ГАЗПРОМБАНК

(Открытое акционерное общество)

APPROVED BY
Resolution of the Management Board of Bank GPB (OJSC) dated 24 September 2008 (Minutes № 35)

With amendments approved by resolutions of the Management Board of Bank GPB (OJSC) dated 30 September 2009 (Minutes № 41), 10 November 2010 (Minutes № 49), 22 March 2012 (Minutes № 11)

Policy on Information Security of Gazprombank (Open Joint-stock Company)

MOSCOW
2008

Table of Contents

1. General Provisions

1.1. This Policy has been developed in accordance with legislation of the Russian Federation and legal rules of information security protection, requirements of statutory instruments of the Central Bank of the Russian Federation, the authorised federal executive body for security, the authorised federal body for countering technical intelligence agencies and for technical protection of information and shall be based, among other things on:

- the Information Security Doctrine of the Russian Federation (dated 09 September 2000, Pr-1895);
- Standard STO BR BSIS -1.0 – 2010 of the Bank of Russia "Information Security of Organisations of the Banking System of the Russian Federation. General Provisions".

1.2. This Policy shall constitute a document available to any Bank employee and any user of its resources and shall be a system of thought officially approved by the management of Gazprombank (Open Joint-stock Company) (hereinafter, the Bank) on information security protection and shall set the principles of the information security management system based on systematic presentation of the Bank's information security goals, processes and procedures.

1.3. The Bank management is aware of the importance and necessity of developing and improving measures and techniques of information security protection in the context of the development of legislation and regulatory norms of banking activities, as well as of developing implemented banking technologies and expectations of the Bank customers and other stakeholders. Compliance with information security requirements shall allow the Bank to create its competitive edge, ensure its financial stability, profitability, compliance with legal, regulatory and contractual requirements and improve its image.

1.4. The Bank's information security requirements shall meet the interests (goals) of the Bank activities and shall be designed to mitigate information security risks to an acceptable level. Risk factors in the Bank's information sphere are related to its corporate governance (management), organisation and implementation of business processes, relationships with counterparties and customers, and internal economic activities. Risk factors in the information sphere of the Bank account for a significant part of the operating risks and are also associated with other risks of the core and management activities of the Bank.

1.5. The Bank strategy for information security and information protection shall, among other things, include implementation of the requirements set forth by:

- Russian legislation on security, IT security and information protection, security of personal data, banking secrecy and other legal acts;
- statutory instruments of the authorised federal executive bodies for providing physical security and technical protection of information, countering technical intelligence agencies and ensuring information security and privacy;
- statutory instruments of the Bank of Russia and standards of the Bank of Russia on information security protection from the set of standards STO BR BSIS;
- statutory instruments of the Bank of Russia and documents of the Bank of Russia on standardisation "Information Security of Organisations of the Banking System of the Russian Federation", approved by Instruction № P-705 of the Bank of Russia dated 21 June 2010 and deemed binding on the Bank in accordance with Order № 179 dated 27 December 2010.

1.6. The Bank personnel and other parties shall strictly comply with the information security protection requirements, as defined by the provisions of the Bank internal normative documents, as well as by the requirements set out in the agreements and contracts to which the Bank is a party.

1.7. This Policy shall apply to the Bank business processes and shall be binding upon all employees and the management of the Bank, as well as on the users of its information resources.

1.8. Subsidiaries and affiliates must take into account the provisions of this Policy in developing their information security policies.

1.9. This Policy shall constitute the **first level** corporate documents in accordance with recommendations for the sphere of standardisation of the Bank of Russia RS BR BSIS 2.0 2007 "Information Security of Organisations of the Banking System of the Russian Federation. Recommended Practices on Documentation in the Sphere of Information Security Protection in Accordance with the Requirements of STO BR BSIS 1.0" approved and put in place by Instruction № P-348 of the Bank of Russia dated 28 April 2007.

1.10. Specific policies on IS protection (hereinafter, Specific Policies) shall constitute documents that provide a more detailed description of the corporate Policy as applied to one or several IS areas, types and technologies of the Bank activities. Such documents shall constitute the **second level** IS documents and shall be drafted as individual internal normative documents of the Bank, developed and agreed in line with the procedure established in the Bank, and shall be approved by the Supervisor.

2. List of Terms and Definitions

This Policy shall employ terms with relevant definitions according to STO BR BSIS –1.0–2010 "Information Security Protection of Organizations of the Banking System of the Russian Federation. General Provisions".

2.1. **Business Process** – a sequence of process-related operations to provide banking products and/or perform a specific type of the Bank supporting activities.

2.2. **Bank Information Security** (IS) – with respect to this Policy, the status of protection of the Bank technology-related and business processes integrating the Bank employees, hardware and software processing equipment as well as information amid threats to the IT environment.

2.3. **Bank Information System** – the set of the Bank hardware and software suites applied to support the Bank business processes. ATMs are not seen as devices that strongly differ from other components of the Bank information system and have their own unique features from the information security prospective.

2.4. **Information Security Incident** – the occurrence of one or several undesirable risk events associated with information security which may entail a high probability of breaching confidentiality, integrity or accessibility of information assets and infrastructure and creating information security threats.

2.5. **IT Block** – the set of the Bank autonomous structural units responsible for the development, operation and support of the information banking systems.

2.6. **Confidential Information** (hereinafter – CI) – information, for which the Bank has established a confidentiality regime.

2.7. **Supervisor** – a Deputy Chairman of the Management Board, supervising the Bank security issues, including information security matters.

2.8. **Threat Model** – a descriptive presentation of properties or characteristics of information security threats.

2.9. **Adversary Model** – a descriptive presentation of experience, knowledge and available resources of potential information interlopers which they need for a IS threat to be materialised, and potential motivation behind their actions.

2.10. **Responsible Unit** – the Security Service (Department). Its main functions in this area are to put this Policy in place, develop, launch and support information security systems.

2.11. **Information System User** - an individual able to access the information system of the Bank.

2.12. **Information Confidentiality Regime –** organisational and technical actions to protect information that allow the CI owner, given the existing or potential circumstances, to increase income, avoid unreasonable expenses, maintain its position on the market of commodities, works, services or obtain some other commercial benefits and that realise CI protection measures, which include the following activities:

- make a list of CI information in accordance with the List of Information for which Bank GPB (OJSC) established a confidentiality regime approved by Order № 47 dated 27 May 2011;

- limit access to CI by establishing a procedure for treating this information and controlling compliance therewith;
- register persons that were granted access to CI and (or) those to whom such information was supplied or transferred;
- regulate relations of CI use by employees on the basis of employment agreements and by counterparties on the basis of civil law contracts and agreements.

2.13. **Information Security Risk Event** – an event arising from an operating risk and resulting or able to result in the Bank's losses and occurring due to an error or failure of banking processes, actions of people and systems, and also due to external events.

2.14. **Information Security Threat** – an operating risk that result in the breach of one (or several) properties of information – integrity, confidentiality, accessibility of protection assets.

3. Description of Assets to be Protected

The main assets to be protected in the Bank's information security system shall be:

- information resources containing a commercial secret, bank secret, personal data of individuals, sensitive data, as well as publicly available information required for the Bank operations irrespective of the form and type of its presentation;
- information resources containing confidential information including personal data of individuals, as well as publicly circulating information required for the Bank's operation irrespective of the form and type of its presentation;
- Bank employees that develop and use the Bank's information systems;
- information infrastructure that includes the systems of processing and analysing information, hardware and software of its processing, transfer and display, including information sharing channels and telecommunications, information protection systems and products, facilities and premises where such systems are located.

4. Information Security Goals and Objectives

The goal of the information security protection activities undertaken by the Bank is to reduce information security threats to the level acceptable by the Bank.

The main objectives of information security activities in the Bank shall be:

- identify potential threats to information security and vulnerabilities[1] of assets to be protected;
- prevent information security incidents;
- remove or minimise identified threats.

5. Information Security Threats

The entire multitude of potential information security threats can be divided into three classes in terms of the nature of their occurrence: man-made, technology-related and natural ones[2] .

[1] In this document, vulnerability shall be understood as the weakness of one or several assets, which may be impacted by one or several threats (GOST R ISO/MEK 13335-1-2006, Article 2.26).

[2] This classification is applied irrespective of operating risk classification based on risk factors envisaged in the Operating Risk Management in the JSB "Gazprombank" (CJSC) № 25-П dated 16 June 2007.

5.1. Man-made threats are caused by human activities. Among them, there are threats that arise from both unintentional (involuntary) actions: threats caused by errors in the design of the information system and its elements, errors due to actions by the personnel, etc., and also threats that arise due to wilful acts related to self-interested, idea-driven or other aspirations of people.

Man-made threats include those related to instability and controversial nature of requirements by the regulators of the Bank and controlling bodies with actions by the leaders and management, inadequate goals and the prevailing conditions, used services and the human factor.

5.2. Technology-related threats are caused by the impact experienced by the asset due to the threat of objective physical technology-related processes, technical status of the environment of the asset under threat or of the asset itself, which do not directly depend on human activities.

The technology-related threats may be failures, including operations-related failures, or destruction of man-made systems.

5.3. Natural threats are caused by the impact experienced by the asset under threat due to objective natural physical processes, acts of God, physical environment conditions which are not directly affected by human activities.

Natural threats include meteorological, atmospheric, geophysical, geomagnetic ones, etc., including extreme weather conditions, meteorological phenomena and natural disasters.

The sources of threats to the Bank's infrastructure may be both external and internal.

6. Adversary Model

For the purposes of the Bank, interlopers may be divided into external and internal ones.

6.1. Internal interlopers.

The Bank shall view as potential internal interlopers:

- registered users of the Bank's information systems;
- the Bank employees who are not registered users and have no access to the Bank's information system resources but have access to the buildings and premises;
- personnel that services the hardware of the Bank's corporate information system;
- employees of the Bank's autonomous structural units, involved in software development and support;
- employees of the Bank's autonomous structural units, responsible for the Bank security;
- leaders of various levels.

6.2. External interlopers.

The Bank shall view as potential external interlopers:

- former employees of the Bank;
- representatives of organizations which interact on matters of the technical support provided to the Bank;
- customers of the Bank;
- visitors to the Bank's buildings and premises;
- lending institutions which are competitors of the Bank;
- members of criminal organisations, security services employees or those who operate by their order;
- persons, that inadvertently or intentionally penetrated the Bank's corporate information system from external telecommunications networks (hackers).

6.3. In respect to internal and external interlopers, the following restrictions are put in place and the following assumptions about the nature of their potential actions are made:

- the interloper conceals his/her unauthorised actions from other Bank employees;
- the interloper's unauthorised actions may result from errors made by users, operating and

servicing personnel, as well as from deficiencies of the approved technology of processing, storing and transferring information;

- in their activities a potential interloper may use any available information eavesdropping tools, any information impact tools and information systems, relevant funds to bribe personnel, blackmailing, methods of social engineering and other tools and methods to achieve their goals;
- the external interloper may act in collusion with the internal interloper.

7. Main Information Security Provisions

7.1. Information security requirements set forth by the Bank shall be binding upon all Bank employees and users of information systems.

7.2. Acting in line with the established procedures, the Bank management shall welcome and encourage activities of the Bank employees and information system users aimed at maintaining information security.

7.3. Failure to perform or poor performance by the Bank employees and information system users of their responsibilities to maintain information security may lead to denial of access to information systems, as well as the application of administrative actions to those at fault and the extent of such actions shall be determined as prescribed by the Bank or the requirements of current legislation.

7.4. The Bank's strategy for countering information security threats shall constitute a balanced implementation of mutually complementary measures to maintain security: from organizational measures at the Bank management level to specialized information security measures for each risk identified by the Bank on the basis of the information security risk assessment.

7.5. In order to support the set level of protection, the Bank shall employ the process-based approach to building the information security management system. The Bank's information security management system shall be based on the following major processes (planning, implementation and operation of protective measures, checking (monitoring and analysis) and improvement) which meet the requirements of Standard STO BR BSIS –1.0 of the Bank of Russia and the provisions of international information security protection standards. These processes shall be implemented as a continuous cycle of –"planning – implementation – checking – improvement –planning" aimed at the continuous improvement of the Bank activities to maintain and improve information security.

At all stages of the life cycle, the Bank shall manage information security by complying with normative documents that define the Bank operating risk management processes.

7.6. The Bank undertake the following actions to maintain information security as part of the planning activities:

7.6.1. Determination and distribution of roles of the Bank personnel related to information security (information security roles).

7.6.2. Assessment of importance of information assets with due regard to the need for ensuring their properties from the information security perspective.

7.6.3. Information security risk management, which includes:

- analysis of impact caused on the Bank's information security by technologies used in the Bank activities, as well as external events;
- identification of information security issues, analysis of their causes and forecasting of their development;
- determination of models of information security threats;
- identification, analysis and assessment of the major information security threats to the Bank;
- identification of potential negative effects to the Bank, which materialise due to the occurrence of information security risk factors, including those related to the breach of security properties of the Bank's information assets;
- identification and analysis of information security risk events;

- assessment of the magnitude of information security risks and identification of those among them which are unacceptable to the Bank;
- processing of results of information security risk assessment based on the methods for operation risk management defined by the Bank;
- optimization of information security risks due to the selection and application of protective measures that counter the risk factors and mitigate potential adverse effects to the Bank, if such risk events occur;
- assessment of the impact of protective measures on the goals of the Bank core activities;
- evaluation of costs of implemented protective measures;
- review and assessment of various options for delivering information security objectives;
- development of risk management plans providing for various protective measures and options for their application, and selection of such measures which implementation will positively affect the goals of the Bank core activities and will be optimal in terms of expenses incurred and expectations;
- documentation of goals and objectives of the Bank's information security activities, update of regulatory and methodological support for information security activities.

7.7. As part of implementation of information security activities, the Bank shall perform the following:

7.7.1. Management of information security incidents, including:

- collection of information on information security events;
- identification and analysis of information security incidents;
- investigation of information security incidents;
- prompt response to information security incidents;
- minimization of negative effects of information security incidents;
- prompt communication of information on the most significant information security incidents to the Bank management and prompt decisions made on them, including regulation of the procedure to respond to information security incidents;
- implementation of adopted decisions on all information security incidents within the set deadlines;
- review of applied information security requirements, measures and mechanisms upon review of the information security incidents;
- improvement of knowledge of the Bank personnel on matters associated with information security;
- ensuring regulation and management of access to software, hardware and services of the Bank's automated systems and information processed therein;
- application of information encryption tools;
- ensuring continuous operation of automated systems and communications networks;
- ensuring renewal of operation of automated systems and communications networks after failures and emergencies;
- application of malware protection devices;
- ensuring information security at the stages of the life cycle of the Bank's automated systems related to design, development, purchase, delivery, commissioning, support (maintenance services);
- ensuring information security in using Internet access and email services;
- control over access to the Bank's buildings and premises.

7.7.2. Ensuring information protection against leaks via technical channels, which includes:

- application of measures and hardware reducing probability of unauthorised receipt of verbal information – passive protection;
- application of measures and hardware creating interference in the unauthorised receipt of information – active protection;
- application of measures and hardware which make it possible to detect channels of unauthorised receipt of information - search.

7.8. For the purposes of checking information security activities, the Bank shall:

- control the correctness of implementation and the operation of protection measures;
- control changes in the configuration of the Bank's systems and sub-systems;
- monitor risk factors[3] and their relevant revision;
- control the implementation and execution of requirements of internal normative documents on the Bank's IS protection by the Bank employees;
- control the activities of employees and other users of the Bank's information systems aimed at detecting and preventing conflicts of interests.

7.9. For the purposes of information security improvements, the Bank shall periodically and, if necessary, promptly specify/review information security goals and objectives (if the Bank changes the goals and objectives of its core activities).

8. Organizational Framework for Information Security Activities

8.1. To meet the information security objectives of the Bank in accordance with the recommendations of international and Russian security standards, the Bank must define the following roles:

- **Supervisor;**
- **Responsible Unit;**
- **Bank Employee.**

If necessary, other information security roles may also be defined.

8.2. The **Responsible Unit** shall perform and coordinate the Bank's operational activities and planning of information security activities. The goals of the **Responsible Units** shall be the following:

- establish the Bank's needs to apply the information security measures set by both internal corporate requirements and those of regulatory acts;
- comply with current federal legislation, regulatory acts of authorised federal executive bodies for security and countering technical intelligence agencies and for technical protection of information, normative acts of the Bank of Russia and standards of the Bank of Russia on information security, information security regulations, privacy and nondisclosure adopted by regulators of markets where the Bank's business and interests are represented;
- develop and review the Bank's internal normative documents on information security, including plans, policies, procedures, instructions, methodologies, the list of data and other types of internal normative documents;
- control the relevancy and consistency of internal normative documents (policies, plans, methodologies, etc.) addressing the Bank's information security matters;
- train, control and work directly with the Bank personnel in the area of information security;
- plan the application of, participation in the delivery and operation of information security devices at the Bank's facilities and systems;

[3] The term "risk factor" is determined in the Operational Risk Management Policy in JSB "Gazprombank" (JSC) № 25-ПР dated 16 June 2006.

- identify and prevent the materialisation of information security threats;
- identify and respond to information security incidents;
- inform responsible persons (Banking Risk Analysis and Control Department) about information security threats and risk events in line with the established procedure;
- forecast and prevent information security incidents;
- curb unauthorised activity of information interlopers;
- maintain the information security incident base, analyse and develop optimum procedures to respond to incidents and train personnel;
- standardize solutions associated with the application of the information security measures and tools and roll over standard solutions across the Bank's branches and representative offices;
- ensure the operation of information security devices and mechanisms;
- monitor and assess information security activities, including the assessment of completeness and sufficiency of the Bank's protective measures and types of activities to maintain information security;
- control the Bank's information security activities, including and on the basis of data about information security incidents, results of monitoring, assessment and audit of information security;
- inform the Bank management and the heads of its autonomous structural units of the Bank about information security threats affecting the Bank business.

8.3. The **Responsible Unit** may set up operational teams to investigate information security incidents, led by an employee of the **Responsible Units** and may involve employees of other autonomous structural units of the Bank to work therein on the basis of combining work in the team with their main job duties if there is a reasonable need and upon agreement with the heads of relevant units.

8.4. Work to implement this Policy provisions shall be financed both from the special purpose budget of the Bank's **Responsible Unit** and from the budgets of business units and IT Block units.

8.5. The main functions of the Supervisor on information security matters shall be the following:

- appoint responsible persons in the IS sphere,
- coordinate and put in place information security activities in the Bank.

8.6. In fulfilling duties assigned to them, and as part of their participation in the operational activity to ensure information security at the Bank, the Bank employees shall have the following main goals:

- comply with information security requirements set by the Bank's normative documents;
- identify and prevent the materialisation of information security threats within their competence;
- identify and respond to information security incidents;
- inform responsible persons (Banking Risk Analysis and Control Department) about detected threats and risk events associated with information security in line with the established procedure;
- forecast and prevent information security incidents within their competence;
- monitor and assess information security within their own area of work (work place, structural units) and within their competence;
- inform their own line managers and the head of the **Responsible Unit** about any threats identified in the Bank's information environment.

9. Responsibility for Compliance with Policy Provisions

The Supervisor shall perform the overall management of the Bank's information security activities.

The head of the **Responsible Unit** shall be responsible for updating this Policy provisions, introducing, coordinating and amending processes of the Bank's IS management system.

The responsibility of the Bank employees for failure to comply with this Policy shall be determined by relevant provisions included in agreements with the Bank employees, as well as by provisions of the Bank's internal normative documents.

10. Control over Policy Compliance

The Supervisor shall exercise overall control over the status of the Bank's information security.

The **Responsible Unit** shall exercise routine control over compliance with this Policy by monitoring and managing the Bank's information security incidents upon the results of information security assessment and also within other control actions.

The Internal Control Department shall monitor compliance with this Policy on the basis of internal audit of information security.

11. Final Provisions

11.1. Requirements of this Policy may be followed up with other internal normative documents of the Bank to supplement and specify the former.

11.2. Should current legislation and other normative acts, as well as the Articles of Association of the Bank be amended, this Policy and its amendments shall be applied where they do not run counter to newly adopted legislative and other normative acts, as well as the Articles of Association of the Bank. In such a situation, the **Responsible Unit** must immediately initiate relevant amendments.

11.3. This Policy shall be amended on a regular and ad hoc basis:

- regular amendments to this Policy should be made at least once in 24 months;
- unscheduled amendments to this Policy may be made upon the results of analysing information security incidents, the relevance, sufficiency and effectiveness of the utilised measures of information security protection, the results of conducted internal information security audits and other control actions.

11.4. The head of the **Responsible Unit** shall be responsible for amending this Policy.

Responsible person	Head of the IT Protection Department of the Information Protection Division of the Security Service (Department)		A.K.Pleshkov