APPROVED BY
14/09/2018
Joint stock company Klaipėdos nafta
Managing Director's Order No. BV-135

MINIMUM INFORMATION AND CYBER SECURITY REQUIREMENTS OF JOINT STOCK COMPANY KLAIPĖDOS NAFTA FOR EXTERNAL PARTIES

1. Scope of application

1.1. The present minimum information and cyber security requirements of Joint Stock Company Klaipėdos nafta (hereinafter referred to as KN) for external parties (hereinafter referred to as the Requirements) apply to all natural and legal persons, with whom KN sign agreements and implementation of such agreements embrace the principles of protection of information and information resources managed by KN and their management actions.

1.2. The document is published on KN website https://www.kn.lt.

2. Basis and object

2.1. The basis of the Requirements – agreement signed between KN and External party and the duty of the parties to the Agreement to ensure adherence to the information and cyber security requirements during the implementation of the Agreement.

2.2. Object of the Requirements – rights and duties of the parties to the Agreement when using KN information and information resources by an External party at the assignment of KN.

3. Definitions

3.1. Personal data – as defined in Paragraph 1, Article 4 of the General Data Protection Regulation, which are provided by KN to an External party for implementation of the Agreement or access to them is provided in accordance with the terms and conditions established in the Requirements;

3.2. Needed for work – access is provided exclusively to the minimum part of the information system or data transmission network needed for appropriate activity.

3.3. Data transmission network – KN divides into the network of information transmission and electronic communications (hereinafter referred to as the General network) and data network of industrial process management systems (hereinafter referred to as the Technological network).

3.4. External parties – service providers, partners, clients, other persons who have or may have access to KN information resources;

3.5. Agreement – an agreement signed between KN and External party, implementation of which embraces work with KN managed information resources, KN information at the assignment of KN and which contains a reference to these Requirements or when application of the Requirements for such Agreement between KN and External party is otherwise agreed;

3.6. Other terms in the Requirements are understood as they are defined and used in the Agreement and legal acts and internal documents of KN regulating information and cyber security.

4. Compliance requirements

4.1. These Requirements define minimum information and cyber security principles that must be fulfilled by any means according to a respective agreement with KN, which contains a reference to these Requirements.

4.2. Upon a request of KN, to allow KN or its authorised person to conduct audit of Information and cyber security or other actions of inspection of Information and cyber security and to provide all necessary information to the extent needed for examination, whether an External party adheres to these Requirements and applied instructions of Information and cyber security legislation.

4.3. KN reserves the right to carry out assessment of External party's information and cyber security to discover any potential breaches.

4.4. Permitted and expected deviations from the Requirements must be clearly marked and documented.

4.5. Depending on access and work with information systems, information and data networks can be subject to additional technical and organisation requirements laid down:

4.5.1. in the Resolution No. 387 of the Government of the Republic of Lithuania of 20 April 2016 'On approval of the description of organisation and technical cyber security requirements applied to information structure of particular importance and state information resources',

4.5.2. Order No. 1-89 of the Minister of Energy of the Republic of Lithuania of 2 May 2013 'On approval of information security requirements of enterprises and facilities attributed to the field of management of the Minister of Energy of strategic or significant importance for national security',

4.5.3. Law on protection of important objects for assurance of national security of the Republic of Lithuania.

5. Security requirements for telework

5.1. Having assessed potential risks and providing an External party with a possibility to work in a remote computerised workplace of an External party or by providing remote access to KN information systems in the General data network, the following is required:

5.1.1. to prohibit remote access if safe VPN communication is not used;

5.1.2. to satisfy oneself that information systems, hardware and data networks, from which remote connection is established, are safe and reliable (updated operating system and other software, installed antivirus software, activated and configured firewall, etc.);

5.1.3. to ensure timely and regular control of access rights;

5.1.4. to carry out ongoing monitoring and control of actions;

5.1.5. to ensure protection of KN confidential and non-public information by technical means;

5.1.6. to ensure control of remote connection communication for the purposes mutually agreed in advance;

5.1.7. to ensure that remote communication connection and provision of remote access are carried out by following the principle of 'Needed for work' and have agreed validity term.

6. Secure software development cycle

6.1. External party determines, documents and implements initiatives that are in compliance with generally accepted information and cyber security standards and practice in order to develop secure software and hardware development processes. Such initiatives must ensure information and cyber security in all stages of development: training, definitions of requirements, design creation, installation, approval, issue and maintenance.

6.2. Product does not have user's accounts, passwords or private/secret keys which could not be changed or removed by an authorised final use of the product.

6.3. Product does not have any user's accounts (individual, general, testing environment), which are not documented (it does not mean that related users' access data must be disclosed).

6.4. External party must exert active measures to improve the quality of product security. Such measures must be in compliance with generally accepted standards and practice of cyber security of industrial process management, and if technically possible, include reliability tests, management of vulnerabilities and programing code security testing (including structure or binary code analysis).

6.5. Hygiene of programing code under development must be ensured (code of model sample data and scenario, links to non-used libraries, tools of coordination code and other used tools are not allowed) when transferring software under development into a working environment.

6.6. Development, testing and working environments of software under development must be separated.

6.7. Software users may not be shown messages of errors of software under development about a programing code or server.

7. Security requirements for staff

7.1. Persons working for an External party are examined in accordance with the Law on protection of objects important for national security of the Republic of Lithuania.

8. Awareness development and training

8.1. External party must carry out development of awareness of information and cyber security for staff by providing technical, procedural and safe activity knowledge.

8.2. Every person of an External party working with KN information resources must be familiarised by a responsible employee of an External party with the effective Information and cyber security policy of KN, which is published on KN website https://www.kn.lt.

8.3. Employees of an External party or persons working for the latter must present an appropriate qualification proof authorising work with a specific information resources of KN, when it is necessary or requested.

8.4. External party must have plans of management of information and cyber incidents and activity continuation approved and other documents regulating actions of External party's staff during information and cyber incidents.

9. Physical security

9.1. External party's representatives and their means of transport can enter KN territories exclusively with permits issued by KN, while if carrying cargo – with documents supporting the cargo.

9.2. Technically untidy vehicles and machinery and vehicles with external cargo are not given access to KN territory.

9.3. All permits bear names, they may not be handed over and/or otherwise transferred to third parties.

9.4. Single permits are issued for a single visit to KN territory with the time specified in the permit and are valid upon presentation of an identity document to a security officer/employee (passport, identity card, driver's licence).

9.5. External parties' representatives suspected of being intoxicated with alcohol, narcotic or toxic substances are not provided access into KN territory.

9.6. Filming or photographing in KN territory is prohibited without a permit of persons responsible for security.

9.7. The following objects may not be brought/transported into KN territory:

9.7.1. all categories of weapons, their accessories and ammunition or their imitations, listed in Law on Control of Weapons and Ammunition of the Republic of Lithuania;

9.7.2. explosive devices and explosive substances or their imitations;

9.7.3. narcotics and narcotic substances and alcoholic drinks;

9.7.4. other dangerous objects using open flame or emitting/causing sparks, except for tools or devices used for direct work, upon a permit issued.

9.8. External parties' representatives can be denied the right to visit KN for failure to comply with these requirements.

9.9. All representatives and vehicles of External parties entering KN territory unlawfully are detained and an officer-on-duty of the Port station of Coastguard Squad of the State Boarder Guard Service and the Police are notified.

10. Information security

10.1. Information in KN is divided into public, undisclosed and confidential.

10.2. External party must be informed about transfer of confidential information, which is defined by KN documents regulating information classification, storage and use.

10.3. It must be specified in the Communication plans that communication of undisclosed and confidential information or data of persons of special categories is carried out with the External party exclusively by using secure communication channel, using secure email and file exchange solution https://box.kn.lt.

11. General cyber security requirements.

11.1. External party must ensure that any new technology installed in KN is sanctioned and KN consent for its use is obtained, and ensure that security of such technology is sufficient.

11.2. Information systems user or administrator must confirm their identity by a password or other identification tool.

11.3. When issuing temporary passwords to information systems users and administrators, such passwords must be unique for each resource user and safely communicated.

11.4. Passwords cannot be stored or communicated in an open text. Only temporary password can be communicated in an open text, but separately from the username, if an Information systems user has no possibility to decode the received encrypted password or technical possibilities to communicate a password to the Information systems user via encrypted channel or secure electronic communications network are not available.

11.5. In all Information systems, prior to putting them into operation, Information systems administrator must change standard (manufacturer's) passwords into passwords in compliance with these Requirements.

11.6. Sections of Information system that confirm Information systems user's identity must prohibit automatic saving of passwords.

11.7. Functions of Information systems administrator must be performed by using a separate username designated for that purpose, which may not be used for performing daily functions of Information systems user.

11.8. Information systems users may not be granted the rights of Information systems administrator.

11.9. Every Information systems user or administrator must be uniquely recognised.

11.10. All redundant manufacturers' user accounts (including guest account) must be deactivated in Information systems.

11.11. In publicly-accessible computerised workplaces, the name of the last user may not be seen when logging in.

11.12. Access must be provided following the principle of 'Needed for work'.

11.13. Remote access to Information systems with administrator's account must be prohibited.

11.14. When logging in by using remote access to Information systems, a user must certify his/her identity with a password or other identification tool.

11.15. Any unsanctioned remote access to KN information systems and data or equipment is prohibited.

11.16. Remote access to KN information systems and data network from public data networks must be encrypted by applying VPN technology.

12. Additional cyber security requirements for industrial process management systems

12.1. Industrial process management systems and their data network and its components may not have remote access from public data networks.

12.2. In the technological data network, separate hardware without an email account, access to public data networks or used for work with confidential information must be used for administration of information resources (servers, switchboards, routers, firewalls, etc.).

13. External party's obligations

13.1. External party's assumes the following obligations:

13.1.1. to adhere to KN Information classification, use and storage guidelines and Information and cyber security requirements and installed processes.

13.1.2. without a prior written consent of KN, not to disclose managed personal data, confidential and undisclosed KN information to any third parties or recipients.

13.1.3. when working with information resources issued by KN (computer, information storage medium, documents, data and information), to adhere and follow the KN Information and cyber security policy, these minimum security requirements, other KN information and cyber security processes installed and established duties, with which a responsible employee of KN familiarised the External party.

13.1.4. to bear responsibility for all harmful actions committed through the fault of information systems users granted by an External party's written request or persons specified in their request to the KN data transmission networks or information systems and losses caused to KN by such actions.

13.1.5. to ensure confidentiality and integrity of electronic information of KN information system, not to interfere with accessibility of electronic information of information system by their acts.

13.1.6. to safeguard managed personal data.

13.1.7. to exercise exclusively such rights of access to information system (to develop, edit, supplement, or delete), which were granted.

13.1.8. upon completion of work or when an information system user leaves his/her workplace, measures to prevent access to information managed in the information system to unauthorised persons must be exerted: logging off from information system, activation of screensaver protected by a password. The requirement of this paragraph does not apply to computerised workplaces intended for industrial process management or monitoring of security systems, when an account created specifically for such functions is used for work.

13.1.9. to use only those functions of information system and such scope of information in information systems, access to which was granted in accordance with the KN documents regulating provision of access to information systems.

13.1.10. without any delay, but in no event later than within 24 hours from the moment it became known, to give a written notice to KN about an incident or information and cyber security, which may be related with KN data or information resources or data transmission network, by calling +370 46 297 009 and sending an email to incidentai@kn.lt, providing all information and data available regarding such breach.

13.1.11. to ensure exertion of sufficient measures to control risks related with subcontractors, works carried out by them and supply chain.

13.2. External party is prohibited:

13.2.1. to scan KN information systems or KN data transmission network, in search for vulnerabilities or otherwise monitor the flow of KN data transmission network. If measures listed in this paragraph are needed for fulfilment of direct duties, they can be used exclusively upon coordination with a person of KN responsible for information and cyber security.

13.2.2. without a separate permit and knowledge of KN, to log on to KN data transmission network or information systems by using equipment other than issued by KN (except wireless network intended for KN guests).

13.2.3. to drink, eat and smoke next to information processing facilities.

13.2.4. to change network parameters (IP address, etc.) arbitrarily.

13.2.5. to use programs that may interfere with the operation of KN information systems and data transmission network (programs of scanning and blocking of data transmission network, etc.).

13.2.6. to modify and repair hardware and software issued by KN independently.

13.2.7. to use hardware and software issued by KN for activities prohibited by the laws of the Republic of Lithuania, activities of defamatory, insulting, threatening nature or in breach of public morality and morals, for sending computer viruses, spams or other purposes that may infringe lawful interests of KN or other persons.

13.2.8. to install, store, use, copy or distributed illegal software breaching copyrights.

14. Liability and dispute settlement procedure

14.1. Any dispute, disagreement or claim arising from the Requirements or in relation with the Requirements, their breach, cancellation and validity must be settled following the procedure established in the Agreement.

14.2. External party is responsible for all necessary measures and actions aimed at compliance with these Requirements and fulfilment of other duties established in applicable legal acts.

14.3. If because of actions or omission to act by the External party when implementing the Agreement, controlling bodies established in the Law Cyber Security of the Republic of Lithuania detect breach of information and cyber security and impose financial sanction on KN, upon a request of KN an External party undertakes an obligation to reimburse the amount of such sanction to KN in accordance with the procedure of fine payment to KN established in the Agreement.

14.4. External party is held liable to KN for proper fulfilment of the Requirements by third parties contracted by the External party.

15. Validity of the Requirements and final clauses

15.1. These Requirements form an integral part of the agreements specified in paragraph 3.5, when stipulated in the Agreement signed with an External party, or when application of such Requirements is otherwise agreed between KN and an External party. Requirements defined in the Agreement and additional agreements, when concluded, have precedence over these Requirements.

15.2. Validity of the Requirements to an External party is integral with the validity term of the Agreement signed between KN and an External party.

15.3. If any clause of the Requirements is declared invalid because of contradiction with the imperative clauses of legislation, such clause is replaced following the general procedure established in the Agreement;

15.4. These Requirements are not subject to signing separately. The Requirements are published on KN website https://www.kn.lt, or any other source accessible to an External party, or by creating a different individual or public access to the Requirements.