

JSC Halyk Bank Information Security POLICY



■ GENERAL	3
■ OBJECTIVES, REQUIREMENTS AND BASIC PRINCIPLES	4
■ PROTECTED OBJECTS, APPLICABLE SCOPE	8
■ INFORMATION SECURITY THREATS	10
■ PROBABLE INTRUDER'S MODEL	12
■ SECURITY MEASURES	15
■ COMPLIANCE WITH LAW	17



JSC Halyk Bank pays special attention to information security, constantly improves information security management system, applicable means and methods of protection against information security threats, as well as ensures continuous training of the Bank employees to keep operation excellence.

This document is prepared in accordance with the requirements of ISO 27001: 2013 "Information technologies – Security methods – Information security management system – Requirements" and is public on the Bank's corporate website.

The document describes information security concept, basic principles, directions and requirements for information protection, as well as contains main sections of the Information Security Policies (hereinafter - the "Policies"), approved by the Management Board of the Bank.

The regulatory framework of the Policies consist of legislative provisions of the Republic of Kazakhstan, in the context of the use of information systems and information security, as well as of the requirements of international standards for information security management.

The provisions of Policies are binding for all Bank employees, interns, trainees, and should be brought to the attention of customers and other third parties that have access to the information systems and documents of the Bank, to the extent of direct relation between the Bank and their activities.

The Policies cover all information assets and documents, which are owned and used by the Bank. Information security - necessary condition for the successful business activities of the Bank. Information is one of the most important bank assets.

The main objective is to minimize damage caused to the Bank from the realization of the identified information security risks through prevention or minimization of consequences of such events, which is to be achieved using all provisions of the Policies.

Information security is not an end in itself, it is necessary to reduce risks and economic losses related to all kinds of threats to the Bank's existing information resources.

For this purpose, it is necessary to support main properties of information, namely:

- confidentiality – property that indicates the need to impose restrictions on certain entities having no access to this information, which is ensured by capacity of the system (medium) to keep this information in secret from entities who are not duly authorized to read, process, store and transmit such information;
- integrity - property of information, it is existence of information in an undistorted form (unchanged with respect to some fixed status of information).
- availability – property that is characterized by the ability to timely unimpeded access to the information of entities who are duly authorized thereto;

The process of ensuring reliable information protection is continuous. In order to implement sufficiently reliable information security system, its parameters must be constantly adjusted and adapted to reflect new threats coming from internal and external environment.

No obstacles must be to the introduction of changes in standards, procedures or Policies, as required.

In accordance with this provision, the following stages of information security management cycle are defined (model **PDCA**: Plan-Do-Check-Act):



Plan – planning (development) - risk analysis, Policymaking, targeting, determination of tasks, processes, procedures, software and hardware related to risk management and improvement of information security for achievement of the results, in accordance with the Bank's general strategy and objectives;

Do – realization (implementation and operation) - the implementation and operation of Policies, controls, processes, procedures, software and hardware;

Check – checking (monitoring and analysis) - assessment where it is applicable, measurement of the running characteristics of processes, in accordance with the Policies, objectives and practical experience, analysis of changes in external and internal factors that affect the security of information resources, reporting to the management for analysis;

Act – adjustment (maintenance and improvement) - corrective and preventive measures based on the results of internal and external audit of the information security status, requirements of the management, and other factors in order to ensure continuous improvement of the information security system.

The information security system of the Bank and its functioning should be built in accordance with the following basic principles:

- legitimacy - any actions taken to ensure information security are carried out on the basis of applicable legislation, using all permitted by the legislation methods of detection, prevention, localization and suppression of negative impacts on the Bank's information asset to be protected;
- focus on business – information security is considered as support process of core activities of the Bank, based on the analysis and assessment of information security risks inherent in such activities. Any measures to ensure information security must not entail serious obstacles to the Bank activities;
- continuity – application of controls for information protection system, implementation of any measures to ensure the information security of the Bank, must be carried out without interrupting or stopping the Bank's current business processes;
- complexity - information resources security throughout their life cycle, at all technological stages of their use and in all operation modes;
- feasibility and economic efficiency – the opportunities and means of protection used, must be implemented at the appropriate level of development of science and technology, justified in terms of a given level of security and must comply with qualifying requirements and standards. In all cases, the cost of implementation of measures and means of information security systems must be less than the potential damage from identified kinds of risk;

- priority – categorization of all information resources of the Bank by importance ranking in assessing the real and potential threats to information security;
- necessary knowledge and lowest privilege level – the user of the Bank's information resources receives minimum privilege level and access only the data that are necessary for performance of activities within the framework of its powers;
- specialization – operation of technical facilities and implementation of information security measures must be carried out by professionally trained and skilled specialists of the Bank;
- awareness and personal responsibility – managers at all levels and performers should be aware of all the requirements of information security and are personally responsible for the fulfillment of these requirements and compliance with established information security measures;
- cooperation and coordination – information security measures are implemented on the basis of interrelation between relevant structural divisions of the Bank, coordination of their efforts to achieve these goals, as well as establishing necessary contacts with external organizations, professional associations, government agencies, corporations and individuals;
- corroboration – important documents and all records – documents confirming fulfillment of the requirements for information security and the efficiency of its management system, must be created and stored with the possibility of immediate access and recovery.

The main information security objects in the Bank shall be deemed the following items:

- information resources containing data classified, in accordance with applicable legislation and the Bank's internal regulations, to banking secrecy, commercial secrecy of the Bank, any other information necessary to ensure normal operation of the Bank (hereinafter – protected information);
- tools and systems of informatization (computer equipment, information-computer complex, networks, systems), in which protected information is processed, transmitted and stored;
- software (operating systems, database management systems, other system-wide and application software) of the automated system of the Bank, which are used to process and store protected information;
- the Bank processes related to the management and use of information resources;
- premises, in which the means of processing and storing of protected information are located;
- workrooms and offices of the Bank's employees, the Bank's premises, designated for private negotiations and meetings;
- the Bank staff with access to protected information;
- hardware and software and systems that analyze public information, but located in the premises in which the protected information is processed.

The information of the Bank to be protected may:

- be In hard copy;
- exist in soft copy (be processed, transmitted and stored by means of computer technology, recorded and reproduced by technical means);
- be transmitted by telephone, facsimile, telex, etc. in the form of electrical signals;
- be present in the form of acoustic and vibration signals in the air and walling during meetings and negotiations.

The Policies are applied to all employees of the Bank and third parties, one way or another having access to the information resources of the Bank, and/or involved in the process of information interaction.

Threats to information security mean a set of conditions and factors that create prerequisites for the occurrence of an information security incident.

Threats to information security are divided into:

- accidental – natural disasters, errors by negligence, hardware and software errors, etc.;
- intentional, i.e. falsification or destruction of data, misuse of data, computer crime, etc.

Among the information security threats are (but not limited to):

- loss of information, constituting the banking secrecy, commercial secrecy of the Bank and other protected information;
- misrepresentation (unauthorized modification, fraudulent alteration) of the protected information;
- leak – unauthorized introduction of protected information to unauthorized persons (unauthorized access, copying, theft, transmission, etc.);
- unauthorized use of information resources (abuse, fraud, etc.);
- unavailability of information as a result of its blocking, hardware or program failure, disruption of WOS, servers, active network equipment, database management systems, distributed computer networks, the impact of viruses, natural disasters and other force majeure and malicious actions.

As a result of mentioned threats, the following negative consequences may arise, which affect the information security status of the Bank and its normal operation:

- financial losses due to leakage or disclosure of protected information;
- financial losses connected with destruction and subsequent recovery of the lost data;
- damage caused by disruption of the Bank activities and the losses associated with the failure to fulfill its obligations;
- damage from management decisions based on biased information;
- damage from lack of unbiased information at disposition of the management of the Bank;
- damage caused to the Bank's reputation;
- damage caused as a result of sanctions imposed by the authorized body on regulation, control and supervision of the financial market and financial organizations and/or the National Bank of the Republic of Kazakhstan;
- another type of damage.

The Bank has adopted the following classification of information security potential violators models:

- insiders – the Bank employees, who unconsciously or maliciously violate the information security mode;
- external intruders – persons who are not employed by the Bank (including trainees and interns) and act from hooligan, mercenary or other motives that may cause damage to the Bank's information resources.

Danger of the intruder is largely determined by the number and importance of information resources available to him. Based on this, the most risky categories should be deemed senior and middle managers, administrators of information resources and those who work with large volume of customer and financial data.

The main types of insiders:

- "untrained/negligent worker" - an employee of the Bank, who commit violation through ignorance or own negligence, which is not malice;
- "competing worker" – an employee of the Bank, who is eager to cause harm to another employee by personal enmity or other reasons. As a result of its actions not only its "target" may be affected, but also the Bank;
- "concerned intruder" – an employee of the Bank, who is interested in misconduct in relation to the Bank by a third party or biased by self-interest. As a general thing, such intruder is interested in keeping further employment in the Bank and will not take actions directly incriminating him. The most probable violation – leak of information (in case of self-interest - financial fraud);

- "planted intruder" – an employee of the Bank, who was employed for the purpose of committing illegal acts in the interests of third parties. Slightly interested in further employment in the Bank;
- "departing employee" – an employee of the Bank, who terminates employment in the Bank without reciprocal claims. The most likely leak of the information to which he had direct access;
- "aggrieved employee" – an employee of the Bank, who is sharply unsatisfied by employment parameters or, alternatively, the Bank's management is clearly dissatisfied with the performance of the employee. There may be any, even the most illogical violations, especially at the time of employment termination.

The main types of external intruders (in this section is used terminology adopted to date in the information security professional association):

- "Script Kiddie" or "Beginner" – a person interested in the hack of any information resource, which has well-known vulnerabilities. Not aimed at hacking just the information resources of the Bank, easily stops attack in the event of serious safeguards. As a general thing, it uses widespread hacking techniques, does not develop its own tools;
- "Black hat" – vs. "Script Kiddie" more persistent hacker of specific resource, considers bypassing security systems as a "matter of honor", can develop simple means of attack. Acts for the purpose of self-expression or for personal gain, can sell its services to criminal world;
- "Consultant" – an employee of service company that has access to information resources. Different scenarios of unauthorized activities are possible, usually within servicing information system;

- "Elite hacker" or "Guru" – high quality specialist for hacking information systems. As a rule, "customized" for criminal world or rivals. In the first case it will be aimed at financial fraud, in the second – at the leakage of information or unavailability of servers and compromise the Bank inside the mind of customers. The arsenal has full range of specialized software and hardware, and also uses social engineering technique;
- "Partner" – an employee of partner organization or subsidiary, who have access to the information systems of the Bank. Insider may be defined by any of the types, but it tends to be less manageable and less aware of the information security requirements, adopted by the Bank;
- "Trainee/intern" - as a rule, has no access to information and information systems, however, constantly stays in the territory of the Bank and can receive information indirectly or through social engineering technique. Can cause serious damage only by neglectful attitude to duties of the Bank employee in charge of the intern/trainee;
- "Customer"- the customer of the Bank, who has access to its remote banking services. It may cause damage if these services are used improperly, loss of identification details, or act as the first three types of external intruders, having albeit limited access to information bank resources.

The main measures to ensure information security of the Bank are:

- administrative, legal and organizational measures;
- physical security measures;;
- software and engineering controls .

Administrative, legal and organizational measures include (but not limited to):

- execution control of the requirements of the legislation of the Republic of Kazakhstan and internal documents;
- development, implementation and control of execution of the rules, techniques and instructions, which support Policies;
- compliance management of business processes with the requirements of Policies;
- awareness and training employees of the Bank to work in the information systems and information security requirements;
- responding to information security incidents, localizing, minimizing the consequences, adjusting the process of responding to information security incidents, assessing the effectiveness of the process of responding to information security incidents;
- analysis of the new information security risks;
- monitoring and improvement of the moral and business climate in the team;
- definition of actions in emergency situations;
- preventive measures upon entry into employment and dismissal of employees of the Bank.

Physical security measures include (but not limited to):

- organization of pass and indoor modes;
- construction of the protected objects security perimeter;
- organization of 24-hour security for the protected objects, including through technical security means;
- organization of fire safety of the protected objects;
- access control of the Bank's employees to private rooms.

Software and engineering controls include IT and IS processes (but not limited to):

- use of licensed software and certified information security means;
- use of perimeter protection means (firewall, IPS, etc.);
- use of comprehensive antivirus protection;
- use of information security tools integrated in information systems;
- regular information backup;
- ensuring that the audit trail is maintained in critical information assets;
- control over the rights and actions of users, firstly of the privileged one;
- use of information protection cryptographic systems;
- failure-free operation of hardware;
- monitoring status of critical elements of the information system.

These Policies and information security system as a whole based on the following regulatory legal acts and international standards (this section presents basic regulations that directly affect the process of creating information security system of the Bank in general; while at the same time there are number of documents that either describe strategic aspects of information security development at the state level, or regulate the rules for information security of certain applications/services):

- The Law of the Republic of Kazakhstan No.2444 dated 31 August 1995 "On Banks and Banking activity in the Republic of Kazakhstan";
- The Law of the Republic of Kazakhstan No.370-II dated 7 January 2003 "On Electronic Document and Electronic Digital Signature";
- The Law of the Republic of Kazakhstan No.418-V 3PK dated 24 November 2015 "On Information Support";
- Law of the Republic of Kazakhstan No. 94-V dated 21 May 2013 "On Personal Data and Their Protection";
- Resolution of the Management Board of the National Bank of Kazakhstan No. 188 dated 12 November 2019 "On Approval of Rules for Formation of Risk Management and Internal Control System for Second-Tier Banks";
- Resolution of the Management Board of the National Bank of Kazakhstan No. 48 dated 27 March 2018 "On approval of the requirements for information security of Banks and organizations conducting certain types of banking operations, rules and deadlines for providing information on information security incidents, including information on violations, failures in information systems";
- Resolution of the Management Board of the National Bank of Kazakhstan No. 47 dated 27 March 2018 "On approval of the Rules and deadlines for banks to submit information on the availability of information security management systems, as well as on compliance with information security requirements to the National Coordination Center for Information Security";
- International standard on information security ISO/IEC 27001: 2013 "Information technologies – Security methods – Information security management system – Requirements";

- International standard PCI DSS, version 3.2.1 (Payment Card Industry Data Security Standard – Payment Card Industry Data Security Standard);
- International standard PCI 3DS (Core Security Standard) - a security standard for organizations that perform or provide payment functions without the physical provision of a payment card;
- SWIFT User Security Concept (CSCF);
- Resolution No. 90 of the Management Board of the Agency of the Republic of Kazakhstan on Regulation and Development of the Financial Market “On Approval of requirements for information security incident response services, internal investigations of information security incidents” dated 21 September 2020;
- Resolution No. 111 of the Management Board of the Agency of the Republic of Kazakhstan on Regulation and Development of the Financial Market “On approval of the information security risk assessment methodology, including the procedure for ranking financial institutions by degree of exposure to information security risks” dated 23 November 2020;
- Resolution No. 89 of the Management Board of the Agency of the Republic of Kazakhstan on Regulation and Development of the Financial Market “On approval of requirements for competencies of managers and employees of information security departments, including requirements for advanced training of persons responsible for ensuring information security” dated 21 September 2020;
- Resolution No. 110 of the Management Board of the Agency of the Republic of Kazakhstan on Regulation and Development of the Financial Market “On approval of the Rules of assessing the level of protection against threats to information security” dated 23 November 2020.

The Bank has implemented appropriate processes to ensure compliance with regulatory legal acts, observance of intellectual property rights, protection of personal information protected by the law, upholding of restrictions on the use of cryptographic facilities.

All the requirements and provisions of the international standards ISO/IEC 27001, PCI DSS, PCI 3DS, SWIFT are binding in their applicable scope, which is determined by relevant documents.

In developing and applying tools and methods of information security, we take into account requirements of contractual obligations and contracts concluded by the Bank with third parties.

Third parties access the information resources of the Bank only after analysis of risks that may arise from such access, and adequate protective measures.

If necessary (particularly, if is regulatory requirement or required by international standards), the Bank checks counterparties (suppliers of goods and services) for compliance with certain requirements (e.g. examination of documents supporting compliance of provided services with the requirements of PCI DSS standard).

Number of internal regulatory sub-documents are developed on the basis of the Policies, governing specific rules and methods of information security, private policies to the extent of applicable scope of standards, etc. Such documents may complement and expand requirements of the Policies, but cannot contradict them.

