APPROVED BY

Order of CEO AO Severstal Management

No. П-14-0000043 dd. 30.10.2014

Manual

for Users of Corporate Information System

of Severstal Group of Companies

(Revision 3 dd. 16.10.2014)

Moscow, 2014

TABLE OF CONTENTS

Section 1. General

1.1. This Manual establishes obligations, responsibility and authorization of the employees of legal entities, who use CIS in their work, Severstal companies (hereinafter "the Companies") and third parties when working with hardware, software and information resources of the Companies.

1.2. The purpose of this Manual is to inform and streamline the users' work and to improve the information security when processing the information with computer equipment.

1.3. All hardware, software and information resources which are part of the Corporate Information System are the property of the Companies.

1.4. This Manual is approved by the Company CEO.

1.5. For business units which are part of Severstal group of companies, the Manual is brought into force by the order of the head of the respective business unit.

Section 2. Normative references

Regulation on Control of Access to Information Resources

Password Protection Policy

Company's Information Security Policy

List of approved means and methods of information security used when digital documents and communications containing a trade secret of OAO Severstal and its contractors are transferred outside of OAO Severstal corporate network.

Behavior Standard for Severstal Employees

Section 3. Main abbreviations

Authorized abbreviation	Full designation
AS	Automated system
CIS	Corporate Information System of OAO Severstal
CDTN	Corporate Data Transmission Network
ISD	Information Security Department
SW	Software
WS	Work station
CE	Computer equipment
HD	Helpdesk

Section 4. Basic terms

4.1. Automated System (AS) is a system which comprises personnel and a package of means to automate the personnel's activities and implements information technology for performing the specified functions.

4.2. Authentification is an authenticity check procedure (for instance, user authenticity check via requesting a password).

4.3. Corporate Information System (CIS) is a totality of information in electronic form, information technologies and technical means for its processing which are used at business units of Severstal group of companies.

4.4. Corporate Data Transfer Network (CTDN) is a telecommunication network which consolidates all structural subdivisions of the company into unified information environment and ensures simultaneous transmission of data, interaction of applications located in different units and access of users to those applications.

4.5. Mobile computer is a portable computer equipment (laptop, PDA, tablet, smartphone, etc.).

4.6. Company is a legal entity within Severstal group of companies.

4.7. Information Security Department (ISD) is a subdivision of the Company, which is responsible for information security and protection.

4.8. CIS user is an individual who has access to resources of the Company's Corporate Information System through computer technology.

4.9. Work station (WS) is either a stationary or a mobile computer provided by the Company to a user for performance of his/her official duties.

4.10. Helpdesk (HD) is group of IT-subdivision specialists whose duties include receiving and processing user requests to recover IT services and advising on any issues related to the use of the Company's CIS.

4.11. Computer equipment (CE) is a totality of software and hardware elements of data processing system which can perform their functions either on their own or as part of other systems.

4.12. Third party (external client) is an organization which has a status of a legal entity, provides or receives services to/from the Company.

Section 5. Rules of providing IT-services

5.1 When connecting to the CIS, each user is assigned a unique user account. The user gets a unique name *(login)* and an initial password which shall be changed when connecting to the network for the first time; the user is personally responsible for the use of his/her user account and password.

5.2 The requirements to the user's password are established in the Password Protection Policy. CIS user must comply with the password protection requirements when setting, changing and entering the password in accordance with the Password Protection Policy in CIS of OAO Severstal.

5.3 Each user is granted access to some basic services by default. Description of services and rules of their use are available at IT-service catalogue: https://itcatalog.severstal.com. The IT-service catalogue is quickly available via an icon located on the desktop. Access to other IT-services is granted only to the employees who require it for the performance of their job duties. The approval route is determined individually according to the rules of providing IT-services.

5.4 In case it is necessary to install, setup any software, computer equipment, means of communication, or to perform any maintenance and other works, and also for any other technical matters connected with the use of CIS hardware and software, the user shall make a request to Helpdesk (HD) by using the corporate digital IT-service catalogue https://itcatalog.severstal.com

or by contacting the HD using the contact information specified in 5.6. hereof.

5.5 Contact Information

Subdivision	Phone		E-mail
Helpdesk	Volgograd	(713) 41-17 (8442) 63-41-17	help@severstal.com
	Vorkuta	(706) 7-29-29 (82151) 7-29-29	
	Kostomuksha	(708) 3-61-61 (81459) 3-61-61	
	Moscow	(701) 64 -00 (495) 926-77-66	
	Olenegorsk	(709) 53-53 (81552) 5-53-53	
	Oryol	(714) 39-12-00 (4862) 39-12-00	
	Saint Petersburg	(7122) 73-31 (812) 334-73-31	
	Yaroslavl	(710) 35 -00	
	Cherepovets	(702) 53-09-90 (8202) 53-09-90	
ISD	Moscow		ib@severstal.com
	Cherepovets	(8202)533194	gzi@severstal.com

Section 6. Obligations of officers involved in automated data processing

6.1. General obligations of the user

6.1.1. To comply with the established rules of working with information resources of the Company, the rules of behavior standard for Severstal employees, the Russian law, this Manual and other regulatory documents adopted in the Company.

6.1.2. To handle the computer equipment and information resources provided by the Company with care and on a sparely basis.

6.1.3. To undergo an information security training prior to connecting to the CIS with the employees of HR subdivision (subdivision of Shared Service Center) or with the persons responsible for information security and to become familiar with a package of documents as per the Regulation on Control of Access to Information Resources.

6.1.4. To perform mandatory checking of removable media devices with integrated anti-virus protection tools each time when connecting such removable media devices to WS following the instruction available in IT-service catalogue (https://itcatalog.severstal.com) in section “Antivirus Protection”.

6.1.5. To readily follow the instructions of the employees of the subdivisions providing technical support of AS, as well as instructions related to the information security matters from employees of ISD.

6.1.6. To immediately inform the Helpdesk of the occurrence of any of the following:

- any deviations in normal operation of CIS elements which could hamper the use of CE;
- breakdown or unstable performance of PC units or peripheral equipment (CD-ROMs, printers, etc.);
- incorrect operation of protection means installed on the PC;
- discovery of any new, unknown, unapproved or unexpected cable tails or devices connected to the PC;
- loss/theft of CE, including removable media devices.

6.1.7. To immediately inform ISD of:

- any facts and suspicion of unauthorized access to protected information (compromise), including secret keys and passwords;
- known channels of information leaks, ways and means of bypassing or destruction of mechanisms of CIS protection and any attempts to use them;
- discovery of undocumented properties and errors in SW or in the settings of protection means which can result in a crisis situation, computer incidents or failures in the network and IS operation;
- any facts of accidental or intended violation of this Manual requirements by the user or other persons.

6.1.8. To give access to CE at the workplace:

- to ISD personnel - immediately;
- to Helpdesk personnel:
  - in case of emergency - immediately;
  - in other cases - upon a preliminary agreement with the user.

6.1.9. To bring CE in/out of the plant territory in accordance with the requirements of Access Control and Site Security Regulations established in the Company. After lengthy use of a mobile computer outside of CIS (more than 1 week), it is advisable to change the password when connecting to CIS; it is also necessary to check the hard drive for viruses by using anti-virus protection.

6.1.10. To apply only approved encryption means (as per the List of Means and Methods for Protecting the Information Being a Trade Secret), to back up the encrypted information onto the centralized resources for data storage or to an external media device which is stored in a protected place (safe deposit box) at the workplace.

6.1.11. To take the printed documents out of printers immediately. It is not recommended to use full-colour printers for printing black and white images.

6.1.12. To save, if possible, important documents in the network resource on order to enable their recovery in case of CE failures.

6.1.13. In case of dismissal, all tangible storage media, access keys, licenses for SW shall be

submitted to IT responsible person or to a direct manager. At that, any proprietary information may be destroyed upon the manager's consent only.

6.1.14. In case of dismissal or change of job duties not related to the use of CE, the provided CE shall be handed over to an inventory custodian or to a responsible IT employee.

6.1.15. If it is necessary to work with confidential information (trade secret, personal data), it is necessary to contact HR personnel or the employees who are responsible for information security in order to review and sign the documents required.

6.2 It is prohibited for the users to:

6.1.16. Connect and disconnect the work station to/from CDTN of the Company in breach of the established rules.

6.1.17. Use - within the perimeter of the Company - external (including public) channels for Internet access on corporate CE, including connection to mobile and external wireless data transfer networks.

6.1.18. Connect personal computer to CDTN, except for guest resources.

6.1.19. Connect work station to guest resources.

6.1.20. Disclose own data for authentication (logins, passwords, secret keys) to any third parties.

6.1.21. Use CE and provided resources for the purposes not related to the performance of job duties.

6.1.22. Create any additional channels to exchange information with internal or external recipients by using software or hardware, or non-corporate external resources. If it is necessary to continuously use the files by several users at the same time or exchange large size files, a corresponding justified request for allocation of shared resource at the file server (refer to p. 5.5) shall be made to Helpdesk.

6.1.23. Organize wireless access points within CIS perimeter without authorization.

6.1.24. Bulk-mail messages containing the information not related to the performance of job duties to both to CIS addressees and outside.

6.1.25. Make unauthorized changes in configuration of the WS software and hardware, including installation of SW and updates; open computer cases; perform CE repair either on their own or involving employees of the company other than personnel of IT subdivisions.

6.1.26. Use inbuilt means of operating systems and any other software for network scanning, unauthorized access and performance of any similar activities.

6.1.27. To dislocate the provided CE (exchange monitors, keyboards and other equipment).

6.1.28. Use data cryptographic protection without the approval of ISD.

6.1.29. Create shared resources on work stations without authorization.

6.1.30. Leave work station unattended when switched-on without activating temporary blocking function.

6.1.31. Use undocumented properties and errors in SW or in protection settings which can result in a crisis situation, computer incidents or failures in the network and IS

performance.

6.1.32. Give unauthorized access to third parties to the computers and the resources of the organization, registration data in information systems, secret codes and information, which disclose the structural elements of information systems.

6.1.33. Distribute reference information, which becomes accessible while connecting to CIS outside of the company, without authorization.

6.1.34. Use any unlicensed and prohibited SW.

6.1.35. Create virtual machines, several boot copies of operating systems, boot work station from external media devices without authorization.

6.1.36. Disconnect the corporate admin tools and protection means installed at the work station.

6.1.37. Start executable files received from unreliable sources without Helpdesk approval and not checked with anti-virus protection.

6.1.38. Collect any confidential information that the employee does not have access to.

6.1.39. Modify, steal and destroy any components of CIS.

6.1.40. Login and work in CIS under someone else's login and password or someone else's access identifier.

6.1.41. Transfer or publish in the Internet indecent, defamatory, threatening or other unlawful information, distribute materials which facilitate the incitement of national dissension, incite to violence, make a call to commit illegal actions, including information explaining application procedure of explosives and other weapons, distribute viruses and other computer codes, files or software designed for malfunction, destruction or restriction of functionality of any computer or telecommunication equipment or software for unauthorized access, as well as serial numbers for commercial software products and programs for their generation, logins, passwords and other means of acquisition of unauthorized access to commercial resources in the Internet, and also putting online links to aforementioned information.

6.1.42. Distribute copyright materials involving any patent, trade mark, trade secret or other property rights and/or author's rights and rights of a third party related thereto.

6.1.43. When using e-mail, it is prohibited for the user to:

- Use the corporate e-mail address for subscription at websites which subjects are not related to the performance of job duties.
- Use non-corporate e-mail for business correspondence, including web-interfaces of public mail services: yandex.ru, mail.ru, hotmail.com and other mail systems.

6.1.44. While working in the Internet, it is prohibited for the user to:

- Download from the Internet any files that are not related to job activity, including audio- and video files, and to use audio- and video streams (online-audio services, radio, online video, television).
- Use unauthorized services for instant messaging (for example, Mail.ru agent, IRC, ICQ, Yahoo messenger, AOL Instant Messenger, etc.), use social networks and forums

for business correspondence without permission.

- Use software and hardware (including anonymous proxy-servers, etc.) which allow to get access to a resource prohibited for use by the Company's IS policy, and also to bypass the restrictions for the use of resources.
- Publish without necessity own e-mail address or addresses of other employees of the company at public Internet resources (forums, conferences, etc.), where the information is not necessary.
- Accept pop-up banners and web-browser suggestions on checking for (discovery of) viruses, vulnerability, on installation of software, etc.
- Use the provided Internet access for unauthorized advertising of the Company's activity, goods and services which are not related to business of the Company and other organizations.

Section 7. Remote access to the CIS resources

This service is provided only to the employees who require remote working with the CIS resources.

7.1. Obligations of the user:

7.1.1. Choose places of remote work respecting physical protection of CE, including physical safety of the building and nearby environment.

7.1.2. Log out remote sessions upon completion of remote work.

7.1.3. Update antivirus bases and operating system at the terminals used for remote access on a regular basis, if possible at least once a day.

7.2. In case of remote access, it is prohibited to:

7.2.1. Provide unauthorized access to the information or CIS resources to anyone, including family and friends.

7.2.2. Leave the remote access means unattended in an unsafe place.

7.2.3. Use unauthorized means of remote access to the CIS resources and services.

Section 8. Authorization and responsibility of officers

8.1 In order to ensure stable and safe operation of information systems of the Company, the specialists of ISD and IT-subdivisions personnel may perform regular checking of the users' activity and their compliance with the provisions of this Manual.

8.2 In case a user breaches any requirements of this Manual, that resulted in threat to corporate interests, the specialists of ISD and the personnel of IT-subdivisions have the right to disconnect the user's work station from all the services of the corporate network of the Company and (or) block his/her account until the threat is eliminated.

8.3 Incidents connected to violation of established rules for working in the AS are subject to internal investigation. Based on the investigation findings, disciplinary, administrative, criminal responsibility may be imposed on the users in accordance with the current legislation of the Russian Federation.

Section 9. Control over compliance with the Manual

9.1 Control over compliance with this Manual in structural subdivisions of the Companies is the responsibility of heads of these structural subdivisions.

9.2 Control over compliance with this Manual by any contractor employees is the responsibility of heads of this contractor and the head of the structural subdivision who concluded the contract with this contractor.

9.3 General over compliance with this Manual is the responsibility of the Business Support subdivision in the Companies.

9.4 This Manual is communicated with written acknowledgment to all users registered in the corporate information computing system.

Section 10. Manual revision procedure

10.1 This Manual shall be revised at least every 5 years.

10.2 ISD and CS of IT are responsible for the manual updating.

10.3 In accordance with the Quality Management System requirements, the following standard procedures are applied when working with the document:

- revision of the document can be initiated by any officer of the Company who is interested in the improvement of work organization;
- any changes in the document throughout its validity period shall be approved by the officer who is generally responsible for the document updating;
- the validity period of the Manual can be extended upon its expiry on the basis of a positive decision of the officer who is responsible for the document updating;
- the Manual shall be revised upon expiry of its validity period similar to the amendment procedure throughout its validity period;
- the document is subject to mandatory updating in case of any changes in management document related to this business procedure.