Appendix # 10
to the decision of the Board of Directors of Rosseti Centre, PJSC
Minutes of 16.06.2022 # 34/22

Approved by the decision of the Board of Directors of
PJSC Rosseti dated 29.04.2022
(Minutes of 04.05.2022 # 492)

Changes
to the Regulation of PJSC Rosseti "On the Unified Technical Policy in the Electric Grid Complex (hereinafter referred to as the Regulation)

1. Make the following changes to section 1.1. «Goals and main tasks of the unified technical policy in the power grid complex»:

1.1. The first bullet of the clause «Goals» shall be read in the following wording:

«• determination of the main technical directions and unification of technical and technological solutions that ensure an increase in the reliability, efficiency and reduction of the resource intensity of the functioning of the electric grid complex in the short and medium term, while ensuring proper safety and reliability of energy supply to consumers»;

1.2. Add bullets to the clause «Goals»:

• ensuring unity of approaches in new construction, operation and decommissioning of power grid facilities;

• ensuring the synchronization of the implementation of industry technologies and equipment and IT - technologies, devices and software;

1.3. Add a bullet to the clause «Tasks»:

• import substitution.

2. Read the paragraph «3.5.3. Production asset management principles» in the following edition:

«The main principles of managing the Company's production assets are:

- focus on achieving the strategic goals of the State, the Company and SDCs;

- systematic decision-making, application of uniform criteria, principles, rules, methods for the processes of planning, implementation, control and evaluation of the effectiveness of the performance of work on operational and investment activities;

- focus on obtaining positive effects in the short, medium and long term by improving the efficiency of managing production assets throughout the entire life cycle of assets;

- ensuring the functioning of the production asset management system in all SDCs of the Company, which are an integral and constituent part of the overall asset management system of the Company;

- reducing the share of equipment, power transmission lines and structures that have high and medium levels of risk associated with their operation, taking into account the consequences of their failure.».

3. Make the following changes to section 3.5.4. «Development tasks of the production assets management system»:

3.1. Read the first clause in the following edition:

« - the transition from the production asset management system according to the planned preventive type of organization of repairs to the organization of repairs according to the actual technical condition, taking into account the probability and severity of the consequences of failure of the main technological equipment (risks);».

3.2. Read the eighth clause in the following edition:

« - ensuring the calculation and monitoring of the indices of the technical condition of equipment of the substation, power transmission lines and structures with an assessment of the probability of failure, the severity of the consequences, the assessment of the risk due to failure and the assessment of the cost of ownership for planning the type and volume of technical impact in accordance with the requirements of the current regulatory legal acts;».

3.3. Read the ninth clause in the following edition:

« - optimization of costs for repair activities, modernization, technical re-equipment of equipment, technological and engineering systems, buildings and structures, ensuring the necessary level of safety, operational reliability and ensuring the required level of quality of power supply to consumers, as well as taking into account the future development of the power grid complex;».

4. Read paragraph 2.1.4.6 of section 2.1.4 «Switching devices» of the Regulation in the following edition:

«2.1.4.6. In distribution networks with a voltage of 6-20 kV, it is additionally recommended to use fuses - disconnectors and disconnectors that meet modern operating requirements, if necessary with the possibility of remote control, as well as disconnectors with separate phase disconnection, using operating tie sticks.».

5. Supplement section 2.1.7 «Transformer and distribution substations of 6-35 kV» of the Regulation with paragraph 2.1.7.13:

«2.1.7.13. In switchgear of 0.4-20 kV of SS, TS, DS, it is recommended to use thermal indicators for periodic monitoring of the temperature regime of electrical equipment.».

6. Read paragraph 2.5.2.6 of section 2.5.2. «Technical solutions for the design, new construction and reconstruction of overhead lines» in the following edition:

«2.5.2.6 When designing overhead lines of 35 kV and above, it is necessary to provide for technical solutions that ensure the safety of their operation, including safe ascent/descent, movement and work at height. The type and location of

installation of personal fall protection systems should be determined when designing overhead lines, depending on the structures used (metal, lattice, multifaceted or reinforced concrete) and the conditions for passing the overhead line as agreed with the Customer.».

7. Read paragraphs 2.5.4.1 – 2.5.4.8 of section 2.5.4 «Wires and lightning protection cables» of the Regulation in the following edition:

«2.5.4.1. On overhead lines with a voltage class of 35 kV and above, a wire should be used:

- wire with a steel core with profiled conductors of the upper layers;
- wire with carbon fiber composite cores;
- wire with increased corrosion resistance of steel cores;
- aluminum alloy wire;
- steel-aluminum wire;

The choice of the variant of the wires used must be justified by technical and economic calculations when designing overhead lines.

2.5.4.2. On overhead lines with a voltage class of 35 kV and higher, steel cables, steel-aluminum wires, steel cables with increased corrosion resistance (galvanized, for especially harsh working conditions), steel-aluminum cables, lightning protection cables with built-in optical cable can be used as lightning protection cables.

The choice of the type of lightning protection cables used must be justified by technical and economic calculations when designing overhead lines.

2.5.4.3. The use in certain sections of overhead lines (large crossings through water bodies, mountains, floodplains, swamps, difficult climatic conditions) of grades and sections of wires, lightning protection cables, as well as phase designs that are different from those used in other sections of overhead lines, must be confirmed by calculations of structural elements of overhead lines and a feasibility study.

2.5.4.4. During new construction and reconstruction of overhead lines with a voltage class of 110 kV and above, at the intersection of overhead lines with roads, engineering structures and communications, when designing, it is necessary to ensure the condition for the further safe operation of overhead lines, taking into account the exclusion of the impact of influencing factors, such as: overlapping of garlands of insulators from impact of chemical reagents during de-icing of roads, damage to overhead lines wires when passing oversized equipment, damage to overhead lines wires from the explosion of gas and oil pipelines, etc. In order to eliminate these factors, it is necessary to consider the use of elevated poles providing increased overall distances from overhead lines wires to crossed objects.

2.5.4.5. If there is a feasibility study at large crossings through water and other natural barriers, it is allowed to use steel ropes from galvanized wires and steel ropes from aluminum-clad wires, as well as wires with a twisted composite core made of carbon fiber.

2.5.4.6. The service life of wires and lightning protection cables on overhead lines with a voltage of 35 kV and above must be at least 50 years.

2.5.4.7. On 6-20 kV main overhead lines, a steel-aluminum bare wire or a protected wire with a cross section of at least 70 mm2 should be used. On linear branches (taps) from the mains, it is recommended to use steel-aluminum wires or protected wires with a cross section of at least 35 mm2.

2.5.4.8. Protected wires are recommended to be used on 6-110 kV overhead lines in the first place:

- when passing the overhead line route through populated areas;
- when passing overhead lines through forests;
- when crossing overhead lines of water barriers;
- in the absence of the possibility of observing overall distances when passing overhead lines in cramped conditions;
- when joint suspension with insulated overhead lines of 0.4 kV.

With an appropriate feasibility study, it is allowed to use a self-supporting cable on a 6-35 kV overhead line.».

8. Paragraphs 2.5.4.10 - 2.5.4.14 8 of section «Wires and lightning protection cables» of the Regulation shall be read, respectively, as paragraphs 2.5.4.9 – 2.5.4.13.

9. Read paragraph 2.10.10 of section 2.10 « Electricity metering system» of the Regulation in the following edition:

«2.10.10. To protect metering devices and (or) the measuring complex for commercial and technical metering of electric energy from unauthorized access, sealing of the terminal covers of metering devices and test boxes, as well as test and intermediate terminal blocks of current and voltage circuits, identification and authentication of subjects and objects of access. When connecting metering devices and (or) measuring complexes for commercial and technical metering of electric energy to wireless communication networks of cellular operators, information protection from unauthorized access should be ensured by using a dedicated APN (VPN) of the data transmission network operator and the topology of the Zvezda network (Hub and Spoke).».

10. Read Chapter 3.6 «Information security» of the Regulation as follows:

«3.6. Information security.

3.6.1. Goals and objectives of information security.

Goals: Ensuring the stable functioning of the critical information infrastructure of the subjects of the electric grid complex of the Rosseti group of companies (hereinafter referred to as the Subjects) when computer attacks are carried out against it, preventing unauthorized access to processed information, destroying such information, modifying it, blocking and disseminating it, as well as other misconduct in relation to such information.

Objectives: Creation of a security system for critical information infrastructure facilities (hereinafter - OKII) and ensuring its functioning, in particular:

- improving the reliability and safety of OKII of the electric grid complex of the Rosseti group of companies through the supply of digital equipment, systems and technical means of information protection that have a minimum set of built-in security functions and meet, in their functional characteristics, the requirements of regulatory and technical documentation in the field of information security and the conditions of use;
- as part of the creation, modernization, operation of OKI, regular assessment of the scale of possible consequences for the Company, social, political, economic, environmental consequences, as well as consequences for national defense, state security and law enforcement in the event of computer incidents at the OKII of the Rosseti group of companies, assigning one of the categories of significance to information infrastructure objects;
- ensuring technological safety and independence from imported equipment, technical devices, components, services (works) of foreign companies and the use of foreign software at power grid facilities by replacing software, microcontrollers and integrated circuits, as well as using only such software as a matter of priority software, information about which is included in the unified register of Russian programs for electronic computers and databases;
- development of corporate standards in the field of information security;
- ensuring the safety of OKII during operation:
- prevention of illegal access to information processed by information infrastructure facilities, destruction of such information, its modification, blocking, copying, provision and distribution, as well as other illegal actions in relation to such information;
- prevention of impact on the technical means of information processing, as a result of which the functioning of the OKII and the processes providing (managed, controlled) by it may be disrupted and (or) terminated;
- automating the processes of detecting and preventing computer attacks on the OKII of the energy complex of the Rosseti group of companies using machine learning algorithms and heuristic analysis;
- ensuring the continuous functioning of technical means of information protection;
- carrying out regular instrumental assessment of the effectiveness of the OKII security subsystem of the energy complex of the Rosseti group of companies;
- ensuring the fastest recovery (self-healing) of OKII;
- interaction with the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation;

- application of risk-based asset management of information infrastructure, organization, as part of the operation process, checking and installing critical software updates for network elements;
- ensuring the safety of OKII during decommissioning;
- conducting internal control in the field of ensuring the safety of OKII by carrying out scheduled or unscheduled inspections;
- increasing the level of knowledge of employees on information security issues, organizing (re)training of engineers, technicians, administrators and operators on information security issues.

3.6.2. Basic principles of development

The security system for information infrastructure facilities should be created in accordance with the requirements and provisions of Federal Law No. 187-FZ of 26 July 2017 "On the Security of Critical Information Infrastructure of the Russian Federation" and Federal Law No. 152-FZ of 27 July 2006 "On Personal Data", and as well as relevant by-laws.

The security system of information infrastructure facilities of territorial distribution complexes should be created as a typical security system, including forces and means designed to detect, prevent computer attacks and eliminate consequences of computer incidents.

The measures taken to ensure the security of OKII should not have a negative impact on the functioning of the automatic control system, the exchange of technological information, the functions of remote control of power grid equipment and smart devices from remote control centres of the Rosseti group of companies (Grid Control Centres) and from dispatch centres of SO UES JSC.

The result of ensuring the security of the information infrastructure should be the preservation of the achieved effects in terms of ensuring the reliability, technological and economic efficiency of power supply and other strategic goals of the digital transformation of the Russian electric power industry.

3.6.3. Basic requirements

3.6.3.1. The objects of protection in the context of ensuring the security of the information infrastructure and processed information are:

- corporate information systems (including computer storage media, workstations, servers, means for processing alphanumeric, graphic, video and speech information, firmware, system-wide, application software) that ensure the sustainability of financial and economic activity;
- automated control systems (including automated workstations, industrial servers, programmable logic controllers, industrial, technological equipment (actuators) that have the functions of both local and remote control, or have functioning network interfaces, firmware, system-wide, application software provision), ensuring reliable supply of consumers with electricity;
- corporate and technological information and telecommunications networks (including telecommunications equipment, software, control system,

communication lines) that form a single information space and digital interaction environment;

- telecommunication networks used to organize the interaction of objects;
- architecture and configuration of information systems, information and telecommunications networks, automated control systems, information (data) about the parameters (state) of a managed (controlled) object or process (including input (output) information, control (command) information, control and measurement information, personal data, other critical (technological) information, including that of commercial value due to being unknown to third parties.

3.6.3.2. Ensuring the security of significant OKII is carried out depending on the established category of significance of objects in accordance with the requirements established by the federal executive body authorized in the field of ensuring the security of critical information infrastructure of the Russian Federation.

3.6.3.3. Ensuring the safety of OKII without an established category of significance is carried out in accordance with the organizational and administrative documents of the Rosseti group of companies and the requirements of this Technical Policy.

3.6.3.4. To ensure the security of OKII, which are personal data information systems, these Requirements are applied subject to the Requirements for the protection of personal data when they are processed in personal data information systems approved by Resolution of the Government of the Russian Federation dated 01 November 2012 No. 1119.

3.6.3.5. If the object of protection is information when making money transfers, then in accordance with the Bank of Russia's Regulation No. 719-P dated 04.06.2020 "On the requirements for ensuring the protection of information when making money transfers and on the procedure for the Bank of Russia to exercise control over compliance with the requirements to ensure the protection of information when making money transfers", it is necessary to be guided by the requirements for ensuring the protection of information when making money transfers, which are determined in the internal documents of the money transfer operator, bank paying agent (subagent), payment system operator, payment infrastructure service provider.

3.6.3.6. Depending on the category of significance, the required level of security and actual threats to information security in the OKII security system, the following organizational and technical measures should be implemented:

- identification and authentication (IAF);
- access control (APC);
- restriction of the software environment (OPS);
- protection of machine data carriers (ZNI);
- security audit (SAU);
- anti-virus protection (AVZ);
- intrusion prevention (computer attacks) (IPS);

- integrity assurance (OCL);
- ensuring accessibility (ODT);
- protection of technical means and systems (ZTS);
- protection of the information (automated) system and its components (ZIS);
- planning of measures to ensure safety (PLN);
- configuration management (UCF);
- management of software updates (OPO);
- information security incident response (INS);
- provision of actions in emergency situations (DNS);
- informing and training of personnel (IPO).

3.6.3.7. As organizational measures to ensure the safety of OKII, the following is applied:

- organization of control of physical access to software and hardware components of OKII and its communication lines;
- implementation of access control rules that regulate the access rights of access of subjects to access objects, and the introduction of restrictions on user actions, as well as on changes in operating conditions, composition and configuration of software and firmware;
- description in the organizational and administrative documents of actions of users and administrators of the OKII components for the implementation of organizational measures;
- definition of the OKII security administrator;
- working out the actions of users and administrators of OKII to implement measures to ensure the security of OKII and restore the information infrastructure and processed information;
- advanced training of information security specialists, increased user awareness.

3.6.3.7.1. Technical measures to ensure information security are implemented primarily through the use of operating systems from the register of Russian software, and the following classes of software and firmware - information security tools (including those built into system-wide, application software):

- means of protecting information from unauthorized access, including means of identification and authentication, access control, software environment restrictions, protection of machine media and information, integrity control;
- firewalls of the network level, the level of the logical boundaries of the network;
- firewalls of the industrial network level;
- means of detection (prevention) of intrusions (computer attacks) of the network level, control and analysis of network traffic;
- means of registration and management of security events;
- means of preventing computer attacks;

- means of protecting information and data during their transmission over communication channels;
- means of secure remote access to the LAN, including terminal access means;
- backup tools, including tools for creating and storing backup copies;
- key information management tools;
- means (systems) of control (analysis) of security, security audit;
- means of anti-virus protection of workstations of administrative and managerial personnel;
- means of anti-virus protection of workstations of production personnel, industrial servers;
- means of anti-virus protection of the network level, mail and web servers, file storages, spam protection;
- means of protecting information when using mobile devices;
- means of controlling change actions;
- means of denial of service threats (DOS, DDOS attacks);
- tools for managing the movement of virtual machines (containers) and data processed on them.

Means of protecting information from unauthorized access include the following protection mechanisms (including those built into general system, application software and (or) firmware):

- means of trusted loading;
- identification and authentication of users;
- discretionary user access control; mandatory access control of users and processes;
- labelling of documents and control of their printing;
- protection of input and output of information on alienable physical media;
- registration of security events in the event log;
- integrity control of critical files and data;
- access control to peripheral devices and input-output ports;
- guaranteed deletion of data on disks and selective overwriting of files, etc.

3.6.3.8. The basic set of technical measures includes:

- means of protecting information from unauthorized access (including built-in security features in general system, application software and (or) software and hardware);
- network level firewalls;
- means of detecting (preventing) intrusions (computer attacks) at the network level, server level, workstation;
- means of anti-virus protection of mail and web servers, file storages and workstations;

- means of protecting information and data during their transmission over communication channels;
- secure remote access to the LAN, including terminal access, two-factor authentication;
- backup tools, including tools for creating and storing backups.

The basic set of security measures is subject to adaptation in accordance with the current threats to information security, the information technologies used and the features of the functioning of OKII. At the same time, measures that are directly related to information technologies that are not used as part of OKII, or that are not inherent in characteristics, can be excluded from the basic set.

3.6.3.9. As a means of protecting information, in a priority order, the means of protecting information built into the software and (or) firmware (if any) are subject to use.

3.6.3.10. If it is impossible to implement the stated goals with built-in information security tools, the corresponding functionality should be provided by the imposed information security tools.

3.6.3.11. To ensure the security of information and telecommunication networks, these Requirements are applied along with the regulatory legal acts of the federal executive body responsible for the development and implementation of state policy and legal regulation in the field of communications, as well as GOST R 62443 “Industrial communication networks. Network and system security (cybersecurity)”, GOST R 56498-2015 IEC 62443-3:2008 Industrial communication networks. Network and system security (cybersecurity). Part 3. Security (cybersecurity) of the industrial measurement and control process.

3.6.3.12. Digital equipment with software is used as a digital equipment that performs the functions of a border router with access to the Internet that passed the assessment of compliance with the requirements of the FSTEC of Russia guidelines on information security in the form of certification.

3.6.3.13. Technical means of information protection must be operated in accordance with the instructions (rules) for operation developed by the developers (manufacturers) of these tools, and other operational documentation for technical means of information protection.

When installing and configuring technical means of information protection, the implementation of restrictions on the operation of these means, if they are available in the operating documentation, must be ensured.

3.6.3.14. The applied technical means of information protection must be provided with warranty and technical support.

3.6.3.15. The procedure for creating information systems, automated control systems, control systems for information and telecommunication networks, the stages of work, as well as the development of technical and working documentation must comply with GOST R 51583-2014 “Information security. The order of creation of automated systems in protected execution. General provisions”,

the provisions of Federal Law No. 187-FZ of 26 July 2017 “On the security of the critical information infrastructure of the Russian Federation” and by-laws, as well as organizational and administrative documents of the Subject.

At the stages of the life cycle during the creation (modernization) of information infrastructure objects, the following is carried out:

- analysis of threats to information security and development of a model of threats to information security or its elaboration (if any), determination of the category of significance, the required level of security of OKII;
- design of organizational and technical measures to ensure information security of OKII, development of working (operating) documentation for OKII (in terms of ensuring its security);
- implementation of organizational and technical measures to ensure information security of OKII, preliminary tests, vulnerability analysis, trial operation, acceptance testing and commissioning of OKII and its security subsystem;
- regulation of processes for ensuring the information security of OKII during operation.

Design solutions to ensure the information security of new construction facilities, expansion, reconstruction, technical re-equipment or modernization of electric grid facilities must be carried out in accordance with standard technical solutions approved by the organizational and administrative documents of the Company.

3.6.3.16. The results of designing a security system for information infrastructure facilities are reflected in the design documentation (draft (technical) design and (or) working documentation) developed taking into account GOST 34.201-2020 “Information technology. Set of standards for automated systems. Types, completeness and designation of documents when creating automated systems” (hereinafter - GOST 34.201-2020) and organization standards, in accordance with the established category of significance.

3.6.3.17. Information protection when using virtualization technologies is carried out in accordance with GOST R 56938-2016 “Information protection when using virtualization technology. General provisions”.

3.6.3.18. The requirements for functional safety of automated enterprise management systems, operational and technological management, and technological management must comply with GOST R IEC 61508-1-2012, 61508-2-2012, 61508-3-2018.

3.6.4. Compliance assessment for information security requirements

3.6.4.1. Commissioning of OKII is allowed if there is an acceptance test protocol (certificate) with a positive conclusion on the compliance and effectiveness of the organizational and technical protection measures taken with the established safety requirements.

3.6.4.2. To ensure the security of OKII, technical means of protecting information that have been assessed for compliance with information security requirements in the form of mandatory certification, testing or acceptance should be used.

Confirmation of compliance of technical means of information protection with the requirements for information security, including the requirements for compatibility with automated process control systems, is carried out as part of the quality check (certification) set forth in Section 3.6.6 of this Regulation.

3.6.4.3. The assessment of the compliance and effectiveness of the organizational and technical measures taken to protect OKII with the established security requirements is carried out by the Subjects independently or with the involvement of organizations that, in accordance with the legislation of the Russian Federation, have licenses for relevant activities in the field of information security.

A re-assessment of the compliance of the adopted organizational and technical protection measures with the established safety requirements is carried out after three years.

3.6.4.4. Assessment of the conformity and effectiveness of the adopted organizational and technical measures for the protection of OKII processing Personal Data is carried out according to the decision of the Subject with the involvement of an organization that, in accordance with the legislation of the Russian Federation, has licenses for the relevant activities in the field of information security.

3.6.4.5. Assessment of the conformity and effectiveness of the adopted organizational and technical measures for the protection of OKII interacting with state information systems is carried out without fail with the involvement of organizations that, in accordance with the legislation of the Russian Federation, have licenses for relevant activities in the field of information protection.

3.6.5. Restrictions on the use of technologies/equipment

3.6.5.1. When choosing information security tools, including the accompanying embedded software, the possible presence of restrictions on the part of developers (manufacturers) or other persons on the use of these tools throughout the Russian Federation should be taken into account.

3.6.5.2. When implementing technical measures to protect information, it is not allowed to use the SHA-1 cryptographic hashing algorithm, SNMP v1, v2 protocols.

3.6.5.3. In OKII it is not allowed:

- availability of remote access directly to software and firmware, including information security tools, for updating or management by persons who are not employees of PJSC Rosseti, as well as employees of its subsidiaries and affiliates;
- availability of local access to software and firmware, including information security tools, for updating or management by persons who are not

employees of PJSC Rosseti, as well as employees of its subsidiaries and affiliates without control by the Subject;

• transfer of information, including technological information, to the developer (manufacturer) of software and firmware, including information security tools, or to other persons without the control of the Subject.

In case of technical necessity, the organization of remote access to software and firmware, including information security tools, the facility takes organizational and technical measures to ensure the security of such access, providing for:

• determination of persons and devices that are allowed remote access to the software and firmware of the object, granting them minimal rights when accessing these tools;

• control of access to software and firmware of the object;

• protection of information and data during their transmission over communication channels with remote access to software and firmware of the object;

• monitoring and registration of actions of persons who are allowed remote access to software and firmware of the object, as well as processes initiated by them, analysis of these actions in order to identify facts of illegal actions;

• ensuring the impossibility of refusal of persons from the performed actions in the implementation of remote access to the software and firmware of the object;

• provision of two-factor authentication for remote access.

3.6.5.4. The software and firmware tools included in OKII that store and process information must be located on the territory of the Russian Federation (except for cases when the placement of these tools is carried out in foreign separate subdivisions of the Subject (branches, representative offices), as well as cases established by laws of the Russian Federation and (or) international treaties of the Russian Federation).

3.6.5.5. Operational and technical maintenance, technical support of software and firmware, including the DBMS, must be provided by the Copyright Holder (developer) or a representative of the Copyright Holder registered in the territory of the Russian Federation.

3.6.6. Quality control (certification) of digital equipment, systems and technical means of information protection

3.6.6.1. Digital equipment and systems that provide search, collection, storage, processing, presentation, distribution of digital information at the facilities of the electric grid complex of the Rosseti group of companies, including technical means of information protection, are subject to quality control (certification).

3.6.2. Quality control (certification) of digital equipment, systems and technical means of information security is the Company’s internal control system and it is aimed at confirming:

• absence of vulnerabilities and shortcomings in the composition of the software that can lead to violations of the design values of the parameters for the performance of target functions and (or) lead to technological violations;

• implementation of the minimum set of security functions by built-in information security tools that meet, in terms of their functional characteristics, the requirements of regulatory and technical documentation in the field of information security and the conditions of use at electric grid facilities of the Company and SDCs;

• availability in operating documentation of a description of conditions for safe operation;

• compatibility of technical means of information protection with automated process control systems;

• implementation by the manufacturer, developer of measures to develop secure software at all stages of the life cycle in accordance with GOST R 56939-2016 “Information security. Development of secure software. General requirements”;

• implementation by the manufacturer, developer of procedures for eliminating deficiencies, vulnerabilities and updating software;

• absence of violations of copyrights for the transfer and use of software at facilities of the electric grid complex of the Company and SDCs.

3.6.6.2. Quality control (certification) is carried out for compliance with the information security requirements established by the regulatory legal acts of the Russian Federation and organizational and administrative documents of the Company and SDCs, as well as for compliance with the technical specifications agreed by the manufacturer, developer with the Company.

3.6.6.3. Quality control (certification) for compliance with information security requirements is organized by the Company in accordance with the decision taken by the Management Board of the Company, in the manner regulated by Order of PJSC Rosseti dated 28 August 2020 No. 391 “On approval of the methodology for checking digital equipment and systems for compliance with the requirements of information security, including conducting quality checks of technical means of protecting information in the electric grid complex”.

3.6.6.4. The results of the quality check (certification) are formalized by the conclusion of the certification commission and approved by the Company, taking into account the conclusions about the possibility of using digital equipment, systems and technical means of information protection at facilities of the electric grid complex of the Rosseti group of companies.

11. Read paragraphs 4.6.3 and 4.6.6 of section 4.6 «Import substitution in the electric grid complex» of the Regulation in the following edition:

«4.6.3. As part of the implementation of import substitution, Resolution of the Government of the Russian Federation dated 17 July 2015 No. 719 “On confirmation of the production of industrial products on the territory of the Russian Federation” defines the requirements for industrial products for the purpose of classifying them as products manufactured in the Russian Federation, Resolution of the Government of the Russian Federation dated 16 September 2016 No. 925 “On

the priority of goods of Russian origin, works, services performed by Russian entities in relation to goods originating from a foreign state, works, services performed by foreign entities" establishes the priority of goods of Russian origin in relation to goods produced in the territory of a foreign state.

Resolution of the Government of the Russian Federation dated 03 December 2020 No. 2013 "On the minimum share of purchases of goods of Russian origin" establishes the minimum share of purchases of goods of Russian origin. Within the framework of the said Resolution, a product of Russian origin is recognized as a product included:

- in the register of industrial products manufactured on the territory of the Russian Federation, or the register of industrial products manufactured on the territory of a state - a member of the Eurasian Economic Union, with the exception of the Russian Federation, provided for by Resolution of the Government of the Russian Federation dated 30 April 2020 No. 616 "On the establishment of a ban on the admission of industrial goods originating from foreign states, for the purposes of procurement for state and municipal needs, as well as industrial goods originating from foreign states, works (services) performed (rendered) by foreign entities, for the purposes of procurement for the needs of the country's defense and state security";

- in the unified register of Russian radio-electronic products, provided for by Resolution of the Government of the Russian Federation dated 10 July 2019 No. 878 "On measures to stimulate the production of radio-electronic products in the Russian Federation when purchasing goods, works, services to meet state and municipal needs, on amending Resolution of the Government of the Russian Federation dated 16 September 2016 No. 925 and the invalidation of certain acts of the Government of the Russian Federation".

4.6.6. The priority areas of technical policy in the field of import substitution are:

- minimization of the use of imported equipment and materials in the formation of design solutions and technical specifications, namely, the priority use in the technical specifications for design and design solutions of equipment and components of domestic production (included in the Register of industrial products manufactured in the territory of the Russian Federation, the Register of industrial products manufactured on the territory of a member state of the Eurasian Economic Union, with the exception of the Russian Federation, or the Unified Register of Russian Radioelectronic Products), equipment and components, the localization of which is carried out in whole or in part at the expense of subsidies, provided from the federal budget in accordance with agreements concluded by manufacturers with the Ministry of Industry and Trade of Russia, as well as equipment and components that are considered to be manufactured on the territory of the Russian Federation in accordance with the requirements of Resolution of the Government of the Russian

Federation dated 17 July 2015 No. 719 “On confirmation of the production of industrial products on the territory of the Russian Federation”.

Imported equipment and components may be used subject to the approval of the specialized structural divisions of PJSC Rosseti in charge of technical policy and international cooperation, if there is an appropriate justification (in the absence of analogues manufactured in the Russian Federation that meet all the technical requirements for them by the customer).

- typification of the equipment used in the power grid complex through the development and implementation of organization standards for electrical products, in order to take into account the production capabilities of domestic manufacturers and eliminate excessive requirements for equipment that lead to the need to purchase imported equipment;
- development of localization of production of high-tech equipment and components on the territory of the Russian Federation.».