

Combobed N.V.

Policy No.: ISS-001CB

Date of Issue: 01-06-2022

Information Security Policy

- CONFIDENTIAL -

Introduction and Scope

The Information Security Policy (hereinafter - IS Policy) determines the scope of the Information Security Management System (ISMS) of Combobed N.V. (hereinafter - Company) and implements a set of policies and procedures for systematic management of Company data and provision of Company services.

This policy applies to all employees, contractors, partners, and any other individuals or entities with access to the Company information systems and data. This Policy encompasses all information assets, including data, systems, networks, physical and virtual environments, and third-party services used for information processing and management of Sportsbook solution and platform (hereinafter- Sportsbook) traded by the Company, and where applicable other Company related information systems as denoted from time to time in this IS Policy or documents related thereto.

Sportsbook is a mission-critical information system, developed, operated and regulated by applicable law. Due to its significance and the strict regulatory environment, the Sportsbook is subject to enhanced security measures, including stringent access controls, continuous monitoring, regular security audits, and data encryption. The IS policy contains special security requirements mandated by authorities or risk assessments in order to ensure compliance and protection against potential threats.

1. Normative references

ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements.

Applicable law of the jurisdiction where the Company operates.

2. Objectives

The purpose of the IS policy is to establish an Information Security Management System to ensure the appropriate protection Sportsbook related information handled by computer networks and to:

- Protect the confidentiality of sensitive information;
- Maintain the integrity and reliability of data;
- Ensure the availability of information and systems when required;
- Comply with relevant legal, regulatory, and contractual obligations;
- Safeguard against unauthorized access and data breaches.

Information Security Management System established by this IS Policy consists of IS Policy and the policies listed below:

- Business Continuity & Disaster Recovery Policy;
- Change Management Policy;
- User Management Policy;
- Asset Management Policy;
- Internal Audit Policy;
- Outsourcing Policy;

as well as procedures issued based on the above listed policies and further internal organizational documents as applicable from time to time.

3. Responsibilities

The CTO has been entrusted with direct responsibility for maintaining this IS policy and providing advice on information security and guidance on its implementation. CTO shall review the IS Policy at least once every year or more frequently, if necessary.

All employees have a responsibility to conduct themselves in an ethical manner. In particular:

- Data/information obtained inappropriately should not be used;
 - Finding a system weakness should be reported immediately and should not be taken advantage of;
 - Every user has a responsibility to carry out his/her work diligently and will be held accountable for misuse of the Company's information system and Sportsbook;
 - When the confidentiality of information is unclear, its classification should be ascertained;
- and
- Report any known violation or system weakness to the person or persons responsible for security.

4. Security risk assessment

Risk of threats and vulnerabilities to the Company information and Sportsbook can never be fully eliminated. An element of risk however remote is always present.

Risks can however be significantly reduced – by carrying out an information security risk assessment. Information security risk assessment is carried out according to the Technical Risk Assessment procedure.

From the information gathered, risks need to be identified, quantified, prioritized and action mitigation controls have been determined and implemented to protect against and reduce risks.

The controls covered by this Policy and Technical Risk Assessment procedure reduce the risks to an acceptable level for the business.

The Company monitors its risk mitigation plan periodically and performs annual security risk assessments to address any changes in the risk levels or security requirements.

5. Data Classification, Data processing integrity and monitoring

5.1. Data Classification

Company information has varying degrees of sensitivity and criticality. The higher the value of the Company information and the higher the sensitivity, the greater the security required. Company information must first be valued. Once a value has been given, a classification can be established and a corresponding security level can be identified and implemented.

In order to determine the asset value, the following factors shall be taken into consideration:

- the level of sensitivity and confidentiality of the information;
- the associated business impact;
- the potential financial implications;
- the business needs for sharing or restricting information.

All Company data is divided into the following four sensitivity classifications:

- **Restricted**
- **Confidential**
- **Internal**
- **Public**

Restricted: These are information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Data covered by state legislation, such as the Data Protection Act or other applicable personal data protection laws and regulations, are in this class. Payroll, personnel and financial information are also in this class because of privacy requirements.

Confidential: Data that would not expose Company to loss if disclosed, but that the data owner feels should be protected in order to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements.

Restricted and **Confidential** information if disclosed would significantly impact the business.

All **Confidential** information sent to the competent gaming authorities that have jurisdiction over (or are responsible for or involved in the regulation of) gambling or gambling activities of the Company (hereinafter – Gaming authority) must be marked as so.

Internal: Company Information marked as Internal should be adequately secured. Internal information can be shared internally but not externally.

Public: Company information which can be shared externally. Information may be handed to anyone.

Before any computer storage media is sent to a vendor for trade-in, servicing, or disposal, all Company Restricted, Confidential and Internal information must be destroyed or concealed according to methods approved by the CTO.

Any documents sent to a Gaming authority, must be properly marked with the appropriate data classification.

Any Restricted, Internal and Confidential documents should be stored in a safe place, or in a cabinet which is locked and only accessible to authorized people.

5.2. Data processing integrity

Company is committed to maintaining the accuracy, consistency, and reliability of the data, thus ensuring the integrity of its data processing activities, maintaining user trust, complying with regulations, and providing a reliable and secure environment for sports betting.

The Company ensures that data is collected from trustful resources and where possible verified by the competent employees. Data relating to the Sportsbook is collected from the following sources:

- User bets are provided by the operators,
- Odds data feeds and/or Sporting event outcomes and/or platform services are provided by the contractors outsourced based on the Outsourcing policy of the Company.

Sportsbook related data is stored in a secure and organized manner, adhering to relevant data protection regulations. Encryption and access controls are employed as per this policy and other Company policies to prevent unauthorized tampering or modifications. To ensure accuracy and consistency of data, the Company verifies odds data and event outcomes to identify discrepancies or anomalies. Data is backed up in accordance with the Data Backup procedure of the Company.

6. Monitoring

The Company must inform itself of the current threats and risks to the security, integrity, and availability of the Sportsbook related betting systems and related components that they operate or supply.

Monitoring and testing shall be performed throughout the life of the Sportsbook to ensure they are operating as approved.

The Company ensures proactive monitoring of the Sportsbook and related components.

The Company employs a sophisticated proactive monitoring and testing approach to ensure the seamless functioning and integrity of the Sportsbook and its related components. Through advanced monitoring tools and automated alerts, the Company continuously oversees every facet of the Sportsbook, including detection of any errors or bugs. This vigilant oversight allows the Company to swiftly identify and address any anomalies, errors, or irregularities that may arise. In particular, the Company performs server performance monitoring, application performance monitoring, log analysis and monitoring, security monitoring, patch and update management, vulnerability scanning, configuration management, user and access monitoring and other monitoring and testing as specified in this Policy or as may from time to time be determined by the CTO to ensure the platform operates as approved.

Specific monitoring process is provided in detail in the Business Continuity and Disaster Recovery Policy.

7. User Management

All access to Company information, resources and services as well as physical access shall be restricted and controlled. Access to Sportsbook system documentation, software applications and hardware infrastructure shall be restricted. Access to logs, personal data, business sensitive information and to intellectual property (“IP”) shall be strictly restricted, assigned on a need-to-know basis and controlled according to risk assessments and relevant law.

All Users shall be assigned access rights to any Company information or information system, including Sportsbook, based on the need-to-know access control principle. Access rights shall be assigned, audited, and removed through an access control procedure ensuring that access to Company information, whether personal or non-personal, Sportsbook resources and services is allowed only on need-to-know or need-to-use basis.

Users shall only be provided with access to the Company premises, information, resources, networks, network services and other services which they have been specifically authorized to use. The assessment of the level of access to grant a particular User shall be based on the following factors:

- risk assessments including any risks associated to;
- insufficient confidentiality, integrity, and availability of information;
- assessments of traceability of resources;
- assessment of the possibility of violation of privacy;
- assessment the possibility of violation of intangible rights.

The role of the User and the nature of the role shall also be factored in.

Users shall be required to sign their contract of employment or for the provision of services in the case of third party staff members and sub-contractors which shall contain adequate confidentiality provisions and provisions related to confidentiality, prior to being provided with any access rights.

In the event that a subcontractor/third party staff member is an organization, any agreement must be signed by its legal representatives. The employees of that organization might be asked to sign a separate non-disclosure agreement and/or data controller-processor agreement prior to being granted access rights.

7.1. User Accounts

Any access to Company information shall be limited via user accounts. User account opening and assignment of access rights for new Users shall be determined, and provided in accordance with User Management Policy.

Users who move cross-functionally, change duties or employment status within the Company shall be immediately removed of their old access rights, if they no longer require the same level of access and granted new access rights based on the need-to-know principle. These changes are to be logged and retained in accordance with User Management Policy.

Users who resign or are released by the Company shall have all their physical, IT, and any other access rights terminated prior to physically exiting the Company premises. Process of termination of user accounts and accesses shall be determined by the User Management policy. Access can only be re-enabled upon approval from the designated member at that period of time by the CTO and COO.

7.2. Authentication and password management

All Users must input a unique User ID and a password in order to be able to access the Company's systems. The following issues shall be addressed in User management policy:

- Unique User ID and password requirements;
- Password system setup;
- Choice and management of passwords;
- Storage of passwords and other authentication data;
- Group logins;
- Loss of the password;
- Session time- out.

8. Access control

8.1. Restricted Physical Access & Controls

Certain areas both within the Company offices and outside the main offices (“Premises”) may be considered more security sensitive than others, such as the server locations.

The Company shall ensure that any service providers hosting key technical setup, or otherwise providing access thereto, are instructed to permit and assist the relevant gaming supervision authority, if required, in checks which the respective Gaming authority may perform according to the applicable law.

Authorisation levels and access rights to Company offices are administered and approved by CTO.

Physical access to the Company’s offices has been controlled by means of the following **measures**:

- Minimum entry points;
- Access card;
- Locks on doors and cabinets.

The Company Premises will be **monitored** with security cameras all times and the footage shall be retained for a limited defined period, after which it shall be properly disposed of in accordance with this Policy (see “Disposal” below). The security cameras will cover the entire area of the premises, with the exception of the restrooms and other areas prohibited by law from being monitored. Appropriate standard operating procedures will be applied to all security camera equipment and applications to ensure effective and ethical management of the equipment as well as appropriate maintenance of the footage by authorized users. The Company will ensure that the below measures are taken in relation to the installation of the security cameras within the Premises:

- All security cameras will be installed in secure areas within the Company Premises;
- Easily visible signs shall be placed in all monitored areas;
- Access to the security camera equipment and footage will be restricted to authorized users;
- The footage will be processed and retained in accordance with data protection legislation and will only be accessed in the event of a security investigation.

The Company acknowledges that the security cameras may also capture and record the movements of its employees during working hours. To this effect, the Company will ensure that all employees will be adequately informed and will obtain the necessary consents from the same for the processing (capture) of their images.

The Company shall regularly monitor the security camera equipment to ensure that each security camera is still appropriate for the task as well as to effect any changes to the positioning of the same following any modifications carried out to the areas/building.

Tracking and monitoring of physical access to the Premises is provided by:

- security cameras;
- the verification of visitors' identity and entry into the premises;
- the logging of exit and entry details from the access card;
- monitoring of network access.

All Company employees shall be trained and fully aware:

- To report any suspicious activity to their manager;
- To escort their visitors throughout the duration of their visit;
- To shred all confidential documents upon completion of the task;
- To authorize and record all movement of material entering and leaving the premises;
- To forbid tail-gating;
- Not to permit photos taken in server facilities;
- To keep their access cards in a safe place when they are not within the Company Premises;
- To report lost or presumably stolen access cards immediately in accordance with the Company's escalation procedure;
- Not to permit others, including other employees/colleagues to use their access card.

8.2. Visitor Physical Access

Visitor access to the Company's Premises is strictly controlled.

Visitors will have to report to the reception area of the Company's offices to gain entry. Entry to the reception area from outside is controlled by the receptionist. Entry within the offices beyond the reception area is not possible until a visitors' badge is issued. Issuing and logging of the visitor is performed with the receptionist. On leaving the company, visitors are logged out and the badges are collected.

8.3. Remote Access to Company information systems for Users

Remote access is any access from outside the system or system network of any information system used by the Company. Remote access provides a similar experience to "working from the office". Remote access may be granted both to employees of the Company and third parties as may be applicable from time to time. Different requirements of remote access apply to access to general Company information and Sportsbook.

Use of any services, solutions or integrations providing remote access to any information system must be approved in advance by CTO. Any remote access must be carried out using a safe method and have an option to be disabled. Unauthorized usage of any remote access solution or tool installed as a hardware/software or built-in in a code is strictly prohibited.

8.3.1.Remote access to general Company related information

Subject to the terms of this Policy, as part of the Company's commitment to secure and efficient operations, however outside the scope of Sportsbook, Company utilizes reputable SaaS (Software as a Service) platforms for collaboration and data storage. These platforms have been evaluated and approved by the information security team, and their use is authorized without the need for VPN access. Access to these SaaS services through their publicly available interfaces is permitted with a Company user account, provided that all users adhere to the Company's IS Policy.

Remote access to Company's information systems (e.g. Jira, Confluence etc.) by Users may be allowed after applying the adequate protective measures in accordance with the results from the Company's information classification or risk assessment.

Remote access to Company's information systems of each User is approved by the CTO. In case of any security concern or when the account is no longer needed, remote access must be disabled entirely or on a per-user or per-service basis.

8.3.2.Remote access to Sportsbook

In order to access Sportsbook related information, once connected the User is placed on the corporate network via a virtual private network ("VPN") connection using the approved VPN client with strong encryption, multi-factor authentication (MFA), and secure tunneling protocols. VPN access codes must be changed at least weekly.

Remote access connections to Sportsbook related systems must be permitted only through firewall configurations and system settings that are explicitly defined and approved by the CTO. Unapproved connections or modifications to firewall rules are not allowed.

Remote access to the Sportsbook related systems must be limited to the necessary functions required for the user to perform its work. Access to non-essential systems, applications, or data is prohibited, and any unauthorized access attempts must be blocked and reported.

Remote access to Sportsbook related systems may be provided to authorized members and representatives of the Gaming authorities, when requested or when necessary and if required by the applicable laws, regulations and/or binding standards of the jurisdiction where the Company operates or by court order within the limits as defined in the specific court order.

Suppliers may be granted remote access to the Sportsbook system and its associated components only with explicit authorization from the CTO. This access is typically granted for Information Systems support and maintenance, including updates and enhancements.

All third party accounts used for remote access to the Sportsbook related systems must be continuously monitored by the team responsible for the system under maintenance. Monitoring includes tracking user

activity and ensuring that access remains within the approved scope. All third-party accounts are managed in accordance with the User Management Policy.

The remote access service (“VPN”) must maintain an automatically updated activity log file, which records all remote access activities. The log file must include the following details:

a) User Identification: The log must capture the identification of all users who perform or authorize remote access, ensuring accountability for all remote access activities.

b) Connection Details: The log must record remote IP addresses, port numbers, protocols, and, where possible, MAC addresses used during the remote connection. This information is crucial for auditing and identifying the source of access.

c) Connection Timing: The log must include the date and time the connection was made, as well as the duration of the session. This helps in tracking and correlating remote access activities with specific events.

All target systems must be capable of conducting the audit trail detailing the activities performed while logged in, including specific areas accessed and any changes made to the system, applications, or data. This level of detail is necessary for forensic analysis and incident response.

8.4. Logon/Logoff Process and monitoring of the usage of system and administrator accounts

All users must be positively identified prior to being able to use any Company multi-user computer or communications system resources.

In case for rooms with a single occupation, the room has to be locked. In case a user forgets to lock their computer, if there has been no activity on a computer terminal, workstation, or personal computer for a certain period of time, the system must automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the user has provided a valid password. The recommended period of time is fifteen (15) minutes. An exception to this policy will be made in those cases where the immediate area surrounding a system is physically secured by locked doors, secured-room badge readers, or similar technology. All other users have to lock their computer whenever they leave their desk.

The Company employs a stringent procedure for monitoring the usage of system and administrator accounts to ensure robust security and accountability. This process involves monitoring that continuously track and log activities associated with these accounts. Usage patterns, access times, and actions performed are closely scrutinized to promptly detect any unusual or unauthorized activities. Regular audits (as determined by the CTO) are conducted to review the logs and assess compliance with established policies. In case of any suspicious actions or deviations, alerts are triggered, and immediate investigation and remediation follow based on **Incident Response procedure** of the Company. This systematic monitoring procedure not only safeguards sensitive data and critical systems from potential threats but also ensures that administrative actions are transparent, traceable, and aligned with the

company's security protocols. The Company has also implemented a whistleblower procedure which provides a procedure of reporting inappropriate use of administrator and system accounts by the Company employees and contractors.

9. General Endpoint Management

9.1. Desktop, Portable Devices, Storage Media and Peripheral Equipment

The Company may provide desktop as well as mobile devices including laptops, mobile phones, tablets and storage media (such as USB pen drives, DVD/CD, etc) (collectively “Devices”) to employees and other Users whose role requires usage of such. Users are able to access internal e-mail, calendars and contacts, as well as other resources and applications available on the internal network from mobile phones, tablets and laptops, as if they are accessing these from their desktops.

Each of these hardware Devices, including peripheral equipment such as printers and photocopiers, has the ability to create, receive, store, access or share Company Information.

Security measures for peripheral equipment include:

- Photocopiers, and printers or other Devices that store or transmit Confidential or Restricted information shall be placed in secure locations and monitored.
- All documents containing Confidential or Restricted information shall immediately be cleared from printers, copiers;
- Access to the settings of the peripheral devices is allowed only to persons designated by CTO.

Portable Devices present a special risk purely due to their mobility and as a result are vulnerable to theft (consequently to data theft) and loss. Therefore, the Company recognizes the importance and necessity of applying extra security measures to protect the Company Information stored within those Devices.

Users who are granted access to the Company’s network or Information Systems shall adequately secure their Devices from unauthorized access.

Best practice security measures implemented by the Company include the following safeguards:

- Devices should be locked when unattended;
- A password system must be used or PIN code must be activated on the Device to protect the contents of the same;
- Devices must be protected at all times from heat, cold, water, smoke, dust, physical damage and magnetic interference;
- Devices should not be used in public places to avoid situations where passers-by might have visibility of the contents of the display;

- USB Mass Storage Devices must be removed from the Device when not in use, stored securely, used for data transfers between other Devices only. Any USB Mass Storage Device must be wiped immediately after the data transfer is completed.
- The Company should be informed immediately if the Device is misplaced, stolen or presumed stolen. This would enable the Company to take the necessary immediate security measures to protect the Company Information stored on the Device, including remote Data Wipe-Out application.

The Company provides local and network storage within the organization to easily manage and store files, thus reducing the use of removable storage Devices for most day-to-day tasks.

Given the large amount of information which removable storage media Devices can store, the Company has defined additional controls to minimize risks.

The Company only allows the use of removable storage media Devices in instances when large amounts of information need to be shared internally or externally. In these cases, the following requirements need to be met:

- Approval needs to be obtained from the CTO;
- Data can only be stored in a Company provided storage device.

The Company does not encourage the use of online file hosting services unless approved by the COO/CTO to reduce risks. Users shall be unable to download such applications onto the company-owned Devices as this functionality will be disabled.

Use of any services, solutions or integrations providing online file hosting services must be approved in advance by CTO. Unauthorized usage of any online file hosting solution or tool installed as a hardware/software or built-in in a code is strictly prohibited.

9.2. Downloading of Data

Electronic Mass Data Transfers: Downloading and uploading Restricted, Confidential and Internal Information between systems must be strictly controlled.

Other Electronic Data Transfers and Printing: Restricted, Confidential and Internal Information must be stored in a manner inaccessible to unauthorized individuals. Restricted information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise.

9.3. Computer Viruses, Worms, and Trojan Horses

The Company is very well aware of the threats and risks that malicious software including viruses, worms and trojan horses, can cause to its systems. The Company shall implement the necessary perimeter

network controls to prevent or minimize the risk of penetration of the Company's network from the outside. Some of the measures taken by the Company include: antivirus applications, firewalls, strict IP whitelisting, VPNs, port knocking and encryption. The Company shall also use intrusion detection and intrusion prevention systems.

Approved and current virus-screening software against viruses, spyware, rootkits and other security threats must be enabled on all Company computer systems and servers. This software must be used to scan all software coming from third parties or other departments and must take place before the new software is executed. Users must not bypass scanning processes that could stop the transmission of computer viruses. It also ensures that the firewall is active and working efficiently to protect against network layer threats.

The willful introduction of computer viruses or disruptive/destructive programs into the Company's environment is prohibited, and violators may be subject to prosecution. Desktop and laptop computer users shall not write, compile, copy, knowingly propagate, execute, or attempt to introduce any code designed to self-replicate, damage, or otherwise hinder the performance of any computer system (e.g. virus, bacteria, worm, Trojan horse, or the like).

Suspected viruses should be reported immediately to the CTO. The Company shall immediately inform the relevant authorities, if required, as soon as malicious code or suspicious codes are discovered in the system. The Company shall also take the necessary immediate steps to ensure that the malicious code does not affect the Company's systems and the Company Information stored therein.

The employee designated by the CTO shall be responsible for eradicating viruses from all personal computer systems. As soon as a virus is detected, the involved user must immediately follow the Incident Response procedure to assure that no further infection takes place and that any experts needed to eradicate the virus are promptly engaged.

Company's computers and networks must not run software that comes from sources other than business partners, knowledgeable and trusted user groups, well-known systems security authorities, computer or network vendors, or commercial software vendors. Software downloaded from electronic bulletin boards, shareware, public domain software, and other software from untrusted sources must not be used unless it has been subjected to a rigorous testing regimen approved by the CTO.

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 where such capabilities exist. Incoming and outgoing emails shall be scanned for viruses and any email attachments shall be scanned for spyware or adware applications. The Company shall ensure that the antivirus/antimalware protection will run continuously and will automatically update virus definitions and software as well as generate audit logs.

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

9.4. Disposal of Media & Equipment

The disposal of electronic records stored on media, computer equipment, and computer software can create information security risks. These risks are related to the potential unauthorized disclosure of Company Information, violations of software license agreements, and unauthorized disclosure of intellectual property that could be stored on storage media, computer equipment, and computer software.

This Policy governs the requirements of secure disposal of media containing Company Information, as well as the secure disposal of Company Information stored on other equipment, by establishing a process which ensures the secure removal of sensitive data or protected information from storage media or from the equipment, prior to disposal.

This Policy covers all fixed and removable storage devices and all equipment such as Devices owned by the Company. This includes, but is not limited to: magnetic media (including fixed disks and other removable drive disks), optical disks, non-volatile memory devices (including memory sticks and cards or USB memory storage), PDAs, laptops, desktops. Any storage devices or Devices currently available, or which may become available in the future due to new technology, are also covered by this Policy.

The CTO shall assign the responsibility of disposal to a member of its staff with a suitable level of authority who shall authorize the disposal and shall be responsible to maintain a full inventory of all equipment including media which has been marked for disposal;

The responsible person will opt for the appropriate disposal methods upon taking into consideration the security vulnerabilities associated with each method;

All electronic Devices and media equipment, including storage media in personal computers and other hardware containing Company Information, must be degaussed (demagnetised) prior to disposal so that the data will not be retrieved and reused. The sanitisation methods used will depend on the type of media and the intended disposal of the media. Non-functioning and/or non-writable media containing Company Information must be physically destroyed if degaussing or other sanitisation is determined to be inadequate.

Disposal of media requires authorisation and tracking by an employee designated by CTO. Where possible, destruction will be performed on-site. Damaged media and drives cannot be sent for repair and must be physically destroyed. All methods of media disposal shall be in compliance with information security best practices and as per Asset removal policy.

The Company reserves the right to either internally re-deploy Devices especially desktops, laptops and mobile phones or donate/sell them to third parties outside the organization, instead of destroying them. The Company shall however make sure that all Company Information including any software and any other residual data are properly deleted from the Devices prior to the redeployment, donation or sale.

10.Logs and event management

10.1. Host Intrusion Detection

Intruder detection is implemented on all servers and workstations that are related to Sportsbook and containing data labeled as Restricted.

Logon attempts to connect with the Company Information Systems must be logged. Sportsbook operating system and application software must also have logging enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems should be enabled.

These logs will be checked on a regular basis; server, firewall, and critical system logs reviewed frequently, automated review enabled and alerts should be transmitted to the IT Department when a serious security intrusion is detected.

Whenever a system is suspected of compromise, the involved computer must be immediately removed from all networks, and procedures followed to ensure that the system is free of compromise before reconnecting it to the network.

After either a suspected or demonstrated intrusion to the Company computer system, the IT Department must immediately notify the system's users that an intrusion is believed to have taken place, and that the status of all passwords on that system must immediately be changed to expired, so that these passwords will be changed at next log on.

10.2. Event Logging

To the extent that systems software permits, computer and communications systems handling Confidential and Restricted information and the Sportsbook must securely log all significant security relevant events. Examples of security relevant events include users switching user IDs during an online session, attempts to guess passwords, attempts to use privileges that have not been authorized, modifications to production application software and data, modifications to system software and data, changes to user privileges, and changes to logging system configurations.

Records reflecting security relevant events must be periodically reviewed in a timely manner by computer operations staff, information security staff, or systems administration staff.

The firewall has an extensive logging mechanism itself, logging all unauthorized login attempts. The firewall applications shall maintain audit log files, disable all communications and generate an error warning if the log file becomes full. The log file shall include the following information:

- a) date and time of all records;
- b) all firewall configuration changes;

- c) all connection attempts, whether successful or not, through the firewall, and
- d) source and destination remote IP addresses, port numbers, protocols and where possible MAC addresses.

10.3. Event Management

All security-related logs, including network, system, and application logs, must be centrally collected and stored in the Security Information and Event Management (SIEM) system. The SIEM system should aggregate logs from various sources, ensuring data integrity, confidentiality, and retention as per regulatory and organizational requirements.

The SIEM system must process collected logs using predefined correlation rules to detect potential security incidents. These rules should be based on known attack patterns, anomalies, and behavior analysis, ensuring timely identification of threats. Detected events should be automatically flagged for further review and investigation by the security team.

All identified security events must be evaluated and processed in accordance with the organization's Incident Response Policy. Events should be prioritized based on their severity, and the appropriate incident handling procedure must be followed. Any escalated incidents must be reported immediately to relevant stakeholders and managed to resolution, with post-incident reviews conducted to prevent recurrence.

11. Network Security

11.1. Network Hardware

Routers and switches are located in the datacenter and must not be separately protected from being physically accessed without explicit permission.

The datacenters chosen by the Company must meet at least the following requirements:

- a) have a sufficient protection against alteration, tampering or unauthorized access;
- b) be equipped with a surveillance system;
- c) be protected by security perimeters and appropriate entry controls to ensure that access is restricted to authorized persons only and that any access and attempts at physical access are recorded in a secure log; and
- d) are equipped with controls to provide physical protection against damage caused by fires, floods, hurricanes, earthquakes, and other forms of natural or man-made disasters.

The above requirements do not require a separate checkup if the respective data center can present a valid ISO 27001 certificate.

Network switches should be used exclusively instead of hubs to manage internal network traffic. This ensures that network traffic is directed only to the intended recipient(s) and does not appear on links or devices for which it is not intended. Using switches helps prevent unauthorized access to network traffic and protects sensitive data from being exposed to unintended devices.

All management connections to network devices must be authenticated, authorized, and encrypted. This includes any administrative access to switches, routers, firewalls, and other network equipment. Access control lists (ACLs) or role-based access controls (RBAC) must be implemented to ensure that only authorized personnel have the necessary permissions to manage network devices. Plaintext protocols (e.g., Telnet) are strictly prohibited.

The failure of any single network component must not lead to a denial of service for the entire Sportsbook.

Any configuration change must be audited and logged. If the audit log is full, the NCE must disable communication or offload logs to a dedicated server for storage.

Network hardware and software must be protected from any programming skills initiated by a user on the server that could result in modifications to the database. Authorized maintenance of network infrastructure or troubleshooting of applications with sufficient access rights by network or system administrators is accepted. The network hardware must also be protected from unauthorized mobile code execution.

11.2. Connectivity and communication protocol

11.2.1. Communication between component of the system frontend and backend

Communication between frontend and backend components is managed using an authorization token system. Each request for a betting operation from the frontend must include a valid authorization token, which is verified by the backend. Tokens are being generated during the enrollment process and have expiration times to enhance security.

Each request for a betting operation must be additionally confirmed by the betting system on the operator's side. No frontend component must be capable of executing any valid betting operation without being registered in a betting platform and in a betting system as a valid system component.

11.2.2. Communication with CDN

To ensure secure communication within our system, all frontend components must communicate with the CDN (Content Delivery Network) exclusively over HTTPS. This requirement mandates that the frontend configuration is updated to utilize HTTPS URLs for all CDN resources. Additionally, the CDN must establish secure connections (HTTPS) when interacting with backend services. It is essential to implement and validate SSL certificates on the backend server to facilitate this secure communication. Each CDN and

backend component must process only the traffic which is attributable to the relevant components of the Sportsbook (this kind of authorization must be enforced by the usage of URL white lists) and complies to the protocol standards (this kind of compliance checks must be enforced with a relevant WAF rules) in order to prevent network intrusions, interference, interceptions and tampering.

11.3. Network Systems

The Company's network systems are protected by firewalls, whitelisting, public key only mode of authentication, passwords and authentication requirements, VPNs and encryption.

Access to the Sportsbook back office applications shall also be restricted to authorized employees and shall be given on a need to have basis. This ensures that nobody has more access rights than what is needed to carry out their duties.

Workstations (end-user devices) must be separated from server subnets to minimize the risk of unauthorized access and lateral movement within the network. This segmentation ensures that compromised workstations do not provide a direct path to sensitive server resources, thereby protecting critical systems and data.

Production subnets must be isolated from beta and pre-production subnets. This separation prevents untested or potentially unstable pre-production applications and environments from affecting the stability and security of production systems. It also ensures that sensitive production data remains secure and is not exposed to less secure or less monitored environments.

Network segmentation must be implemented using firewalls, WLANs, and other network security controls to enforce strict access controls between different subnets. Access between segmented networks should be limited to only what is necessary for operational purposes and must be monitored and logged. Access control lists (ACLs) should be used to restrict traffic between segments to authorized connections only. Any communication between workstation subnets, server subnets, and different environment subnets (production vs. beta/pre-production) must be explicitly defined and justified.

All network devices and services must be protected against unauthorized access. Unused services and ports on network devices must be disabled.

The primary virtual machine(s) and its replica must be physically separated across hypervisors. The master and slave may operate on the same cluster of hypervisors.

Stateless protocols (e.g., UDP) should not be used to transmit sensitive information without stateful transport. HTTP is permitted when using TCP.

All changes to the network infrastructure must be recorded in a log.

Antivirus scanners and detection programs must be installed and regularly updated across the entire platform.

11.4 Intrusion Detection/Prevention System (IDS/IPS):

The IDS/IPS must be configured to detect patterns and traffic anomalies indicative of Distributed Denial of Service (DDoS) attacks. Upon detection of such attacks, the IDS/IPS shall immediately initiate predefined mitigation strategies to minimize impact and maintain network availability.

The IDS/IPS must continuously monitor for shellcode or malicious payloads attempting to traverse the network. The system should be able to detect and prevent the execution of any network traversal shellcode, thereby protecting against unauthorized remote access and code execution.

The IDS/IPS must be capable of identifying ARP spoofing attempts or ARP cache poisoning, which could be used to redirect network traffic or intercept communications. Upon detecting ARP forgery, the IDS/IPS must take immediate action to prevent the attack, such as alerting the network administrator and blocking the malicious IP addresses.

The IDS/IPS must detect indicators of Man-In-The-Middle (MITM) attacks, such as abnormal ARP requests, rogue DHCP servers, or suspicious certificate anomalies. If a MITM attack is detected, the IDS/IPS must immediately cease communication for the affected connection and alert network security personnel to prevent data interception or manipulation.

In addition to monitoring wired network traffic, the IDS/IPS must also extend its protective capabilities to Wireless Local Area Networks (WLANs) to ensure comprehensive network security:

a) Scanning for Unauthorized Access Points:

The IDS/IPS must scan for unauthorized wireless access points at least once every quarter. This includes the detection of rogue access points that could potentially be used to bypass network security controls or conduct unauthorized activities on the network.

b) Automatic Blocking of Unauthorized Devices:

Upon detection of unauthorized devices, the IDS/IPS must automatically block these devices from accessing the network. This includes rogue devices, unauthorized access points, or any devices that do not belong to the constantly maintained MAC address whitelist.

c) Maintenance of Historical Wireless Access Logs:

The IDS/IPS must maintain a comprehensive log of all wireless access attempts and activities for at least 90 days. This log must include details such as the device's MAC address, time of access, and duration of connection. Alternatively, the IDS/IPS may be configured to offload audit logs to a dedicated secure server. This offloading process must be automated and encrypted to prevent tampering or unauthorized access to log data. These logs are crucial for auditing, forensic analysis, and ensuring compliance with security policies.

11.5 Network Communication Equipment (NCE)

All NCE must be designed and constructed to withstand physical damage that may occur during normal use. This includes using robust materials and hardware components that are resistant to tampering, impact, and environmental factors. Furthermore, the firmware and software contained within the NCE

must be protected against corruption and unauthorized modification to ensure continued reliable operation and data integrity. No home appliance must be accepted for use in production environment. NCE must be physically secured to prevent unauthorized access. This involves implementing access controls such as locks, surveillance systems, and restricted access areas where the equipment is housed. Only authorized personnel shall be allowed to access these areas, and access shall be logged and monitored to detect and respond to unauthorized access attempts promptly.

System communication via NCE must be logically protected against unauthorized access. This includes implementing strong authentication mechanisms, encryption of data in transit, and network segmentation to ensure that only authorized users and devices can communicate with the NCE. All access to the NCE must be authenticated, and all communication must be encrypted using industry-standard protocols to prevent interception and unauthorized access.

NCE must maintain an audit log of all significant activities and events to ensure traceability and accountability. In the event that the audit log file reaches its capacity and there's no remote log forwarding implemented, the NCE shall immediately disable all communication to prevent unlogged access or actions. Alternatively, the NCE may be configured to offload audit logs to a dedicated secure server. This offloading process must be automated and encrypted to prevent tampering or unauthorized access to log data. Regular monitoring of log file status and automated alerts should be established to ensure that log files do not reach capacity without prompt administrative action.

11.6 Wireless networking

Wireless networks shall be password protected and used solely by the Company staff. Should guests wish to utilize an internet connection, a separate wireless connection shall be put in place, which is segregated from the Company network.

To enhance network security, MAC address filtering will permit only authorized devices. Default admin credentials must be changed, and WPA3 or WPA2 encryption will be enforced.

Regular firmware updates must be performed according to the manufacturer's recommendations.

11.7 Firewall and Web Application Firewall (WAF)

To protect the Sportsbook against web application threats, the Company shall deploy a Web Application Firewall (WAF). The WAF will detect and block attacks, providing real-time monitoring and analysis of HTTP traffic. It will ensure robust protection of Sportsbook web applications and databases available for external and/or public use.

All communications, including remote access, with the Sportsbook must pass through at least one approved application-level firewall.

Firewall Requirements shall be as follows:

a)Firewall Placement:

Firewalls must be strategically located at the boundary between different security domains. This positioning is critical to control and monitor the flow of traffic between trusted and untrusted networks, ensuring that all inbound and outbound communications are scrutinized according to the organization's security policies.

b)Network Path Integrity:

Devices that share the same broadcast domain as the system host must not possess any features or capabilities that allow them to forward network traffic to create an alternative network path that bypasses the firewall. All network traffic must be routed through the designated network gateways with traffic filtering features to maintain consistent security controls and monitoring.

c)Redundant Network Paths:

If alternative network paths are established for redundancy purposes, these paths must also be configured to pass through at least one traffic filtering device. This ensures that all network traffic is inspected and controlled, even in failover scenarios, thereby maintaining the security posture of the organization.

d)Dedicated Functionality:

The firewall unit must be dedicated solely to its purpose. No application features, aside from those directly related to the network traffic delivery and security operations, may reside on the firewall components.

e) Limited User Access:

The number of user accounts on the firewall must be strictly limited to essential personnel, such as network or system administrators. This minimizes the risk of unauthorized access and reduces the attack surface. Each user account must have a unique username and be protected by a strong password, with access granted based on the principle of least privilege.

f) Default Deny Policy:

The firewall must operate on a default deny policy, rejecting all connections by default unless they have been explicitly approved. This means that only pre-authorized services, ports, and IP addresses are permitted to communicate through the firewall, significantly reducing the risk of unauthorized access.

g) Source Address Verification:

The firewall must reject all connections originating from destinations that do not match the source addresses explicitly accepted in its policy rules.

h) Secure Remote Access:

Remote access to the firewall must only be permitted through the use of the most up-to-date encryption protocols. This ensures that any remote management or maintenance of the firewall is conducted securely, protecting against eavesdropping, man-in-the-middle attacks, and unauthorized access.

The Company will regularly review and update the firewall configurations to ensure compliance with this policy and to adapt to evolving security threats. Continuous monitoring will be conducted to analyze traffic patterns and detect any potential security breaches.

It is the responsibility of the IT department to implement, maintain, and monitor the WAF and associated firewall policies.

12. Safeguarding of Sportsbook related data, Applications and Equipment

Industry accepted components, both hardware and software, shall be used where possible on the Sportsbook.

Any connection or interface between the Sportsbook and any other system, whether internal or external third party, shall be monitored, hardened and regularly assessed to ensure the integrity and security of the Sportsbook. The regularity of assessment shall be defined by the CTO.

The normal operation of any equipment that stores data related to the Sportsbook must not contain options or mechanisms that could compromise the data.

No equipment related to the Sportsbook should have a mechanism in which an error causes data to be automatically erased.

No equipment storing data related to the Sportsbook may allow removal of information unless it has first transferred such information to the database or other secure components of the Sportsbook.

Sportsbook production databases must reside on a separate network from the servers hosting any user interface.

Sportsbook related data must be maintained at all times, regardless whether the services are being supplied with power or not. Sportsbook related data must be stored in a way to avoid data loss when the parts or modules are replaced during routine maintenance. Detailed provisions related to data back-up are provided in the Business continuity and disaster recovery policy and procedures related thereto.

Alteration of any accounting, reporting or significant event data shall only take place with supervised access control. In case of change in any data mentioned the following information shall be documented:

- a) unique ID number for the change;
- b) altered data element;
- c) value of the data element before the change;

- d) value of the data element after the change;
- e) time and date of the change, and
- f) identification of the user who made the change.

12.1. Asset management

Life-cycle and inventory maintenance of assets pertaining to Sportsbook, management, processing and communication of information attributable thereof is defined in Asset Management policy.

12.2 Safeguarding of Applications

Privacy and security are integral components of software development life-cycle. All applications developed by the Company that are related to Sportsbook must have documented security analysis included in the specification and design documentation, following a security risk assessment. A privacy impact assessment must also be carried out in the early stages of development to cater for any privacy risks prior to the deployment of the application ("**Privacy By Design**").

Software development methodologies used for the Sportsbook shall be clearly documented, regularly updated and stored in an accessible, secure and robust manner.

Any modification to core functionality of the Sportsbook must be peer reviewed. All software development roles shall be segregated during and after release of code to a production environment.

Any application modifications of the Sportsbook with security and/or privacy implications must be approved by the CTO before a release. Notwithstanding the security and privacy impact assessments, all applications must still be tested for common security and privacy weaknesses before deployment and no application should be released containing known security and/or privacy vulnerabilities.

All developers must be familiar with current and common application security and privacy weaknesses. The production environment must be strictly separated from the development and test environments, both logically and physically. In cases where cloud systems are utilized, it is imperative that there are no direct connections between the production environment and any other environment to maintain robust isolation.

Development teams are prohibited from having any access to make code changes directly within the production environment. This measure ensures that all modifications are rigorously tested and approved before deployment, maintaining the integrity of the production system.

To prevent the risk of sensitive information leakage, a documented method must be established to ensure that raw production data is never used within testing environments. Anonymization or data masking techniques should be employed when production data needs to be replicated for testing purposes.

No test or debugging functionality can be present in final product builds. Development code shall not be present in the production environment.

Management interfaces must only be reachable through the internal network and never exposed publicly, even if restricted to a set of addresses or if protected by a password.

Application development project management system used by the Company must include particular issues for developing and maintaining security controls and security testing routines. Each application is integrated with static source code analysis nightly build. All applications must be classified in order of required security level. Critical applications are subject to an annual internal audit plan.

Third-party components in our developed applications fall inside scope. Due diligence must be performed on all acquired gaming system technology to ensure security and processing integrity requirements are met.

To ensure software is appropriately secured and access is appropriately restricted throughout development the Company employs various controls including but not limited to the following:

- role-based access control and logging,
- approval and testing documentation,
- secure development environment (development environments are isolated from production systems and networks to prevent unauthorized access to sensitive data),
- Code encryption and obfuscation (techniques like encryption and obfuscation to protect sensitive code and algorithms from reverse engineering),
- regular technical risk assessments,
- other controls specified in Company policies and procedures.

Source code and built images are securely stored. Images are constructed with embedded SHA sums, ensuring the integrity of the containerized software and allowing external verification.

12.3. Verification application and procedures

Company has implemented the following verification procedures (critical control program) to ensure that the sportsbook solution and platform in the production environment are identical to officially released images:

- a) Hash Algorithm that shall produce a message digest of at least 128 bits;
- b) Component Monitoring to track all critical components;
- c) Version Verification to ensure that the correct version is used during deployment components.
- d) The results of the authentication procedure shall be retained in an unalterable version in a log file or a system report for no less than 90 days and accessible on request of the Regulatory Authority. Results of the authentication procedure must be recoverable in the event of a system failure. Results of the authentication procedure must detail verification results for each authentication.
- e) Any event of a failure in the authentication procedure for program components, must be notified to the CTO or an employee approved by the CTO and upon request - to the Regulatory Authority.

A secure hash algorithm used for verification shall produce a message digest of at least 128 bits (e.g., MD5, SHA-256). The hash function must be capable of detecting any changes or alterations to the software components by generating a unique hash value for each officially released image. The generated hash values must be compared against the hash values of the deployed components in the production environment to verify integrity and authenticity.

All critical components of the sportsbook solution and platform must be continuously (once in 24 hours) monitored to ensure that they remain unaltered and in compliance with the officially released versions. The monitoring system must log any changes or anomalies detected in the production environment and alert the appropriate personnel as per the defined escalation process.

During the deployment of any components, a version verification process must be conducted to ensure that the correct and authorized version is used. This process involves checking the version identifiers of the components against the officially released versions to confirm accuracy and compliance.

The results of all authentication procedures, including hash comparisons, component monitoring, and version verifications, shall be retained in an unalterable log file or system report. These logs or reports must be securely stored and retained for no less than 90 days. They must be accessible and recoverable upon request by the Regulatory Authority or in the event of a system failure. The logs or reports must provide detailed information on the verification results for each component and must not be alterable once recorded.

Any event of a failure in the authentication procedure for program components must be immediately reported to the Chief Technology Officer (CTO) or an employee approved by the CTO. Such events must be treated as highly critical information security incidents and lead to immediate activation of response procedure which includes a search of the root cause and a full sequence of actions that led to the incident and a redeployment of altered components from trusted sources. In addition, such failures must be reported to the Regulatory Authority upon request. The notification must include a detailed report of the failure, the components affected, and the steps taken to address and resolve the issue.

The information security team must regularly review and update the verification procedures to align with evolving regulatory requirements and best practices.

12.5. Technical controls

12.5.1. DNS requirements

For the purposes of the Sportsbook the Company shall use a secure primary DNS server and a secure secondary DNS server that are logically and physically separate from each other to prevent a single point of failure and ensure redundancy and high availability. The primary DNS server must be physically located in a secure data center or hosted on a virtualized or cloud environment with appropriate security measures implemented in order to protect against unauthorized physical or virtual access and the necessary level of fault tolerance to ensure the necessary availability.

Logical and physical access to DNS servers must be restricted to authorized personnel only. Access controls should include role-based access controls (RBAC) and comprehensive logging of all management access attempts.

Transfers of DNS zones to arbitrary hosts should not be allowed. Only authorized secondary DNS servers should be permitted to receive zone transfers to prevent unauthorized replication of DNS data.

A method to prevent DNS cache poisoning, such as DNS Security Extensions (DNSSEC), must be implemented. DNSSEC provides a cryptographic assurance that the DNS data received has not been tampered with and is authentic.

Multi-factor authentication must be enabled for all access to DNS management interfaces and systems to ensure that only authorized individuals can make changes to DNS settings.

Any request to change DNS servers or DNS records must be manually made or verified/approved by authorized personnel to prevent unauthorized changes that could lead to service disruptions or security breaches. No automatic changes of DNS records must take place without manual verification. In case of any automation of DNS management, record blocking must be in place in order to prevent any unauthorized infrastructure change.

12.5.2. Encryption

Restricted data attributable to Sportsbook, whether at rest or in transit, must be encrypted using approved cryptographic methods. Encryption must be applied to at least a single storage instance of every bundle of Restricted data attributable to Sportsbook to ensure its integrity and prevent any kind of unauthorized alteration. All kinds of network connections attributable to Sportsbook Restricted or betting data (including bettor data, sensitive information, bets, results, financial information and bettor transaction information) which are established via untrusted environments outside of the security domain external boundaries must be encrypted in order to protect the data from incomplete transmissions, misdirections, unauthorized message modifications, disclosure, duplication or repetition.

Email exchange must be encrypted using TLS in every case, including internal company emails, account management to clients' emails. Account managers receive emails using only TLS as well. Whenever information is stored or transported in computer-readable storage media, it must also be in encrypted form.

The Company acknowledges that encryption alone is not sufficient. Whilst encryption ensures that the information remains confidential, it cannot authenticate the information, and this might lead to the risk of repudiation.

Sportsbook related data that does not require confidentiality but must be authenticated to ensure its integrity and origin must utilize message authentication techniques, such as Hash-based Message Authentication Code (HMAC) or digital signatures. These techniques should be integrated into the data handling processes to protect against tampering and ensure that only authorized sources can modify or generate the data.

Authentication mechanisms must utilize security certificates issued by approved and trusted Certificate Authorities (CAs). Self-signed certificates are not permitted unless explicitly authorized by the Information Security Officer for specific internal use cases.

The organization must maintain an up-to-date inventory of all certificates in use and ensure they are renewed before expiration. The security of certificates must be regularly reviewed to avoid vulnerabilities.

The class and strength of encryption used must correspond to the sensitivity level of the data. For example, highly sensitive data should be encrypted using stronger algorithms such as AES-256, while less sensitive data may use AES-128.

The encryption algorithms and protocols in use must be periodically reviewed by the Information Security team to ensure they remain secure and are not susceptible to newly discovered vulnerabilities or cryptographic advances.

These reviews should be conducted at least annually or more frequently if required by regulatory changes, new security threats, or significant updates in cryptographic research.

When a weakness is identified in a currently used encryption algorithm or protocol, corrective changes must be implemented as a matter of priority. This includes applying patches, updates, or reconfigurations as necessary.

If a weakness cannot be mitigated through updates, the affected algorithm must be replaced with a more secure alternative. Transition plans should be developed to ensure continuity of operations during the replacement process.

In the case of critical vulnerabilities, an emergency response protocol must be developed and activated to replace or upgrade the encryption method as quickly as possible to minimize exposure.

Encryption of information in storage or in transit must be achieved through products approved by the CTO.

Encryption keys must be generated using approved cryptographic algorithms and methods that comply with industry standards and regulatory requirements. Only designated personnel or systems with appropriate privileges should be authorized to generate encryption keys.

Encryption keys used for the Company information are always classified as Confidential or Restricted information. Such keys shall be stored on secure and redundant media. The storage media must be physically secure, with access restricted to authorized personnel only. Redundant storage ensures that keys remain available even in the event of hardware failure or disaster. Unless the approval of the CTO is obtained, encryption keys must not be revealed to consultants, contractors, temporaries, or other third parties.

Keys should be distributed securely, using encrypted channels or secure key exchange mechanisms. Otherwise, before the distribution keys must be encrypted using a secondary encryption method or a different encryption key to add an additional layer of security.

Encryption keys must have a defined lifespan based on the sensitivity of the data they protect and the organization's risk management practices.

Prior to the expiration of an encryption key, a new key must be generated and securely implemented to replace the old key. The process for rotating keys should be automated where possible to minimize operational risk and ensure continuity of encryption.

The organization must maintain a monitoring of key expiration dates and ensure that keys are rotated or retired before they expire.

In case an encryption key is compromised, suspected of being compromised, or is no longer needed, it must be revoked immediately. The revocation process should include the removal of the key from all systems and applications where it is in use.

Configurations of systems and applications that used to refer to the revoked key must be updated to use a new key or cease operations until a new key is available.

Any renewal and revocation activities must be registered as separate issue in the internal task/project management system.

In case any data cannot be re-encrypted with a new / spare key or its backup requires to keep revoked keys for further recovery, that revoked keys must be stored or archived with the same retention period as the data with the necessary security considerations.

If data recovery is required, the archived key can be temporarily reactivated or used in a secure environment to decrypt the necessary data. After recovery, the key shall be securely destroyed if it is no longer needed.

Wireless networks in use must always be configured to employ encryption.

Encryption algorithms and key lengths shall be regularly (as determined by the CTO) assessed for security vulnerabilities by the person designated by CTO.

12.5.3. Operating System Security Policy of the Sportsbook

All systems have a vendor supported version of the operating system installed. All systems must have the current security patches installed.

System integrity checks should be performed for both host and server systems which are housing the Restricted Company data.

13. Technical security, vulnerability and penetration testing of the Sportsbook

Periodic technical security testing, vulnerability assessment and penetration testing shall be performed on Sportsbook. The procedure of the technical security testing, vulnerability assessment and penetration testing of the Sportsbook shall be determined in Vulnerability Management Procedure.

14. Communication of Policies

The Company shall ensure that employees get acquainted with the company policies and procedures upon starting work with the company, and upon introduction of amendments thereto.

15. Violations

The Company employees who violate this policy will be subject to disciplinary action up to and including termination of the employment agreement in place.

16. Review and Updates

The Policy shall be reviewed and updated by the Chief Technical Officer as necessary at least once every year or at shorter intervals as may be required by the circumstances. Without limiting the generality of the immediately preceding, a review of this document may be prompted by updates in regulations or other regulatory documents necessitating the respective changes.

17. Log of Changes

Version	Editor	Date	Reason of change
0.1	CTO	01/06/2022	First release
0.1	CTO	30/05/2023	Review

0.1	CTO	31/05/2024	Review
0.1	CTO	30/05/2025	Review