APPROVED
Minutes of the Supervisory Board
Of JSB "UKRGASBANK"
dated "30" December 2024 No. 46
Chairperson of the Supervisory Board
_____ Sanela PASIC

AGREED
Minutes of the Management Board
Of JSB "UKRGASBANK"
dated "19" December 2024 No. 109
Acting Chairperson of the Management Board
_____ Rodion MOROZOV

AGREED
Minutes of the Information Security Management Committee of JSB "UKRGASBANK"
dated "13" December 2024 No. 13
Chairperson of the Committee
_____ Andriy SAMOKHVALOV

The JSB "UKRGASBANK"
Information Security Policy

Kyiv - 2024

CONTENTS

Section I. GENERAL PROVISIONS

1.1. The JSB "UKRGASBANK" Information Security Policy (hereinafter referred to as the Policy) is an internal document of JSB "UKRGASBANK" (hereinafter referred to as the Bank) that defines the purpose, goal, objectives; scope of information security and cyber defence of the Bank; general principles, requirements, rules (organisational and technical measures) aimed at protecting the Bank's information assets; definition of functions and responsibilities for ensuring information security and cyber defence of the Bank.

1.2. The Bank is a critical infrastructure facility in the banking system of Ukraine, which is taken into account by the Bank in terms of ensuring cyber security in the Bank.

1.3. The Policy is based on the requirements of the laws of Ukraine, regulations of the National Bank of Ukraine on information security and cybersecurity and has been developed with due regard to the requirements:

- The Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine";
- The Regulations on the Organisation of Measures to Ensure Information Security in the Banking System of Ukraine, approved by Decision of the Board of the National Bank of Ukraine No. 95 dated 28 September 2017;
- The Regulations on Information Protection and Cyber Defence by Payment Market Participants, approved by Decision of the Board of the National Bank of Ukraine No. 43 dated 19.05.2021;
- The Regulations on the Organisation of Cyber Defence in the Banking System of Ukraine, approved by Decision of the Board of the National Bank of Ukraine No. 178 dated 12.08.2022;
- The national standards of Ukraine on information security DSTU EN ISO/IEC 27000:2022 "Information technologies. Methods of protection. Information security management systems. Overview and glossary of terms", DSTU ISO/IES 27001:2023 "Information security, cybersecurity and privacy protection. Information security management systems. Requirements", DSTU ISO/IES 27002:2023 "Information security, cybersecurity and privacy protection. Means of information security control";
- The international standards on information security, generally accepted principles of information security and cyber defence;
- other internal documents of the Bank.

Section II. DEFINITION OF TERMS

A business process - a systematic and consistent performance of certain operations (functions) aimed at obtaining a specific result (product/service) that is valuable for internal

(officials/structural units/employees of the Bank) and external (customers of the Bank, other companies, government agencies, etc.) customers.

The Bank's Chief Information Security Officer (CISO) - a person appointed by the order of the Chairperson of the Management Board of the Bank and has the authority to make management decisions.

Threat - any circumstances or events that may cause a breach of confidentiality, integrity, availability of data in the Bank's ICT Systems and/or damage to the Bank's ICT Systems.

Information security - a multi-level complex of the Bank's organisational measures, software and hardware that ensure the protection of information from accidental and intentional threats that may result in a breach of the security principles of availability, integrity and confidentiality.

Restricted information - information constituting a state secret, information for official use, banking secrecy, professional secrecy, insurance secrecy, commercial secrecy, personal data, proprietary information, and FTE data.

ICT (Information and communication technology) - information and communication technologies, which cover any technologies and tools used to process, transmit, receive, store and exchange information through electronic means of communication. It includes ICT systems and separate software (system and application software), hardware (server equipment, computers, peripherals) and communication networks.

The Bank's managers - the Chairperson, his deputies and members of the Supervisory Board, the Chairperson, his deputies and members of the Management Board, and the Chief Accountant.

Client (the Bank's customer) - any individual or legal entity using the Bank's services.

An emergency is a disruption of the Bank's normal operating mode caused by a natural disaster, unavailability of ICT Services, virus threats, cyber attacks, spread of an epidemic/pandemic, escalation of military conflicts, natural or man-made hazards, human actions that may harm human health and/or cause significant material losses, and occurs from the moment the Emergency Recovery Team decides to resume operations.

Critical Business Processes (CBP)/Critical Business Areas (CBA) resources - the ICT Systems used within the CBP/CBA.

An information and communication technology system is a system designed to store, retrieve and process information, which is an organisational set of resources (human, software, technical) that provide and distribute information.

ICT services – the services provided through information and communication technology systems to internal or external users, including data entry, data storage, data processing and reporting services, as well as monitoring and business support and decision-making services.

ISMS - information security management system - a list of goals, management principles, methods, measures to protect information and ensure the sustainability of business processes in the Bank's information infrastructure.

Third party - (company, supplier, contractor, provider, partner, legal entity client) - a legal entity or individual with sufficient knowledge and qualifications to provide the necessary services to the Bank or a legal entity that receives/intends to receive the Bank's services, with which information is or may be exchanged in the course of interaction or intentions to interact.

Other terms used in this Policy shall have the meanings defined by the laws of Ukraine and regulations of the National Bank of Ukraine (hereinafter referred to as the NBU).

Section III. PURPOSE, GOAL, OBJECTIVES AND SCOPE OF INFORMATION SECURITY AND CYBER DEFENCE OF THE BANK

3.1 The purpose of ensuring information protection, cyber defence and information security of the Bank is to maintain confidentiality, data integrity, availability of information and systems, information security and cyber risk management, protection against cyber threats, compliance with regulatory requirements, protection of the Bank's reputation, financial security, improvement of cyber resilience, training and awareness of personnel.

3.2. The purpose of ensuring information protection, cybersecurity and information security of the Bank is to ensure comprehensive protection of the Bank's information assets, maintain customer confidence and compliance with high security standards in the face of modern cyber threats, ensure reliable operation of the CBP/CBA, protect information and resources of the CBP/CBA from threats. Sources of threats may include intentional/accidental human actions and/or sources not based on human actions. The Bank has identified external and internal circumstances that are important for achieving the goal of ensuring information protection, cyber security, information security of the Bank and affect the ability to achieve the planned ISMS result. External and internal circumstances are regulated in more detail in the documents on the Bank's information security management system.

3.3. The objectives of ensuring information protection, cyber defence and information security of the Bank are to ensure continuous operation of the Bank, to help minimise risks of the Bank's operating activities, and to create a positive reputation of the Bank in dealing with customers.

3.4. The scope of information protection, cyber security and information security of the Bank includes all the Bank's CBPs/CBAs/ products/ ICT Systems/ ICT Services.

Section IV. PRINCIPLES, RULES, REQUIREMENTS OF INFORMATION SECURITY AND CYBER DEFENCE OF THE BANK

4.1 The main principles of information security to which the Bank adheres are to maintain proper protection of information and ensure its security:

- **Integrity** - a property of information that means that the information cannot be modified by an unauthorised user and/or process;
- **Confidentiality** - a property of information that means that the information cannot be obtained by an unauthorised user and/or process;
- **Accessibility** - a property of information when it is processed by technical means that ensures unhindered access to it for authorised operations of familiarisation, modification or destruction.

4.2. The principles of cyber security to which the Bank adheres are as follows:

- proportionality and adequacy of the cyber defence measures implemented to real and potential cyber threats;
- prioritisation of preventive measures;
- minimising cyber risks in the Bank's operations;
- compliance with the requirements of the NBU's regulations/recommendations on information security and cybersecurity, recommendations of the NBU, including those that may be provided by the NBU based on the results of control;
- ongoing support by the Bank's governing bodies for the Bank's cyber resilience by organising effective cyber risk management.

4.3. The objects subject to protection are:

- ICT systems/ICT services, equipment, data carriers, data transmission channels for which the Bank ensures an appropriate level of information protection;

- internal documents of the bank/regulatory and methodological documents of the bank (VDB/NSDB) regarding processing, storage, transfer of information owned by the Bank or which is the subject of professional, business, production, commercial and other interests of the Bank.

4.4. The Bank shall distinguish information with restricted access from other information. The list of information classified as restricted information is determined by the documents on the Bank's information security management system.

4.5. The following types of CBP/CBA resources are considered to be subject to information security and cyber defence:

- **ICT systems** - ICT systems used by the Bank's structural units to perform their functions as defined in the list of ICT systems;

- **engineering infrastructure** - power supply, grounding, air conditioning and ventilation systems, access control and video surveillance systems, fire alarms, etc;
- **facilities** - restricted areas, such as (specialised) restricted areas, server rooms, switching rooms, etc., where engineering infrastructure, server and network equipment is located;
- **staff** - heads of independent structural units that ensure decision-making and general management of the CBP/CBA resources; employees of the Bank that ensure the functioning of the ICT Systems and ICT Services; employees of the ISD that ensure the proper level of information security/cybersecurity, ICT Systems and ICT Services; employees of the Bank that use the ICT Systems and ICT Services (this category includes all employees of the Bank that are not heads of independent structural units and employees of the Bank,

4.6. The Bank shall protect the information and resources of the CBP/CBA by physical, hardware, software, regulatory and civil law means.

4.7. The Bank shall comply with the following rules and requirements in terms of ensuring information security, cyber security and business continuity:

- the Bank's employees and employees of third parties shall participate in maintaining an appropriate level of information security and cyber defence within their duties and powers and shall be liable for its violation within the limits established by the laws of Ukraine and the Bank's documents;
- compliance with information security and cybersecurity requirements during the development, implementation and operation of ICT Systems/ ICT Services;
- the Bank's public services and internal network meet the requirements of information security and cyber defence;
- The Bank establishes and monitors compliance with all information security and cybersecurity requirements in agreements with third parties, in particular with regard to participation in international payment and money transfer systems (stakeholder requirements);
- the Bank's employees are systematically trained in information security and cyber security standards and measures, personal data protection, and information technology;
- the Bank's employees, within the limits of their authority, shall familiarise themselves with the documents on the Bank's information security management system, which contain the requirements and rules of information security and cyber defence in the Bank;
- The Bank has emergency and cyber-attack plans in place, which are systematically tested and updated:
  - The JSB "UKRGASBANK" business recovery plan;
  - The JSB "UKRGASBANK" Business Continuity Plan;
  - The Business continuity plans for critical business lines;

- The Plan for ensuring continuity and restoration of JSB "UKRGASBANK" ICT systems functioning;

- The Plan for ensuring continuous operation of JSB "UKRGASBANK" Directorates and branches.

4.8. The Bank's employees shall immediately notify their immediate supervisor and the Bank's Information Security Department of any information security incident / cyber incident. In accordance with the documents on the Bank's information security management system, the Bank provides for analysis and response (including at the level of communication) to a particular information security incident/cyber incident. Based on the results of the analysis, measures are taken to prevent the recurrence of such information security/cyber incidents.

4.9. The content of the Policy shall be communicated to all employees of the Bank in accordance with the procedure established by the Bank.

4.10. The content of the Policy shall be available, if necessary, to the interested parties. The Policy is available on the Bank's website https://www.ukrgasbank.com, in the section "About the Bank" - "Internal Documents".

4.11. All employees of the Bank shall sign an obligation to keep information with restricted access of the Bank and an obligation to comply with JSB "UKRGASBANK" information security requirements. These obligations shall remain in force during the entire period of the employee's employment with the Bank and indefinitely after his/her dismissal.

4.12. All third party employees who have access to ICT Systems/ICT Services shall sign the Agreement on Non-Disclosure of Restricted Information (hereinafter referred to as the Agreement) before taking up their duties, which shall remain in force for the entire period of validity of the Agreement with the third party and after the Agreement expiration within the period specified in this Agreement.

4.13. All employees of the Bank, employees of third parties, regardless of the level of access to information, ICT Systems, ICT Services and resources of the CBP/CBA, shall comply with the requirements of this Policy.

4.14. The Bank, when receiving services provided by third parties who have been granted access to the ICT Systems/ICT Services, shall require that the third parties comply with the provisions of this Policy.

4.15. The Bank uses the following approaches to ensure information security and cyber defence:

- a list of information containing restricted information was created and approved;
- a list of CBPs/CBAs was created and approved, according to which information security risks are assessed and further processed;

- rules of access to the ICT Systems/ICT Services are established;
- control of physical and logical access to all designated ICT Systems/ICT Services;
- password protection of ICT Systems/ICT Services is ensured;
- anti-virus protection of ICT Systems/ICT Services is provided;
- ensuring the protection of the Bank's network;
- secure remote access to network resources (local and Internet) is provided;
- protection of electronic information resources accessible from the Internet and other global data transmission networks against cyber attacks;
- an inventory of the designated CBP/CBA resources is maintained;
- cryptographic protection of information is ensured;
- Internal ISMS audits and ISMS analysis by the Bank's management are conducted;
- ISMS is monitored and improved.

4.16. Compliance with the requirements of this Policy and the Bank's information security and cyber security requirements will minimise information security risks that may have negative consequences for the Bank.

4.17. The Bank is guided by a risk-based approach that ensures understanding, monitoring and mitigation of risks in those areas of the Bank's activities that are subject to higher risks, in particular operational risk, including information security/cyber risks. The principle of risk-based approach is regulated in more detail by the Bank's internal documents on the Bank's information security management system.

4.18. In order to implement the risk-based approach, the Bank has an intruder model and a model of threats to the Bank's cyber defence/information security (Annex 1 to the Policy). The intruder model is based on the analysis of the type of intruder, the level of his/her authority, knowledge, theoretical and practical capabilities.

The intruder model and the model of threats to the Bank's cyber defence/information security are used in the assessment of the Bank's information security risks.

Section V. FUNCTIONS OF PARTICIPANTS IN THE PROCESS OF ENSURING INFORMATION SECURITY AND CYBER DEFENCE OF THE BANK

5.1. The CISO:

- ensures implementation of the measures provided for by Regulation No. 95, including strategic management of the Bank's information security, determination of the Bank's information security development areas, their compliance with the Bank's development strategy, compliance of information security measures with the needs of the Bank's business processes/products and control over implementation of information security measures in the Bank;

- ensures the implementation of the measures provided for by Regulation No. 178, including the priority implementation of cyber security measures for the Bank's critical information infrastructure;

- ensures that payment market participants implement the measures set out in Regulation No. 43, including information security and cyber defence.

5.2. The JSB "UKRGASBANK" Information Security Management Committee (hereinafter referred to as the Committee) is a collegial body of the Bank on ISMS implementation and functioning, which coordinates activities of the Bank's structural units on ISMS functioning and is responsible for the following main tasks:

1) review and approval of the JSB "UKRGASBANK" Information Security Policy and Strategy for 2023-2025;

2) approval of implementation of new projects, directions, strategic tasks on information security/cybersecurity of the Bank and information security measures;

3) review, approval and control over the implementation of projects on the development, implementation, operation, monitoring, review, maintenance and improvement of the Bank's ISMS;

4) determining the optimal resources required to implement information security/cybersecurity measures;

5) organisation of practical measures to raise awareness/training of the Bank's personnel on information security/cybersecurity (including ISO/IEC Group 27000 standards), Payment Card Industry Data Security Standard (PCI DSS) and VISA PCI PIN Security (PIN Security) standards, as well as the SWIFT User Security Concept and information security principles;

6) ensuring timely monitoring of the implementation and efficiency of the Bank's ISMS with further assessment of improvement opportunities and the need for corrective actions.

The Committee's tasks, functions and responsibilities are defined in detail in the Regulation on the Information Security Management Committee of JSB "UKRGASBANK".

5.3. The Information Security Department shall perform the functions of ensuring the information security/cybersecurity regime, the main tasks of which are as follows:

1) ensuring and controlling the development of requirements for security settings of the Bank's ICT systems;

2) development or participation in the development of documents on the information security management system;

3) organising and controlling the implementation of measures to ensure information security at all stages of the life cycle of the Bank's ICT systems;

4) organisation and control of the information security/cyber incident management process;

5) interaction with structural units in the process of restoring the Bank's ICT systems after failures due to information security/cyber incidents.

Tasks, functions and responsibilities of the Information Security Department are defined in detail in the Regulations on JSB "UKRGASBANK" Information Security Department.

5.4. The Bank's employees shall be aware of the importance and necessity of paying attention to the information security/cyber defence of the Bank, shall comply with and unconditionally fulfil all rules, procedures and requirements of documents on the information security management system, instructions/decisions of the Bank's Managers/Committee and the Information Security Department to maintain the proper state of information security/cyber defence, and shall contribute to the development of information security/cyber defence in the Bank, if necessary.

Section VI. CONTROL AND RESPONSIBILITIES

6.1. The description of the internal control system of the business process "Information Security Methodology" is defined in Annex 2 to the Policy.

6.2. The Bank's managers clearly understand that the Bank's information security and cyber defence are the basis of the Bank's vital activity and ensure (organisationally and financially) implementation, maintenance and control of the appropriate level of the Bank's information security and cyber defence.

6.3. The Bank's managers support information security and cyber defence within the Bank through clear regulation, confirmed commitments, clear assignments and recognition of responsibility.

6.4. The CISO is responsible for information security and cyber defence of the Bank.

6.5. Each employee is responsible for compliance with the Bank's information security and cyber security standards.

6.6. Each structural unit of the Bank shall participate in maintaining an appropriate level of information security and cyber defence of the Bank within its functions and powers, and shall be responsible for their violation within the limits established by the current legislation of Ukraine and internal documents of the Bank.

6.7. The ISMS subjects shall be responsible for performing their functions stipulated in Section 5 of this Policy. Responsibility of the ISMS subjects is determined in accordance with the legislation of Ukraine and the Bank's documents.

Section VII. FINAL PROVISIONS

7.1 This Policy shall come into force from the date of its approval by the Bank's Supervisory Board.

7.2. Amendments and additions to this Policy shall be approved by the Supervisory Board and shall come into force from the date of their approval.

7.3. In the event of amendments to the legislation of Ukraine or regulatory legal acts of the National Bank of Ukraine, this Policy shall be effective to the extent that it does not contradict the legislation of Ukraine until the relevant amendments are made, updated or a new version is issued in accordance with the procedure established by the Bank.

7.4. This Policy is subject to periodic review at least once a year.

7.5. If, when reviewing this Policy within the period specified in clause 7.4 of this Policy, the Policy Holder establishes compliance of the current version of the Policy with the legislation of Ukraine, including regulations of the National Bank of Ukraine applicable to the Bank, this Policy shall be deemed relevant and subject to subsequent review no later than the period specified in clause 7.4 of this Policy.

DRAFTED BY:

The Director of the Information Security Department	Sergiy NEDZELSKY

AGREED BY:

The Deputy Chairperson of the Management Board	Andriy SAMOKHVALOV
The Director of the Legal Department	Igor PRISHKO
The Director of the Compliance Department	Rajami JAN