Information security (IS) policy of JSC CB GLOBUS (public)

General principles of information security of the Bank

1. The Bank uses the following approaches to ensure information security (hereinafter referred to as IS):

1) a list of information containing information with restricted information;

2) a list of critical business processes has been created and approved, which are used to information security risks are assessed and further processed;

3) rules for access to information resources and software and hardware systems are established;

4) control of physical and logical access to all designated resources are controlled;

5) password protection of software and service resources is provided;

6) anti-virus protection of software and service resources is provided;

7) network protection is provided;

8) identification and authentication of all designated resources;

9) cryptographic protection of information is ensured;

10) audits of the information security management system (hereinafter referred to as ISMS) and analysis of the ISMS by the Bank's management;

11) monitoring and improvement of the ISMS.

2. The Bank adheres to the following rules in terms of ensuring security and business continuity activities:

1) employees of the Bank and third parties participate in maintaining the appropriate level of within the scope of their duties and powers and are responsible for its violations within the limits established by the current legislation of Ukraine and acts of internal regulations of the Bank;

2) during the development, implementation and operation of software and hardware systems software and hardware systems shall take into account the requirements of the IS;

3) public services of the Bank and internal networks of the Bank shall comply with the IS;

4) the Bank ensures the establishment and monitoring of compliance with all IS requirements, that are available in agreements with third parties regarding participation in international payment systems and money transfer systems;

5) the Bank shall comply with the Bank's IS and Information Technology Development Strategy;

6) the Bank's management shall create conditions for the Bank's employees for systematic training in IS standards and measures to reduce the risks of of IS incidents;

7) the Bank shall develop, implement, systematically test and update plans in case of various unforeseen critical situations:

- business continuity plan in case of emergency business continuity plan;

- a plan to ensure the continuous operation of information systems in case of emergency systems in the event of an emergency.

3. Information created, processed or held by the Bank in connection with the banking activities, as well as the processes of processing information and information assets used by these processes are important business resources of value to the Bank.

The Bank takes measures to protect information and information assets from threats of unauthorised use, modification, destruction, blocking of access, and as well as to ensure the integrity, controllability and observability of information information processing.

The main task of the IS is to minimise the Bank's IS risks associated with banking activities in accordance with the activities in accordance with the requirements of the Bank's IS Policy.

4. Setting goals, developing and implementing the strategy and main directions of the Bank's IS, control over their implementation shall be within the competence and prerogative of the Management Board of the Bank.

The functions of managing and maintaining the IS regime, as well as developing and updating the the Management Board of the Bank assigns to a separate structural unit of the IS.

All employees of the Bank must be familiar with, correctly understand and fulfil their duties and functions to ensure the Bank's security. The security regime is understood and unconditionally supported by the Bank's management.

5. The Bank's IB policy is based solely on its production interests in accordance with the requirements of the legislation of Ukraine, contracts, obligations to be fulfilled by the Bank.

In case of discrepancies, the requirements of the legislation of Ukraine shall take precedence over the requirements of other regulatory acts.

6. All information at the disposal of the Bank in connection with the conduct of banking activities shall be banking activities, shall be classified by categories of access restriction and criticality in relation to the performance of such activities.

The Bank shall ensure, in accordance with the requirements of the legislation of Ukraine, restriction of access to information relating to the activities and financial condition of customers, as well as unpublished information on issuers and their securities, if this information is classified as information is classified as ‘bank secrecy’ and ‘insider information’ respectively.

The Bank shall ensure, in accordance with the requirements of the legislation of Ukraine, restriction of access to personal data processed in the Bank's personal databases, in respect of which it acts as the owner or manager, except for personal data of certain categories of citizens or their exhaustive list, which are prohibited from being classified as restricted information (hereinafter referred to as RI) by the legislation of Ukraine.

The Bank shall exercise the right to restrict access to information related to its activities and declaring them a trade secret or confidential information if disclosure of such information may harm the interests of the interests of the Bank, except for the information that, in accordance with the legislation of Ukraine, may not may not be classified as a trade secret, confidential information or information, access to which cannot be restricted.

The Bank's employees and outstaffers are granted access to the PII only if they sign a non-disclosure agreement.

Access to PII and other critical information is granted to third-party organisations that have business relations with the Bank, is granted only if they have legally significant documents that define the requirements of the IS and the obligations of the parties to protect this information.

Personal data may be disclosed only with the consent of the individual in respect of whom in respect of whom his/her personal data is processed in accordance with the law.

7. IS requirements for the Bank's interaction with other participants in payment systems are based on the model of mutual distrust.

8. The Bank shall have the right and obligation in cases determined by the legislation of Ukraine to to defend, using all legitimate measures necessary for this purpose, its rights and the rights of its customers in cases of unauthorised disclosure of PII or other unauthorised actions regarding critical information or information assets at the disposal of the Bank in connection with the conduct of banking activities.

9. IS ensured by applying a set of IS control measures (information information security system - IS), which implements the requirements of the Bank's IS Policy.

The IPS shall ensure:

1) impossibility of disabling or bypassing the IPS;

2) integrity and continuity of protection at all stages of the information life cycle information life cycle;

3) optimality - minimum sufficiency of the degree of protection;

4) delimitation of access and powers of executors to information assets of the Bank and information processing processes based on the principle of minimum sufficiency (‘need-to-know’ principle);

5) minimisation of the number of gateways between internal processing environments controlled by the Bank and external uncontrolled environments ;

6) building bank automation systems with the use of modern technologies and cryptographic algorithms for information security, secure operating systems and database management systems and database management systems;

7) maximum level of protection of key information of IPS;

8) minimisation of the ‘human factor’ in the process of applying protection means information.

10. The Bank's personnel is an important and integral part of the IPS.

The Bank establishes the level of requirements for the professional level and reputation of the personnel that performing key roles in ensuring IS.

The Bank takes measures to communicate the requirements of the IS Policy, raise awareness and qualification of the Bank's employees in the field of IS.

10. The Bank's staff is an important and integral part of the IPS.

The Bank establishes the level of requirements for the professional level and reputation of the personnel performing key roles in ensuring IS.

The Bank takes measures to communicate the requirements of the IS Policy, raise awareness and qualification of the Bank's employees in the field of IS.

11. The Bank analyses IS risks and the level of compliance of the the level of compliance of the IPS with these risks. The Bank's IS Policy is subject to periodic review and adjusted to take into account and minimise the current level of IS risks.

12. The Bank introduces a mechanism for notification and response to IS incidents.

13. The Bank constantly monitors the operation of the IPS and critical information processing systems. information processing systems. The Bank declares its right and carries out, within the limits provided for by the legislation of Ukraine, to monitor the actions of personnel and third-party organisations regarding access to the IPS, critical information and information assets of the Bank.

14. The Bank shall proactively plan measures to ensure continuity of banking activities in terms of information processing, preservation of critical information and information assets , and preventing disclosure of the Bank's PII in emergency situations. The Business Continuity Management Policy is approved by the Management Board of the Bank and provides for a set of measures to preserve critical information (including commercial and banking secrets).