Information Security Policy

1. Purpose

This Policy is the main document regulating the activities of Noventiq Group in the field of information security.

Corporate requirements in the field of information security are applied to all production regions and all business units of Noventiq Group.

2. General Provisions

Information security is a state of data protection, characterized by the ability of staff, technical facilities and information technology to ensure confidentiality, integrity and availability of information when processing by technical means.

Information Security Policy was developed in accordance with the provisions of ISO / IEC 27001: 2013.

Policy shall be reviewed regularly at least once a year.

3. Information Security Objectives

In the field of information security Noventiq Group established the following strategic objectives:

- Improving the competitiveness of business of Noventiq Group;
- Compliance with the requirements of legislation and contractual obligations in terms of information security;
- Improving business reputation and corporate culture of Noventiq Group;
- Effective information security management and continuous improvement of information security management system;
- Achieving adequate protection measures against information security threats;
- Ensuring the security of corporate assets of Noventiq Group, including staff, material and technical values, information resources, business processes.

4. Information Security Challenges

Information security system of Noventiq Group should solve the following tasks:

- Involvement of senior management of Noventiq Group in the process of ensuring information security: information security activities initiated and monitored by senior management of Noventiq Group;

- Compliance with the local, global requirements: Noventiq Group implements information security measures in strict compliance with current applicable legislation and contractual obligations;

- Coherence in order to ensure information, physical and economic security: actions to ensure information, physical and economic security are carried out on the basis of a well-defined cooperation between the involved departments of Noventiq Group and are agreed among themselves on the objectives, tasks, principles, methods and means;

- Application of cost-effective measures: Noventiq Group aims to choose information security measures considering their implementation costs, the likelihood of information security threats and the size of possible losses from their implementation;

- Checking of workers: all candidates for the vacant positions in Noventiq Group must necessarily be checked in accordance with established procedures;

- Documentation of information security requirements: in Noventiq Group all the requirements in the field of information security are fixed in the developed internal regulatory documents;

- Raising awareness of information security: the documented requirements in the field of information security are communicated to the employees of all business units of Noventiq Group and contractors with respect to the part related to them.

5. Information Security Principles

5.1 Systemic approach

In Noventiq Group assets are considered to be interrelated and mutually influencing components of a single system. In case of information security threats, the maximum possible amount of system behavior scenarios is taken into the account. The protection system is built considering not only all known channels of obtaining unauthorized access to information, but also considering the possibility of appearance of fundamentally new ways to implement security threats.

5.2 Complexity approach

A wide range of measures, methods and means of information protection is used in order to ensure information security. Their complex using implies the coordination of heterogeneous means in constructing the integrated protection system which blocks all

the existing channels of threats and containing no weaknesses at the junctions of its separate components.

5.3 The Separation Principle

One cannot rely on a single protective line, no matter how safe it may seem. Information security system is constructed in such a way that the most protected security zone is placed inside other protected zones.

5.4 The principle of equal strength

The effectiveness of protection mechanisms must not be reduced to nothing by a weak link, arising as a result of underestimation of the real threats or the use of inadequate protection measures.

5.5 The Principle of Continuity

In Noventiq Group the ensuring of information security is a continuous and purposeful process, which implies taking the appropriate measures at all stages of the asset lifecycle.

5.6 The principle of reasonable sufficiency

Noventiq Group Management assumes that it is impossible to create an "absolute" protection of assets. Therefore, the choice of means of assets protection adequate for real existing threats (i.e. providing the allowable level of potential damage in case of threats implementation) and is based on risk analysis.

5.7 The principle of legality

During the selection and implementation of measures and means to ensure the information security of the Noventiq Group strictly observes the legislation of the Russian Federation, the requirements of normative legal and technical documents in the field of Noventiq Group information security.

5.8 The controllability principle

All information security management and assurance processes in Noventiq Group must be controlled, i.e., it should be possible to monitor and measure the processes and components, to identify in time the information security violations and to take appropriate measures.

5.9 The principle of personal responsibility

Each employee is responsible for ensuring the assets safety within his powers.

6. Violations of this Policy

Where Noventiq is informed of any breaches of this Policy or any event or circumstance that gives rise to an actual or suspected breach of the established rules of work, the employee may be limited to access rights to such assets and it will initiate an appropriate internal investigation thereof and involve law enforcement and other competent authorities, if necessary.

All Employees bear responsibility for their compliance with this Policy and any other documents aimed at its implementation. Failure to comply with the requirements of this Policy will be grounds for disciplinary action up to and including dismissal, or termination of business relationship.

7. Revision history

Issue No	Version No	Issue Date	Summary of Changes
1	1.0	2020	Final Document

S.V. Chernovolenko, Global CEO of Noventiq