Approved by

the Resolution of the Board of Directors of

Freedom Finance Global PLC

(Minutes dated July 23, 2026)

Effective

from July 23, 2026

Information Security POLICY

Astana

2026

C O N T E N T S

Chapter 1. GENERAL PROVISIONS

1. The Information Security Policy of Freedom Finance Global PLC (hereinafter referred to as the Policy) has been formulated in pursuance to the Astana International Financial Centre rules and regulations, the legislation of the Republic of Kazakhstan, the regulations of the competent government authority exercising government regulation, control and supervision of the financial market and financial institutions (hereinafter referred to as the Applicable Law), the requirements of Freedom Holding Corp., and the internal regulations of Freedom Finance Global PLC (hereinafter referred to as the Company).
2. This Policy establishes the goals, objectives, core principles and requirements for the Information Security Management System (hereinafter referred to as the ISMS), defines the scope of the ISMS, and specifies the security measures to be implemented.
3. The requirements set forth herein apply to all information systems and documents owned or used by the Company. The Policy is applicable to all Company employees, including personnel engaged under contracts of employment and/or civil law contracts, as well as to third parties granted access to the Company's information assets or involved in information exchange processes pursuant to an agreement or contract, except as otherwise provided for under the legislation of the Republic of Kazakhstan.
4. The Chief Executive Officer of the Company oversees Information Security (hereinafter referred to as IS) matters for the Company.
5. One of the Company's most critical assets is information relevant to its operations, including information obtained in the course of interaction with external entities and individuals.
6. Ensuring IS within the Company encompasses requirements for: the organisation of the ISMS; categorisation of information assets; management of access to information assets; protection of the information infrastructure; use of cryptographic information protection tools; ensuring IS when third parties access the Company's information assets; IS status internal assessments; ISMS processes. This is a prerequisite for the successful conduct of the Company's business. Non-compliance with IS requirements may lead to serious consequences, such as financial losses, legal sanctions, damage to the Company's reputation (including loss of trust among clients and partners), and reduced competitiveness of the Company.
7. The Company pays particular attention to information protection matters, continuously improves the ISMS and the tools and methods used to mitigate IS threats, and ensures ongoing awareness of its employees in the field of information protection.

Chapter 2. GOALS, OBJECTIVES, CORE PRINCIPLES AND REQUIREMENTS

8. Ensuring information security (IS) within the Company is necessary to mitigate risks and economic losses associated with various threats to the Company's information assets. To this end, the Company maintains the following core properties of information:
    1) **Availability** — the property characterised by the ability to provide timely and unimpeded access to information for authorised subjects duly empowered to access it;
    2) **Confidentiality** — the property indicating the need to restrict the scope of persons authorised to access the information, ensured by the system's (or environment's) capability to keep such information secret from persons without authorisation to access it;
    3) **Integrity** — the property of information existing in an unaltered form (unchanged relative to a certain fixed state of such information).

9. The primary goal of the ISMS is to ensure the confidentiality, integrity and availability of information at all stages of its lifecycle, and to continuously maintain conditions within the Company whereby risks related to the protection of the Company's information assets are consistently monitored and kept at an acceptable level.
10. Achieving this goal enables the Company to:
    1) Protect the Company's information assets from all types of threats (external and internal, intentional and unintentional);
    2) Minimise potential and financial damage resulting from IS incidents, thereby ensuring the continuous operation of the Company's business processes.
11. The above goal is achieved through the following objectives:
    1) Ensuring the operation and continuous development of the ISMS, defining its participants and their respective areas of responsibility;
    2) Maintaining documented IS procedures that comply with the requirements of the Applicable Law;
    3) Regular identifying, analysing and preventing threats and vulnerabilities related to the Company's information assets at all lifecycle stages to manage IS risks, including risk assessment and minimisation;
    4) Conducting inventory and categorisation of the Company's information assets to determine their criticality level and ensure an appropriate degree of protection;
    5) Managing access to the Company's information assets, including adherence to the principle of least privilege, required levels of authentication, and maintaining control over user accounts;
    6) Ensuring the security of the information infrastructure, including protection of the network infrastructure, vulnerability management and updates of information systems/software;
    7) Using cryptographic information protection tools and employing secure data transmission channels;
    8) Ensuring IS when third parties access the Company's information assets;
    9) Monitoring IS activities and measures to counter attacks and prevent IS incidents;
    10) Managing and monitoring IS incidents, including processes for response, detection, registration of IS events and incidents, analysis of root causes, investigation of incidents, and collection, consolidation and storage of IS incident information;
    11) Conducting regular internal audits of the ISMS to verify compliance with the Company's internal IS regulations and relevant regulations of the Applicable Law;
    12) Raising awareness among the Company's employees and providing regular training on IS procedures.
12. The Company's ISMS shall be designed and operated in accordance with the following core principles:
    1) **Secure Architecture** means that information security aspects are taken into account when designing business processes and building information systems;
    2) **Adequate Level of Motivation and Engagement** means that managers and employees actively participate in achieving IS goals, recognising the importance of their actions and accepting responsibility for complying with established principles and requirements. This includes internal and external incentives aimed at supporting awareness, commitment to the Information Security Policy and proactive behaviour when handling information assets;

3) **Holistic Approach** means that the ISMS encompasses all elements necessary to ensure IS: a set of documentation (policies and procedures), IS processes, the ISMS organisational structure, IS culture, competent personnel, infrastructure and applications;

4) **Least Privilege** implies that users and systems within the Company should have the minimum access rights necessary to perform their tasks. This helps limit potential vulnerabilities and misuse;

5) **Defence in Depth** means that multiple layers of protection are implemented when deploying IS controls;

6) **Training and Awareness** entails ensuring that all Company employees are aware of IS risks and threats and understand the importance of adhering to protective measures;

7) **Transparency** means that all actions and processes within the Company related to information protection must be logged in audit trails, be understandable and documented. This allows monitoring of security measures' implementation and ensures trust from users and regulators;

8) **Segregation of Duties** means that no single user should be granted sufficient rights to compromise an information system or critical business operations independently;

9) **Compliance with IS Legal Requirements** means that non-compliance with laws in the field of IS is unacceptable. All discrepancies must be rectified or, at a minimum, their resolution planned within appropriate action plans;

10) **Risk Management** aimed at systematically assessing risks to information systems and data, and making decisions to minimise these risks through appropriate security measures;

11) **Efficiency and Control** aimed at verifying that measures correspond to assessed risks and at evaluating the completeness and quality of their implementation. The efficiency of measures should be assessed based on the extent to which set objectives and outcomes are achieved.

13. The Company shall define the procedure for managing users' access to information created, stored and processed within information systems. The Company reserves the right to monitor information and access to it. Access to information shall be granted to employees to the extent necessary to fulfil their assigned job duties.

14. This Policy, subordinate documents, information systems and the IS system as a whole, as well as measures to identify and analyse threats, counter attacks and investigate IS incidents, shall be analysed and assessed at least annually based on the results of the following activities:

    1) Analysis of the ISMS status;

    2) Ongoing checks of the IS status;

    3) Scanning information systems for vulnerabilities and conducting penetration tests, performed by the IS Department or qualified external auditors;

    4) Identified IS incidents and violations of IS requirements;

    5) Checks of the IS status during audits;

    6) Other audits and reviews of the IS system.

15. Audit activities requiring verification of existing systems must be planned and coordinated in such a way as to minimise the risk of disrupting business processes.

16. Information about IS incidents obtained through monitoring of IS activities shall be consolidated, systematised and stored.

17. Following the processing of an IS incident, a comprehensive analysis of the causes, mechanism and consequences of the IS incident shall be conducted.

Chapter 3. SCOPE OF APPLICATION

18. The primary objects of the Company's IS protection shall be the following elements:
    1) Information assets that contain data classified as the Company's trade secret under the Applicable Law and the Company's internal regulations, as well as any other information necessary to ensure the normal operation of the Company (hereinafter referred to as Protected Information);
    2) IT infrastructure and systems (computing equipment, data processing complexes, networks, and systems) used for the processing, transmission, and storage of Protected Information;
    3) Software tools (operating systems, database management systems, and other system and application software) of the Company's automated information system used to process Protected Information;
    4) The Company's processes related to the management and use of information assets;
    5) Premises housing the equipment used to process Protected Information;
    6) Workspaces, employees' offices, and the Company's premises designated for confidential negotiations and meetings;
    7) The Company's personnel who has access to Protected Information;
    8) Technical tools and systems processing unclassified information but located in premises where Protected Information is processed.
19. Protected Information may:
    1) Be stored on paper media;
    2) Exist in electronic form (processed, transmitted, and stored using computing equipment; recorded and reproduced using technical means);
    3) Be transmitted via communication channels (including telephone, facsimile, e-mail, messaging systems and other telecommunications services) as electrical signals.

Chapter 4. SECURITY MEASURES

20. The primary measures to ensure the Company's IS shall include:
    1) Administrative, legal, and organisational measures;
    2) Technical security measures;
    3) Software and technical measures.
21. Administrative, legal, and organisational measures shall include (but are not limited to):
    1) Control over compliance with the requirements of the Applicable Law and the Company's internal regulations;
    2) Formulating and implementing IS protection requirements, providing IS-related methodological support (rules, procedures) for processes;
    3) Control over alignment of business processes with the requirements stipulated herein;
    4) Awareness and training Company employees on the use of information systems and IS requirements;

5) Responding to IS incidents, containing them, and minimising their consequences;
6) Analysing and minimising IS risks;
7) Defining actions to be taken in the event of emergencies;
8) Implementing appropriate IS protection measures during the hiring and dismissal of the Company's employees in accordance with the requirements of the Company's internal regulations.

22. Technical security measures shall include (but are not limited to):
    1) Establishing access control and on-site security regimes;
    2) Creating a security perimeter for protected objects;
    3) Implementing video surveillance and fire safety measures for secured facilities;
    4) Controlling employees' access to restricted-access premises.
23. Software and technical measures shall include (but are not limited to):
    1) Using licensed software and certified information protection tools;
    2) Timely installation of security updates for information assets;
    3) Applying comprehensive antivirus protection;
    4) Using built-in IS tools provided by information systems;
    5) Configuring user identification and authentication mechanisms for information assets, including maintaining an appropriate password policy;
    6) Control over changes to security settings and the integrity of system and configuration files, as well as ensuring the immutability of audit trail logs in information assets;
    7) Ensuring regular data backup and secure data recovery;
    8) Managing and monitoring user accounts, access rights, and user activities, including those of privileged users;
    9) Applying cryptographic information protection systems;
    10) Ensuring the fault-tolerant operation of hardware;
    11) Monitoring the status of critical elements of the information system.

Chapter 5. FINAL PROVISIONS

24. Liability for improper performance and/or breach of the requirements of this Policy shall rest with Company employees within the scope of their assigned functional duties.
25. The Policy is subject to review in the event of threats to the Company's security, changes in Applicable Law or the Company's internal processes pursuant to the procedure stipulated by the internal regulations.
26. Issues not addressed by this Policy shall be resolved in accordance with the Applicable Law, the Company's internal regulations, and resolutions (decisions) of the Company's bodies and officials duly adopted within their respective authority.