Information Security Policy

NOVARA, S.A. DE C.V.

El Salvador

August 2025

TABLE OF CONTENTS

INTRODUCTION

NOVARA, S.A. DE C.V. (hereinafter the **Company**) believes that information security management is the process of maintaining the Company's secure computing environment and is an important part of its infrastructure. Information security is a managerial activity within the corporate governance structure that provides a strategic direction for security. This activity is aimed at managing information security risks and using information resources correctly. Given that the Company operates as a Digital Asset Service Provider (DASP/BSP) relying on external custodians, liquidity providers, payment processors, compliance technology and cloud-based systems, information security management applies both to internally managed infrastructure and outsourced or cloud environments.

Objectives of the information security management process:

- Provide a focus on all aspects of IT security and the management of all IT security actions.
- Protect the interests of those who rely on information and telecommunications systems that provide information from damage resulting from accessibility, confidentiality and integrity failures.

The Company believes that safety objectives are met if:

- Information is available and usable when required.
- Information providing systems can resist attacks, recover from failures, or prevent failures.
- Authorised users have access to the required information when they need it (availability).
- Information is available or disclosed only to those who have the right to know it (confidentiality). and
- The information is complete, accurate and protected from unauthorised modification (integrity).

INFORMATION SECURITY POLICY

To achieve effective information security management, the Company's management has established and maintains an information security management system. The task of the information security management system is to ensure the proper management and control of the security of the provision and support of services according to the needs and risks of the business.

The information security management system includes:

- Information security policy and its supporting documents (special policies, standards, management procedures and guidelines).
- Communication, implementation and enforcement of security policies.
- A security strategy closely related to business goals, strategies and plans.
- Organisational security structure.
- A set of security controls that support information security policies and manage risks associated with access to services, information, and systems.
- Documentation of all security controls along with the operation and maintenance of controls and associated risks.
- Identification and classification of information assets.
- Evaluation and management of information security risks.

- Monitoring and managing all security breaches and serious security incidents.
- Analysis, reporting and reduction of the volume and impact of security breaches and incidents.
- Calendar planning and execution of information security analyses, audits and penetration tests.
- Management of suppliers and contracts in terms of access to systems and services, including oversight of critical third-party providers such as Custodians, Liquidity Providers, Payment Service Providers (PSPs/EMIs) and Travel Rule/KYT technology providers.
- Documents and records, ensuring that sensitive data such as KYC/KYT information, custodial wallet data, and client transaction metadata are stored, processed and transmitted securely.

The developed information security management processes together with the methods, tools and techniques constitute the security strategy.

Special Information Security Policies

Information security management operates in accordance with this information security policy and a set of supporting special security policies. These special policies include:

- Policy on the use and abuse of IT assets.
- Access control policy.
- Password management policy.
- Email policy.
- Internet policy.
- Anti-virus policy.
- Information classification policy.
- Document classification policy.
- Remote access policy.
- Policy on supplier access to IT services, information and components.
- Policies for disposing of assets.

- Mobile Device Management (MDM) and Endpoint Protection policy (disk encryption, remote wipe, patching).

- Cryptographic Key and Secret Management policy (generation, storage, rotation, revocation, and use of KMS/HSM/MPC solutions).

- Third-Party and Cloud Security policy, covering due diligence, contractual clauses, onboarding/offboarding, monitoring and access reviews for critical service providers.

The presence of special policies or their complexity depends on the business needs of the Company. The Company considers it possible not to issue these policies as separate documents, but to include them in specialised procedures. These policies must be available to all employees of the Company, and if necessary, customers and users. All security policies are reviewed and, if necessary, revised.

Identification and Classification of Information Assets

Identification and classification of information assets is provided:

- Maintaining an inventory of all assets (for example, computers, communications, industrial equipment, documents) necessary to provide the service, including digital asset custody records, KYC/KYT data, client wallet addresses, and transaction metadata subject to Travel Rule obligations.

- Classification of each asset according to its criticality to the service and the required level of protection.
- By designating the owner responsible for providing this protection.
- By imposing responsibility for the protection of an asset on the owner of an asset who can delegate day-to-day responsibility for security management.
- By ensuring that all sensitive information assets are encrypted in transit and at rest, and are subject to retention and secure deletion requirements consistent with applicable laws and internal policies.

Evaluation of Information Security Risks

Information security risk assessment is carried out at set intervals. Evaluation results are documented to help understand what can affect the managed service and support decisions on the management methods used.

Risks for information assets are assessed in relation to their nature (incorrect software operations, operational errors, communication failures), probability, potential impact on the business, past experience.

In course of risk assessment, special attention is paid to:

- Disclosure of classified information to unauthorised parties.
- Imprecise, inaccurate or invalid information.
- Unavailable information (for example, due to power failures).
- Physical damage or destruction of equipment necessary to provide services.
- Compromise or misuse of cryptographic keys, custodial wallet data, or secrets.
- Unauthorised or excessive access in cloud, SaaS, or third-party integrated environments.
- Failure or unavailability of critical third-party providers such as Custodians, Liquidity Providers, Payment Service Providers (PSPs/EMIs), or Travel Rule/KYT vendors.

Ensuring Security and Availability of Information

Ensuring security and availability of information includes the following aspects:

- Staff security - checking the Company's personnel for the right to process data, carrying out necessary checks before granting access to the system.
- Application security - all business-critical applications must be protected from unauthorised access. This includes means of identifying and authorising users of the system. All applications must enforce multi-factor authentication (MFA), single sign-on (SSO) where feasible, and role-based least-privilege access
- Security of middleware - middleware software provides transparent operation of applications in a heterogeneous network environment and provides services for integrating application parts distributed across different network machines (calling remote procedures, sending messages, storing data in databases). There must be confidence that the data is not viewed, not distorted and not modified.
- Operating system security - the operating system controls access to hardware and provides access to higher-level services, such as databases. Operating systems must be hardened, patched regularly, and configured to disable unnecessary services.

- Hardware security - the security of computer hardware, storage and printing environments that can contain or provide access to business systems. Endpoints must implement disk encryption, endpoint protection, and remote wipe capabilities under Mobile Device Management (MDM).
- Network security - the network transfers system data in electronic form. The appropriate security system protects this data from unauthorised viewing and interference. This includes segmentation of networks, use of firewalls and Web Application Firewalls (WAF), intrusion detection/prevention, and monitoring of cloud network environments.
- Room security - physical locks and alarm systems that restrict access to the room to authorised personnel only.
- Security of exit points - this includes (but is not limited to) mail, electricity, garbage. and
- Activities that include external organisations that have access to information systems and services of a service provider must be based on a formal agreement defining all necessary security requirements. Third-party access must be provisioned with minimum necessary rights, protected with MFA, time-bounded, and subject to regular review and immediate revocation upon termination of engagement.

Information Security Management Tools

The Company has developed a set of information security management tools. These tools shall be documented and cover:

- Determination by the Company's management of the information security policy, communicating it to the staff and customers and ensuring its effective implementation.
- Defining and assigning roles and responsibilities for managing information security.
- The organisation of information security, including the management of information security within the Company and during external contacts.
- Management of assets, including liability for assets and classification of information.
- Ensuring information security in the use of human resources, including security measures prior to hiring, during employment and during the completion of work.
- Measures of physical protection and environmental protection, including protection of working premises, protection of assets and prevention of work interruptions.
- Information security of communications and production management services: planning and accepting systems, protecting against malicious and mobile code, applying backup, managing network security, media protection tools, information security measures for the exchange of information, monitoring organisation.
- Managing access to the Company's assets and information resources, including access control policies, managing user access, user responsibility, controlling access to the network and operating systems, controlling access to applications and information, mobile communications and portable computers.
- Measures of information security in the development and support of products and services, including correct data processing in applications, the use of cryptographic methods, the security of system files, the management of technical vulnerabilities. This includes secure cryptographic key and secret management (generation, storage, rotation, revocation), regular penetration testing, vulnerability scanning with defined remediation SLAs, and secure development lifecycle controls.
- Management of information security incidents. and
- Continuity management.

The Company's management maintains security within the organisation through directives, demonstrating its commitment, clear allocation and recognition of information security responsibilities.

MANAGEMENT OF INFORMATION SECURITY WITHIN THE COMPANY

For the organisation of information security, the Company has allocated a special role - the owner of the information security process.

The Company's management has assumed the following obligations:

- Defining information security objectives so that they meet the Company's requirements and are integrated into relevant processes.
- Formulate, analyse and approve information security policies.
- Analyse the effectiveness of information security policy.
- Provide clear direction and visible support to security initiatives.
- Approve the appointment of employees to specific roles and determine the responsibility of such roles for information security throughout the Company.
- Ensure coordination of information security management measures throughout the Company.
- Information security management is coordinated by the owner of the information security process.

Coordination of information security management measures work includes:

- Checking the compliance of actions of various groups with the requirements and standards of the Information Security Policy.
- Identification of nonconformities and determination of necessary corrective and preventive actions.
- Coordination of information security methodologies and processes, for example, risk assessment methods, information classification, etc. .
- Recognition and identification of significant changes in threats and susceptibility of information and information processing tools to these threats.
- Assessment of the adequacy and coordination of the application of control methods.
- Effective promotion of new knowledge for use in training employees.
- Developing a consistent assessment of information obtained from monitoring and analysing information on incidents, developing recommendations for actions in response to information security incidents.
- Escalating material incidents or vulnerabilities to regulatory authorities (CNAD, SSF) when legally required.

INFORMATION SECURITY MANAGEMENT IN EXTERNAL CONTACTS

Interaction with "external parties" includes cases when employees of Clients or contractors get access to programs, data and networks of the Company, as well as cases when employees of the Company work on the territory of Clients (on business trips, during negotiations, etc.). The Company identified risks for information and technical means of information processing from external factors, i.e. natural phenomena, individuals and organisations, in the performance of business processes involving contact with such external factors.

The most important case, when the employees of the Clients get access to the Company's equipment, are cases of installation of equipment in the premises of the Company's Data Centres with the participation of specialists from the Client. During such work, there is the possibility of unintentional or intentional reconfiguration of equipment connections in the rack. Before granting access, appropriate control methods are applied. In the current operating model, this extends to cloud and SaaS environments, where external providers may have privileged access that must be managed through contracts, technical safeguards, and monitoring.

In addition to employees of the Clients, employees of organisations playing the role of a “third party”, i.e. employees of organisations supplying equipment and services, employees of regulatory organisations, consultants and auditors, temporary staff, developers of software or equipment installed in the Company can be the source of threat.

The general rule for the organisation of such interaction is the following - access to Clients or third- party employees to information is not provided until the appropriate information security management measures appropriate for the situation in question are implemented. All third-party access must be authorised, logged, protected with MFA, time-bounded, and subject to quarterly review and immediate revocation upon termination of engagement.

When concluding agreements under which it is planned to provide Clients with access to information or assets of the Company, all identified security requirements must be taken into account. This includes contractual clauses requiring third-party providers (Custodians, Liquidity Providers, PSPs/EMIs, KYT/Travel Rule vendors) to meet security standards and notify the Company of incidents without undue delay.

Before a prepared technical solution is transferred to a potential Client, it undergoes expert examination by specialists who evaluate, among other things, the compliance with the requirements of the Information Security Policy. Upon the completion of the development and before the transfer of the system to the operation for the Clients, the information systems are tested taking into account information security requirements.

MANAGEMENT OF THE COMPANY’S ASSETS

The Company's assets that are subject to accounting, control and protection include information resources, equipment, software, etc. At the same time, the necessary steps are the classification of assets and the appointment of persons responsible for storage and protection. These measures are included in the line of actions to ensure information security, referred to as asset management of the Company.

Responsibility for Assets

For each asset of the Company, an owner is identified. The owner is responsible for:

- information and assets related to information processing hardware to be classified.
- ensuring that access restrictions and membership in a particular class for a given resource are identified and periodically analysed with regard to applicable access control policies.
- ensuring encryption in transit and at rest for sensitive assets, including client identification data, transaction metadata, and cryptographic keys.

The asset owner has the right to delegate routine tasks to other employees, but the responsibility remains with the owner of the asset. It is allowed in complex systems to define a group of assets, which together provide a specific function such as a service. In this case, the owner of the service is responsible for the provision of the service, including the functioning of the assets that provide this service.

Classification of Information

The Company has established the following principles for classification:

- Information is classified in terms of its importance, compliance with regulatory requirements, levels of confidentiality and criticality for the organisation.
- Classification of information must be repeated regularly in order to take into account changes in the requirements of business, technology, etc..
- The asset owner is responsible for classifying the asset, periodically reviewing the classification and keeping the classification up to date.
- The level of protection is determined by the results of the classification of the information resource taking into account the level of confidentiality, integrity and availability requirements, as well as other information-related requirements.

The Company has developed and implemented procedures for labelling information and handling it. As a rule, information marking is performed as one of the actions of the configuration management process. For non-configuration information resources, labelling is performed by naming and tracking the creation date of the information resource.

For each level of classification, procedures for safe processing, storage, transfer, category change and destruction of information (resource) are defined. Secure deletion and data minimisation principles apply, especially for sensitive personal data and financial information, in line with applicable legal and regulatory requirements.

ENSURING INFORMATION SECURITY IN THE USE OF HUMAN RESOURCES

The Company is aware that people can be a major security threat - employees of the Company or Clients, as well as people trying to gain unauthorised access to resources. At the same time, the Company's employees potentially have more opportunities to cause - by accident or intentionally - significant damage to the Company. Therefore, all employees, contractors, consultants, and temporary staff are subject to background verification, confidentiality agreements, security training, and ongoing monitoring of compliance with information security, AML/CFT, and data protection requirements.

Security Measures Before Hiring

Roles in providing security and duties of employees are determined by personal job descriptions, procedures, work instructions, 'Confidentiality Agreement' and contract documents. The description of roles and responsibilities for compliance with information security include:

- requirements to perform actions in accordance with the Company's Information Security Policy.
- requirements to protect assets from unauthorised access, disclosure, modification, destruction or interference.
- rules for the safe execution of specific security processes and actions.
- provisions on liability for actions taken.
- requirements for reporting on information security events (real and potential), as well as organisation security risks.
- acknowledgement of AML/CFT responsibilities, including escalation of suspicious activities to the Compliance Officer.
- commitment to protect client funds and confidential data, including KYC/KYT information and wallet addresses, under strict segregation and confidentiality.

When applying for a job with the Company, a candidate's suitability is checked, including an assessment of the candidate's ability to comply with the requirements of the Information Security Policy. The audit analyses the biographical data and the candidate's qualifications, the experience of his previous work, and the feedback about the candidate (if any).

As part of the contractual obligations to the Company, the new employees hired by the Company agree and sign the terms of the employment agreement and confidentiality agreements, which clearly state their responsibility and the organisation's responsibility for information security.

Security Measures During Employment

Company's management requires all employees to comply with the requirements of the Information Security Policy.

The management of the Company assumes responsibility for the fact that each employee is:

- Instructed of its role and responsibility in accordance with the access rights granted to it.
- Provided with relevant guidelines.
- Motivated to implement security policies.
- Aware of the security requirements and their respective roles and responsibilities.
- Follows the information security policy and organisation-accepted methods of work.
- Keeps and develops relevant skills and qualifications.
- Receives periodic training on information security, AML/CFT obligations, phishing prevention, secure handling of client funds, and data protection practices.

The Company has a formal disciplinary process for employees who violate the requirements of the Information Security Policy.

In the case of serious violations, the disciplinary process must include immediate suspension from duties, deprivation of access rights and privileges, immediate removal from the premises. Violations related to AML/CFT obligations or client fund handling are considered major breaches and escalated to Senior Management and regulators when required.

Security Measures in the Period of Completion or Change of Employment

Upon completion or change of employment, employees are required to return all assets transferred to them for use. The termination process includes the return of all previously provided software products, corporate documents and equipment. Such assets as mobile computing equipment, credit cards, access cards, manuals and information stored in an electronic environment must also be returned.

In cases where an employee has information that is relevant to current operations, this information is documented and transmitted to the Company. The rights of access to information and information processing equipment are removed for all Company employees immediately upon termination of their employment, contract or agreement.

For leaving employees of the Company, access rights are removed, including physical and logical access, key access, identification cards, technical means for information processing, subscriptions, and deletion from all lists and documents identifying them as employees of the Company. If the resigning employee knows the passwords for the remaining valid accounts, then such passwords must be changed. All credentials, cryptographic keys, and privileged accounts must be rotated immediately. A formal exit checklist is completed to confirm access removal, and any obligations related to AML/CFT or client fund protection remain binding under confidentiality agreements.

MEASURES OF PHYSICAL PROTECTION AND PROTECTION FROM THE ENVIRONMENT

Workplace Protection

To protect the premises containing information and technical means of information processing, security perimeters (walls, turnstiles, receptions, surveillance systems) are used.

The Company's physical security perimeters meet the following requirements:

- Exterior walls of the building are durable.
- External doors are protected from unauthorised access by alarm systems.
- Reception and/or presence of security guards is organised to control the access of employees and visitors to the building.
- Access to the building has only authorised personnel.
- All fire exits through the perimeter of security have alarm devices.
- Installed intrusion detection system that is regularly tested for availability of all external doors and windows available.

- Where cloud infrastructure is used, equivalent logical perimeters (segmentation, VPCs/VNets, access control lists, and logging) must be applied and monitored as substitutes for physical access controls.

The physical security of each office building of the Company has three perimeters:

- The territory adjacent to the buildings where the Company's offices are located - security is provided by security guards with the use of surveillance cameras.
- Office premises - building security is provided by walls, alarms, fire alarms, video surveillance and video recording systems, security guards at the entrance, turnstiles and lockable doors at the entrance to the floors and rooms together with the system of individual electronic passes with data on the access level of the owner.
- Server rooms and restricted access rooms - lockable doors with an individual electronic access system, having data on the access level of the owner, or with keys issued to authorised employees.

The physical security of data centres has four perimeters:

- Guarded territory (outside the building) - provided with alarms, video surveillance and security guards at the entrance to the territory. access to the territory is allowed only to authorised employees.
- Data centre premises - building security is provided by walls (external), alarms, fire alarms, lock entrance to the building, video surveillance and video recording systems, security guards at the entrance to the building.
- Data centre modules - the module security is ensured by the walls (internal), the video surveillance and video recording system, the locked doors with the system of individual electronic passes, having data on the access level of the owner.
- Equipment racks - the security of the racks is ensured by the external enclosure, the motion response system, the video surveillance and video recording system, and the locks on the door of the racks.

The Company's business premises are protected by the following controls that ensure access by authorised personnel only:

- Access in the area where confidential information is stored and processed is controlled and limited only by authorised personnel.
- Authentication is used to authenticate access.
- Records are kept of all access cases.

The premises of public access, shipment and loading are controlled (video surveillance, security) and isolated from the premises with technical means for information processing (separate rooms).

Asset Protection

Equipment owned by the Company is housed or protected in such a way as to reduce risks from environmental exposure and unauthorised access. Technical means for information processing are placed in such a way as to reduce the viewing angle for unauthorised personnel. Storage facilities (warehouse) are protected from unauthorised access. Equipment that requires special protection (rack) is located in isolated workrooms, which helps reduce the overall level of threats.

In the premises where the equipment is concentrated (server rooms, data centre modules), environmental conditions are monitored (temperature, humidity). The office premises are centrally air-conditioned and heated. Outside the building, protection against lightning is provided, and all incoming power and communications lines are equipped with filters.

Technical means for processing classified information are protected from information leakage through radiation.

The Company's computational and network facilities are protected from interruptions in power supply and other impacts through the use of auxiliary equipment. Uninterruptible power supplies are used for critical business operations. Telecommunication equipment of the Data Centre is connected to the networks of several providers, which ensures high fault tolerance of the Company's network. For cloud infrastructure, redundancy and high availability must be ensured through multi-zone deployment, automated failover, and service level agreements with providers.

Maintenance and repairs are carried out only by authorised personnel who have been trained. If necessary, the staff undergoes a special check. Where third-party data centres or service providers are involved, contractual terms must require equivalent maintenance and access restrictions.

The Company provides security measures for equipment located outside the workplace, taking into account the various risks of working outside the organisation.

The Company has determined that equipment, information (data, documents) or software cannot be moved outside the organisation without prior authorisation. Any remote work equipment must be encrypted, monitored, and protected with Mobile Device Management (MDM) controls.

INFORMATION SECURITY OF COMMUNICATIONS AND PRODUCTION MANAGEMENT OF PRODUCTS AND SERVICES

Usage of Operational Procedures and Assigning Responsibilities

Operational procedures, i.e. the procedures under which actions are performed during the execution of the Company's production processes are documented and maintained up to date. As a rule, operational procedures are developed for work related to information processing and communications equipment (procedures for starting and shutting down computers, backing up information, maintaining equipment, handling media, managing mail, security, etc.).

The Company considers change management an effective means of protecting information. In the course of making changes, all entries are made in a special database (‘log), which allows you to control the correctness and compliance with information security requirements.

To reduce the possibility of unauthorised or unintended modification or misuse of assets, the Company uses a division of responsibilities and areas of responsibility of employees and divisions.

Restricted access, consistent with the profile of employee responsibilities, ensures confidentiality, integrity and availability of information.

The use of equipment in the Company meets the requirement of separation of functions, i.e. the equipment on which services are performed to Clients is not used for development or testing purposes. This ensures, firstly, the integrity of information (data, software) on the operated equipment, and secondly, the availability of the service is maintained by eliminating failures in the design and testing. Any remote work equipment must be encrypted, monitored, and protected with Mobile Device Management (MDM) controls.

Information Security Management for Third-Party Services

In the contract documents, the Company defines security measures, a description of the services and levels of service provided by the 'third party'. The functional responsibilities of employees interacting with the 'third party' formulate requirements for monitoring the fulfilment of obligations by a 'third party', including obligations to implement information security measures.

The Company maintains sufficient control and has a clear understanding of the security aspects of the 'third party'. This control is carried out both remotely (via telephone, e-mail and the exchange of documents in electronic form), and during meetings or during business trips. As a rule, change management, vulnerability identification, and reporting of security incidents from a 'third party' are included in the scope of such management.

For critical service providers such as Custodians, Liquidity Providers, Payment Service Providers (PSPs/EMIs), and KYT/Travel Rule vendors, contractual clauses must require compliance with Company security standards, encryption of sensitive data, timely incident notification, and cooperation with audits or regulatory inspections.

Third-party access to Company systems must be provisioned via Company-controlled identity management with multi-factor authentication, least-privilege roles, and quarterly access reviews. Immediate revocation of access is required upon termination of the contractual relationship.

Planning and Acceptance of Systems

As part of the capacity management process, the Company monitors, optimises capacity application and capacity planning to ensure the required system performance.

In the process of developing and changing systems, the requirements for the power of IT infrastructure components (hardware, software) are determined. If necessary, systems are adjusted, the effectiveness of which is confirmed by performance monitoring. Performance monitoring also serves to timely detect and prevent problems. During monitoring, special attention is paid to resources with a long acquisition time and high cost.

The Company has established and documented the basic requirements for information security, as well as the criteria for accepting new information systems, updates and new versions. Acceptance (validation) of systems confirms that the system performs the required functions in accordance with the basic and, if necessary, additional information security requirements.

During the acceptance of the following is considered:

- Meeting the requirements for system characteristics and performance (power), including information security requirements.
- Availability of documented and tested operational procedures (testing for compliance with the Company standards).
- Availability of system security management methods consistent with the methods adopted by the Company.
- Availability of a New System Operation Manual.
- Presence of a Deployment Plan for a System containing actions to reduce or prevent the
- negative impact of the introduction of a new system on existing systems.
- Presence of positive analysis results confirming that the impact of the new system on the overall security in the Company will not lead to the emergence of security incidents.

Protection Against Malicious and Mobile Code

The Company uses licensed anti-virus and anti-spam systems. Recovery of data destroyed due to the entry and activation of a malicious code is provided by the backup procedure. Users are notified of all cases of manifestation of malicious code and of planned or recommended measures to neutralise it.

A preventive security measure aimed at reducing the risks from malicious code is to regularly update systems (operating systems and applications). This includes automated patch management for endpoints, servers, and cloud workloads, with defined service level agreements (SLAs) for critical vulnerabilities.

In the Business Continuity Plans, particular attention is paid to protection against the introduction of a malicious code during servicing and in emergency situations, when some protection methods used in a regular situation may not be applicable.

The Company prohibits the use of any mobile code that has not been specially tested by specialists in the Company. Therefore, downloading mobile code from unreliable sources is by default denied in Internet browser settings.

For centralised protection against malicious mobile code, firewalls and specialised software are used in the Company's corporate network. In addition, in order to prevent the hidden entry of malicious mobile code into users' workplaces, all users at the domain policy level are deprived of the right to install any software on their own.

Backup Application

The Company carries out the process of backing up information in its network. For data backup, the Company uses licensed equipment and software that meets modern requirements for reliability and performance.

The backup operation includes a self-test procedure that allows you to assess the quality of the backup performance. In addition, regular (at least 1 time per quarter) special testing of recovered data backups is performed. Critical backups, including client transaction records, wallet addresses, KYC/KYT data, and compliance logs, must be tested more frequently and validated for integrity.

The Company has identified the information resources to be backed up, as well as the number of copies (copy depth) of the data. A weekly full reservation is made of all information resources determined for preservation. An incremental reservation is made daily, i.e. saving modified files. Storage depth - 1 month

(4 full copies). Backup media (tapes) are tested each time before data is written to them. The backup system automatically maintains accurate and complete records of the created copies (log).

Backups are stored in the system library. In addition, one copy is kept in a remote and protected place (in a safe) at a sufficient distance to avoid damage in the event of an accident in the main building. For cloud-hosted data, encrypted offsite backups must be maintained across multiple availability zones or regions, ensuring redundancy and compliance with applicable regulations. Access to backup repositories must be restricted, logged, and reviewed periodically.

Network Security Management

The Company pays special attention to the protection of networks, since networks are the most important resource for the efficient and simultaneous operation of a large number of employees.

Network equipment administrators use special control methods and software developed by the vendor. Professional use of this equipment, the timely use of software updates and the organisation of continuous monitoring of connections ensure the requirements for maintaining the confidentiality and integrity of data. The software automatically records (audit) the status of networks to create the ability to take security actions when a network attack is detected.

When documenting the level of security of a network service, the parameters for providing connections, the number and version of network equipment, the software used, the presence of protection perimeters and intruder alarm systems are taken into account.

The Company conducts regular monitoring of network connections. Monitoring data serve as a basis for assessing the actual level of service provision and recording incidents. Service level agreements with network service providers are analysed and discussed as part of the service level management process.

Measures to Protect Storage Media

The Company regards tape cassettes, compact disks, flash cards, replaceable hard disks, DVDs, and also printed documents as ‘replaceable information carriers’.

The general rule is to limit the use of removable media carriers only in those cases where it is necessary to perform production tasks. The use of media in such cases is authorised by the owner of the information resource.

At the same time, the Company adheres to a liberal policy regarding the use of small-capacity portable media (flash cards, diskettes). The Company believes that the use of these portable media allows employees to increase the efficiency of their tasks by working at home and on business trips.

The ability to use laptops and similar portable computers is limited to the list of people who need it to perform production functions.

A special case is the use of removable high-capacity media carriers, such as disks, magnetic cassettes, etc. The removal of such media to perform production tasks can be carried out only if there is authorisation from the owner of the relevant information resource, and a record of such an event must be made.

The Company has established procedures for handling and storing information to protect against unauthorised disclosure or misuse. The basic principle of protecting information is to restrict access to authorised personnel only. This principle applies to information in documents, computing systems, networks, mobile computers and carriers, mail, voice mail, voice messages, mail services, the use of fax machines, and items such as check and invoice forms.

Storage of information carriers in the Company is organised in accordance with the manufacturer's specifications. Storage of licensed software is organised on a network resource.

Information Security Measures in the Exchange of Information

The Company uses formal policies, procedures and methods of protecting the exchange of information developed by manufacturers of communication equipment. The use of licensed and constantly updated software and hardware, the Company considers as the most adequate method of protection against threats of interception, unauthorised copying, modification, incorrect routing and destruction.

Encryption is used to protect transmitted sensitive and confidential information. Employees who transmit and receive sensitive or confidential information are given special instructions on how to safely use email.

In the contract documentation, the Company establishes agreements on the exchange of information with Clients and ‘third-parties’.

The Company considers the transmission in electronic form via communication channels to be the main method of transmitting information. The physical transfer of information takes place when data transfer is required that is prohibited from being transmitted electronically or when the electronic form is not legitimate, such as printed and signed contract documents containing signatures and stamped seals.

The Company considers e-mail as a tool for business communication and does not allow it to be used for non-production purposes. Therefore, the volume of mail messages, as well as the volume of user mailboxes are limited.

Monitoring Organisation

The level and scope of monitoring is determined for information resources based on the results of risk assessment. The results of monitoring information security events are analysed weekly by the owner of the information security process.

The Company has established the following monitoring facilities:

- Characteristics of authorised access, including such details as user ID, date and time of key events, types of events, files that were accessed, used programs / utilities.
- All privileged types of operations, such as using privileged accounts, starting and shutting down the system, connecting/disconnecting input/output devices.
- Characteristics of unauthorised access attempts, such as unsuccessful or rejected user actions, unsuccessful or rejected actions using data and other resources, access policy violations and registration for network gateways and firewalls, alarms from intruder alarm systems.
- Alarms or system failures, such as console alarms or messages, system log exceptions, network alarms, alarms from an alarm system.
- Changes or attempts to change system security settings and control methods.

Protection of system logs is carried out through log access control. As a rule, only two system administrators or applications have access to a particular log.

Actions of system administrators and system operators are recorded in special system files - 'registration logs' or 'logs'. Logs are generated by operating systems or applications. As a rule, log records are analysed in the resolution of incidents, including information security incidents.

MANAGEMENT OF ACCESS TO ASSETS AND INFORMATION RESOURCES OF THE COMPANY

Access Control

An access control of the Company prescribes for the rules and access control rights for each user or group of users taking into account both physical and logical access control. In course of access control management, the Company shall consider the following:

- Rules for the distribution and authorisation of information, for example, the principle of 'I know only what I need', levels of security and information classification.
- Rules for coordinating access to information for different systems and networks.
- Access profiles for a standard user who performs normal work in an organisation.
- Access control rules in a distributed and networked environment.
- Separation of access control roles, for example, access request, access authorisation, access administration.
- Rules of withdrawal of access rights.

Access User Control

The Company has procedures for registering and deregistering users to grant and revoke access rights to all information systems and services.

Access rights are established based on user roles in accordance with the requirements of the Company's business processes. Job descriptions of employees contain provisions that define the responsibility and possible sanctions in the case of attempts by staff to implement unauthorised access.

The Company has defined the rules for the appointment and use of privileges. These rules are restricted to privileged users only. The privileged users include those who have access to the functions of control, monitoring or system administration (for example, system administrators, system programmers, etc.).

The Company has defined the rules for creating and changing passwords, which is one of the main mechanisms for controlling access to electronic information resources.

User Responsibility

The Company requires employees to observe security rules in the selection and use of passwords. This requirement is supported by setting the rule for generating and updating passwords in the operating system included in the standard of the user's workplace.

If an employee needs access to multiple services, systems, or platforms that require different passwords, you are allowed to use one password if each service, system, or platform has a sufficient level of protection to store the password.

The Company requires users to provide sufficient protection for the workstation, in particular:

- Close active sessions at the end of the work or provide protection with an appropriate locking mechanism, for example, password protection of the screen.
- Log out computers, and not just turn off the computer screen when leaving work at night, when going on vacation, on a business trip.
- Unused office equipment must be turned off.
- The Company has established and adheres to a 'clean table' policy for papers and portable media and a 'blank screen policy' for information processing equipment.
- Users are given access only to those services for the use of which they have received authorisation. As part of the Company's configuration management process, networks and network services are identified such that can be accessed.

Network Access Control

To control the access of remote users, the Company uses passwords, just as it does when connecting within a local network. At the same time, the Company limits the range of resources with which a remote user can work (e-mail).

The Company does not use equipment that has ports for remote diagnostics and configuration. Diagnostics and configuration of equipment is carried out using physical ports, access to which is protected by the placement of equipment in enclosed spaces and server racks.

The Company uses a separation of information services, users and information networks by creating subnets that unite groups according to the type of interaction within the Company's common system. The presence of several local subnets provides greater information security of the entire system.

Control of network connections is supported by the network equipment used in the Company. The Company uses routing control as one of the effective methods for protecting networks.

Access Control to Operating Systems

Login security for an operating system session is used. When entering a session, a password is requested, and certain rules are used when selecting a password.

All users have a unique identifier (user ID) intended only for their personal use. Together with the identifier, a corresponding user authentication technique is used.

Identification is the mechanism by which the system asks the user: 'Who are you?'. Users identify themselves with user accounts that are unique identifiers. To ensure the uniqueness of user accounts, the Company has established the following rules for naming account names:

- User accounts should be easily remembered by the user.
- User accounts should not create difficulties for administrators to create them.
- Administrators must be able to determine the owner of any user account.

To authenticate when connecting to the network, the authentication system of the user workstation based on 802.1x technology is used.

The Company uses modern password management systems that provide interactivity and use of password creation rules.

The Company has established rules for the use of system utilities that could violate the integrity of information resources.

The Company uses the practice of terminating inactive sessions to exceed the specified period of inactivity. This practice reduces the risks associated with the possible unauthorised use of the compounds established during the session.

The Company has identified critical systems for which the duration of the connection is limited.

Access Control to Applications and Information

The Company has established the following rules for access to information contained in applications:

- User and support staff access to information and functions of application systems is limited.
- Access restrictions are based on requirements for the use of specific business applications.
- User access to application systems takes place through the menu.
- Various permissions are set for example, to read, write, delete, execute.
- Output data of the application that manages sensitive information contains only relevant information and is transmitted only to authorised terminals. Such output is periodically analysed by the owner of the information resource to remove redundant information.

Mobile Communication and Laptop Computers

The Company limits the risks associated with the use of mobile communications (mobile phones, smartphones, communicators) and laptop computers (laptops, compact computers). The Company requires users the following devices:

- Ensure physical protection of mobile devices and business information located in these devices.
- Restrict access to devices of unauthorised persons.
- Create backup copies of information placed on the basis of production needs on portable
- devices.
- Prohibits the creation on the basis of cellular networks and networks of another format points of exit from the Company's local network to the Internet.
- Requires virus checking of any files being contributed to workstations from mobile communications and portable computers.

The Company allows work in a remote mode in very limited scope. The use of this practice is explained by the presence of serious threats that remote work represents. The only type of widely used type of remote work is to work with e-mail.

INFORMATION SECURITY MEASURES IN THE DEVELOPMENT AND SUPPORT OF PRODUCTS AND SERVICES

Correct Data Processing in Applications

In the applications used by the Company, internal verification procedures are built in to determine the occurrence of any information distortion due to input, processing or intentional actions errors. Designing applications in accordance with the specified requirement minimises the risk of failures in the processing of information.

Examples of internal data processing controls in applications are validation of the format and limit values of the input information, validation of input data for employees, and validation of requests.

The analysis of information security requirements for the integrity of messages, as in the general case, is carried out on the basis of a security risk assessment conducted. The risk analysis identifies the need for message integrity and identifies the most appropriate methods for meeting the requirements. At the same time, to achieve the integrity and reliability of the message, cryptographic methods can be used.

The Company uses both built-in storage for messages from operating systems and applications, as well as special storage facilities.

The applications used in the Company have built-in procedures for confirming (validating) the output data. Validation of application output is necessary to ensure confidence in the processing of information and its suitability to circumstances.

The fact of validation (approval) takes place each time when the contractual documentation, procedure, order or work instruction is put into effect, with the inscription ‘I approve’, the date and signature of the manager who has the right to approve. In this case, the output data refers to the parameters of the agreement, enshrined in the contract documentation, procedures, orders or work instructions.

Use of Cryptographic Methods

The Company will use cryptographic methods for protecting information in order to achieve various security objectives, including:

- Confidentiality: Use encryption to protect sensitive or critical information (stored or transmitted).
- Ensuring integrity and authenticity: using digital signatures or message confirmation codes to protect the integrity and authenticity of secret or critical information stored or transmitted.
- Ensuring strict fulfilment of obligations: the use of cryptographic techniques to confirm the presence or absence of an event or action.

Key management is part of the Company's policy on the use of cryptographic methods and aims to support the use of cryptographic methods.

In addition to the secure management of private and personal keys, the Company takes into account the validity of public keys. The process of authentication is carried out using certificates of public keys, which are issued by specially authorised organisations.

The Company uses two types of cryptography:

- Secret key methods when two or more interacting parties use the same key to encrypt and decrypt information.
- Public key methods when each user has a cryptographic pair: a public key (can be shown to everyone) and a private key (must be kept secret). public key techniques can be used to encrypt and create digital signatures.

System Files Security

The Company has identified the means to protect the system files of the operating systems used.

Since the results of testing systems contain configuration information that, if disclosed, may be detrimental, the Company has identified requirements for the protection of such data. Additional requirements are formulated for the test results of the databases in use. These include a ban on the storage of test results in the databases operated by them.

Security Measures in Development and Support Processes

The Company considers the use of configuration management procedures and change and release management procedures to be the main means of ensuring information security in the development and maintenance of programs and systems.

Information security requirements are provided by conducting a risk assessment, including an analysis of the impact of changes, and a specification of how to manage the security of new systems and products.

The Company introduced the practice of analysing the work and testing of critical applications after the introduction of changes in the operating environment. In particular, it is verified that the applications have not lost functionality and the integrity of data and settings is not compromised. In addition, a change in the operating environment may be accompanied by corresponding changes in plans for availability and business continuity.

The Company discourages program changes since a change to an individual program can create a technical vulnerability of the entire program system and equipment supporting the Company's processes. Therefore, changes are carried out only in cases where they are regarded as necessary. At the same time, all changes are strictly controlled within the framework of change and release management processes.

When making a change, the original software remains inviolable, and changes are made in a clearly identifiable copy.

Since the reason for the updates is the detection of new security vulnerabilities, the Company has implemented an operating system update management process. In accordance with the process, the proposed changes are tested by system administrators so that you can determine the impact on the system as a whole. Only after the successful completion of tests, updates and changes to programs are made in full.

The Company has developed a system of measures to prevent the possibility of information leakage. These measures include:

- Scanning media for hidden information and hidden communication ports.
- Masking and modulating system operation modes and communication channels to reduce the likelihood of tracking information (application of tunnelling, encryption — described in the 'Procedure for controlling access to information').
- The use of systems and software that are considered the most secure, i.e. use of products that have undergone independent evaluation.
- Prevent unauthorised access to devices on the network

Technical Vulnerability Management

The Company believes that a complete and continuous inventory of assets is a prerequisite for the effective management of technical vulnerabilities. Such information is collected as part of the configuration management process. Managing technical vulnerabilities is considered part of change management, which makes it possible to fully take advantage of the processes and change management procedures.

The following measures are taken for identified technical vulnerabilities:

- Roles and responsibilities for managing technical vulnerabilities are defined, including monitoring, risk assessment, minor repairs, asset tracking and coordination.
- Identification of information resources that are affected by technical vulnerabilities. these resources are updated based on inventory results or when resources are updated and modified.
- Determination of actions to respond to technical vulnerability notifications and their temporal order.

Once a technical vulnerability has been identified, the risks associated with the vulnerability are identified, as well as the actions to be taken and the timing of implementation. Risks for critical systems are evaluated first.

Depending on the timing of response to technical vulnerability, actions taken may be carried out as part of change management or in accordance with security incident response procedures.

INFORMATION SECURITY INCIDENT MANAGEMENT

Reporting Information Security Incidents

In the event that an information security event resulted in a loss or damage to the Company's information resources, reduced the ability to perform services, or is in violation of the Information Security Policy, such an event is recorded as an information security incident.

The Company has established a formal procedure for reporting information security events, procedures for responding and escalating, as well as actions to be taken upon receipt of an information security incident report. In the course of taking actions, reporting procedures are performed.

The reporting procedure includes:

- Feedback actions (those who reported on the incidents must be notified of the results of the resolution and closure of the event).
- Formats of reporting on information security events to support reporting actions and to assist an employee in identifying all necessary actions.
- Requirements for correct behaviour in the event of an information security incident (note all important details, take no action, immediately report the event to the point of contact).
- Link to the established disciplinary process for those who committed security breaches.

Information Security Incident Management

The Company has established responsibilities and procedures for quickly, efficiently and systematically responding to information about security incidents. In addition to reporting security events, the Company uses security perimeter monitoring to detect information security incidents and events.

The Company has established procedures and responsibilities for managing various types of security incidents (information system failures and service loss, malicious code, denial of service, errors due to incomplete or inaccurate business data, breaches of confidentiality and integrity, misuse of information systems).

The Company requires the registration of actions on incidents in the control logs, which are stored in the analysis of internal problems, use as forensic evidence, negotiations on compensation with suppliers of software and services.

Employees who perform actions to respond to an event or weakness in an information security system are responsible for recording actions.

The Company has developed procedures to monitor recovery actions after a security breach and correct system failures. Actions are documented. If information security incidents go beyond the boundaries of the Company, the owner of the information security process informs external organisations (Clients, supervisory authorities) and organises coordination of joint activities.

The Company considers information security event recordings as valuable material for analysing and preventing the repetition of similar events.

CONTINUITY MANAGEMENT

The Company has developed internal procedures for collecting and presenting certificates.

The Company has established and maintained an IT service continuity process that takes into account information security requirements. As part of this process, key elements of continuity management are integrated:

- Determination of risks in terms of their impact (damage), including identification and ranking of the affected processes.

- Identification of all assets included in key processes and services.
- Determination of the impact that security incidents can have on processes and services.
- Acquisition of appropriate insurance, which can be both part of the overall business continuity management process, and part of operational risk management.
- Identification of additional preventive and mitigating effects of management measures.
- Determination of sufficient financial, organisational and technical resources to take into
- account established information security requirements.
- Ensuring the safety of personnel and protection of devices for processing information and property of the organisation.
- Formulation and documentation of service continuity plans, taking into account information security requirements.
- Regular testing and updating of plans and processes.

The Company has identified information security incidents that may cause a business interruption, as well as the likelihood and impact of such events. Such incidents include equipment failures caused by human errors or intruders, theft, fire, natural misfortunes and acts of terrorism.

The Company conducts a risk assessment to determine the likelihood and impact in terms of service unavailability time, damage and recovery period. During the assessment, all the Company's business processes are considered. Based on the results of the assessment, the Company's continuity strategy, as well as plans for ensuring continuity, are clarified.

In the course of planning, services and resources are determined, including staffing, resources not related to information processing, and measures to neutralise the malfunction.

Continuity plans describe the Company's vulnerabilities, and therefore are themselves confidential information. Thus, measures are taken to protect them.

The Company maintains a unified structure of plans for ensuring availability and business continuity. This structure ensures the consistency of all plans, consistent consideration of information security requirements and uniform priorities for testing and support.

The Company regularly conducts testing plans to ensure continuity. The versions of these plans are updated based on the results of a regular risk analysis (at least once a quarter).

Test results are documented, and necessary actions are taken to improve the plans.

Version Control Table

Approval date	Changes description	Sole Director’s signature
27.08.2025	First issue	
