Annex 1
to Order No. _____ of _____
issued by of PJSC “Rosseti Lenenergo”

PUBLIC JOINT-STOCK COMPANY ROSSETI LENENERGO

CORPORATE RULES **R-19.1-001-2022**

PJSC “ROSSETI LENENERGO”

INFORMATION SECURITY RULES

Version 1

Saint Petersburg
2022

CONTENTS

TERMS AND DEFINITIONS

Term	Definition
Automated System	a system consisting of a set of automation tools which implements information technology for the performance of the required functions, and personnel who ensures its operation. GOST R 59853-2021. Russian National Standard. Information Technology. Set of standards for automated systems. Automated Systems. Terms and Definitions".
Automated Control System	a set of software and hardware designed to control the process equipment and/or production equipment (executive devices) and their processes and to control such equipment and processes (in accordance with Federal Law No. 187-FZ of July 26, 2017 "On the Security of the Critical Information Infrastructure of the Russian Federation".
Information Technology	processes, methods of searching, collecting, storing, processing, providing and disseminating information and the methods for implementing such processes and methods (in accordance with the Federal Law of the Russian Federation No. 149-FZ of July 27, 2006 "On Information, Information Technologies and Information Protection").
Critical Information Infrastructure	a set of available services and systems, networks, hardware and software, data, automated processes which ensure information support for the operations of PJSC "Rosseti Lenenergo".
Information Resources	individual documents or sets of documents, documents or sets of documents in information systems.
Information System	the information contained in databases and the information technologies and equipment which ensure its processing (in accordance with the Federal Law of the Russian Federation of July 27, 2006 No. 149-FZ "On Information, Information Technologies and Information Protection").
Company	PJSC "Rosseti Lenenergo"
Information Security	Information Security Division responsible for the planning, management, implementation and supervision of information security activities.
Verification Center	a division which ensures creation, issuance and maintenance of digital signature certificates.
Employee	an individual employed by PJSC "Rosseti Lenenergo" under an employment contract.
User	an individual involved in the operation of the Information System or using the results of its operation.
Software	a set of software components of data processing systems which can function independently or as part of other systems.
Multifunction Printer (MFP)	a device which incorporates the functionality of a printer, scanner, fax machine, and copier.
BIOS, UEFI	A set of firmware which implements an interface to operate computer hardware and devices connected to it.
Antivirus Software	Antivirus Software

Workstation	Workstation
Automated Control System	Automated Control System
GIS	National Information or Government Services System
Information Security	Information Security Division
Information System	Information System
Online Banking	Online Banking
Computer equipment	Computer equipment
Regulations and Guidelines	Regulations and Guidelines
Rules	Information Security Rules of PJSC “Rosseti Lenenergo”
Service Desk	User Support Service

ACRONYMS AND ABBREVIATIONS

Abbreviation	**Meaning**
IT	Information Technology
IN/TN	Information/Telecommunications Network
LAN	Local Area Network
VPN	Virtual Private Network

1. General information

1.1. Purpose of the document

These Rules set out the procedures for handling confidential information, safe operation of the critical information infrastructure, steps to be taken in the event of computer incidents or other emergencies with the Employees or third parties who have access to confidential information or the Company’s critical information infrastructure under the existing contracts and agreements.

1.2. Corporate Cybersecurity Center

Rosseti Group has in place a Corporate Cybersecurity Center to manage the processes of detecting, preventing, and responding to cyberattacks on critical information infrastructure.

2. General provisions

2.1. These Rules shall apply to the following Users:

- employees of PJSC “Rosseti Lenenergo”;
- individuals acting under civil law contracts;
- individuals who act with respect to the information infrastructure or buildings hosting the information infrastructure of the Company, including audits, internships, cleaning;
- individuals employed by legal entities acting as contractors with respect to the information infrastructure or buildings hosting the Company’s information infrastructure under existing contracts or on any other legal basis.

2.2. In ensuring and maintaining the security of the Company’s information infrastructure and confidential information, the following assets are protected:

- corporate information systems (including machine readable media, workstations, servers, alphanumeric, graphic, video and speech information processing tools, firmware, system-wide, application software) ensuring the stability and sustainability of the Company’s business and financial operations;
- automated control systems (including workstations, industrial servers, programmable logic controllers, production and process equipment (executive devices) which have the features of both local and remote control or which have operating network interfaces, firmware, system-wide, application software) ensuring reliable supply of electricity to consumers;

- corporate and information/telecommunication networks (including telecommunications equipment, software, control system, communication lines) creating a single information space and digital interaction environment;
- digital devices and peripheral equipment (including printers, scanners, IP phones, digital cameras, smartphones);
- telecommunications networks used for the interaction between facilities and information transfer, Internet access points;
- architecture and configuration of the information systems, information and telecommunications networks, automated control systems, information (data) on the parameters (status) of the managed (controlled) facility or process (including input/output information, control/command information, control information, personal data, other confidential information, including information of trade value for not being known to any third parties.

2.3. Users shall strictly comply with these Rules when using information systems, automated control systems, information and telecommunication networks, including their parts (workstations, servers, switching, network or other equipment), and when handling confidential information.

2.4. The Company uses reasonable steps and methods of technical protection of the critical information infrastructure and the confidential information which it processes, and other steps not conflicting with the Russian law.

2.5. To focus the Users on the matters of information security, information stands or panels at the Company's sites (including power grid facilities) shall have a memo for the Employees who deal with the critical information infrastructure (Annex to these Rules).

3. Rules for confidential information treatment

3.1. The information processed by the Company includes:

- open information;
  - public information;
  - service information;
- restricted information:
  - confidential information;
  - trade secrets;
  - personal data;
- information involving state secret;
- other information the Company wishes to protect.

3.2. The list of confidential information is defined in accordance with Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies and Information Protection" and Decree of the President of the Russian Federation No. 188 of March 6, 1997 "On Approval of the List of Confidential Information" and approved by the Company's respective regulations and guidelines.

3.3. Information processed by the critical information infrastructure shall be treated as protected electronic information.

3.4. The Company uses and processes information electronically and/or in a paper form.

3.5. Confidential information is processed in accordance with the local/division regulations and other applicable regulations and guidelines.

4. Rules for safe use of critical information infrastructure

4.1. Users may not:

1) take photos or videos of workstation screens, offices or computer rooms if it is not required for the exercise of job duties set out in the Employee's job description;

2) do covert audio and video recording of meetings or negotiations;

3) throw away printed information constituting confidential data into wastebaskets (hard copies shall be destroyed by using shredders);

4) print or scan documents with confidential information on shared MFPs (placed in corridors, halls, recreation rooms, other places or rooms easily accessible by unauthorized persons);

5) discuss confidential information in the presence of third parties or in places where third parties can hear such information;

6) leave paper or electronic media with information in meeting rooms or other public places, including shared MFPs;

7) attempt to independently change settings of the operating systems or security settings of information protection tools installed on the workstation.

4.2. An Employee shall promptly report the following to the Information Security division by email **oib@lenenergo.ru** or telephone +7 (812) 595-87-88 ext. 5-87-88:

- detection of suspicious activity in a workstation;
- detection of viral activity;
- loss of service information media or a mobile workstation;
- disclosure of password information;
- loss or compromise of authentication keys (key media);
- detection of unidentified key media, information media;
- detection of unidentified devices connected to a workstation or LAN;
- detection of vulnerabilities in any part of a workstation, server, LAN, information system or automated control system;
- detection of errors in the configuration or operation of an information system or automated control systems or communication network giving an access to an area not specified in the initial access request;
- detection of publicly available in any form user credentials (password and login);
- detection of unauthorized access by other parties to information or Software;
- third party attempts to obtain password information;
- failure of information security tools.

4.3. All equipment with network interfaces shall be assigned to the Company Employees.

5. Rules for using accounts

5.1. The Company uses three types of accounts:

- User: "Unprivileged accounts";
- Administrator: "Privileged Accounts";
- Service: "Privileged accounts".

5.2. All Users are provided by default with the "User" corporate account, which only provides access to the workstation.

5.3. Access to information systems, including electronic document management systems, systems for planning and performance of business and financial operations or other resources required to perform job duties is provided upon request of the division head sent to the Service Desk by creating an individual account (login) and a one-time password.

5.4. Access to automated control systems, other technology systems is provided in accordance with the procedures set out in the operating and design documentation of such systems.

5.5. Access to a workstation, corporate personalized e-mail box, network folders and the Internet is provided to individuals who are not Company Employees upon request of the division

head (contract/agreement supervisor) sent to Service Desk and after the Information Security Division has approved the request.

5.6. The "Administrator" or "Service" account may be created or a higher access level given to an existing account subject to approval by the Information Security Division.

5.7. All accounts shall be personalized, unless the use of an impersonal account is due to the technical requirements of such information system, automated control system or information and telecommunications network equipment.

5.8. If several Users need to share an account, the division who is the owner of the information system shall develop and approve regulations setting out a list of persons authorised to use such information system (automated control system, information and telecommunications network equipment) using such account.

5.9. Accounts inactive during 45 business days or more shall be automatically blocked.

5.10. When the Employee ceases to be employed or completes the tasks specified in section 5.9 hereof, the Employee accounts shall be blocked.

5.11. Unblocking of accounts, password resetting in the existing accounts, granting access to the account of a dismissed Employee or other actions with accounts shall be approved by the Information Security Division.

5.12. If two-factor authentication is used linking a telephone number to the account, the number used to get the second factor shall belong to or be assigned to the Employee (if the Employee uses a corporate telephone number).

6. Rules of using passwords

6.1. A password shall contain (password complexity requirements):

- lowercase latin letters: abcd...xyz;
- uppercase latin letters: ABCD...XYZ;
- numbers: 123...90;
- special symbols: !%()+ etc.

6.2. A password shall not use a standard pattern or consecutive keyboard or alphabet characters (qwerty, 1234567, abcdefgh, etc.), nor shall it include a single word, the issued identifier, name, nickname, passport data or insurance number.

6.3. Password length requirements:

- For the “User” type of account, the password shall have at least 8 characters;
- For the "Administrator” type of account (local/domain), the password shall have at least 15 characters;
- for “service” identifiers or shared keys, the password shall have at least 14 characters;
- for SNMP Community Strings, the password shall have at least 10 characters.

6.4. Frequency of mandatory password change:

1) for Administrator accounts: every 60 days;
2) for User accounts: every 90 days;
3) for Service accounts: at least twice a year;
4) for shared keys SNMP Community Strings: at least once a year.

6.5. Passwords may not be stored or transmitted in plaintext through public networks (local area network, Internet, e-mail).

6.6. Default passwords may not be used. Passwords other than the manufacturer passwords shall be chosen.

6.7. If a password is compromised, the account owner shall promptly change all passwords.

6.8. When using passwords, it is prohibited to:

1) store or write passwords on paper, including on objects, or in places accessible to third

parties;

2) store or record passwords electronically without cryptographic protection;

3) provide or disclose personal password to third parties (unless a division manager or responsible Employee stores passwords in accordance with the division regulations and/or job description);

4) register third parties using your password;

5) transmit passphrases to users openly by email or otherwise through the Internet without any password or cryptographic protection;

6) enter a password if it can be seen accidentally or intentionally by a third party;

7) use the same passwords for different information systems (automated control systems, information and telecommunications network equipment);

8) create accounts or profiles on third-party Internet services or information systems (including public e-mail services) using the corporate workstation password;

9) use the "Remember Password" feature in the software.

6.9. Where it is not technically possible to use passwords which meet this section requirements, password requirements shall be set at the phase of design or development of manuals for such Information Systems, Automated Control Systems or IN/TN.

7. Rules for using the workstation

7.1. Users shall be skilled to use the hardware and software.

7.2. To perform business tasks, the Employee is provided with a corporate workstation, which incorporates computer equipment (personal computer), virtual computer network resources, peripheral, mobile or other equipment contemplated by the Employee's job duties and the relevant regulations and guidelines of the Company.

7.3. workstations for individuals who are not the Company Employees may be arranged at the request of the division head or the contract/agreement supervisor subject to approval by the Information Security Division.

7.4. It is prohibited to connect personal computer equipment to the Company's Information/Telecommunications Network (personal computer, laptop, smartphone, tablet, modem, router, access point, IP video camera, digital TV set-top box, etc.).

7.5. The User shall access the workstation:

- using its personal domain account;
- using its local personalized or shared account;
- using secure remote access.

7.6. Local accounts may be used:

- if so is provided by the manual or design documentation for the system;
- for workstation maintenance (by Technical Support Employees);
- in individual cases subject to an approval of the Information Security Division.

7.7. A workstation may be accessed remotely:

- if so is provided by the manual or design documentation for the system;
- if the Company’s order introduces a remote mode of work, other than connecting to a workstation which is a part of an automated control system or other technological system;
- in individual cases subject to an approval of the Information Security Division.

7.8. All workstations (including virtual workstations) shall have anti-virus protection tools.

7.9. Access to the AWP BIOS settings, MFP settings, network and switching equipment settings shall be through a password.

7.10. When arranging secure remote access to workstations or information systems using two-factor authentication by using an authentication key and a certificate, it is not permitted to

transfer the authentication key or certificate to third parties, including the User's family members, friends or co-workers.

7.11. Remote connection of contractors to corporate workstations shall be subject to an approval of the Information Security Division.

7.12. At the end of workstation session or if it is necessary to leave the workplace, the User shall lock the computer screen (the personal computer screen is locked by pressing the Win + L key or by pressing the Ctrl + Alt + Del and selecting the "Lock Computer" option).

7.13. When using a workstation, it is prohibited to:

1) use computer equipment with disabled or absent anti-virus protection and security tools built into the operating system (MS Windows Defender);

2) leave the workplace without blocking the computer screen;

3) for purposes other than direct intended use;

4) use workstations to do work which do not meet the information security requirements;

5) permit third parties to use the Employee's workstation, except for Technical Support Employees or Information Security Employees;

6) break seals, open the case of a personal computer, assembly and disassembly a computer independently;

7) use vulnerabilities and undocumented features of the software;

8) change the workstation hardware and software configuration;

9) store personal information unrelated to the job duties on the workstation and network resources;

10) download anything to the workstation from external and network media;

11) access the BIOS or UEFI of a personal computer;

12) use the workstation with local accounts;

13) interfere with the operation of information security tools or bypass them;

14) independently connect peripheral or external devices to the workstation, including:

- printers, scanners and multifunction devices;
- modems and communication adapters;
- mobile phones, tablets or other similar devices;
- personal media;
- dual-use devices hiding built-in functionality;

15) use the workstation with simultaneous connection to the LAN or other network;

16) leave computer equipment (laptop, smartphone, tablet) unattended in public places;

17) connect (wired or wireless connection) personal mobile devices (smartphone, tablet, modem or other external devices) to the workstation, including to charge them;

18) independently deinstall/install Software on the workstation.

7.14. Upon dismissal of the Employee, information on the hard drive of the Employee's personal computer and network resources is subject to transfer to the immediate supervisor of the Employee, whereafter the personal computer and other computer equipment received by the Employee shall be handed over to the division who issues computer equipment.

7.15. Upon acceptance of the dismissed Employee workstation, the information shall be deleted and a new copy of the operating system and application software installed.

7.16. When computer equipment is handed for maintenance or otherwise transferred to third parties (including write-off and disposal), hard drives shall be dismantled.

7.17. The transfer of computers with hard drives or the hard drives for maintenance shall be subject to approval by the Information Security Division.

7.18. When writing off or disposing hard drives or other storage media, the information shall be deleted so that it cannot be recovered.

7.19. Physical access to workstation rooms shall be provided using access control and management tools or other control methods to prevent unauthorized access of unauthorized persons

to such rooms.

7.20. Access to workstation rooms, server rooms, distribution rooms or other rooms hosting information infrastructure parts for representatives of contractors, counterparties or other individuals who are not the Company Employees (including for the purposes of cleaning, maintenance, audit, internship etc.) is provided upon approval of the Information Security Division.

7.21. Access to workstation rooms, server rooms or rooms hosting the switching equipment which process technology information (including information on critical information infrastructure) is provided to third parties only if accompanied by an Employee of the Information Security Division.

8. Rules for using information systems

8.1. In using information systems (automated control systems, information and telecommunications network equipment), users may not:

1) exploit vulnerabilities and undocumented features of software and hardware;

2) use (for any purpose) system errors;

3) commit destructive influences on the software and the data stored in the information systems (automated control systems);

4) without an authorization, change or destroy data stored in the information systems or on external media;

5) without an authorization, install any additional software or hardware components or devices on the workstation;

6) access under someone else's credentials;

7) make backup copies of information on personal media, cloud services, external email services;

8) publish open access information about the architecture and configuration of corporate and process information and telecommunication networks, telecommunication networks used for the interaction of facilities and information transfer, including for the Internet access.

8.2. In using process systems (including automated control systems), the User shall focus on the information security.

8.3. The procedures for using process systems are set out in the manuals or design documentation for such systems.

9. Rules for using the local area network

9.1. To perform job duties, the Employee is provided with access to a LAN from a stationary workstation.

9.2. Remote access to internal corporate web-services and information systems, including by using third-party computers, shall be through a “single window” via a secure communication channel by using terminal access tools or a VPN gateway using the HTTPS protocol and two-factor authentication, including by using certificates issued by the Verification Center.

9.3. These Rules shall apply to the computer equipment (personal computer, laptop, tablet) used for a remote access to information systems, including corporate workstations.

9.4. In the event of remote or local access to the Company's LAN from a workstation of a work/service provider for the Company, such access is only provided subject to an agreement on protection and transfer of information with such contractor and an agreement/terms of contract on compliance of such contractor employees with these Rules, and also if such agreement/contract sets out liability for breach of these Rules. Provided that such contractor’s workstation shall meet the information protection requirements and measures as adopted by the Company.

9.5. In using a LAN without prior approval from the Information Security Division, users may not:

1) connect remotely to a workstation or the LAN, or connect any devices to the LAN;

2) access the LAN from personal devices;

3) have network access to other workstations;

4) connect computer equipment with built-in and external wireless communication devices to the LAN;

5) connect the workstation to wireless networks.

9.6. In using a LAN, users may not:

1) connect to the LAN any computer equipment with disabled or absent protection tools or settings which do not meet the information security requirements;

2) scan and analyze the LAN and network nodes;

3) intercept traffic in the LAN;

4) commit attacks on workstations, LANs, servers, switching and other equipment, including information systems and automated control systems;

5) exploit vulnerabilities in protocols and configurations of network equipment in the LAN;

6) arrange entry points or gateways for external networks;

7) create wireless access points at the site of the Company.

10. Rules for using the Internet

10.1. Access to the Internet resources is provided to Employees to exercise their job duties.

10.2. The Information Security Division keeps updating the list of and blocks access to the prohibited Internet resources.

10.3. When using the Internet, it is prohibited to:

1) bypass the filtering mechanisms of the prohibited Internet resources using specialist Internet services (anonymizers, proxy servers, VPN servers);

2) arrange external networks tunneling;

3) click on banners and advertisements;

4) follow suspicious links;

5) use the resources:

- with obscene content;
- not related to the job duties of the Employees;
- violating the requirements of the current laws;

6) spread information prohibited by the Russian law, including materials of a terrorist, national, racist, sexual, religious, entertainment or other nature or information which offends the honor, dignity or business reputation of legal entities or individuals;

7) ignore workstation system messages and error warnings;

8) without an authorization, post any information on behalf of the Company, including to publish information on social networks, Internet messengers, or forums;

9) use external e-mail addresses for business correspondence;

10) publish on the Internet corporate e-mail addresses and telephone numbers of the Company Employees;

11) acquire, store and distribute information prohibited by law or capable of damaging the image of or causing financial damage to the Company;

12) independently attempt to fix failures when connecting to the Internet as they occur;

13) use the Internet using accounts with the administrator access rights;

14) use the following resources[1]:

[1] For access to be permitted in case of a business emergency, an Employee shall send an access request to the Technical Support team explaining the reason why he/she requests the services, and get the request approved by the Information Security Division.

- gaming and entertainment;
- social networks;
- peer-to-peer networks;
- mail services;
- file sharing services and cloud storage, except for file-sharing services of PJSC “Rosseti” and PJSC “FGC UES” (https://exfile.rosseti.ru/ и https://data.fsk-ees.ru) and the Company;
- forums and conferences (for posting messages);
- communication services (Telegram, WhatsApp, Instagram, Skype (except for the corporate version) or other services), unless the use of such service is required for job duties in accordance with the division’s regulations, job description or other regulations of the Company;
- video telephony services (Zoom, Google Meet, TrueConf, etc.), except for the corporate versions of such software required for the job duties;
- remote workstations outside the LAN beyond the approved design solutions, including by using remote access programs (rAdmin, TeamViewer, etc.);

15) lower the existing level of information protection;

16) save and run files received from the Internet, unless the use of such files is required for the job duties in accordance with the division’s regulations and/or job description.

10.4. It is not permitted to arrange connection to the Internet on workstations and servers of the technological segment.

11. Rules of using e-mail

11.1. Access to corporate e-mail is provided to Employees only for the purposes of their job duties.

11.2. All official correspondence shall only be exchanged by using a personal corporate email address.

11.3. The Employee shall check enclosures in e-mail messages for the presence of executable files (exe, bat, cmd, msi, or others, and if there are any, do not run the executable file and report the receipt of such a letter to the Technical Support at the Service Desk. It is advised to open only such enclosures as have the following format: documents (Word, Excel, PDF, txt, etc.), images (JPG, PNG, etc.).

11.4. It is advised that the sender confirm the sending of a letter.

11.5. When using e-mail, it is prohibited to:

1) send mass or targeted mailings not related to business needs or job duties (spam);

2) send confidential information without the use of cryptographic information protection tools through open (unprotected) data transmission channels, including through public networks and the Internet;

3) use any other e-mail services other than the corporate e-mail, unless otherwise contemplated by the job duties;

4) reduce lower the existing level of message information protection;

5) open emails from unknown senders with unknown enclosures;

6) follow external links in e-mails, if such e-mail is not related to the job duties;

7) register accounts or profiles on third-party Internet resources (including social networks) by indicating the corporate email address.

11.6. After receiving a mass mailing from the Information Security Division, the Employees shall be more vigilant when receiving emails.

11.7. Upon receipt of a suspicious letter, the Employee shall:

1) upon receipt of a letter of dubious content and/or from an unknown user with an enclosure, not open it, or if opened, not open the enclosure or follow the links in the letter;

2) in the event of accidental opening of the letter and suspicious behavior of the workstation, it is not permitted to disconnect the workstation from the power supply;

3) inform the Information Security Division on receiving and opening an enclosure to a suspicious letter;

4) Do the following when confirming that the letter is a SPAM mailing:

– click on the letter with the right mouse button;

– select Junk Mail;

– select Block Sender.

12. Rules for using storage media

12.1. Using external storage media "by default" is permitted on the workstation of a manager holding the position of deputy head of a division or higher, or on the workstations of assistant division head.

12.2. If it is necessary to use an external storage medium to record (copy) information on the workstation, the Employee shall send a request to the Service Desk Support Service and provide an explanation.

12.3. Employees of the Information Security may block the external storage media ports if the User breaches the media use requirements, if there is a threat of spreading malicious software, or in other cases when the confidentiality, integrity or availability of information is at risk.

12.4. If an external storage medium is used to transfer confidential information, such storage medium shall be labelled and all information on the storage medium encrypted. Encryption shall use cryptographic algorithms approved for use in the Russian Federation.

12.5. Storage media with confidential information (including personal data) shall be accounted for and labelled by an authorized Employee of the division which processes such information.

12.6. After achieving the purposes of processing information (including confidential information) on the storage media, all information on such storage media shall be destroyed so that it cannot be recovered.

12.7. Connection of external storage media to the automated control systems, workstations or servers (including the switching equipment) of the technological segment is only permitted for the Users who maintain and support such equipment. Such storage media shall be labelled and accounted for.

12.8. If it is necessary to connect an external storage medium to a workstation or server located in the technological segment and not equipped with any antivirus software, the storage media shall first be tested on a workstation isolated from the technological segment and the Internet and having up-to-date antivirus databases.

12.9. When using storage media, it is prohibited to:

1) without an authorization, connect to and use external storage media both on workstations and servers or other equipment;

2) connect personal storage media to the workstation;

3) use the Company's corporate media for personal use, including for remote work on personal computers.

13. Rules of using Digital Signatures (Authentication Keys)

13.1. The Company uses two types of digital signature:

- encrypted qualified digital signature;
- unqualified digital signature.

13.2. The encrypted qualified digital signature is used for:

- legally important electronic document management;

- acceptance of payment requests in the Company's information systems (Treasury automated control system);
- remote banking services;
- connection to the national information system;
- connection to the government service systems;
- other purposes contemplated by the Russian law and the Company's regulations.

13.3. The unqualified digital signature is used for:

- encryption of information, including emails;
- access to the Company's information systems;
- secure remote access;
- other purposes contemplated by the Company's regulations.

13.4. Digital signature certificates are issued as set out in relevant regulations of the Company.

13.5. When using authentication keys (tokens), it is not permitted to:

1) extract the private key from the container;
2) transfer the authentication key and/or the password to a third party container;
3) use other people's authentication keys;
4) leaving the medium in the workstation at the end of the session using a digital signature, unless continuous presence of the medium is required by the information system and/or the information system manual.

13.6. If an Employee is no longer employed by the Company, the Employee shall return the authentication key to the Information Security Division.

14. Rules for using Online Banking systems

14.1. Access to a workstation with installed Online Banking systems is provided only to the Company Employees authorized by the relevant regulations.

14.2. The workstation with installed Online Banking systems shall be placed in a separate room equipped with physical access control devices.

14.3. It is not permitted to use the Internet on the workstations with installed Online Banking systems, except for the client-bank connection.

14.4. Remote connection to Online Banking systems, including to workstations with installed Online Banking system is not permitted.

14.5. The required information protection tools shall be installed and configured on the workstation in accordance with the terms of banking services.

14.6. If an Employee is dismissed as in section 14.1 hereof, all accounts of such Employee shall be blocked. If the Online Banking system was used with a non-personalized account, such account passwords shall be changed, and the authentication key container password shall be changed and/or the digital signature certificate of such Employee blocked (revoked).

14.7. For private authentication keys only external retrievable storage media shall be used.

14.8. Authentication keys media shall be kept in a place inaccessible to unauthorized persons, such as a metal cabinet or a safe box.

14.9. It is not permitted to use the authentication key medium for any purposes other than using Online Banking, including to store files or electronic documents.

15. Controls

15.1. Compliance with these Rules shall be controlled by the Information Security Division.

15.2. The Information Security Division shall use automated and automatic tools to

control and prevent information leaks from the Users' workstations and the LAN, to control access to information systems (including remote access), and to counteract computer attacks on the Company's information assets.

15.3. To control and counteract any attempts of unauthorized access to confidential information or information systems, including automated control systems and information/telecommunications network equipment, the Employees of the Information Security Division may:

1) involve security officers if the attackers show resistance;

2) block without notice, by sending a mandatory email notice to the Technical Support, the User's access to:

- LAN;
- workstation;
- Internet;
- information/telecommunications network;
- information systems;

3) suspend the authentication key validity;

4) require the User personally (with a notice to the User's immediate supervisor) or through the User's immediate supervisor to provide explanations as to the revealed breach of these Rules;

5) require the User, through the User’s immediate supervisor, to stop using the workstation;

6) require the User to return the storage media and computer equipment provided by the Company;

7) request to hold the User liable for a breach of these Rules;

8) access the information processed on the User's workstation or network resources, including network folders of the Company's divisions, without notifying the User and/or the head of the division who is the owner of the network resource;

9) take away the computer equipment and storage media assigned to such User and owned by the Company.

15.4. To improve information security, Employees of the Information Security Division shall constantly test the operation of information protecting tools designed to identify threats and block unauthorized access to confidential information.

15.5. If any acts are revealed in breach of the information security law of the Russian Federation, Employees of the Information Security Division shall record such breach, notify the law enforcement agencies and assist the law enforcement agencies, including in administrative and criminal cases initiated in respect of such breach.

16. Liability

16.1. The Company Employees are personally liable for the compliance with these Rules.

16.2. Upon request of the Information Security Division sent to the Deputy General Director for Security and Director for Human Resources and Organizational Design - Head of the Department for Human Resources and Organizational Design, an Employee may be subject to disciplinary penalties as prescribed by the Russian law.

16.3. When deciding on whether to hold an Employee disciplinary liable, the gravity and the circumstances of the offence shall be taken into account.

Annex
to the Information Security Rules
of PJSC “Rosseti Lenenergo”

Instruction Sheet
for Critical Information Infrastructure Users

(This Annex is available on the Content page in the Corporate Electronic Document System)