TGT

# TGT Information Security Policy

**Author(s)**

DILJITH PADIKKAL KANDY
Version: 3.0

## Documentation Approval

| Role | Name | Title | Date | Signature |
|---|---|---|---|---|
| Author(s) | Diljith Padikkal Kandy | Senior IT Security Specialist | 05-June-2023 | |
| Approver(s) | Saad Bargach | Chairman & Chief Executive Officer | 05-June-2023 | |
| Approver(s) | Andre Sayeh | Chief Financial Officer | 05-June-2023 | |

## Documentation Change History

| Version | Effective Date | Description of Change | Change Made By |
|---|---|---|---|
| 1.0 | 26-December-2017 | | Roman Komissarenko |
| 2.0 | 02-February-2021 | Rebranding changes | Roman Komissarenko |
| 3.0 | 05-June-2023 | Routine Revision and Minor Changes | Diljith Padikkal Kandy |

# Contents

## 1. Introduction

The Information Security Policy of TGT Oilfield Services (the "Company") defines the purposes and tasks of the information security ("IS") system and introduces a set of IS rules, requirements and guidelines for the Company to observe when doing its business.

## 2. Purpose

The Purpose of the Information Security (IS) Policy are to safeguard the Company's information and ensure the smooth functioning of the entire information and computing infrastructure in alignment with the activities defined in the Company's Charter. The CEO of TGT Oilfield Services assumes overall responsibility for managing the process of ensuring information security within the organization. The department heads are accountable for ensuring compliance with the IS requirements within their respective departments.

All employees of the Company are required to adhere to the procedures for handling confidential documents, important information carriers, and other secure information, as well as comply with this IS Policy.

## 3. Policy Statement

The Information Security (IS) Policy is designed to protect valuable information assets from threats posed by unauthorized actions of intruders, minimize risks, and mitigate the potential negative consequences of accidents, unintentional employee errors, technical failures, and incorrect process and organizational decisions during the handling, transmission, and storage of information.

The IS Policy, along with the corresponding IS management system, serves as the most effective means of mitigating compliance risks related to information security for the company.

The IS strategy encompasses pre-defined response measures against potential attacks and encompasses software, hardware, and organizational solutions that enable the company to minimize potential losses arising from accidents, failures, and staff errors.

The objectives of the IS Policy are to:

- Management of the Company's IS System
- Define Information Security (IS) Policy
    - Virus Protection Policy
    - User Account Policy
    - Information Resource Access Policy
    - Automated Workstation Security Policy
    - Backup Policy
    - Password Policy
    - Sensitive Date Processing Policy
- Define Information Security (IS) Support Procedures

## 4. Scope

This policy is applicable to all individuals employed by the Company, including employees, contractors, consultants, temporaries, and other workers, as well as personnel affiliated with third parties. It encompasses all information assets owned or leased by the Company.

## 5. Validity and Amendments

The Policy comes into effect on the directive of the CEO of TGT Oilfield Services. The Policy is deemed invalid upon the directive of the CEO of TGT Oilfield Services. Any amendments to the Policy are implemented in accordance with the directive of the CEO of TGT Oilfield Services.

Amendments to the Policy may be initiated by:

- CEO TGT Oilfield Services
- Information Security (IS) Specialist.

The Policy shall be updated on an annual basis to ensure the security activities defined in the Policy are relevant to the current information security requirements.

An unscheduled update of the Policy shall be performed in case of

- Implementation of new laws, regulations, or industry standards that impact the information security requirements.
- Incidents or breaches that highlight the need for policy enhancements to prevent future occurrences.
- Recommendations from internal or external audits, assessments, or security reviews that indicate the need for policy updates.

The Information Security (IS) Specialist shall be responsible for monitoring compliance with and updating (scheduled and unscheduled) of the Policy.

## 6. Compliance

Compliance with the organization's Information Security Policy is Mandatory for all users. Compliance checks will be performed on a regular basis by the Information Security team of the company. Any breaches or alleged breaches of this Policy will be investigated and directly reported to the Head of the concerned department to take Disciplinary action.

## 7. Role and Responsibilities

The Information Security (IS) Specialist is responsible for defining actions and ensuring information security. The responsibility for the implementation of the policies shall be allocated as follows:

- Development and maintenance of supporting information security policies and procedures (including communication and distributing the policies and procedures to the employees, as well as providing training to ensure their understanding and compliance).
- Monitor information systems to detect non-compliance with internal policies, information security anomalies (events and incidents).
- Overall responsibility for information security and related issues.
- Responsible for delivering security awareness and training to the employees.

## 8. Secured Information Resource Access Authorization

Employees may access the Company's secured information resources only after reviewing this Policy and other internal information system documents. Non-employees seeking access to information resources must agree to the access rules established by the Data Owner.

**Confidential Information**: All business or technical information of Discloser, whether it is received, accessed or viewed by Recipient in writing, visually, electronically or orally. Confidential Information shall include, without limitation, technical information, marketing and business plans, databases, specifications, formulations, tooling, prototypes, sketches, models, drawings, specifications, procurement requirements, engineering information, samples, computer software (source and object codes), forecasts, identity of or details about actual or potential customers or projects, techniques, inventions, discoveries, know -how and trade secrets. "Confidential Information" also includes all such business or technical information of any third party that is in the possession of the Discloser.

**Public Information**: The information derived from public sources, including mass media, television, radio, and other similar channels, is intended for publication in external public media outlets.

**Open Data**: Information sourced from individuals or business entities and such individuals or business entities have cancelled its confidentiality in terms of distribution and processing of such information. It is information generated during the operations of the Company and which shall not be treated as confidential subject. It is information which is made publicly available and used during the Company's operations.

**Limited Access Information**: Information which is not classified as any other type but should have limited access for certain types of users.

Company's approach to information security issues primarily revolves around preventing unauthorized or unintentional actions on data which classified as Limited Access Information and critical information resources essential for the Company's operations.

For these purposes the Company performs the following:

- Define procedures for dealing with documents, samples, etc. containing confidential information.
- Identifies users with access to such information and enforce relevant user access procedures.
- Develops controls for confidential documentation.

Third party confidential information is secured subject to contracts signed by TGT Oilfield Services with other entities. Personal data of an employee of the Company is the information the employer needs for the purposes of employment and is related to a particular employee.

## 9. Information Security Management System

The Information Security Management System (ISMS) of the Company is used to create, implement, operate, monitor, analyze, support and upgrade the information security at the Company.

To ensure successful operations of ISMS, the following processes shall be implemented:

- Defining and specifying the scope of ISMS and selecting an approach to assessing information security risks
- Defining and specifying the scope of ISMS based on the results of operational and legal risks assessment held by the leaders of the Company's departments.
- Evaluation and assessment of information security, along with the consideration of options for managing information security risks related to critical information assets.
- Identifying and specifying the information security purposes and security activities and their feasibility in terms of IS risk mitigation.

- Accepting residual risks by the management and deciding on how to implement, operate/improve ISMS. The information security residual risks shall be correlated with the operational risks of the Company, and their impact on the ability of the Company to reach its goals shall be assessed.

As part of Information Security Management, the following processes shall be implemented:

- Drafting an Information Security risk processing plan:
- Implementing the IS risk processing plan and implementing security tools, work and resource management processes related to the implementation of ISMS.
- Identifying and responding to security incidents
- Ensuring continuous operations and after failure recovery.

## 10. Risk Management

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the operational damage likely to result from security failures. The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls to protect against these risks.

The assessment of information risks within the Company involves the following stages:

- Identification and quantitative or qualitative assessment of critical information resources for the Company's operations.
- Evaluation of potential threats.
- Assessment of existing vulnerabilities.
- Evaluation of the effectiveness of information security tools.

## 11. Information Resource Access Policy

### 11.1 Purpose

The Policy defines the general rules of authorizing employees with access to secured information resources of the Company.

### 11.2 Provisions

Access to information resources is provided to users who have reviewed the rules of using information resources and responsibility for non-compliance with the rules and this Policy.
Each employee of the Company authorized to work with a certain information resource shall have a unique username (user account) to be used for signing up and working in the information system.
If necessary, some employees may have several usernames (user accounts). It is FORBIDDEN to have one and the same username ("group account") being used by several employees.

### 11.3 User account creation

A new user account shall be registered (created) and a temporary user account shall be extended subject to a request specifying the following:

- Job position (with a full name of the unit/department), full name and mobile telephone number of an employee

- Grounds for registration (number of the Order on Employment with the Company or any other agreement specifying a need for authorizing access to the information resources of the Company).

The request shall be sent by the Chief HR Officer or designee. Upon agreement with the IT Manager, the request is forwarded to a System Administrator who reviews the request and carries out the necessary operations to create or delete the user account. This includes assigning a password and providing minimum access rights to the Company's resources. Once the user account is registered, a notification is sent to confirm the completion of the task.

**11.4 Granting (modifying) User Authority**

Authority to access resources of the Company is granted (or modified) subject to a request of an employee or their manager.

The request shall specify the following:

- Job position and full name of an employee
- Username (user account) of the employee
- Name of the information asset (system, resource) to which the access is to be provided (or user authority is to be modified)
- Authorities which are subject to cancellation or additional granting (by specifying tasks the user is working on using certain information resources of the Information System) specifying allowed types of access to the resource (roles).

The request is agreed with the head of the department and forwarded to a System Administrator for completion. After the changes have been made to the request, the System Administrator sends a notification that the task has been completed.

**11.5 User Account Deletion**

When the term of the user authority expires (contract termination, dismissal), the user account shall be blocked immediately.

It is preferred to have the accounts of dismissed users disabled automatically through the use of relevant information systems.

The Chief HR Officer or designee shall file requests to disable accounts of dismissed employees in a timely manner, not later than a day before the end of the user term of office.

The request shall specify the following:

- Position and full name of an employee
- Username (user account) of the employee
- Date the user authority expires.

After the request has been reviewed, the system administrator disables the user account and sends a relevant notification that the task has been completed. If personal documents (user profile) must be kept at the Automated Workstation of the user after the termination of the office, the employee (or their immediate manager) shall in a timely manner (not later than three days before the end of the term of office) file a request to disable the user account specifying the term of storage of such information. The request shall be filed even if the accounts of dismissed employees are being disabled automatically.

Such a request shall be preliminarily agreed with the IT Manager and, after the account has been disabled, forwarded to a system administrator to address the data storage request.

### 11.6 Storage of Completed Requests

Completed requests shall be stored in the IT department for two years from the moment of disabling access to the information resources of the Company. Copies of completed requests shall be stored with the IT Manager.

The Copies may be further used:

- To restore user authorities in case of failures with the Information System of the Company
- To control validity of the right to access the information resource assigned to a particular user.
- By any system resource, to review any conflicts.
- By a system administrator, to verify if user access authority levels have been set correctly.

If a request cannot be completed, a reasoned rejection with the request attached shall be sent to the requester.

## 12. User Account Policy

### 12.1 Purpose

This Policy defines general rules of assigning user accounts to the users of the information assets of the Company

### 12.2 Provisions

Registration accounts are divided into:

- User accounts are used to identify/ authenticate users of information assets.
- System accounts used for the needs of the operating system.
- Service accounts are used to ensure the functioning of certain processes or applications.

Each user of the Company's information resources is assigned a unique registration user account. One user (e.g., a user with different levels of authority) may have more than one user account.

In general, it is forbidden to create and employ a group user account. If there is a need for doing so due to a special type of an automated business process or workflow (e.g., a team or shift work), the group account shall be ticked on user properties on the server and such specification shall explicitly identify the current owner of the user account at any specific time.

One and the same group account shall not be used by different users at one and the same time. System registration accounts are created by the system and shall be used only as specified in operating system documentation. Service registration accounts shall be used to start a server or application only.

The system or service account shall not be used in registering users with the system.

## 13. Password Policy

### 13.1 Purpose

The Policy defines general rules for passwords used in accessing secured information assets of the Company.

### 13.2 Provisions

Passwords must be created and managed in accordance with this section.

- Passwords must be changed immediately upon issuance for the first use. Initial passwords must be securely transmitted to the individual.
- All user-level passwords shall expire every 90 days and must be changed.
- New passwords cannot be the same as the previous four passwords.
- Passwords must be at least eight characters in length. Longer is better.
- Passwords must contain both uppercase and lowercase characters (e.g., a-z and A-Z).
- Passwords must contain at least one number and special characters (e.g., 0-9 , *<@).
- Accounts shall be locked after 5 failed login attempts within 30 minutes and shall remain locked for at least 10 minutes or until the System Administrator unlocks the account.
- Multi Factor Authentication should be enforced where possible.

## 14. Virus Protection Policy

### 14.1 Purpose

The Policy defines the general rules of implementing virus protection within the Company.

### 14.2 Provisions

All computer devices connected to the TGT Oilfield Services network and networked resources shall have anti-virus software installed and configured so that the virus definition files are current and are routinely and automatically updated. The anti-virus software must be actively running on these devices. Anti-virus software shall comply with current security requirements and shall not slow down PCs. The anti-virus software shall be secured with a password against any unauthorized disabling by a malware or intentional disabling by a user.

If deemed necessary to prevent propagation to other networked devices or detrimental effects to the network or data, an infected computer device may be disconnected from the Company network until the infection has been removed.

User Should:

- Avoid viruses by NEVER opening any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately then remove them from the Trash or Recycle Bin
- Delete spam, chain, or other junk mail without opening or forwarding the item.
- Never download files from unknown or suspicious sources.
- Back up critical data on a regular basis and store the data in a safe place.

## 15. Automated Workstation Protection Policy

### 15.1 Purpose

The Policy defines general rules and requirements for protecting personal data and other confidential information of the Company against unauthorized access, loss or modification.

### 15.2 Provisions

- When working with confidential or sensitive information, any review of it by unauthorized individuals or entities shall be prevented.
- When leaving a workplace for any reason, the workstation shall be blocked and portable machine-readable media with confidential information shall be kept in a locked room, locker, desk drawer or safe.
- Any unauthorized use of printing, facsimile, copying and scanning equipment shall be prevented by locating them in restricted access areas, using passwords or any other available techniques to control user access authority levels.
- Employees get access to resources of the computer network after they have reviewed documents approved by the standards of the Company (subject to the job position).
- Access to the components of the operating system and commands for system administration at user workstations shall be limited. The right to access such components shall be granted only to programmers of R&D on request by the R&D Leader. End users shall have access only to commands necessary to execute their job responsibilities.
- Access to information shall be provided only to individuals with reasoned needs for working with such data to execute their job responsibilities and may be completely limited by the management of the Company without any explanations, including access to the AW. Users shall not install unauthorized software on PCs. At any time, a system administrator may review the software configuration to control if any unauthorized software has been installed.
- Maintenance shall be provided only on request by a user to the system administrator.
- Any local maintenance shall be performed in the presence of the user.
- Any distance maintenance shall be performed only with the use of special-purpose software and the process shall be controlled.
- When performing maintenance, a minimum set of necessary actions shall be taken to address the problem described in the relevant request. At the same time, any actions shall be taken to further identify the initiator of such changes.
- Any copying of confidential information and temporary withdrawal of carriers of confidential information (including elements of the AW) shall be allowed only subject to permission of the user. If the carriers of confidential information have been withdrawn, the user shall be entitled to be present during the following operations.
- Software shall be installed from special resources or portable carriers and in conformity with the license agreement with its copyright holder. AWs where confidential information is supposed to be processed shall be assigned to relevant employees of the Company. Other users shall not use such AWs without agreeing with the Company's Information Security (IS) Specialist. If the AW is transferred to another user, a guaranteed erase of hard drive (formatting) shall be performed. A system administrator shall be entitled to reject handling a problem caused by software or equipment installed or set up at the workstation against this Policy.

## 16. Backup Policy

### 16.1 Purpose

The Policy defines general rules and requirements for protecting personal data and other confidential information of the Company against unauthorized access, loss or modification.

### 16.2 Provisions

To ensure data physical integrity and to prevent intentional or accidental loss or modification of secured information and information system configurations, a Hyper-V Virtual Farm has been created allowing backing up by burning a disc image. Such backup is performed on the servers of the Company in an automatic mode with the help of installed system tools.
Data storage servers are equipped with version control. Version control allows a user to restore the previous state of the file.

The following types of information shall be backed up:

- User personal data (personal directory on file servers).
- User group information (group directories of divisions and departments).
- Information necessary to restore servers and database management systems (DBMS)
- Information of automated systems including databases
- Data of reference and information systems (ERP, 1C, Consultant Plus, etc.)
- Production copies of installation software components of workstations
- Registration information of data security system of automated systems.

To ensure continuous operation of servers, RAID (Redundant Arrays of Inexpensive Disks) technology is used. The technology provides mirroring on all local servers of the Company.

Mirroring is a technology which enhances system reliability. In a RAID mirrored array, all data is replicated on one or more hard disks simultaneously. In case of failure of one of the disks, all the information remains safe on the other disk and the system administrator gets informed about the system failure.

For the backup purposes, a separate virtual machine-based server has been created. The server has the functions of backup system control and backup storage. All servers are backed up daily at **01:00 (Moscow time).** The servers of reference and information systems of general use are **backed up twice a day, at 12:00 and 18:00 (Moscow time)**. After each backup the system administrator is automatically sent a status report on each backup information system component. Workstations are not backed up.

To backup Microsoft SharePoint data, geo-replication is used. Geo-replication is a mirror replication of data in other Microsoft data processing centers online.
The system administrator of the Company shall be responsible for the results of and control over all backup processes. A unique backup key shall be stored for at least 14 days.

If necessary, the system administrator of the IT department restores data backed up on the basis of the backup server to the server subject to restoration or to the backup server.

## 17. Information System Support

Information security (IS) of information systems shall be ensured at each stage of the information system lifecycle (LC) when automating processes and also considering all the parties involved in the LC processes (developers, customers, suppliers of products and services and operating and supervising divisions of the Company). Drafting of specifications, design, development, testing and acceptance of information system security tools and systems shall be performed with the involvement of the Information Security (IS) Specialist and IT Manager. The development and implementation of information systems shall be subject to regulation and control.

Information systems shall be developed in compliance with the requirements, methodology guidelines and certain standards.

Commissioning, operation and retirement of the information system in terms of information security shall be performed with the involvement of the Information Security (IS) Specialist.

At the stages related to the information system development (definition of the requirement of related parties, analysis of requirements, architectural design, implementation, integration and verification, supply and commissioning), the developer shall ensure security against the following threats:

- Incorrect description of information system requirements
- Selection of inadequate lifecycle model including inadequate selection of lifecycle processes and participants
- Incorrect design solutions
- Defects added by the developer on the level of design solutions.
- Non-documented features of the information system added by the developer
- Inadequate (incomplete, conflicting, incorrect, etc.) implementation of information system requirements
- Poor quality documentation
- Assembly of the information system by the developer in conflict with the requirements resulting in availability of non-documented features of the information system or inadequate compliance with requirements
- Incorrect configuration of the information system
- Acceptance of the information system non-compatible with the requirements of the customer
- Non-documented features added to the information system in the course of acceptance testing by using non-documented features of functional and information security tests.

Entities specializing in and engaged to develop information systems security tools and systems on a contractual basis shall be licensed to do so.

When purchasing ready-to-use information systems and their components, the developer shall provide documentation containing the description of protective activities performed by the developer against information security threats.

The developer shall also provide documents describing protective actions performed by the developer of the information system and its components to ensure security, safe delivery, operation and lifecycle support including the description of the lifecycle model and vulnerability assessment. The documents may be provided as part of the statement of compliance or as a result of compliance assessment performed subject to relevant assessment procedures.

The supply agreement/contract for the information system and its components should include provisions on lifecycle support for the goods delivered. If such provisions cannot be included into the agreement/contract, the acquisition of a full package of design documentation shall be considered to ensure the ability to support the information system and its components without any assistance of the developer. If neither of the options is acceptable, e.g., because of high costs, the management of the Company shall ensure the analysis of the effect the threat of inability to support the information system and its components may have on the continuity of operations.

At the stage of operations, security against the following threats shall be provided:

- Intentional unauthorized disclosure, modification or destruction of information
- Accidental modification or destruction of information
- Non-delivery or wrong delivery of information
- Rejection of services or poor quality services.

In addition, a repudiation threat is relevant. At the stage of support, security against the following threats shall be provided:

- Modifications to the information system causing failures in its functionality or availability of non-documented features.
- Failure of the developer/supplier to make changes necessary to maintain proper operation and condition of the information system.

At the stage of retirement, the following information shall be deleted:

- Information, the unauthorized usage of Information which may cause damage to the Company, and information used by security tools from read-only memory or external media. Information system specification requirements shall be included in all supply contracts and agreements at all the stages of the information system lifecycle.

**17.1 Preventive Compliance Control**

Preventive control of information security policy compliance is understood as routine works on ensuring information security, prevention of potential information security failures in the Company and activities to build information security awareness with users.
Information security routine works cover control testing (inspection) procedures for the functioning of information security tools. Such routine works ensure the efficiency of the information system until the period of testing. The control testing of the functions of information security tools may be partial or complete.

The task of preventing potential information security failures in the information system of the Company is completed as the following events take place:

- Adding new software and hardware to the Information system of the Company (new workstations, server or communication equipment, etc.) if any new vulnerability areas become observable with data security tools of the information system of the Company.
- Changing the configuration of the Information system software and hardware (changing the configuration of software at workstations, servers or communication equipment, etc.) if any new vulnerability areas become observable with data security tools of the information system of the Company.
- Any data on identified areas of vulnerability in operating systems and/or software of equipment employed in the information system of the Company becomes available.

The Information Security (IS) Specialist (possibly with the help of an outsourced entity specializing in information security) collects and analyses information on identified vulnerabilities of operating systems and/or software in relation to the information system of the Company. Such information may be sourced from mass media or publications of different companies, non-governmental associations and other organizations specializing in information security and other data.

The Information Security (IS) Specialist (possibly with the help of an outsourced entity specializing in information security) performs regular inspection of information security tools of the Company by modelling potential attempts of unauthorized access to secured information resources.

To ensure control over information system security, testing tools are used to test security techniques and functions implemented as part of the Information Security Tools of the Company's Information System. Any scheduled activities to build awareness of these policies and training of the Company's staff on internal information security regulations are performed via e-mail and face-to-face.

Any non-scheduled activities to build awareness of these policies and training of the Company's staff on internal information security regulations are performed if these policies have been amended and any non-compliance incident has taken place. A new employee shall go through induction on the provisions and requirements of these policies.

As part of the prevention of potential cyber threats, for auditing, it is allowed to use the built-in information processing tools on the office 365 portal (including eDiscovery, audit, etc.) by TGT employees who are responsible for the company's IT security. The obtained data can be used only with the permission of the CEO.

**17.2 Remediation of Non-Compliance**

The Information Security (IS) Specialist, using data generated as a result of the use of information security control (monitoring) tools, shall duly identify information security failures and facts of unauthorized access to secured information resources and take actions for their localization and mitigation.

If the data security subsystem identifies a fact of information security failure or unauthorized access to secured information resources, it is recommended to inform the Information Security (IS) Specialist and/or IT Manager on that and then follow their instructions.

After the incident has been addressed, a report on the failure and remedial actions shall be issued and e-mailed to the CEO of the Company

**17.3 No-Compliance Liability**

The Information Security (IS) Specialist, using data generated as a result of the use of information security control (monitoring) tools, shall duly identify information security failures and facts of unauthorized access to secured information resources and take actions for their localization and mitigation.

## 18. Terms and Definitions

**Automated System** is a system consisting of employees and tools used in automating their operations. The Automated System implements information technology expected to perform set functions.

**Information Security (IS) Specialist** is an employee of the Company controlling the processes of ensuring that all of the Company's data is kept secure and safe. The Information Security (IS) Specialist arranges operations on identifying and preventing potential information leakage channels, potential opportunities for an Unauthorized Access to secured data.

**Risk Analysis** is a systematic use of information to identify risk sources and assess risks.

**Information Security Audit** is conducted in order to review compliance with data security regulations. It may be conducted by both the Company (internal audit) and independent organizations (external audit). Audit results may be reported in a free form (for internal audit) and in the form of an auditor's report if an external auditor was engaged.

**Authentication** is a process of verifying if the identity provided by the access subject belongs to this access subject; the action of proving the identity is true and valid. In most cases, Authentication begins when a type in the password using the keyboard.

**Access** to Information is an ability to get and use information.

**Request** is a formal request or notification to give or cancel access to information assets. The Request is made in a free form and e-mailed in advance.

**Secure Data Transmission Channel** is a logical and physical network communication channel secured against potential intruder tapping by encryption or actual isolation and location within a secured area.

**Access Identifier** is a unique quality of the access subject or object.

**Identification** is assigning an identity to the access subject (users, processes) and access objects (information resources, devices) and/or verifying the offered identity against the list of assigned IDs.

**Information** is an asset which, along with other assets of the Company, has its value and hence must be duly protected.

**Information Security** is a security mechanism ensuring confidentiality, integrity and accessibility of information, a secure state of the Company's information assets in the threatening IT environment. Threats may be caused by unintentional failures of staff, incorrect hardware operation, natural disasters or accidents (fire, flood, power failures, telecommunication channel failures, etc.), or by intentional failures causing damage to information assets of the Company.

**Information System** is a combination of software and hardware used to store, process and transfer information to complete the tasks of the Company's units. The Company employs different types of information systems to facilitate management, accounting, training and other processes.

**Information Technologies** are processes and methods of searching, collecting, storing, processing, providing and distributing information as well as the ways of implementing such processes and methods.

**Information Assets** are information systems, information media and information resources.

**Information Means** are software, hardware, linguistic, legal and organizational means (software; computers and telecommunications equipment; dictionaries, thesaurus dictionaries and classifiers; manuals and methods; regulations, charters, job descriptions; charts and their descriptions; other operational and support documentation) used or developed to design information systems and ensure their operation.

**Information Resources** are the combination of information located in the database and technologies used to process such information.

**Information Security Incident** is an actual, attempted or potential violation of information security resulting in failures in the accessibility, confidentiality and integrity of the Company's information assets.

**Threat Source** is an intention or method designed to a deliberate use of vulnerability or is a situation or method which may by chance trigger vulnerability.

**Confidential Information** is limited access information (containing no data of state secret) with limited access.

**Confidentiality** is access to information allowed to authorized users only.

**Critical Information** is such information when any failures in its access, integrity or confidentiality may have a negative effect on the operations of the Company's units and cause property or any other damage to the Company.

**Local Area Network (LAN)** is a group of computers and associated devices interconnected by one or several autonomous high-speed data transmission digital channels within one or several adjacent buildings.

**Firewall** is a combination of software and hardware used in controlling access to and from LANs within a network, and to and from the network of the Company and external networks (Internet).

**Information Security Continuous Monitoring** is continuous observation over objects affecting information security as well as collection, analysis and integration of the observation outcomes subject to the set targets. Depending on the targets, monitoring may cover an automated system or a part of it, IT processes within the Company, IT services of the Company, etc.

**Unauthorized Access to Information (UAI)** is access to information contrary to the rules of user access authority levels.

**Risk Processing** is a process of selecting and implementing actions to modify a risk.

**Residual Risk** is a risk that remains after the risk has been processed.

**Information Security Policy** is a set of interrelated guidelines and relevant rules, procedures and practices employed in the Company to ensure information security and safety.

**LAN User** is an employee of the Company (permanent, part-time, contract based, etc.) and other individuals (contractors, auditors, etc.) who have duly registered with the network and received the right to access resources subject to their job responsibilities.

**Risk Acceptance** is a decision to accept a risk.

**Software** is a set of software installed on a server or computer.

**Workstation** is a personal computer used by a network user to complete job tasks.

**User Account** includes the name of a user and their unique digital identifier unambiguously identifying the user in the operating system (system, database, application, etc.). The User Account is created by an administrator when registering the user with the computer operating system, database management system, network domain, applications, etc. It may also have such user data as their name, department, phone number, e-mail, etc.

**Backup** is saving the current state of information (system) without necessarily saving the previous state.

**Server Resource (the Resource)** is a directory, data file, software or service on the server.

**Role** is a set of authorities and privileges to access an information resource necessary to complete certain job responsibilities by the user.

**Information Security Management System (ISMS)** is the part of the general management system which is based on a business risk approach in terms of creating, implementing, functioning, monitoring, analyzing, supporting and improving information security.

**System Administrator** is an employee of the Company responsible for supporting automated systems and functioning of the Company's local network and PCs.

**Access Control List (ACL)** is a list of network packet filtering rules set up at routers and firewall and defining filtering criteria and actions to be done with the packets.

**Owner** is an individual or entity with assigned management obligations to monitor the development, support, use and safety of assets. The term Owner does not mean that the individual or entity holds real ownership rights for the asset.

**Cryptographic Techniques** for Information Security include encryption, prevention of false data entry, digital signature, coding, tools to develop key documents (irrespective of a key information carrier), key documents (irrespective of a key information carrier).

**Threat to Data Security** is a potentially existing threat of accidental or intentional destruction and unauthorized receipt or modification of data due to the structure of data processing and conditions of data processing and storage. It is a potential ability of a threat source to successfully identify a certain vulnerability of the system.

**Information Security Management** is a set of actions covered by the information security policy and performed in the threatening IT environment. Information Security Management includes such procedures as management object assessment (e.g., risk assessment and risk management), selection and implementation of management actions (planning, implementation and servicing of security activities).

**Vulnerability** is faults or weaknesses of information assets which may cause failures in information security of the Company if threats take place.

**Information Integrity** is the state when information is being protected, which is characterized by the ability of the Automated System to ensure that confidential information remains safe and unchanged in case of any unauthorized or accidental action takes place while processing or storing the confidential information.

**SharePoint** is a platform developed to ensure collaboration of users while working with data in the single environment. The platform is expected to ensure efficient corporate content management. SharePoint may be used in designing websites offering collaboration for users. SharePoint based websites may be used as a storage for information, knowledge and documents and for the use of online applications facilitating collaboration.

## 19. Acronyms

| | | | |
|---|---|---|---|
| **AW** | Automated Workstation | **AS** | Automated System |
| **DB** | Database | **DP** | Data Protection |
| **IS** | Information Security | **ISY** | Information System |
| **ITS** | Information Telecommunication System | **CA** | Controlled Area |
| **UAA** | Unauthorized Access | **OS** | Operating System |
| **SW** | Software | **CA** | Computer Aids |
| **IST** | Information Security Tools | **DTS** | Data Transmission System |
| **CTIS** | Cryptographic Techniques for Information Security | **PC** | Personal Computer |
| **ISMS** | Information Security Management System | **EDS** | Electronic Digital Signature |
| **EDMS** | Electronic Document Management System | | |