This Regulation has been
APPROVED
by order of CEO
AO Severstal Management
No. P-OD-700-00-23-37 dd. 23.10.2023

Regulation
on Control of Access to Information Resources of Severstal Group of Companies

Moscow,
2023

TABLE OF CONTENTS

INFORMATION ON THE DOCUMENT

Document name	*Regulation on Control of Access to Information Resources of AO Severstal Management*
Document number	
Revision	*3*
Approved by	*Order of CEO AO Severstal Management No. P-OD-700-00-23-37 dd. 23.10.2023*
Effective as of	*October 23, 2023*
Revision date	*October 30, 2025*

1. PURPOSE OF THE DOCUMENT

1.1 This Regulation establishes uniform procedure of control of access to information resources in Corporate Information System (CIS).

1.2 The purpose of this Regulation is streamlining of granting and changing the access to information resources in CIS.

1.3 The requirements of this document are applicable to employees of legal entities within Severstal group of companies (hereinafter the Companies) and external parties who use CIS when dealing with information resources of the Companies.

2. NORMATIVE REFERENCES

Information Protection Policy of the Company
Information Security Standard of Severstal Group of Companies

3. MAIN ABBREVIATIONS

Authorized abbreviation	Full designation
CIS	Corporate Information System
PDN	Process Data Network
CDTN	Corporate Data Transmission Network
IS	Information service
IR	Information resource
ISD	Information Security Department
UST	User Support Team
TS	Trade secret
PD	Personal data
PKI	public key infrastructure

4. BASIC TERMS

Authentication	A procedure to verify authenticity, e.g., user authentication by comparing the password entered by such user against the password stored in a user account database.
Information resource owner	A company employee who is authorized to determine development, advisability of using an information resource and rules for accessing such resource. Only a single owner is assigned to each resource.
Group account	An impersonal account for logging on to a computer by several employees of a company in case it is impossible to organize work using personal user accounts. For example, working in applications that do not allow multi-user authentication or on computers in personnel training classrooms.
Domain (Active Directory)	A hierarchical directory service that stores information about objects (user accounts, passwords, computers, printers, shared resources, etc.) and allows users of the same network to access this information.
Information	Information (messages, data) regardless of the form of their presentation.
Information subject to protection (protected information)	Information constituting a trade secret as defined by the List of Information Constituting a Trade Secret of the Company, personal data as defined by the List of Personal Data Processed in the Company, other legally protected information and restricted access information.
Information resource (IR)	A domain-specific scope of information which may contain documents, directories, databases accessed via the information service.
Information service (IS)	Hardware and software suite which grants access and maintains the user interaction with different information.
Changing of access rights to IR	Increasing or decreasing privilege level for use of the information resource.
Corporate information system (CIS)	A set of information in electronic form, all information technologies and technical means ensuring its processing used at Severstal group of companies.
Corporate data transfer network (CDTN)	A telecommunication network that consolidates all structural divisions of the company into a single information environment and ensures simultaneous data transfer, interaction of applications located in different nodes and access to them by users.
Authentication means	Password, pin code or other code to authenticate the user account.

Process data network (PDN)	A telecommunication network that consolidates the elements of APCS into a single information environment and ensures simultaneous data transfer, interaction of applications located in different nodes and access to them by users.
Corporate IT Department	Employees of IT Department, whose duties include processing of user requests to restore IT services and providing advice on issues related to the use of the Company's CIS; provision of IT services.
Corporate user	An individual who has access to the resources of the Company's corporate information system through computer technology and a valid employment contract with a legal entity within Severstal group of companies.
Corporate device	A workstation or other device to which CIS policies and settings shall apply.
Mobile computer	A portable computing device (laptop, tablet, industrial mobile terminal, etc.)
Incompatible privileges	Privilege level for use of the information resource which exceeds the basic duties of the Company employee or results in conflicting privileges.
Critical privileges	Privileges which grant access to strictly confidential trade secrets, special and biometric personal data, as well as privileges and accesses in information systems, which use/application may cause damage to the Company.
Company	A legal entity within Severstal group of companies.
Person in charge	An employee of the Company having a corporate E-mail address who belongs at least to one of the following categories: - line manager of the user; - approving manager of the user and/or his deputy assigned in the access approval system; - person on the part of the Company who is in charge of arranging connection to information resources for contractor employees; - dispatcher of the shop; - person on the part of the Company who is in charge of group account.
Regulation	Regulation on Control of Access to Information Resources of AO Severstal Management.
User	An individual who has access to the resources of the company's corporate information system through computer technology
Work station (WS)	A desktop or mobile computer provided by the Company to the user for performance of his/her business duties

Employee of IS function	A Company employee whose duties include organization of information security management system and ensuring its performance
Phone number for SMS informing –	A user mobile phone number which is used for notifications of events taking place with his/her account (expiry of password validity period, changing of password, etc.), registered in "SAP Personal account" and/or on the corporate portal in "My contacts" service by the user or by a responsible person, subject to the appropriate application has been signed by the user.

5. GENERAL

5.1 Access control means a process of granting the users with a set of minimum required privileges based on their functional duties in order to limit the use of IR by users who do not have the right thereto.

5.2 Access to the IR is provided on the basis of the information specified in the requisition and recorded in the relevant accounting system, subject to approval by the persons in charge.

5.3 The information resource owner, together with an Information Security Department employee and the corporate IT department, determines the approval route for IR requisitions and whether the requisition requires approval by any Company employees. The approval route is displayed in the requisition. The approval route can be revised based on the requisition in the accounting system.

5.4 The IR owner determines the category of information subject to protection (protected information) that is acceptable for processing using this IR. This information is recorded in the corresponding accounting system.

5.5 The IR owner may assign his/her deputy and delegate his authority to him/her in the appropriate registration system. For periods of lengthy absence of the IR owner (e.g., vacation), a deputy must be assigned on a mandatory basis .

5.6 The requisition shall be made for each user of the IR and for any change in access rights.

5.7 Set of services to be connected and access level depends on the attribute assigned to the connected company (contractor). The corporate IT department employees prepare and keep updated the contractor directory which was established for this purpose; in cooperation with the Legal function employees, the corporate IT department assigns the "corporate/external" attribute to the connected company.

6. PROCEDURE OF GRANTING, CHANGING AND TERMIANTION OF ACCESS TO IR

6.1 In order to grant access to IR for the users, a requisition in the form individually developed for each information service or resource shall be made.

Requisitions for access to information resources are placed in electronic form in the appropriate registration system.

6.2 If the route of requisition approvals includes the "Manager" position, then the approving manager of the applicant defines whether the requested access rights to the IR can be provided based on the duties of the user, and whether the potential risks of incompatible privileges are absent or can be accepted. In case of a positive decision, he/she approves the requisition.

6.3 The IR owner defines whether the requested access rights to the IR can be provided based on the requirement of the Company's Information Security Policy to minimize the privileges and checks compliance of the requested access to business objectives. In case of a positive decision, he/she approves the requisition.

6.4 If the request approval route includes the "IS" position, then the IS function employee shall perform the following checks of the data specified in the requisition within 2 working days after receiving the request:

- availability of access to the requested information;
- signed confidentiality agreement;
- no risks of incompatible privileges;
- no conflicts with internal regulations;
- availability of any other information that prevents using the IR by the applicant;

If, during the checks, any additional information is required from the applicant, the time period for checking the information specified in the request shall be extended in proportion to the time of response from the applicant. If no response follows within 7 working days, the requisition shall be denied.

6.5 In case of detecting any non-conformities with the conditions specified in pp. 6.2 - 6.4, hereof, the requisition shall be denied and supported with a comment on the non-conformity detected.

6.6 Employees of the Corporate IT Department shall take the necessary technical actions within the time period set out in the appropriate regulations for execution of requests.

Requisitions which did not pass the defined approval procedure cannot be accepted for execution.

6.7 Access rights can be changed in case the basic duties of the employee are expanded or restricted; changing access rights shall performed in accordance with the procedure specified in pp. 6.1 – 6.6 hereof.

6.8 Access to the IR can be terminated upon the request of an immediate manager of the user, owner/manager of the system or an employee of IS function. In this case, a corporate IT Department employee shall block the access and record the blocking event in information systems.

6.9 Upon receiving an employee's application for dismissal, the employer has the right to terminate/suspend access to certain information resources and critical privileges.

7. PROCEDURE OF CHECKING ACCESS RIGHTS TO IR

7.1 The IR owner shall perform regular checks (at least once a year) of the valid privileges of the users by comparing the existing privileges in the IR against those specified in the requisition for access. User privileges shall be checked by using the specialized software; one of the functions of such SW is to notify the IR owner of the need to perform the check. The IR owner shall respond to such notifications and close the activities within the specified time period.

7.2 An employee of IS function shall monitor compliance of the current configuration of the IR access control subsystem with the approved requisitions for granting/changing/termination of access to the IR.

7.3 An employee of IS function shall regularly check the correctness of granted access rights.

7.4 In case of any discrepancies between the valid privileges of users and the information specified in the approved requisitions, an employee of IS function shall investigate such case in accordance with the current regulatory documents on management of information security incidents.

8. LIFE CYCLE OF THE USER ACCOUNT

8.1 Depending on the IS used by the user and the authentication method used therein (local account, CDTN account, PDN account), corresponding accounts may be created for the user.

8.2 Before creating any account, the user shall be familiar with the regulations in the field of IT and information security. The fact of acknowledgment shall be recorded:

- in paper form in the acknowledgment /responsibility registration sheet (Appendix No. 1), a copy of which is attached to the requisition;
- electronically in a separate form of the specialized information system.

The original of the acknowledgment sheet shall be kept:

- in HR department of the company if the user is a company employee;
- with the applicant if the user is an external person.

8.3 The user account shall have the uniqueness features, enabling unambiguous identification of the person who uses it during the period of his/her employment and not repeat the properties of the archived accounts. The user account name is created using the Latin alphabet. Cyrillic alphabet shall be transliterated into Latin alphabet following recommendations in Section IV Part 1 of ICAO International Standard Doc 9303.

8.4 In order to work with the IS, where authentication uses the accounts of CTDN domain, a unique personal account shall be created for the user in the corresponding CTDN domain. An account shall be created for a company employee who has an employment contract or a civil law contract (CLC) after the HR department person has entered an event code in the SAP HCM system, or based on the request of the HR department which personnel records are kept in other systems.

An account for a company employee who has a civil law contract shall have limitations on the period of use, which is specified in SAP HCM.

8.5 In order to work with the IS, where authentication uses the accounts of PDN domain, a unique personal account shall be created for the user in the corresponding PDN domain.

8.6 In order to work with the IS, where authentication is possible with a local account only, an additional account at the IS level can be created for the user.

8.7 An account for an external user can be created based on the requisition from any user. The requisition shall be supported with scanned copies of the documents listed in Appendix 2. The requisition shall be agreed with the person responsible for the process under which the account is created and with the employee of IS function. When creating such an account, a limit on its validity period shall be established and duration of that period may be defined by the applicant. The validity period limitation for this category of account shall match the validity of the contract under which such account is created or shall be a period of one year, whichever comes first. In case extension of the account validity period is required, an appropriate requisition shall be

registered.

8.8 The user's account in CIS shall be blocked within 1 calendar day, on which either of the following events occur:

a. expiry of validity period of the account;
b. employee dismissal without subsequent hiring within Severstal Group;
c. transfer of a company employee to light labor, maternity leave and childcare leave;
d. suspension of employment contracts with employees who were called up for military service upon mobilization to the Armed Forces of the Russian Federation;
e. transfer of an employee to another legal entity within Severstal Group; f. suspension from work (prevention from work) for reasons stipulated by the law;
g. upon demand of the IS function employee.

8.9 If an employee is transferred to another department, the employee's current immediate supervisor shall make the decision to retain or revoke the existing privileges of the employee's account.

8.10 If it is necessary to retain the account privileges upon occurrence of the events specified in p. 8.8 (except for subparagraphs "d" , "e", "f" and "g"), the person in charge shall create an appropriate request for retaining the account privileges level, which approval shall follow the route established in accordance with p. 5.3 hereof.

8.11 In case of occurrence of the event specified in subparagraph "e" of p. 8.8, privileges of the blocked account may be reassigned to the employee's account created at the new place of work. The reassigned access privileges shall be confirmed by participants of the IR access approval routes within 14 calendar days, after which unconfirmed privileges shall be automatically revoked.

8.12 In case of mass transfers of employees to another legal entity within Severstal group with retention of their functional responsibilities (the HR department has entered the relevant event code in the accounting system or created a request for mass transfer), the employee's account shall not be blocked and the existing access privileges shall not be revoked.

8.13 In case of occurrence of the events specified in subparagraphs "f" and "g" of p.8.8, the blocked account can be unblocked only if the conditions of the blocking occurrence are removed.

8.14 The account may be blocked at the motivated request of the immediate manager. In this case, an employee of the corporate IT department shall block the account and record this event in information systems.

8.15 The account of a company employee may be blocked automatically after 14 calendar days from the moment of its creation if the employee fails to pass the obligatory e-learning course "Initial Briefing on IS" on the portal "My Training and Development".

8.16 Group account cannot be used for protected information IR that support additional personal identification of users. In special cases (e.g., to maintain continuity of the production process) using a group account by several employees is allowed.

8.17 Each group account shall have an owner assigned by the subdivision manager of that employee. Any changes related to such account shall be agreed with the account owner.

8.18 If a group account is used, the Corporate IT department shall ensure:

- records of group account owners and their regular (at least once every 6 months) inventory;
- availability of information in the accounting system on personal accounts of all employees claimed to use a particular group account;
- initiating the group account password change procedure in case of occurrence of the events specified in p. 8.8with respect to the group account owner;
- records of the group account and the equipment/IR it will be used on.

8.19 The group account owner shall check the list of group account users on a regular basis (at least once a year). The user list shall be checked by using the specialized software; one of the functions of such SW is to notify the group account owner of the need to perform the check. The group account owner shall respond to such notifications and close the activities within the specified time period.

8.20 The user account shall be blocked if it is not used during 180 days.

8.21 The blocked user account shall be deleted after 14 calendar days upon the user termination/dismissal or upon expiry of his/her employment contract.

8.22 The corporate IT department shall keep the information on the deleted account including access details to the corporate domain (unique identifiers, including date and time of deletion) during 3 years.

9. ORGANIZATION OF PASSWORD MANAGEMENT

9.1 Requirements to authentication tools are established in the Password Protection Policy of Severstal Group of Companies, which is approved and put into effect by the order of the Company's CEO.

9.2 The account password can be changed:

– personally by the user-owner;
– in case of forced change - upon request from the IS function employee.

9.3 Primary password can be communicated to the user in the following ways:

- by SMS to the phone number specified for SMS informing;
- to the corporate e-mail address;
- in a sealed envelope.

9.4 Transfer method of the user primary password is determined by the following algorithm:

a) send SMS to the phone number specified for SMS informing;

b) if SMS cannot be sent (the phone number was not specified or it is not valid, or SMS message has not been delivered to the addressee), then the password is sent to the corporate e-mail address of the user;

c) if the user does not have a corporate e-mail address or the user is unable to access it, the password is sent to the corporate e-mail address of the responsible person specified in the requisition.

d) password for the group account is sent to the corporate e-mail address of the responsible person specified in the requisition.

e) if technical communication channels cannot be used, the password is transmitted directly to the user on paper in a sealed envelope.

9.5 Passwords and other user account authentication codes must not be stored in the open without security measures taken (password storage software (KeePass) in electronic form accepted for use at Severstal; lockable metal cabinets or safes for storing passwords on paper in sealed envelopes).

10. ORGANIZATION OF REMOTE ACCESS

10.1 Remote access to CIS is granted to employees on the basis of a request registered in the respective accounting system, subject to approval by the persons in charge.

10.2 Remote access to CIS is arranged by using multi-factor authentication means (PKI certificate, application code, Push-notifications, OTP, SMS). For the Company's employees, whose categories are listed in Appendix 3, access can be provided by using a PKI certificate only; PKI certificate is recorded on a physical medium in a secure version.

10.3 Remote access cannot be provided for employees of special subdivisions, as well as for HR-employees who keep military records.

10.4 Organization of any IT services using remote access technologies in CIS is performed by the Corporate IT Department.

10.5 The software required for remote access to CIS shall be installed and configured on the corporate equipment by the specialists of the Corporate IT Department.

10.6 The type of remote connection to CIS shall be selected in accordance with Appendix 4.

10.7 Each remote access session shall be re-authenticated.

10.8 For information resources and information systems to which remote access is provided, an event audit log shall be enabled. The logs shall include the start time and end time of remote access session, network source address, network destination address, connection type, user ID and device ID from which the connection was made.

10.9 All remote connections shall be restricted by network access control and checked by information security measures.

11. RESPONSIBILITY

11.1 The person in charge shall be responsible for:

- compliance with the procedure for granting, changing, terminating access;
- confidentiality of the user password communicated through him/her;
- user identification at the time of communication of his password.

11.2 The user shall be responsible for:

- confidentiality of his/her passwords;

- timely updating of his/her contact information used for obtaining or recovery of the password;
- changing of the primary password to the account;
- completeness and accuracy of the information provided in the requisition.

11.3 The employee of Corporate IT Department is responsible for maintaining confidentiality of the data created for initial identification of the user in the system.

11.4 The employee of IS function is responsible for timely processing of incoming incidents as per the rules established in the Company for management of information security incidents.

11.5 The information resource owner is responsible for making decisions on creation and liquidation of the resource, determining the rules of user access to the resource respecting the principle of minimum required privileges and acceptable risks.

11.6 The group account owner is responsible for timely informing the Corporate IT Department of any changes in the list of employees using the corresponding group account.

11.7 When the user's immediate manager approves the access, he/she shall make sure that the set of IR access privileges requested in the request matches the functional duties of the user taking into account the principle of minimum required privileges and acceptable risks.

12. FINAL PROVISIONS

12.1 The time and procedure for entry of this Regulation into force shall be defined by the order on its approval. This Regulation is valid indefinitely.

12.2 If, as a result of any changes in the law, any provision of this Regulation contravenes the law currently in force, such provisions shall become invalid.

12.3 Alterations and amendments to this Regulation shall be made by the order of the Company CEO.

_____

_____

(company/department name)

_____

_____

(area name)

Acknowledgment / Responsibility Registration Sheet

_____

(full name, title)

_____

Item No.	Document name	Personal signature[1]	Date
1	AO Severstal Management Policy in Information Security.		
2	AO Severstal Management Policy in Personal Data Processing.		
3	Password Protection Policy of Severstal Group of Companies.		
4	Instruction for Users of Corporate Information System of Severstal Group of Companies.		
5	Regulation on Control of Access to Information Resources of AO Severstal Management		

Herewith I give my consent to send informational SMS messages to my phone number

_____

_____

phone number

_____

(user signature)

Employee's personal signature is WITNESSED by me

_____

_____ _____

(Full name and phone number of subdivision manager) (signature, stamp for external organizations)

1 Herewith I confirm with my handwritten signature that I have read all the documents listed above and that I understand their contents.

Appendix 2

List of documents to be provided

Group of users	Documents to be provided
External user (not employed with the Company)	1. Acknowledgment / responsibility registration sheet 2. Grounds for creation of the account (reference to contract/resolution/instruction, etc.). 3. Non-Disclosure Agreement (NDA) between an external individual or legal entity and the Company in the case of access to the IR containing information that constitutes a trade secret of the Company

Appendix 3

List of categories of employees for whom the use of PKI certificate on a hardware key (token) as a second factor of authentication is mandatory

1. Top-12 and Top-100 managers.
2. CEO, functional directors, heads of departments.
3. Secretaries and (or) assistant managers specified in pp. 1 and 2.
4. Employees of the following business units: OOO Severstal Shared Services Center, AO Severstal Infocom, OOO Severstal Digital, OOO Severstal SCIF, OOO Deletron.
5. Employees of the following departments: Business Security Department, Risk Management and Internal Control Department, Internal Audit Department, finance function.
6. Employees and contractors involved in setting up and maintaining information systems and equipment at critical information infrastructure facilities.
7. Employees involved in maintenance of the APCS infrastructure (networks, controllers, servers, workstations).
8. Employees having access to strictly confidential information, biometric and special categories of personal data.
9. Employees working with bank-client systems.
10. External contractors developing and maintaining information services and systems.

Appendix 4

Types of Remote Access

Type of remote access	Resources for access	Device type	User type
Access to IT resources from the Internet from corporate laptops or PCs (VPN-Corp)	Resources declared as general corporate resources	Corporate	Corporate
VPN-Util-<code_project>	Access to a single resource (list of resources)	Corporate and non-corporate	Corporate, non-corporate
VPN-Adm-<code_project (process)>	Resources declared as general corporate resources and additional claimed resources	Corporate	Corporate
Access to IT resources from the Internet (to terminal RDSFarm-Corpusers)	Resources declared as general corporate resources	Corporate and non-corporate	Corporate
Access to IT resources from the Internet for non-corporate users (RDSFarm-ExtUsers)	Limited list of corporate resources	Non-corporate	Non-corporate
Access to IT resources from the Internet for access to SAP external developers (stal-rds-dev)	Limited list of corporate resources	Corporate and non-corporate	Corporate, non-corporate
Remote access to IT resources from the Internet from non-corporate laptops/PCs to PC (RDP to workstation (GW))	Access to a single resource (list of resources)	Corporate, non-corporate,	Corporate
Remote access to IT resources from the Internet via RDP to windows server via Remote Desktop Gateway (RDGW)	Specialized resources	Corporate, non-corporate	Corporate, non-corporate
Remote access to IT resources from	Specialized resources	Corporate and non-corporate	Corporate, non-corporate

monitoring gateway (PAM)			
Remote access to IT resources from virtual workplace (VDI)	Resources declared as general corporate resources, specialized resources	Corporate and non-corporate	Corporate, non-corporate