INFORMATION AND CYBER SECURITY POLICY

No. POL002

VERSION 1.0

INFORMATION AND CYBER SECURITY POLICY

TABLE OF CONTENT

I. INTENDED PURPOSE

Information and cyber security policy (hereinafter referred to as Policy) is intended to lay down uniform and effective principles for management of KN information and cyber security (hereinafter referred to as the Security), managerial position in respect of information and cyber security and to ensure effective implementation of KN information and cyber security management process.

II. SCOPE OF APPLICATION

The present Policy is binding to all KN employees, contractors, temporary consultants or other persons working for KN, including employees working for external parties, and applies to each process of KN activity, where information is managed, transmitted or otherwise processed, industrial processes managed.

III. REFERENCES

Law on Cyber Security – established organisation, management and control of cyber security system, defines bodies developing and implementing cyber security policy, their competences, functions, rights and duties, duties and responsibilities of managers of information infrastructure of peculiar importance and measures ensuring cyber security.

Information security requirements apply to enterprises of significant importance for national security attributed to the responsibilities of the Minister of Energy – define principles, grounds and of organisation of information security and main information security requirements of enterprises and facilities of strategic or significant importance, attributed to the field of management of the Minister of Energy.

Cyber security requirements apply to information structure of peculiar importance – establish organisational and technical requirements of cyber security for managers of information infrastructure and public administration subjects of peculiar importance, who control and/or manage information resources of the state.

IV. TERMS AND DEFINITIONS

Information – any element of knowledge presented in the form suitable for use, storage, transmission or processing. Information includes data expressed and summarised or interpreted in oral, written, audiovisual, digital or any other form.

Information security – assurance of confidentiality, integrity and accessibility of information. When expedient, other criteria, such as responsibility, accounting, authenticity/reliability, non-denial and privacy can be additionally included.

Information environment – individuals (users), organisations and/or systems that correct, process or spread information. And the information itself.

Information system – information processing systems and the whole of organisation resources (information itself, human resources, technical means, finances, etc.) intended for information processing, developing (creating), spreading (sending and receiving). It is a structured collection of processes and procedures, in which data is collected, organised and transmitted to a user.

Information resources – information (databases, data files, agreements and other documents, systemic and project documentation, training materials, operation and maintenance procedures, continuation and restoration plans); software (applied and systemic software, its development means);

hardware (data files, organisational, computer and communications equipment); services needed for functioning of information technologies and telecommunications (hereinafter referred to as ITT); ITT services and infrastructure resources provided by external parties; employees' qualifications and skills.

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

Cyber environment – users of information and industrial process management systems, networks, hardware, software, information transmitted or stored, services and systems which can be accessed directly or indirectly through electronic communications networks.

Cyber security – KN capacity to protect KN electronic communications network, information and industrial process management systems in cyber environment and to protect them in case of cyber attacks. It is the whole of legal, information dissemination, organisational and technical means intended for preventing cyber incidents, to detect, analyse them and to respond to them and for restoration of usual operation of electronic communications networks, information and industrial process management systems, once such incidents take place.

Confidentiality – a feature of information ensuring its accessibility exclusively to natural or legal persons (users) holding such right.

Accessibility – a feature of information guaranteeing accessibility of information and resources needed to access it to sanctioned user when needed.

Integrity – a feature of information specifying its accuracy and protection of its completeness and preventing modification or destruction of information accidentally or unlawfully.

Industrial process management system – system consisting of equipment based on information and communications technologies intended to monitor industrial processes or manage industrial, energy, transport, water supply services also in other sectors of economic activity.

KN – Joint stock company Klaipėdos nafta.

V. PURPOSES OF IMPLEMENTATION OF THE POLICY

Safe and reliable information and cyber environment of KN ensuring high level of security of electronic communications networks, information and industrial process management systems and information – it is strategically important and necessary prerequisite of successful activities of KN and its further development and preservation of KN assets and reputation.

Main purposes of assurance of information and cyber security:

- To ensure secure and reliable information and cyber environment of KN, taking into consideration the strategic goals of KN and without exceeding the level of risks managed and assumed by the Management;
- To ensure security of KN information – i.e. confidentiality, integrity and accessibility of KN information;
- To ensure continuation of KN activity – i.e. uninterrupted operation of hardware and software of electronic communications networks, information and industrial process management systems, incident management and timely restoration of operation;
- To search for new modes and means ensuring security without reducing convenience for users and technical staff operating the systems;
- To ensure and manage compliance with the requirements of legal acts regulating information and cyber security and personal data protection.

VI. MAIN PRINCIPLES/OBLIGATIONS

Security of KN information and cyber environment, information and industrial process management systems of business is ensured and managed by developing and improving a uniform security system, which consists of legal, technical, organisational and educational (training) means selected in order to control risk and to minimise down to the risk level acceptable to the KN management.

In pursuit of information and cyber security, the KN management set forth the following principles of Information and cyber security management:

- *Processional approach* – Activity ensuring security must be organised in KN following the processional approach. Results of the systems of management of information and cyber security must be measured and assessed on a periodical basis, in order to ensure continuous improvement of processes and adaptation to the changing business environment;
- *Harmony* – strengthening of information and cyber security through systematic even improvement of security in all fields of activity of KN, consistent installation of good cyber security practices (SANS/CIS, CSC20) and continuous identification and strengthening of security system links;
- *Standardisation* – information and cyber security procedures must be clearly regulated and known to everyone, managed through the established uniform standardised process. When installing and improving *Security* processes, the requirements of the information security management system standard (ISO 27001) and ITIL methodology have to be adhered to;
- *Prioritisation* – when ensuring Security in information systems, security measures are assessed in the following aspects, by prioritising them as follows: confidentiality, integrity, accessibility. *Security* in industrial process management systems is implemented by establishing priorities as follows) accessibility, integrity and confidentiality;
- *Classification ('Need to know')* – all KN information must be grouped by the levels of confidentiality; all undisclosed information must be clearly marked, while its access to KN staff and third parties is provided strictly adhering to the principle of '*Need to know*';
- *Adequacy (security before convenience*) – restrictions and technical and organisational measures ensuring Security are installed by prioritising *Security* but without exceeding the necessary limit needed for minimisation of risk down to the level acceptable to the KN management, and securing a possibility for authorised KN staff and external parties to use KN digital services;
- *Rationality* – installed new tools and other technical and organisational measures ensuring *Security* and protection against cyber threats and vulnerabilities must comply with the value of protected information. When installing them, the principle of *Harmony* is followed, available KN resources and competences are assessed and used;
- *Efficiency* – ongoing monitoring of information and cyber environment and effective response to cyber incidents and management of information and cyber security incidents (crises) are ensured;
- *Prevention* – bigger attention must be assigned to prevention rather than response to incidents and other consequences.

To fulfil the established principles of information and cyber security management, the KN *Management* undertakes the following obligations:

- Promotion and propagation of measures of incident prevention and universal cyber hygiene (awareness) and *Security* culture;
- Assignment of resources needed for ongoing planned improvement of qualifications and skills of the staff ensuring *Security*;
- Granting competences and powers to the managers to coordinate and approve documents related to assigned *Security* management process.

VII. IMPLEMENTATION AND CONTROL OF THE POLICY

Actions of implementation, control, organisation and assurance of this Policy and responsibilities are described in the *Information and cyber security guidelines* and related procedures.

To assess compliance of the KN Policy with the requirements of legal acts and to submit proposals regarding improvement of the Policy, the Managing director forms a Security commission, the tasks, functions and work organisation principles of which are defined in the working regulation of the Security commission.

Authorised person of information and cyber security at least once in 2 (two) years must initiate internal inspection to determine whether this Policy is properly implemented in practice and draw and submit proposals on the need of amendments to this *Policy* to the Security Commission.