



BroadHub

ISMS-GOV-01 Information Security Policy

Release	Date	Author	Release notes
1.0	30 Dec 2025	Hennadii Semibratov	Document creation and approval

1. Introduction

The purpose of Information Security Policy is to define and describe the approach to Information Security and serves as a basis for specific policies, procedures and guidelines.

Scope of the Policy as well as maintenance, updating and distribution is governed according to the [ISMS-DH-02 Document and Data Control Procedure](#).

2. Information Security Overview

2.1. Information Security and its Goals

Information Security is the way to address information-related risks, which consists of processes and technologies, managed by people in order to ensure confidentiality, integrity and availability of ConvoX information:

- Confidentiality – ensuring that information is accessible only to authorized persons, inside and outside of ConvoX,
- Integrity – safeguarding the accuracy, completeness and timeliness of information during storage, processing and transfer,
- Availability – ensuring that authorized persons can access information when necessary.

In accordance with ConvoX strategic vision, Information Security is pursuing following business goals:

- Fulfill requirements of the customers,
- Gain competitive advantages in the market,
- Increase transparency of security investments,
- Avoid or minimize damages from incidents related to violation of confidentiality, integrity and availability of information
- Protection of privacy, and
- Building the reputation of a technology leader.

Information Security is an integral part of ConvoX. Changes in organization and business processes, as well as ConvoX-wide projects, are implemented considering the Information Security matters.

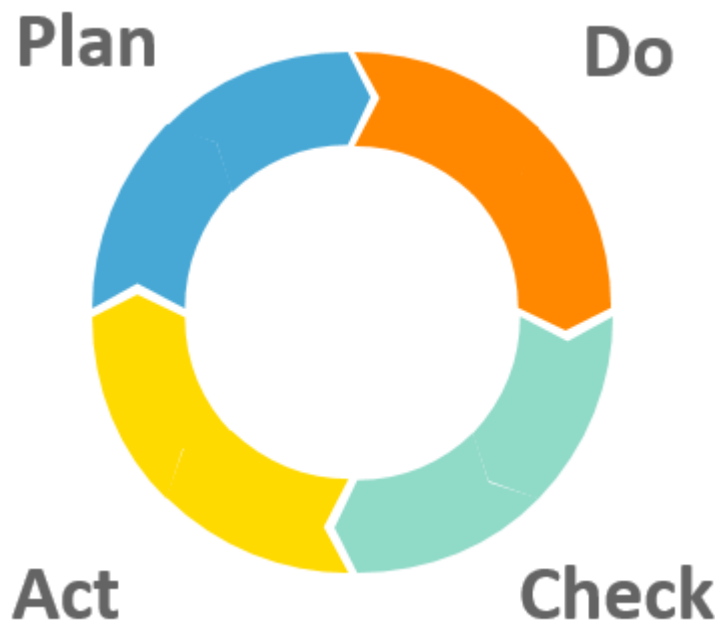
2.2. Information Security Management System

ConvoX follows an established systematic and continuous approach to management of Information Security – Information Security Management System (hereinafter – ISMS) – in accordance with international standard ISO/IEC 27001:2022 "Information security management systems — Requirements".

Information Security at ConvoX applies to development, distribution, sales, operation and support of information systems-for offering games of chance, the result of which is based on a random number generator and other games of chance that are all offered via the internet.

2.3. Information Security Management System Operation

ISMS operates based on the continuous improvement according to Plan-Do-Check-Act lifecycle:



The cycle repeats annually.

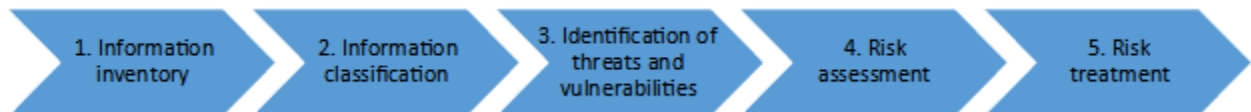
Lifecycle stage	Stage description
Plan	- Review and update Information Security Policy and other security regulations; - Review and update approach to Information Security risk assessment and risk treatment; - Plan and budget necessary resources for Information Security (people, finance,

	technology, etc.).
Do	- Identify and assess Information Security risks; - Review and update existing risk treatment measures, design new ones and implement them; - Educate in Information Security.
Check	- Review and measure Information Security effectiveness; - Conduct internal Information Security audits; - Identify gaps in Information Security operations. - Report to the Top Management.
Act	Design and implement actions to address identified gaps in Information Security.

Information Security is an integral part of daily business operations. Information security function operates in ConvoX continuously.

3. Management of Information Security Risks

ConvoX has established an Information Security risk management process aimed at identifying the risks related to the leakage, loss and undesirable modification of the ConvoX information, and at establishing measures related to the addressing of these risks. The risk management process consists of the following steps:



For additional information about Information Security risk management methodology, refer to the [ISMS-RM-02 Information Security Risk Assessment, Review and Treatment Procedure](#).

3.1. Information Inventory

Inventory of information assets and resources is performed in order to identify valuable information within ConvoX, define its owners and identify storage places, processing and transmitting means. The inventory covers information stored in databases of information systems, located on the network and cloud drives, in the paper documents, and so on. Owners of information assets defined during Information resource inventory are responsible for secure operation of the asset. For additional information about Inventory of Information Resources, refer to the [ISMS-RM-01 Information Asset Inventory Procedure](#).

3.2. Information Classification

Each information asset or resource is categorized by evaluation of its confidentiality, availability and integrity aspects by assessing possible damages in case of information leakage (violation of confidentiality), undesirable modification (violation of integrity) and data loss (violation of availability). The following types of potential damages are considered for classification:

- financial losses
- delays in business processes
- damages to reputation, and
- regulatory sanctions.

3.3. Identification of Threats and Vulnerabilities

Storage places, transmitting and processing facilities have their own vulnerabilities. These threats and vulnerabilities are determined and analysed in order to define risks of probability of information leakage, loss or undesirable modification.

3.4. Risk Level Assessment

Risk Level is defined as a combination of potential damage and its probability. Using the results of classification, where the potential damage was determined, and threats-vulnerabilities analysis, where the risk probabilities were evaluated, Information Security risk levels are assessed according to the following scale:

- critical
- high
- medium, or
- low

Depending on the risk levels, different treatment options are used to address the risks.

3.5. Risk Treatment

There are four options to address (or treat) the risks:

- minimization – implementation of security measures in order to reduce probability of a risk and the damage caused by it,
- avoidance – renunciation of the processes or technologies that cause the risk,
- acceptance – deciding to accept the risk, mostly applicable for the low risks, and
- transfer – insurance or contract with a third party to cover the damage caused by the risk.

Treatment options for each risk are selected considering the risk level and treatment costs.

4. Human Resource Security

Since Users work with sensitive and proprietary information when fulfilling their job duties, respective Information Security measures are established to contribute to the protection of ConvoX information against

leakage, loss and undesirable modification. These measures are applied during the whole employment cycle from the job application to the employment termination.

For additional information about HR Security, refer to the [ISMS-HR-01 Human Resources Security Policy](#).

5. Information Security Awareness

Information Security awareness is a set of activities aimed at raising awareness in ConvoX employees and contractors regarding the Information Security risks and the measures to treat them.

Detailed information security awareness program is managed by the Information Security team. The Information Security team controls the completion of training.

6. Use of ConvoX Resources and Information

6.1. Office Premises

ConvoX premises shall be perceived as premises with free access. The same rules and policies should be applied during working in ConvoX offices as working at any other location.

6.2. Workstations, Email, Internet, Information Systems and Services

Each ConvoX employee and contractors shall follow these rules:

- Passwords to workstations, information systems and services must be kept secret
- Workstation must be locked when idle
- It is prohibited to install unlicensed software
- Corporate email accounts must be used for business purposes only
- Any suspicious or unknown email attachments and links must not be opened
- Limited personal use of the corporate Internet resources is allowed as long as it does not conflict with the ConvoX business interests
- Inappropriate use of the corporate Internet resources is prohibited, including storing of unlicensed content, drug trading, porn, and other indecent uses
- It is prohibited to download and store any malicious files from the Internet
- It is prohibited to attempt to hack, deny services of ConvoX resources, or eavesdrop any communications
- To gain remote access to the ConvoX network and information systems, secure connections must be established
- It is prohibited to use removable media to store or transfer ConvoX information
- Any suspicious activity on a workstation or within other ConvoX resources must be reported immediately to the Information Security team

For more information about Workstation Use refer to [ISMS-GOV-03 Acceptable Use Policy](#).

7. Access Management

To ensure access to ConvoX information is restricted only to the authorized individuals based on least-privilege principle, the access management process was established. This process is applied to ConvoX employees, contractors and third parties representatives at the sites where information is processed and stored, including:

- information systems,
- network and cloud resources,
- source code repositories,
- ConvoX network, operating systems, databases.

Access management process as described below covers the following types of access:

- user standard – access rights according to perform job duties,
- administrative – privileged access rights for administrative purposes, and
- technological – privileged access rights for information systems.

Specialists of the Information Security team shall identify and register all privileged operations associated with each system product, e.g., operating system, relational database management system and applications. Each component in use may have a set of privileged operations. All privileged user accounts and groups need to be reported to the Specialist of Information Security team.

Privileges must be allocated based on the roles, such as, Security administrator, Computer operator, System administrator, Database administrator etc. Privileges may be assigned to an individual in exceptional cases. Alternatives to granting privileges to roles or to individuals shall be considered where roles cannot be used. These situations shall be addressed in appropriate risk assessments.

Privilege access must be monitored and revoked when an individual no longer has need for the use of the access.

Accounts shall be automatically or manually locked by the System Administrators based on the following criteria:

- Not more than 5 consecutive failed logons (account will automatically be locked for minimum 15 minutes). The failed logon counter shall reset automatically to zero whenever a successful logon is achieved
- Reached the expiration date
- Inactive for more than 120 days
- Suspicion of being involved in a security incident.

Locking and unlocking of an account shall be an audited event. System Administrators shall maintain a proper registration of the account unlocking frequency and involved user accounts and inform Specialist of Information Security team whenever demanded.

8. IT Security

ConvoX applies a number of technical security measures in order to avoid and minimize Information Security

risks related to information systems, operating systems (OS), database management systems (DBMS), network and their physical infrastructure. These measures include the following:

- access control – use of authentication and authorization mechanisms, logging of access instances,
- cryptography – encryption of data storages, laptop hard drives, removable media, network connections and other data carriers,
- specialized security tools – firewalls, antivirus protection, security information and event management (SIEM) system and Virtual Desktop Infrastructure (VDI),
- management of technical vulnerabilities – automated and manual scanning for vulnerabilities, penetration testing.

For additional information about IT security requirements, refer to [ISMS-GOV-07 IT Security Controls Guideline](#).

9. Information Preservation

ConvoX has established a business continuity management process that ensures availability of ConvoX resources for business operations. The process covers risks related to violation of ConvoX information availability. Within this process, requirements to the availability of ConvoX information are identified and measures for data loss risk treatment are established, in particular:

- information processing, transmission and storage facilities redundancy,
- data and records backup.

Information Security team shall ensure that information security continuity is established with due regard to the results of the Information Security risk assessment.

For additional information about Reservation, refer to [ISMS-BCM-01 Information Backup Policy](#).

10. Security in Information Systems Lifecycle

Information Systems are acquired, developed and maintained considering the information security matters, including the following:

- authorization – acquisition and development of new information systems, as well as analysis and authorization of each change prior to the development for correspondence with business needs and compliance with information security requirements,
- development – after authorization, the business analysis is performed and technical specifications are developed. Based on the technical specification, the information system is acquired or developed,
- testing – after being developed, an information system or change is tested by the QA specialists and business users against test cases,
- approval – if testing is successful, an information system or change is approved prior to the implementation in the production environment by the respective owner,
- assessment and monitoring procedures – after being implemented in the production environment, the respective information system is monitored. In case of any mistakes, they are communicated to the developers for fixing. In addition, periodic reviews of changes, introduced in the production

environment, are performed to ensure that an IS change was introduced under the established process.

Development, testing and production environments of information systems are segregated. Refer to [ISMS-SBD-02 Secure Development Guideline](#) for details.

11. Third Party due diligence

Prior to contracting with a third party, it should be assessed as to credibility by means of its background check. In addition, if a third party is granted access to ConvoX information, the state of its information security is assessed by means of questioning and review of security measures. The severity of this assessment depends on the level of access that is going to be granted to the third party.

12. Information Security Incident Management

Information Security incident management is a process aimed at detecting and responding to the security breaches in a timely manner in order to avoid or minimize damage to ConvoX.

12.1. Incident Definition and Properties

An incident is any event which is not part of the standard operation and which causes or may cause an interruption to, or a reduction in, the quality of the service. Incidents also result from inadequate or failed operation of internal processes, people or systems, or from external events, whether intentionally, by error or inherently.

An information security incident is defined by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

A Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data. This includes breaches that are the result of both accidental and deliberate actions.

12.2. Incident Record Properties

All incident management processes must have the necessary incident properties to enable recording, tracing and resolving of incidents in a systematic and structured way. These are also important for centralized reporting and data collection. The following rules must be applied when incident properties are defined.

- Every incident must be uniquely identifiable and traceable
- Information about actual and suspected incident is confidential and should be shared on a strict need to know basis
- All incidents must be categorized
- All necessary dates related to the incident must be recorded.

- All necessary information gathered during the lifecycle of the incident must be recorded.
- A structure must be in place to prioritize incidents.

The [ISMS-IM-02 Information Security Incident Management Procedure](#) describes the definition, categorization and the structure of information security incidents in more detail.

13. Compliance

ISMS is established in accordance with the following industry regulations and national laws in the countries where ConvoX operates.

14. Deviations and exceptions

Information Security deviations are the nonconformities that can be identified during the 'Check' stage of the PDCA lifecycle. All Information Security deviations must be registered by information security analysts in the nonconformities database contains at least the following information:

- Issue / Observation description
- Needed actions description
- Planned fix date
- Responsible person
- Evidence and results.

Information Security exceptions are the situations in which the regular information security requirements are not technically or organizationally applicable. All Information Security exceptions must be registered by information security analysts in the appropriate register of the nonconformities database to permanently control weak points of the ISMS. Exceptions register must state at least the following information:

- Exception description
- Non-complied regulatory or process requirement
- Date of identification
- Responsible person from the business
- Description of the applied compensating controls.

All Information Security exceptions must be approved by the Information Security Team.

15. Information Security Review and Improvement

ConvoX Information Security shall be regularly monitored and continuously improved. Performance of the ISMS is measured by the Information Security team by performing operational testing of the controls. Based on the operational test results, the Information Security team prepared a report with the identified gaps and developed corrective actions including consequences for non-compliance.

16. Disciplinary actions

Violation of this Policy will be handled by local management following the standard operating procedures on disciplinary actions. Violations may therefore lead to verbal warnings, written warnings and, in severe or repeated cases, to dismissal.