

Luckywayz Limited B.V.

Information Security Policy

Policy Owner	Luckywayz Limited B.V.
Approver	Jelizaveta Jakuseva, Managing Director
Date approved	31 Mar 2025 
31 Mar 2025	31 Mar 2025
Review frequency	Annual
Next review date	Mar 2026
Responsible for document management	Rudite Vege, MLRO
Security classification	Private and Confidential

TABLE OF CONTENTS

1. STATEMENT	4
2. SCOPE AND PURPOSE	4
3. PRINCIPLES	5
4. LEGAL AND REGULATORY OBLIGATIONS	6
5. INFORMATION SECURITY FRAMEWORK	6
5.1 Security risk assessment	6
5.2 Access controls, physical safeguarding	6
5.2.1 User management	6
5.2.2 Joiners, Movers and Leavers	7
5.2.3 Remote access	7
5.2.4 Usage of Personal Devices	8
5.3 Information Classification	8
5.4 Safeguarding of Equipment	9
5.4.1 Network Hardware	10
5.4.2 Email	11
5.5 Antivirus/Antimalware Protection and other Perimeter Controls to Minimise Threat of Intrusion	11
5.5.1 Antivirus/Antimalware solutions	11
5.5.2 Encryption and Authentication	12
5.6 Retention	13
5.7 Backup	13
6. INCIDENT HANDLING	13
7. REVIEW AND DEVELOPMENT	13
8. DIRECTOR CONTACT DETAILS	14

1. STATEMENT

Luckywayz Limited B.V. (or the Company) is committed to conducting business in accordance with robust information security principles to ensure the confidentiality, integrity, and availability of its data. This policy outlines the Company's approach to safeguarding its gambling and business systems from unauthorized access, data corruption, and other security threats. Clear definitions of personnel access to these systems and provisions for the physical security of essential equipment are included to mitigate financial and reputational risks. Supporting documents provide additional guidelines to ensure comprehensive protection of the Company's information assets.

2. SCOPE AND PURPOSE

Information security at Luckywayz Limited B.V. relies on securing the gambling platform, business systems, and related processes, preventing unauthorized access to information. This document clearly defines personnel access to both the gambling and business systems, limiting unauthorized access and ensuring data integrity through proper input validation. It also includes provisions for the physical safeguarding of essential equipment. Ensuring the confidentiality, integrity, and availability of information is vital for the Company's operations and governance. This policy outlines the Company's information security approach, providing guiding principles and responsibilities to protect its information systems. Further details are provided in supporting policies, codes of practice, procedures, and guidelines. The Company is dedicated to robust Information Security Management, applying these principles to all physical and electronic information assets. The primary purposes of this policy are to:

- Ensure the protection of all operator's information systems, including computers, mobile devices, networking equipment, software, and data, mitigating risks of theft, loss, misuse, damage, or abuse.
- Ensure users are aware of and comply with all relevant legislation.
- Provide a safe and secure information systems working environment for staff and authorized users.
- Ensure all authorized users understand and comply with this policy and associated policies, adhering to relevant codes of practice.
- Ensure users understand their responsibilities for protecting the confidentiality and integrity of the data they handle.
- Protect the operator from liability or damage due to IT facilities misuse.

- Respond to feedback and update the policy as needed, promoting continuous improvement.

3. PRINCIPLES

Failure to protect information assets can lead to unauthorized access, use, disclosure, and destruction, with significant risks to the Company and its customers, including financial losses, legal actions, loss of reputation and trust, and potential bans on data processing by authorities. Protecting Company Information from theft or fraud is as crucial as safeguarding any valuable asset. Inadequate security can have severe consequences. Effective information security is a vital investment, significantly reducing threats and vulnerabilities, and minimizing potential financial losses or damages. This requires assessing risks, identifying threats and vulnerabilities, and implementing necessary procedures and controls to ensure confidentiality, integrity, and availability of information.

The following information security principles provide overarching governance for the security and management of information at the Company:

- Information should be classified according to appropriate levels of confidentiality, integrity, and availability, in compliance with relevant legislative, regulatory, and contractual requirements, as well as the Company's policy.
- Staff responsible for specific information must ensure its proper classification, handle it according to its classification level, and adhere to relevant policies, procedures, or systems.
- The Company's platform includes functionality to automatically log off users after a defined period of inactivity, customizable per brand.
- All users must handle information appropriately according to its classification level.
- Efforts must be made to ensure data is complete, relevant, accurate, timely, and consistent.
- Information should be secure yet accessible to those with a legitimate need, based on its classification.
- Information must be protected against unauthorized access and processing.
- Information must be safeguarded against loss or corruption.
- Breaches of this policy must be reported (see Sections 5.3 Information Classification and 6 Incident Handling).

4. LEGAL AND REGULATORY OBLIGATIONS

Operator has a responsibility to abide by and adhere to all current EU legislation as well as a variety of

regulatory and contractual requirements. Relevant legislation includes:

- General Data Protection Regulation ([GDPR](#));
- Information security, cybersecurity and privacy protection — Information security management systems ([ISO/IEC 27001:2022](#))
- Information security, cybersecurity and privacy protection — Information security controls ([ISO/IEC 27002:2022](#))

5. INFORMATION SECURITY FRAMEWORK

5.1 Security risk assessment

The risk of threats and vulnerabilities to Company Information can never be entirely eliminated, as some element of risk always remains. However, these risks can be significantly reduced through a thorough information security risk assessment. The Company has evaluated its current infrastructure, compiled an inventory of all assets, and identified processes for accessing Company Information. Based on this information, risks have been identified, quantified, prioritized, and appropriate mitigation controls have been implemented to protect against and reduce these risks. The controls outlined in this policy reduce risks to an acceptable level for the business. The Company periodically monitors its risk mitigation plan and performs annual security risk assessments to address any changes in risk levels or security requirements.

5.2 Access controls, physical safeguarding

5.2.1 User management

All access to Company Information, resources, services, and physical premises shall be restricted and controlled. Access to system documentation, software applications, logs, personal data, business-sensitive information, and intellectual property shall be strictly limited and assigned on a need-to-know basis, according to risk assessments and relevant laws. Access rights shall be assigned, audited, and removed through an access control process ensuring that access is allowed only when necessary. Users shall be provided access only to company premises, information, resources, networks, and services they are specifically authorized to use. Access levels shall be determined based on risk assessments considering confidentiality, integrity, availability, traceability, privacy breaches, and

immaterial rights violations, as well as the user's role and responsibilities. Users, including third-party staff and subcontractors, must sign employment or service contracts with adequate confidentiality and data protection provisions before being granted access rights. If the subcontractor is an organization, agreements must be signed by its legal representatives, and its employees may be required to sign separate non-disclosure or data controller-processor agreements before access is granted.

5.2.2 Joiners, Movers and Leavers

Access rights for new users shall be determined and provided according to the User Management section above.

Users transitioning to new roles or duties within the Company will have their previous access rights revoked if deemed unnecessary and will be granted new rights based on the requirements of their new role and the need-to-know principle.

Users who resign or are terminated will undergo the exit procedure outlined in the Exit Procedure, which includes:

- Collecting Company's Assets;
- Removing Permissions;
- Removing Physical Access.

Access can only be re-enabled with approval from the Director.

5.2.3 Remote access

We encourage teleworking within our company, offering remote access that simulates the office experience. Users connect to the corporate network through an approved virtual private network (VPN) connection, utilizing two-factor authentication for security.

Access to Company Information remotely is permitted after implementing appropriate protective measures based on information classification or risk assessment results.

When accessing Confidential data remotely or on mobile devices, it's crucial to assess the associated risks and take appropriate measures to ensure security. For data classified as Confidential under the Company's Information Classification Standard, the following minimum standards apply:

- Ensure all system updates are applied, including Windows, iOS, and application updates;
- Install and regularly update Anti-Virus and anti-spyware tools where applicable;

- Control access to devices with a username/password or complex passphrase for tablets/smartphones;
- Set device screens to lock after periods of inactivity, requiring password authentication to re-enter;
- Avoid accessing, processing, or storing data on public machines (e.g., internet cafes).

For processing Confidential data on mobile devices, the Company recommends additional steps:

- Encrypt the device's hard drive or storage area;
- Encrypt any external storage devices;
- Encrypt data before transit if sending to/from the device;
- Regularly backup important data.

Approval for each user's remote access is controlled by the Director and is limited to authorized individuals.

5.2.4 Usage of Personal Devices

For all authorized individuals without Company-supplied mobile devices, tablets, or laptops requiring remote access to the Company email account, calendar, and contacts, permission from the Director is necessary to connect their personal mobile devices to the company systems. The following requirements apply:

- Employees are restricted to accessing internal email, calendar, and contacts only; other services cannot be accessed via personal devices;
- Adherence to best practice security measures is mandatory.

5.3 Information Classification

The following information provides a summary of the information classification levels that have been adopted by the Company.

- **Confidential:** Information of significant value to operators and customers, where unauthorized disclosure could lead to severe financial or reputational harm. Access must be restricted to those explicitly requiring it.
- **Restricted:** Information subject to controlled access, typically limited to a small group of authorized staff. Restricted data must be stored in a manner preventing unauthorized access, such as on systems requiring valid user logins before granting access.

- **Internal Use:** Information that can be disclosed or shared by its owner with appropriate members of an operator, partners, and other individuals as deemed suitable by information owners, without restrictions on content or timing of publication.
- **Public:** Information that can be disclosed or disseminated without restrictions on content, audience, or timing of publication, provided such actions comply with applicable laws and regulations, including privacy rules.

5.4 Safeguarding of equipment

The Network Hardware Safeguarding section outlines comprehensive measures aimed at protecting information handled by computer networks, including prevention of unauthorized software installation, user access control, securing corporate email, enforcing password security, data encryption, anti-malware tools implementation, and continuous improvement strategies. Typically, the Company utilizes firewalls, password protections, authentication protocols, VPNs, and encryption to secure its network systems. The Company undertakes the following measures:

- **Policy Development:** Formulating comprehensive policies outlining information security protocols, access controls, and data handling procedures;
- **Employee Training and Awareness:** Providing regular training sessions and awareness programs to employees regarding information security best practices, protocols, and their responsibilities in safeguarding company information;
- **Regular Auditing and Monitoring:** Conducting regular audits and implementing monitoring systems to detect and respond to security breaches or suspicious activities promptly;
- **Incident Response Plan:** Establishing a well-defined incident response plan to address security incidents effectively, including procedures for reporting, investigation, and mitigation;
- **Encryption:** Utilizing encryption technologies to protect data both in transit and at rest, thereby safeguarding against unauthorized access;
- **Patch Management:** Ensuring timely installation of security patches and updates for all software and systems to mitigate vulnerabilities and potential exploitation;
- **Backup and Disaster Recovery:** Implementing robust backup and disaster recovery procedures to ensure data availability and continuity of operations in the event of system failures or security incidents;

- **Regular Security Assessments:** Conducting periodic security assessments, including vulnerability assessments and penetration testing, to identify and address any weaknesses in the company's security posture.

5.4.1 Network Hardware

To implement administrative directives, procedural requirements, and technical guidance aimed at ensuring the appropriate protection of information handled by computer networks, the Company undertakes the following measures:

- **Prevention of Unauthorized Software Installation:** Implementing controls to block the installation or execution of unauthorized software or content.
- **User Access Control:** Restricting non-admin users from logging in as administrators or root, thereby limiting access to sensitive system functions.
- **Securing Corporate Email:** Converting incoming HTML content to plain text and default blocking of file extensions, except for approved exceptions, to mitigate email-based threats.
- **Password Security:** Enforcing password policies requiring long passwords (8 characters or more for normal users, 15 characters or more for admin accounts) and implementing account lockout mechanisms to enhance password security.
- **Security Domains Enforcement:** Defining and enforcing security domains to segment network resources and identifying abnormal traffic patterns for potential security breaches.
- **Data Encryption:** Utilizing encryption techniques to safeguard confidential data, particularly on portable devices and media, to prevent unauthorized access.
- **Anti-Malware Tools Implementation:** Deploying antivirus, anti-spam, and anti-spyware tools at the gateway and/or host level to detect and mitigate malware threats.
- **Automated Security Measures:** Implementing automated security measures to streamline security processes and enhance threat response capabilities.
- **Comprehensive Network Safety Measures:** Taking all necessary steps to ensure the safety of computer networks, including regular maintenance, monitoring, and updating of security measures to address emerging threats and vulnerabilities.
- **Compliance Adherence:** Ensuring compliance with relevant regulatory requirements and industry standards pertaining to information security;

- **Continuous Improvement:** Establishing a culture of continuous improvement by regularly reviewing and updating security measures in response to emerging threats and evolving technologies.

Typically, the Company secures its network systems through the use of firewalls, password protections, authentication protocols, VPNs, and encryption.

5.4.2 Email

The Company's email system is strictly prohibited from being used for unlawful activities, including the creation or distribution of illegal, disruptive, or offensive messages, such as spam. While the Company reserves the right to monitor its systems, it respects the privacy of email content. However, under exceptional circumstances, such as suspicion of unlawful activity or threats to company security, the Company may require access to users' corporate emails for investigation purposes.

Acknowledging that users may utilize a reasonable portion of company resources for personal emails, the Company deems this acceptable. Personal emails must be stored separately from work-related correspondence. Users are responsible for ensuring that company information is not inadvertently transmitted and are advised against sending internal emails to external parties.

Any suspicious emails, including those suspected of containing viruses or originating from unknown sources, should be promptly reported to the Director.

5.5 Antivirus/Antimalware Protection and other Perimeter Controls to Minimise Threat of Intrusion

5.5.1 Antivirus/Antimalware solutions

The Company will establish perimeter network controls to mitigate the risk of external network breaches. Measures implemented include antivirus applications, firewalls, VPNs, and encryption. Additionally, the Company will employ intrusion detection and intrusion prevention systems to enhance network security.

The Company will deploy antivirus/antimalware protection across its infrastructure to safeguard critical desktop and server operating systems from viruses, spyware, rootkits, and other security threats. It ensures the firewall remains active and effective against network layer threats. All incoming and outgoing emails undergo virus scans, while attachments are checked for spyware or adware applications. Continuous operation of antivirus/antimalware protection, automatic updates of virus definitions and software, and the generation of audit logs are ensured.

Desktop and laptop users are prohibited from engaging in activities such as writing, compiling, copying, knowingly propagating, executing, or attempting to introduce any self-replicating code designed to disrupt computer systems (e.g., viruses, worms, Trojan horses).

Any suspected viruses must be promptly reported to the Company. Upon discovery of malicious or suspicious code, the Company will immediately notify relevant authorities and take necessary steps to prevent the code from affecting Company systems and stored information.

5.5.2 Encryption and Authentication

The Company recognizes the paramount importance of maintaining robust system security through the implementation of necessary and adequate controls to prevent unauthorized access, use, and disclosure of Company Information. Encryption stands as a pivotal measure in this regard.

Encryption entails encoding information in a manner that only individuals or entities possessing the correct decoding key can revert it to its original form. It is imperative to employ encryption when transmitting strictly confidential information over data networks to thwart interception risks. This includes accessing network services requiring authentication, such as usernames and passwords, or transmitting or accessing strictly confidential data, such as in emails. All mobile devices storing or accessing confidential data, irrespective of ownership, must undergo encryption (utilizing "full disk" encryption).

Strictly confidential data stored in public, cloud-based storage facilities must undergo encryption before storage to prevent the cloud service provider from decrypting the data. Additionally, data subject to agreements with external organizations should be handled in accordance with their specified encryption requirements when stored, transmitted, or processed.

The exchange of classified confidential or sensitive information, as per our Information Classification system, via email or other means, must be encrypted. Personal or commercially sensitive data should only be sent via the Company email system when necessary, and when done so, must be transmitted in encrypted form. It is advisable to attach the data as an encrypted file to one email and send recipient decryption instructions in a separate email to mitigate interception or accidental or malicious distribution of sensitive data.

Encryption keys, usually in the form of passwords or passphrases, are critical. Losing or forgetting these keys renders encrypted information unusable, highlighting the importance of effective key management. While the responsibility for key management lies with individual members, it is recommended to securely back up keys and consider storing copies with trusted third parties.

Acknowledging that encryption alone may not suffice, the Company will implement authentication measures such as digital signatures to mitigate the risk of repudiation, thereby ensuring comprehensive information security.

5.6 Retention

The Company may need to hold onto its information due to legal, regulatory, or business obligations. Information shouldn't be kept longer than required, except when there's a justified need to prolong retention for certain documents.

5.7 Backup

Server systems must undergo regular backups using a standardized methodology. Backup media should be routinely transferred and securely stored either on-site or off-site. Sensitive and confidential Company Information must be encrypted during the backup process and remain capable of authorized decryption for the duration mandated by legal or regulatory compliance. Backup systems must undergo periodic testing to verify that procedures function as intended. Backup media should be archived for the duration specified in the Retention section.

6. INCIDENT HANDLING

The Company's management system (which may be changed from time to time) serves as a platform for managing system changes, offering detailed insights into the timing, authorship, nature, and progression of each alteration. The collective capabilities of these tools, coupled with the expertise of staff members, enable the Company to thoroughly analyze data and promptly address any incidents, past or potential. The primary oversight and accountability for incident management rests with the Company's Director.

If a company's staff or other authorized users are aware of an information security incident, they must report it to the Director of the Company.

7. REVIEW AND DEVELOPMENT

This document, issued by the Company, forms an integral part of the organization's policy framework. It outlines the minimum standards for human resource management, communication and operation management, access control, and the future development of the Company's gambling system. Intended for Gambling Authorities, employees, and third-party service providers, it applies to all data owned, processed, or held by the operator, regardless of its primary or secondary status and storage location. Throughout this policy, the term "Company's data" is used interchangeably with "information."

8. DIRECTOR CONTACT DETAILS

The Director at Luckywayz Limited B.V. is Jelizaveta Jakuseva. Email: director@luckywayz.com.