business.

No system or network subnet can have a connection to the Internet without the means to protect the information on those systems reflecting its confidentiality classification.

Data custodians are responsible for creating data repositories and data transfers which protect data in the manner appropriate to its classification.

High risk data and confidential data must be encrypted during transmission over insecure channels.

All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.

Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

5.2 Access Control / Password Policy

Data must have sufficient granularity to allow the appropriate authorised access. There needs to be a balance between protecting the data and permitting access to those who need to use the data for authorised purposes.

Access to the network and servers and systems should be achieved by individual and unique logins and should require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.

All systems which store sensitive information such as passwords must do so using non-reversible encryption.

Users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. Exceptions may be allowed under specific scenarios and under specific authorisation by the Information Security Manager. All users must secure their username or account, password, and system access from unauthorised use.

Users are accountable for the security and use of their user accounts and passwords. All accounts, including operating system, back office application and payment application, are log in via Google accounts:

Password Maximum Age: 30 days

Password Minimum Length: 12 characters

Password Automatic Expiry: 30 days

System user accounts should regularly be reviewed and audited for malicious, obsolete, and unneeded accounts. Inactive accounts should be disabled.

Passwords associated with Logon IDs must comply with the Password policy of the Company. All users must have a strong password. Basics for creating a strong password include minimum length being of eight characters which should include a mix of uppercase, lowercase, and numerical characters. Empowered accounts, such as administrator, must be at least eight characters long, contain at least one numerical and one special character, and be regularly changed.

Any sensitive system supporting the infrastructure or that would allow indirect access to data should be protected with multi factor authentication such as Google Authenticator to prevent access of such systems even if usernames and passwords are leaked. The infrastructure should additionally be restricted to be able to be accessed only by certain physical computers and via a private VPN.

Should a user of any system forget his or her password, the password will be reset by the

system administrator. The system must prompt the users to enter a new password immediately upon the first login attempt.

Encrypted passwords should be enabled on any devices where it is not on by default. Back-end systems should have an automatic inactivity log-off period of 1 hour.

Users who leave their workstations must lock their workstation or log off to prevent unauthorised access. Users which fail to comply with this policy will be held liable for the use of their account and disciplinary action may be taken.

Default passwords on all systems must be changed after installation. Terminated employees should have their accounts disabled.

Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.

Accounts should be locked automatically after multiple password failures in any system which supports such functionality. If a system does not support such a feature, the Information Security Manager should regularly review the access logs of that system, to ensure that user accounts are not being mismanaged.

Activities performed as administrator or super user must be logged by the system and where the system does not allow such logging, compensating controls put in place.

Personnel who have administrative system access should use other less powerful accounts for performing non-administrative tasks.

System logs should be reviewed regularly. The audit logs which record staff members user activities, exceptions, and information security events are kept for a minimum of five years

The Access Control / Password Policy should be reviewed at least every 12 months.

5.3 Process for Verifying and Authenticating Critical Control Program Components

The Company implements a verification and authentication process for all critical control program components. The procedure includes the following key steps:

- The Company verifies that all critical components of the programs and files affecting gaming operations of the gaming platform in the production environment match those approved by the authorised Certification Laboratory according to the compliance certificate after any installation/update. In practice, installations or updates typically occur two to four times within a 30-day period. Once the verification process is completed post-installation or update, no changes or deletions to these components will be permitted until the next scheduled update, as enforced by the Company's configuration settings within Kubernetes.

- **Analytical Comparison:** An analytical phase is built into the system to systematically compare the digital signatures of critical components obtained during verification against those stored in the compliance certificate.
- **Record-Keeping:** The results of all verification processes are logged in a file on the Technology Platform. These records are maintained for at least 90 days, accessible to the regulator in an approved format, and are part of the platform's recoverable records in case of disaster or system failure.
- **Failure Notification:** In the event of a communication failure or any issue with a critical component, the Company will notify the regulator.
- **Authentication Failure Response:** If the verification or authentication process identifies a failure or inconsistency, a predefined response procedure is triggered.

5.4 Test Account Policy

5.4.1 Procedure for Authorising Testing Activity and Assigning Test Accounts

Testing activity within our online gambling platform is conducted to ensure system functionality, compliance with regulatory requirements, and to validate technical integrity. The procedure for authorising testing activity is as follows:

Authorization of Testing: Testing activities are authorised by the Chief Information Officer (CIO). All testing requests must be submitted in writing, outlining the purpose, scope, and duration of the test.

Approval Process: Once a testing request is received, it is reviewed for appropriateness. Approval is documented in an internal document.

Assignment of Test Accounts: Upon approval, the CIO is responsible for assigning test accounts. Test accounts are generated in the back-office system and assigned to authorised personnel. Each test account is issued with a unique identifier and is linked to the testing project for traceability.

5.4.2 Procedure for the Issuance of Funds for Testing

To conduct testing in a real-world environment, funds may need to be issued into test accounts. The procedure for the issuance of funds is as follows:

- 1) **Authorised Personnel:** The issuance of funds for testing is strictly limited to the CIO. These individuals are the only personnel authorised to approve and issue funds for testing purposes.
- 2) **Issuance of Funds:** Upon approval of the test request, the authorised personnel may issue funds. A formal request must be submitted, stating the purpose of the test and the required amount of funds.
- 3) **Maximum Fund Amount:** The maximum amount of funds that may be issued for testing per account is \$200 USD, unless otherwise specified by the requesting personnel and

with prior approval from the CIO for amounts exceeding this threshold.

- 4) Documentation: All fund issuance requests and approvals are recorded in an internal document.

5.4.3 Access Permissions for Issuing Funds

Access to the system for issuing funds is restricted to specific personnel to maintain security and prevent unauthorised use of funds. The following staff members have access:

- CIO: Full access to approve, release funds for testing and initiate the issuance process.
- Director, Requested Personnel: Access to the funds to verify fund issuance but does not have the ability to release funds.

5.4.4 Procedure for Maintaining Records of Test Accounts

To ensure proper record-keeping of all testing activities, the following procedures will be in place for the management of test accounts:

- 1) Creation and Activation: Each test account is created upon approval of a testing request. The account is logged in the test account registry in the back office, which includes the following details:
 - Date of creation
 - Unique test account identifier
 - Purpose of the test
- 2) Maintenance: The CIO is responsible for maintaining the test account registry in the back office. Each account is regularly reviewed to ensure it is only active for the duration required for the test. Inactive test accounts are deactivated and recorded as such.

5.4.5 Procedure for Auditing Testing Activity and Fund Accountability

To ensure proper oversight of testing activities, the following auditing procedures are in place:

- 1) Testing Audit: All testing activities and the use of funds are audited on a case-by-case basis. This includes reviewing:
 - The purpose and scope of each test
 - Fund issuance and usage reports
 - Test outcomes
- 2) Fund Accountability: For each test, The funds issued, used, and returned will be verified. Any discrepancies are investigated immediately.

5.5 *Virus Prevention Policy*

The introduction of computer viruses into the Company's environment is prohibited, and

violators may be subject to prosecution.

All laptops, desktop systems, servers and workstations that connect to the network must be protected with an approved, licensed anti-virus software product that is kept/automatically updated.

Headers of all incoming data including electronic mail must be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned.

System or network administrators should inform users when a virus has been detected.

Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

Users must not tamper with or disable anti-virus software installed on their workstations.

Users must do their best to contain any spread of malicious software within the company's environment.

5.6 Encryption Key Management Procedures

a) Obtaining or Generating Encryption Keys and Secure Storage

Encryption keys are generated for 384 bits length by secure systems that are certified for cryptographic use.

- Secure Storage: Encryption keys must be stored in secure key management solutions that comply with the company's security standards and regulatory requirements.
- Key Access Controls: Only authorised personnel with the necessary security clearance and role-based access may access encryption keys. Strict access controls and auditing are applied to all key management systems.
- Encryption of Keys: Encryption keys must be further encrypted (key wrapping) when stored to ensure their security.

b) Management of Encryption Key Expiration

- Key Lifespan: Encryption keys must have a defined lifespan and expiration date, depending on the sensitivity of the data they protect and regulatory requirements.
- Key Expiration Notification: Automated systems must be in place to notify key owners and system administrators of upcoming key expirations.
- Key Renewal: When an encryption key is close to expiration, a new key must be generated, and the old key must be securely retired according to the revocation and key change procedures outlined below.

c) Revocation of Encryption Keys

- 1) Revocation Triggers: Encryption keys must be revoked immediately in the following cases:
 - A security breach or suspected compromise of the encryption key.
 - The key has expired or is no longer required.
 - There is an organisational change in access privileges or responsibilities.
- 2) Revocation Process: Upon revocation, the encryption key must be marked as invalid in the key management system, and all systems dependent on the key must be updated to use a new key or be taken offline for further security review.
- 3) Post-Revocation Data Handling: Any data encrypted with a revoked key must be securely re-encrypted with a new key, where applicable, to ensure data security continuity.

d) Secure Change of the Encryption Key Set

- Key Change Protocol: When encryption keys are updated, replaced, or rolled over (e.g., upon expiration), the following procedures must be implemented:
- New encryption keys are securely generated and stored.
- Any data previously encrypted with the old key set must be decrypted and re-encrypted using the new keys.
- A record of the key change, including the reason and personnel involved, must be logged for audit and compliance purposes.
- Minimising Disruption: Key changes must be performed in a manner that minimises disruption to ongoing operations and access to data.

e) Recovery of Data Encrypted with Revoked or Expired Encryption Keys

- Data Recovery Period: information security of key management is controlled by google solution as described in:
<https://cloud.google.com/security/products/security-key-management?hl=en>.
- Key Archiving: Expired encryption keys must be archived in a secure, tamper-evident manner to facilitate the decryption of data, should the need arise during the recovery period.
- Secure Key Recovery: When data recovery is needed, authorised personnel must securely retrieve the archived encryption key and use it to decrypt the data in a controlled environment.
- Data Re-Encryption: Once data has been recovered, it must be re-encrypted using a valid, active encryption key.

5.7 Intrusion Detection

Intrusion detection and security monitoring is very important to protect resources and data. This section is the policy and guideline over intrusion detection implementation of the organisational networks and hosts along with associated roles and responsibilities. Every host on the organisational network and the entire data network are covered. The ISO should ensure:

- An increased level of security via active searching for signs of unauthorised intrusion.
- Prevention or detection of any threats to the confidentiality of organisational data on the network.
- Preservation of the integrity of organisational data on the network.
- Prevention of unauthorised use of organisational systems.
- Hosts and network resources are continuously available to authorised users.
- Increased security by detecting weaknesses in systems and network design early.

All systems accessible from the internet or by the public must operate ISO approved active intrusion detection software during any time the public may be able to access the system.

All host based and network-based intrusion detection systems must be checked on a daily basis and their logs reviewed.

All intrusion detection logs must be kept for a minimum of 30 days.

Any suspected intrusions, suspicious activity, or system unexplained erratic behaviour discovered by administrators, users, or computer security personnel must be reported to the ISO which may report incidents in line with the respective policy.

5.8 Internet Security Policy

All connections to the Internet must go through a properly secured connection point to ensure the network is protected when the data is classified high risk and/or confidential.

5.9 Email Policy

Email equipment and messages are property of the Company.

Messages that are created, sent or received using the Company's email system are the property of the Company.

The Company reserves the right to access and disclose to relevant entities the contents of all messages created, sent or received using its email system.

Users must be very careful when opening email attachments.

All email communication must be handled in the same manner as a letter, fax, memo or other

business communication.

Sensitive data in the email or any attachments must not be transmitted in clear text over the Internet.

Any urgent Virus warnings should be channelled to the Information Security Manager for verification of authenticity.

Email messages should not have any content that may be considered offensive or disruptive. Offensive content includes but is not limited to obscene or harassing language or images, racial, ethnic and sexual or gender specific comments or images or other comments or images that would offend someone on the basis of their religious or political beliefs, sexual orientation, national origin or age.

Employees may not retrieve or read email that was not sent to them unless specifically authorised by the Responsible Key Person or by the email recipient.

Employees may not execute attachments to emails received when these are executable files.

Company email may not be used for personal reasons.

5.10 Portable Computer and Media Policy

Personnel computers, laptops and workstations issued by the organisation are viewed as the company's assets and must be adequately protected.

Laptops, and their peripherals are popular targets for thieves. Since these assets are highly vulnerable to unauthorised access or theft, they present unique risks in the areas of disclosure, modification or destruction of proprietary information.

During the normal workday, whether working in an office or at an off-site location, employees are strongly encouraged to use a security cable to fasten the laptop to a desk, chair or other fixed object.

Employees should never leave a laptop on the desk, in the work area or in any other visible location overnight. Portable media should be locked in a secured area at the end of the workday.

When transporting a laptop or peripheral, employees should never leave it unattended in a visible location or in an unlocked vehicle.

When travelling with a laptop, never check it with other baggage.

In the event a laptop is stolen (regardless of where the theft occurs), employees should immediately file a police report and notify the Responsible Key Person immediately. A copy of the police report should be submitted to the Information Security Manager/ Management Team.

All assigned laptops, peripherals, related equipment and media remain the property of the company and are to be returned upon request, or when a staff member leaves.

All of the organisation's owned or leased facilities, equipment, related components and resources should be protected from unauthorised physical access, damage, loss from theft or other risks.

All media that becomes obsolete such as PCs, hard-drives, USB memories, CDs must be handed in to the Information Technology & Technical/ Management Team for proper disposal in accordance with the media disposal policy.

Adequate building security should be provided, and all facilities should be well-maintained, clean and free from safety or fire hazards.

Users must ensure that their portable PC is securely stored when not in use.

When outside of the office, employees should avoid leaving their PC unattended in their car. If it is inevitable to leave a PC in a car, it should be stored out of sight, e.g. in the boot.

PCs must never be left unattended while travelling on public transport.

5.11 System Security Policy

All systems connected to the Internet should have a vendor supported version of the operating system installed.

All systems connected to the Internet must be current with security patches.

System integrity checks of host and server systems housing high risk data should be performed.

All player activity shall be communicated over a secure communication protocol.

5.12 Redundancy and Failover Process to Prevent Denial of Service

To ensure that the failure of any single system component does not result in a denial of service (DoS) or disrupt critical operations, this section outlines the redundancy and failover processes implemented across the Technology Platform.

1) Redundancy and High Availability

The Platform is designed with redundancy at multiple levels, including infrastructure, network, and application layers. The following measures are in place:

- The platform uses multiple servers in a load-balanced configuration. In the event of a failure of any individual server, traffic is automatically redirected to other operational servers to maintain service availability.
- Databases are replicated across multiple nodes. Should a primary database node fail, the system will automatically fail over to a secondary node to ensure data accessibility and minimise downtime.
- Redundant network infrastructure, including switches, routers, and internet connections, is in place to prevent network-related failures from impacting system availability. If one network path fails, traffic is routed through alternative paths.
- The data centre housing the platform's critical components is equipped with uninterruptible power supplies (UPS) and backup generators to protect against power outages.

2) Failover Process

In the event of the failure of a critical component, such as a server, network device, or storage unit, the system automatically shifts operations to a redundant component without manual intervention. This ensures seamless service availability to end users.

Continuous monitoring tools are deployed to detect failures in real time. In the event of an issue, automatic alerts are sent to the IT team for immediate action. These alerts trigger the failover mechanisms as required.

Failover mechanisms are regularly tested to ensure they function as intended. This includes simulating failures of individual components and verifying that the system successfully transfers operations to redundant components without data loss or service interruption.

3) Disaster Recovery Process

In addition to redundancy and failover mechanisms, the Business Continuity and Disaster Recovery outlines the procedures for responding to more extensive failures or disasters.

6 ACCEPTABLE USE & ETHICS

1. Any computer resources must be used in a manner that complies with the Company's policies.
2. The company will monitor the use of office systems.
3. All control system events are logged.
4. Unauthorised access to office systems is an offence.
5. It is against our policy to install or run software requiring a licence on any computer without a valid licence.
6. Use of the Company's computing and networking infrastructure by employees unrelated to their positions must be limited.
7. Use of the Company's computer resources for personal profit is not permitted.
8. Decryption of passwords is not permitted, except by authorised staff performing security reviews or investigations.
9. All data contained on, or passing through corporate assets is subject to monitoring and remains the property of the corporation.
10. Under no circumstances is an employee authorised to engage in any activity that is illegal under local or international law while utilising company-owned resources.
11. Employees must not use company accounts to post publicly accessible messages or posts without permission.
12. Users are expressly forbidden to install any software on their workstations without prior approval from their supervisor.
13. Portable personal media should not be connected to company equipment and should not contain company documents.
14. Users may not perform vulnerability scans, monitor network traffic, or perform any action that is designed to escalate privileges or gain access to information that was not expressly intended for them.
15. Users must not reveal any information about company clients, employees, business practices, technology, schedules, or any other information not already publicly available to any outside resource or person without expressed permission from their supervisor.

16. Users must not use their company email accounts for purposes other than the conduct of company business. Forbidden actions include any and all forms of harassment, phishing, solicitation, spamming, forwarding chain letters and pyramid schemes, conducting personal business, and general personal correspondence.

6.1 *Firewalls*

All firewalls must be configured with a “Deny All” default policy. Only explicitly permitted traffic (both inbound and outbound) required for business operations shall be allowed.

Firewalls must filter both incoming and outgoing network traffic, restricting connections to only those that are necessary for business functions.

Devices within the same broadcast domain must not be able to establish alternate network paths that bypass the firewall. Network segmentation shall be enforced to ensure all traffic passes through the designated firewall.

Dedicated Firewall Operations

Firewalls must be dedicated to firewall operations only. No non-firewall related applications or accounts may be installed or maintained on firewall devices. Only authorized administrative accounts, as defined in the configuration baseline, may have access to firewall devices and applications.

Access Control

Firewall access is strictly limited to workstations that are part of the approved configuration baseline and authorized by the company’s change management policy. All access attempts from any other device or network segment must be automatically rejected. All administrative access to firewall devices must require strong authentication, and must be logged and monitored.

6.2 *Servers and Workstations*

Databases will only store entire credit card details if the company acquires a PCI compliance certificate. The company currently encrypts all credit card details stored in the database.

Publicly accessible web servers should be located on a network which is both logically separated and secured from the internal systems network.

Mobile computers that connect to the internet must have a personal firewall and up-to-date anti-virus software installed.

Antivirus scanners should be installed on all servers and workstations and should be updated with the latest virus definitions.

All development, testing, and production systems should be updated with the latest vendor security patches.

6.3 *Assets Deployment and Maintenance*

All changes to firewalls must be reviewed and authorised by the Information Security Manager and logged for future reference. Changes to the production environment should be authorised and logged before being implemented.

When an employee leaves the company, that employee's company user accounts and passwords should be immediately revoked.

Remote maintenance accounts should be enabled when needed and disabled when the maintenance process is completed.

Access to sensitive data should be logged where practically possible.

Successful and unsuccessful login attempts and the accessing of the audit logs should be logged.

System clocks should be synchronised, and log files should contain date and time stamps.

The firewall, router, and wireless access point logs should be regularly reviewed for unauthorised traffic.

Audit logs should be regularly backed up, secured, and retained for at least three months online and one year offline for all critical systems.

Wireless analyzers should be periodically run to identify all wireless devices.

Vulnerability scans or penetration tests should be performed on all applications and systems before they are put into a production environment. Before going into production, all devices must undergo a lockdown procedure where unnecessary or default services, protocols, settings, accounts, and passwords are changed or disabled.

Only secure, encrypted communications should be used for remote administration of production devices.

6.4 *Physical Security and Access Control*

Multiple physical security controls should be implemented to prevent unauthorised access to data centres.

Equipment and media containing sensitive information should be physically protected from unauthorised access.

The distribution and disposal of backups and other media containing sensitive information should be in accordance with a procedure approved by the Information Security Manager.

Media that contains sensitive information should be inventoried and securely stored.

Media that contains sensitive information should be deleted, shredded, or degaussed before disposal.

6.5 *Wireless Communications*

All wireless access points must be configured with encryption, MAC filters, or technology

that limits access to those devices that are explicitly authorised.

Networks with wireless access should be separated by a firewall from networks that handle sensitive information.

Wireless access points that support WPA2 should be configured to use it.
Wireless communications should be encrypted with WPA2, or 128-bit SSL.

6.6 *Clean Desk and Clear Screen Policy*

Clear desk and clear screen policy used to reduce the risks of unauthorised access to, or loss of, or damage to, information.

Ensure that appropriate facilities are available in the office in which, depending on their security classification, computer media (disks, tapes, CDs) and paper and paper files can be stored and locked away, including in lockable pedestals, filing cabinets and cupboards.

Personal computers should be locked when not in use and should be password protected.

Everyone should be required to use a password protected screen saver that automatically fires up after only a few minutes of inactivity.

Incoming and outgoing mail collection points should be protected or supervised so that letters cannot be stolen or lost, and faxes and telexes should be protected when not in use.

All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

7 Security in Supplier Relationships Policy

7.1 *Purpose*

The purpose of this policy is to ensure proper protection of the Company's assets that are accessed by suppliers.

7.2 *Scope*

This Security in Supplier Relations Policy applies to all business processes and data, information systems and components, personnel, and physical areas of the Company.

7.3 *Policy*

Information Security in Supplier Relationships:

- Procedures surrounding risk mitigation of a supplier's access to the Company's assets must be documented, reviewed, and agreed upon by the Company and the specific supplier.
- All suppliers that access, process, store, or provide various IT components must be in agreement with the Company's security requirements around suppliers' relationship with the assets.
- Types of information access should be defined that different types of suppliers will be allowed, as well as monitoring and controlling the access
- Types of obligations applicable to suppliers should be defined to protect the organisation's information.
- Security requirements agreements for suppliers must also include details on addressing risks surrounding the handling, processing, and communicating of assets or services.
- Processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
- Legal and regulatory requirements, including data protection, intellectual property rights, and copyright, etc. should be clearly identified and addressed.

7.4 *Supplier Service Delivery Management:*

- A process must be developed to monitor and assess the service delivery of a supplier to ensure it is meeting appropriate business and security requirements, as well as meeting any contract or SLA requirements.
- A change management process must be in place to address any alterations to an existing policy, including documentation of said change and ensuring it is in alignment with business processes and follows appropriate re-assessment of risk involved, if necessary.
-

8 Third Party Access Policy

Third parties occasionally conduct business/provide services to the Company and thus require network communication. Access is only given to third parties after request is received from one of the company Executives who must also specify the level of access required by such person which must be assigned by the Chief Technology Officer.

The following guidelines apply in giving access to third parties:

- The third party must be covered by a contractual undertaking which binds the third party to security measures which are equivalent to the measures specified within the security policies of the company. Where no such contractual undertaking is present, the third party must sign a declaration confirming acceptance of the security policies of the company.
- Access to third parties must respect data protection laws. The third party shall only be given access to the databases of the company where it is absolutely necessary for the third party to have access to them given the nature of the work and service the third party must provide to the company.
- Where a third party requires a remote connection to the company's network the remote access policy shall be read in conjunction with this policy. The third party's access shall be closely monitored and removed immediately when the purpose for which it was given has been exhausted.
- All third party network connections will be reviewed on a yearly basis and information regarding specific third party network connections will be updated as necessary. Obsolete third party network connections will be terminated immediately.
- Third party access to contracted service providers must be terminated as and when software contracts are terminated/expired.
- The services, reports and records provided by the third-party service providers will be monitored and reviewed at least annually or as required by the regulator.

8.1 Document, Equipment and Media Disposal

The company hardware and media is co-located on the premises of hosting and cloud service providers. This document explains the company's procedure to make sure that information is not made available to unauthorised personnel in case any equipment / media is to be removed from the premises mentioned above or in case that a piece of equipment is to be made entirely redundant.

Equipment / Media containing confidential data must be marked "Confidential" to indicate this without requiring it to be read.

8.2 Faulty Equipment / media located at the ISP

If any equipment / media is faulty it will have to be replaced, the ISP will be providing such equipment. Changes will be carried out by authorised personnel at the ISP and if need arises by an appointed third party authorised personnel. Personnel authorization forms will be provided and kept up to date with the ISP to ensure that only authorised

persons can enter the data centre and work on the company's servers. In case faulty hardware/media will cause non-compliance with the law and/or local regulations, the Responsible Key Person and the appointed third party authorised personnel shall have 24 hour access to the data centre. The regulator may be informed that the incident will cause non-compliance with the law and/or local regulations through the submission of an incident report within 24 hours after the incident. If any equipment needs to be removed from the data centre then the approval of the Responsible Key Person must be sought. Any equipment /media that is to be removed from the data centre falls under the Responsible Key Person's care and custody.

Hardware / media that has been cleared for removal from the data centre and for its subsequent disposal/recycling is to first be checked to ensure that it contains no data or information; it will then be safely stored in a locked cabinet in Malta under supervision of the Responsible Key Person. The Responsible Key Person will then be responsible for the full disposal/recycling. Hardware / media will be demagnetized / degaussed prior to manual disposal / recycling. Any failing hard drives will be immediately exchanged for new hard drives. Failing hardware / media that does not contain any data will be destroyed and disposed of / recycled. If any equipment is to be installed to replace the faulty equipment the installation will be completed to allow the operation to continue.

9 Report Requirements

This section outlines the security, access control, and retention protocols for reports stored on our electronic retention system. All reports generated, stored, and accessed via our systems must adhere to the following requirements to ensure integrity, security, and traceability.

9.1 *Version Control and Integrity*

All reports stored in modifiable formats must be configured to retain the original version along with all subsequent versions reflecting any changes. A unique verification signature must be generated and maintained for each version of the report, including the original version, to ensure its authenticity and integrity.

9.2 *Change Logging and Traceability*

The electronic retention system must maintain a complete change log for all reports, documenting the following:

- Who made the changes (tracked via user ID)
- When the changes were made (recorded by date and time)

This change log must be readily accessible for audit purposes and must reflect all alterations made to any version of the report.

9.3 Indexing and Identification

Reports must be indexed in a way that allows for easy identification and retrieval. The system must provide fields for, at a minimum, the following data:

- The date and time the report was generated
- The application or platform used to generate the report
- A title and description of the report
- The user identification of the person generating the report
- Any other relevant information that aids in the identification of the report and its purpose

9.4 Access Controls and Modification Restrictions

Access to modify or add reports to the Platform must be restricted to authorised users through logical security measures (e.g., user-specific accounts with limited privileges). Users without the appropriate permissions must not have the ability to modify, delete, or create new reports.

9.5 Administrative User Activity Monitoring

The system must be configured to provide a complete audit trail of all administrative user account activity. This includes:

- Actions taken by users with elevated permissions (administrators)
- Changes made to system settings or report configurations

The monitoring records are:

- Generated in each critical component of the Platform to monitor and rectify anomalies, failures and alerts;
- Stored for an appropriate period to assist in future investigations and access control monitoring;
- Protected against tampering and unauthorised access; and
- Reviewed periodically using a documented process.

9.6 Logical Security Measures

Logical security must be enforced to safeguard the electronic retention system, including:

The use of individual user accounts with appropriate access levels

- Maintenance of event logs with appropriate levels of detail (including access attempts and actions performed)
- Version control documentation to ensure that all changes to reports are tracked accurately

9.7 *Physical Security of the Retention System*

All components of the electronic retention system must be physically secured in an appropriate environment to prevent unauthorised access or tampering. This includes, but is not limited to securing servers and storage devices in controlled access data centres.

9.8 *Data Availability and Redundancy*

The retention system must be equipped with hardware and software redundancies to prevent disruption of report availability. Measures must include:

- Regular backups to secure, redundant storage locations
- Best practices for disaster recovery to prevent data loss in case of system failure or security incidents

9.9 *Backup and Disaster Recovery*

Reports must be included in the Company's Business Continuity and Disaster Recovery Policy. This includes maintaining:

- Regularly scheduled backups of all report data and metadata
- Secure off-site storage or cloud redundancy
- Testing of backup restoration procedures to ensure data can be recovered promptly in case of data loss or system failure