SIA "Koksnes Plūsmas Datu Centrs"

IS Data Security Policy

Version number: 1.4.

Version date: 15 January 2024

Riga, 2021

Table of Contents

1. Purposes and Objectives of the IS Security Policy

1.1. The purpose of the Information System (hereinafter – IS) Security Policy of SIA "Koksnes Plūsmas Datu Centrs" (hereinafter – KpDC) is to implement economically justified and well-balanced IS protection corresponding to the business objectives of the company, so information and technical resources of KpDC are protected against external and internal security threats.

1.2. The IS Security Policy is binding on all users of the IS of KpDC.

1.3. The Security Policy has the following objectives:

1.3.1. To ensure availability of information.

1.3.2. To ensure integrity of information.

1.3.3. To ensure confidentiality of information.

1.3.4. To protect the IS information resources.

1.3.5. To protect the IS technical resources.

1.3.6. To identify potential IS security threats.

1.3.7. To assess the IS security risks.

1.3.8. To determine measures for mitigating potential security risks.

1.3.9. To discover potential IS security incidents.

1.3.10. To restore IS operation after a security incident.

1.3.11. To define the conditions for control over the IS Security Policy.

2. Terms and Abbreviations Used in the IS Security Policy of KpDC

Term/Abbreviation	Definition
Outsourcing	Any type of agreement between a market participant and a service provider, according to which this service provider ensures a process, provides a service or performs any other activity that would otherwise be performed by the relevant market participant itself.
Audit Trail	Records available for analysis, which document data on specific IT events (access, data entry, modification, deletion, output, etc.).
AUI	Automated measurement system
DEAC	SIA "Digitālās ekonomikas attīstības centrs", the company that provides data centre services to KpDC.
Security Incident	An event, where IS threats have adversely affected the IS operation by exploiting their deficiencies.
Security Measures	Technical or organisational measures that are defined within the framework of risk management and mitigate the IT risk to an acceptable level.
Security Policy	Information Systems Security Policy
Incident	An event, where KpDC IS threats have adversely affected the IS operation by exploiting their deficiencies.
Integrity of Information	Maintaining complete and unchanged information.
Confidentiality of Information	Disclosure of information only to persons authorised to receive and use it.
Availability of Information	Access to information within a specified period upon an information request.
IS Security Threat	A deliberate (intentional) or negligent act or event that may cause changes, damage, destruction of information or technical resources of the system, or make them available for unauthorised persons or as a result whereof the access to information resources of the system may be impeded or impossible.
IS Information Resources	Files, including those containing information to be stored and processed in the system and available to users of the system, and system documentation.
IS Technical Resources	Computers, software, data carriers, network hardware and other technical equipment ensuring the operation of the system.
IS (Information Systems)	A structured set of information technologies and databases used for performing data entry, storage, processing, output and transmission, ensuring the fulfilment of certain functions.
IT	Information technologies
Controls	Methods and measures for risk mitigation.
KpDC	Koksnes Plūsmas Datu Centrs
User	A person that uses an IT system within the limits of the granted authority.

Risk	Probable inability to fully and in due quality perform the fulfilment of certain obligations or functions in relation to the functioning of the IS.
SSL	Secure Sockets Layer. Encrypted data transmission over the network, which guarantees that the data to be transferred are protected by a secure encryption algorithm and are not accessible to third parties for unauthorised viewing.
VPN	A virtual private network is a connection between one or more networks within a network or multiple networks (e.g. the internet).

3. Company's IS Description and Analysis in the Field of Security

3.1. The IS Security Policy has been developed for the systems owned by KpDC – IS Apse, IS Ciedrs, IS Linda, IS Dace, including the Reporting System Database – the Register.

3.2. Functions of the IS:

3.2.1. IS Ciedrs is the central data accounting system for all wood measuring data, from which further calculations are made in IS APSE to generate Testing Reports.

3.2.2. IS Apse is the system where the specification of processing of measuring data (Matrix) is imported to and used for automatic generation and sending testing reports to IS Dace.

3.2.3. IS Linda – a system providing direct data flow from automated measurement instruments (AUI) in the case of individual measuring.

3.2.4. IS Dace is a communication platform ensuring the exchange, generation and sharing of business documents involved in the wood flow between systems and users. *Inter alia*, by ensuring the management of identity of users and corporate users and maintenance of various industry classifiers. Functionalities of IS DACE:

3.2.4.1. wood measuring data input;

3.2.4.2. maintenance of complete chain of wood documents;

3.2.4.3. reporting module – generation of reports;

3.2.4.4. database – the Register is the register of data contained in the documents;

3.2.4.5. specification used in wood transactions (Matrix);

3.2.4.6. file register;

3.2.4.7. register of classifiers.

3.3. The IS processes and stores data and information classified as "restricted access" information.

3.4. The data of following classifications are entered, stored and processed in the IS:

3.4.1. Wood measurement data;

3.4.2. Data of complete chain of documents;

3.4.3. Identity data of buyers, sellers and surveyors;

3.4.4. Classifiers of wood and spoilage assortments;

3.4.5. Specifications (matrixes);

3.4.6. Transport classifier;

3.4.7. Testing report data.

3.5. The IS resources are classified as follows:

3.5.1. IS Information Resources;

3.5.2. IS Technical Resources.

3.6. The IS users are divided as follows:

3.6.1. The KpDC users who fulfil the functions of the administrator, development and maintenance.

3.6.2. Forest industry representatives who ensure data and information input and have signed an agreement with KpDC on the relevant service:

3.6.2.1. Wood sellers;

3.6.2.2. Wood buyers;

3.6.2.3. Wood carriers;

3.6.2.4. Wood surveyors.

3.7. The IS are developed by purchasing standard software, outsourcing software development to external developers and developing new software with in-house resources. Each development system has its own development, test and production environment. Depending on the system specification, several test environments may be used.

3.8. The functions of the KpDC systems are designed to support the forestry sector, including a significant part that supports wood measuring. KpDC maintains and develops not only the systems it owns, but also the systems used in wood measuring.

2.1.Figure 1 shows a wood measuring data flow chart.

3.8.1. IS Ciedrs receives data from wood measuring input systems – Electronic Calliper, IS Linda, IS Kadikis, Photo Web, Load Mon.

3.8.2. From IS Ciedrs, data are transferred to IS Apse.

3.8.3. From IS Apse, wood measurement data are sent to IS Dace and customer systems according to the availabilities defined in the Matrix.

3.8.4. For ensuring control functions, data are sent to the Control Assortment and Control Package systems.

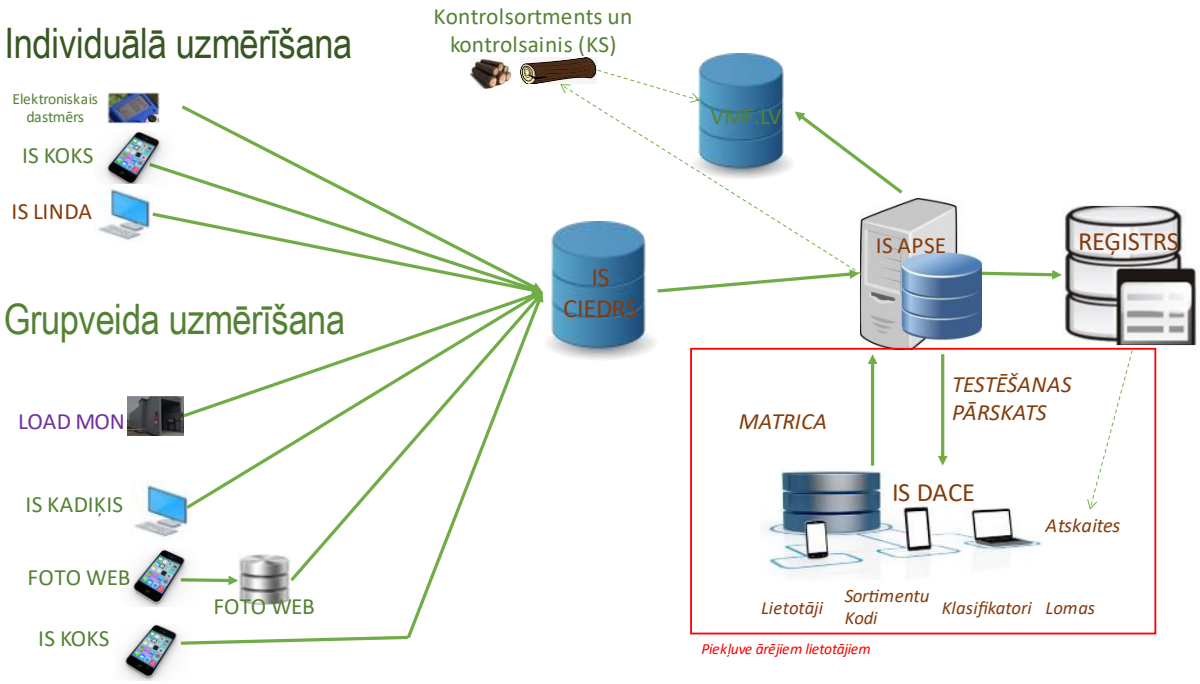

Figure 1. Wood Measuring Data Flow

3.9. KpDC provides an IS service for the companies ensuring wood measurement, including system maintenance and change development.

3.10. System maintenance:

3.10.1. IS Apse and maintenance and introduction of changes are ensured by in-house resources.

3.10.2. For the maintenance and change development of IS Ciedrs, IS Linda and IS Dace outsourcing is ensured, as well.

3.11. Databases and infrastructure are maintained in the corresponding European level external data centre. Infrastructure availability and business continuity are contractually ensured by an SLA concluded between the company and the data centre.

3.12. Server data backup and storage is ensured in the *Bite* data centre.

3.13. Internet connection is ensured by external service providers.

3.14. A secure SSL certificate is used for data transmission encryption.

3.15. Staff work with the systems is protected by means of a secured internal computer network (VPN).

3.16. The company uses an internal data network provided by external service providers.

4. Security Management

4.1. The company regularly enhances a set of documents and measures, the implementation whereof ensures the achievement of the purpose of the IS Security Policy. Any KpDC employee may propose introducing changes to the IS Security Policy by submitting proposals to the head of KpDC.

4.2. The company ensures ongoing coordination and monitoring of the implementation of the Security Policy.

4.3. In cases where employees fail to comply with the requirements set by the Security Policy, the management of the company may initiate disciplinary proceedings in accordance with the laws and regulations.

4.4. The company has a clearly defined allocation of responsibilities for the IS security.

4.5. The head of the Company:

- 4.5.1. Is responsible for the IS security.
- 4.5.2. Establishes and approves the IS Security Policy.
- 4.5.3. Ensures the necessary means and support for the implementation, maintenance and enhancement of the IS Security Policy.
- 4.5.4. Determines the allocation of roles and responsibilities with respect to the IS security.
- 4.5.5. Establishes a control mechanism for the IS security management.

4.6. The person responsible for IS security management is the IS security manager, whose functions are fulfilled by the IT project assistant:

- 4.6.1. Ensuring the maintenance and implementation of the necessary IS security documents.
- 4.6.2. Preparing procedures for the implementation and maintenance of the IS Security Policy.
- 4.6.3. Organising the IS risk analysis.
- 4.6.4. Carrying out monitoring of compliance with the set security requirements.
- 4.6.5. Informing the involved parties of the progress of the investigation and remediation of the Security Incident.

4.7. The following managers of Information and Technical Resources are appointed:

4.7.1. IS Apse – IT project manager;

4.7.2. IS Ciedrs – IT project manager;

4.7.3. IS Dace – IT project manager;

4.7.4. IS Linda – IT services manager.

4.8. The manager of Information and Technical Resources:

4.8.1. Determines the security requirements for an Information Resource.

4.8.2. Defines the mechanism of access rights to the Information Resource.

4.8.3. Is responsible for access control to the Information Resource.

4.8.4. Gathers information about the security risks for the Information and Technical Resources under their management.

4.8.5. Conducts an investigation of the Security Incident.

4.8.6. Within the scope of their competence, carries out the prevention of the Security Incident.

4.8.7. Is responsible for the acquisition, development, operation and maintenance of the IS Technical Resources.

4.8.8. Ensures technical and logical protection measures of the IS.

4.8.9. Is responsible for the management of access rights to the IS.

4.8.10. Provides the IS resumption measures in the event of a failure of the system operation.

4.9. The Incident manager, whose duties are fulfilled by the IS primary user:

4.9.1. Gathers information about information security events and Incidents.

4.9.2. Forwards Incidents for prevention to the responsible persons.

4.9.3. Controls the prevention of information security events and Incidents.

4.10. The developers, whose duties are fulfilled by the programming system engineer or a company with which the outsourcing agreement has been concluded:

4.10.1. Ensure separation of development, test and production environments.

4.10.2. Use the development and test environment.

4.10.3. Ensure that unauthorised persons cannot access the source code.

4.10.4. Ensure that the source code, as far as possible, is not stored in production systems.

4.10.5. Carry out the development according to what is stipulated in this Policy.

4.10.6. Prevent IS Security Incidents as necessary.

4.11. Users – report system information security events and Incidents.

5. Legal Framework

5.1. The requirements of the laws and regulations of the Republic of Latvia in the field of information technology and information security have been complied with in the IS.

5.2. Unless stated otherwise, all software, training materials, documents and other materials developed by the Company represent the intellectual property of the organisation.

5.3. All copyright, software licence and usage requirements of the IS resource manufacturer must be complied with when working with the IS resource.

6. IS Security Principles

6.1. IS user accounts:

6.1.1. The IS users carrying out the System administration work use dedicated user accounts (hereinafter – the System Administrator Accounts) that are not used for performing everyday activities.

6.1.2. Administrator level access to the IS and the database is only provided from registered IP addresses.

6.1.3. Each user account is linked to a specific natural person.

6.1.4. Role checking for each step is used as a means of restricting access.

6.1.5. IS Dace user access is granted on the basis of a mutual agreement/contract concluded with the IS manager on the creation of an organisation profile. The user with administrator rights is entitled to change the IS roles.

6.1.6. The IS Apse role is assigned solely on the part of the system administrator. The user cannot change the role in the system.

6.1.7. The error messages displayed to the IS users contain only the minimum necessary information – a description of the error and an error identifier.

6.1.8. When creating a new organisation user account, the verification of the e-mail address is ensured. It is not possible to enter a value other than an e-mail address.

6.1.9. The IS user profile only displays information about the organisation whose user profile has been created.

6.1.10. One user with their access rights can only use the IS as a representative of one organisation.

6.1.11. The IS users are reviewed once a year.

6.2. Requirements for passwords:

6.2.1. Access to the IS is protected by a username and password.

6.2.2. Passwords for the IS users should be at least 8 characters long, contain at least one uppercase letter, at least one lowercase letter and one number or symbol.

6.2.3. The IS user password is not fully displayed to the user at the time of entry.

6.2.4. All passwords are stored in an encrypted form, so that the system administrator does not have access to them. If the system administrator needs to reset the password, this should be done via a specific function call that generates the new password and sends it to the client's registered e-mail address.

6.2.5. Equipment, incl. the infrastructure equipment that supports the functioning of the system does not use default passwords (set by the manufacturer or distributor).

6.3. Traceability:

6.3.1. The IS Audit Trail summarising the inspection information is generated and stored for at least 6 months after the record is made. The rest of the Audit Trail is kept for at least 12 months.

6.3.2. The IS Audit Trail includes information on logging in or logging out of the system, data selection, as well as account creation, modification or deletion, recording the time of the event that coincides with the Coordinated Universal Time (UTC) of the actual event, the internet protocol address from which the action was made, a description, as well as information on the action initiator – identifier, connection metadata.

6.3.3. All access to the system is traceable up to a specific IS user account or internet protocol (IP) address.

6.3.4. Every action in the system is logged, including every action that is performed directly on the database by the IS maintainers.

6.3.5. The person responsible for IS security management shall ensure scheduled supervision and analysis of the contents of the System Audit Trail, in order to detect Incidents.

6.4. Updates:

6.4.1. The IS managers carry out the assessment of the available software updates and testing thereof in the test environment.

6.4.2. The IS must have all necessary software updates installed.

6.5. At database level:

6.5.1. Access is provided via an API (application programming interface) using a user key assigned by the system.

6.5.2. Access at system level is ensured by direct connection to the database using a unique username and a secure password for each system as described in Clause 5.2. Access is only possible with an IP address assigned by KpDC.

6.5.3. Access for system maintenance and development is ensured by direct connection to the database via a DBMS (database management system) using a unique username and secure password for each user as described in Clause 5.2.

6.5.4. Access is not publicly available.

6.6. Data from the IS are sent only to the specified recipients.

6.7. The IS is subject to security audits according to OWASP standards, which confirm the security of data availability.

7. The IS Protection Measures

7.1. All Technical Resources of the employees of KpDC used everyday to connect to the system are equipped with anti-virus functionality.

7.2. Physical access to equipment ensuring the operation of the IS is only allowed to persons authorised by the institution or accompanied by such persons.

7.3. Data traffic between the information system and its users, and between the information system and other information systems, is controlled using a firewall solution.

7.4. Access to IS Apse and IS Ciedrs is ensured only from the IP address of the KpDC office.

7.5. Access to IS Linda is ensured via a WPN connection of KpDC.

7.6. It is not permissible to create threats to the integrity of the stored data of the production environment when performing development or testing of the System. A system development and test environment has therefore been set up for this purpose.

7.7. The system development code is stored in the GitHub host of KpDC. Only an authorised KpDC developer has access to this host.

7.8. No sensitive information is available on staff computers. All data are stored in the European level data centre DEAC.

8. The IS Security Risk Analysis and Management

8.1. For the purposes of the risk management of Information and Technical Resources of KpDC, the Security Risk Management Plan has been developed.

8.2. The risk analysis in the Institution has the following purposes:

8.2.1. To gather information about the risk level of the System.

8.2.2. To determine steps to be taken for the risk management of the System:

8.2.2.1. Risk acceptance;

8.2.2.2. Risk management;

8.2.2.3. Risk mitigation measures.

8.3. Risk analysis should be carried out throughout the life cycle of the IS at the frequency specified in this plan.

8.4. The list of the IS security threats is used in performance of the risk analysis.

8.5. The performance of the risk analysis is ensured by involving the persons responsible for the security management of the System.

8.6. Risk mitigation measures are determined on the basis of proportionality of their costs and potential losses.

8.7. A responsible person and possible term for fulfilment is set for each risk mitigation measure.

8.8. The person responsible for the security management of the System controls the implementation of risk mitigation measures.

8.9. The risk analysis is carried out based on the methodology described in the document "IS Security Risk Analysis Regulations" (KPDC.DP.7_IS_drosibas_risku_analizes_ noteikumi).

8.10. Based on the results of the IS security risk analysis, security risk mitigation measures are prepared.

8.11. During each subsequent risk analysis, the person responsible for the security management of the System assesses the efficiency of each risk mitigation measure.

8.12. If the mitigation measure has been inefficient (e.g., the relevant risk level has not been mitigated), another mitigation measure is identified.

8.13. The Plan of the IS Security Risk Mitigation Measures is reviewed at least annually, as well as in the following cases:

8.13.1. If changes to the IS may affect the security of the System;

8.13.2. If security threats to the IS have changed or new security threats have been discovered;

8.13.3. If the number of IS Security Incidents increases or a major system Security Incident has occurred.

8.14. The Plan is updated, if such necessity is detected, when reviewing it.

9. Security Criteria

9.1. The period of uninterrupted operation of the IS is 24 hours a day, 7 days a week.

9.2. Support for network connection points must be provided 365 (366) days per year.

9.3. In the event of a Security Incident, actions are taken in accordance with the KpDC IS Security Incident Management Regulations and the IS Business Continuity Recovery Plan.

10.Control of the Implementation of the IS Security Policy

10.1. An IS security audit is organised as necessary, but at least once a year, to ensure the compliance of the IS with the Security Policy.

10.2. Tests of the IS incident management procedure are organised as necessary.

10.3. The IS security manager introduces the IS Security Policy to the employees of KpDC.

10.4. The IS security manager organises and controls the accounting of all Company IS resources, their owners, custodians and users.

10.5. The IS security manager organises the risk review on an annual basis.

11.Final Provisions

11.1. The IS Security Policy is reviewed at least annually, as well as in the following cases:

11.1.1. If changes to the system may affect its security;

11.1.2. If security threats to the system have changed or new security threats have been discovered;

11.1.3. If the number of system Security Incidents increases or a major system Security Incident has occurred.

11.2. The Policy is updated, if such necessity is detected, when reviewing it.