Appendix to the Order
of General Director

No. P-OD-700-00-22-18 dd. April 12, 2022

PASSWORD PROTECTION POLICY
of SEVERSTAL Group of Companies

Password Protection Policy of Severstal group of companies covers all information systems and services owned or used by AO Severstal Management, its managed companies and their subsidiaries, as well as other companies within Severstal group (hereinafter collectively referred to as the Companies). The Policy also applies to individuals and/or legal entities that use the above information systems and services as part of their contractual relationship with the Companies.

Goal of the Policy

To prevent unauthorized access to information assets and their processing means owned or used by the Companies.

Main tasks

- To ensure necessary and sufficient organizational and technical measures for the use of passwords, pin codes and other user authentication codes.
- To ensure implementation of quality requirements for passwords, pin codes and other user authentication codes in all information assets and their processing means owned or used by the Companies.
- To ensure using multi-factor authentication in all information assets and their processing means that support such technology.
- To ensure user's responsibility for compliance with the requirements to unauthorized access protection regarding the information protected by the Companies.

Main guidelines

- Password, pin code and any other user authentication code are means of authentication and refer to protected information; users have no right to disclose them to anyone or create conditions that would facilitate their disclosure.
- For all information assets and their processing means owned or used by the Companies, authentication means that meet the quality requirements specified in the Appendix shall be used.
- For all information assets and their processing means owned or used by the Companies, use of multi-factor authentication technology shall be considered in the first place.
- Generation, use, change and termination of authentication mean for each information system shall be structurized and specified by the IT department during the system commissioning.

Guarantee of compliance with the guidelines

- Each employee is personally responsible for implementation of this Policy, and may be subject to disciplinary action for any violation of the requirements in accordance with the effective laws.
- Severstal Group management ensures continuous monitoring of compliance with the requirements of this Policy.
- Control over the actions of users and personnel who is responsible for the system maintenance when working with the authentication means is the responsibility of

user’s managers, IT specialists in charge of the support of information system and services, as well as employees of the Information Security Department.

Requirements to Authentication Mean Quality

General requirements

- Password shall be stored in information systems as a hash sum resulting from transformation using a cryptographic hash function with an input modifier. Password must not be stored as a plain text.
- Password must not be displayed when typing. Using the functionality that allows for temporarily displaying of the entered characters is allowed.
- Manufacturer's default passwords must be changed in all information systems.
- When the user logs in for the first time using the assigned initial (temporary) password, the system must require changing this password.
- When generating passwords, the following must not be used as a password or part of it:
    - passwords similar to those established for personal accounts of publicly available e-mail services, social networks and other non-corporate services;
    - easily computable combinations of symbols (first names, surnames, names of information systems, pet names, phone numbers, birth dates, etc.);
    - lexicalized words, including Russian words in English layout as transliteration (OCTOBER2020, JRNZ<HM@)@), etc.)
    - common abbreviations (PC, LAN, USER, etc.);
    - repetitive characters and characters located next to each other in the alphabet or on the keyboard (111111, qwer4321, Aq1Sw2De3, etc.).
- Special software and systems can be used to generate strong passwords. At that, no on-line services shall be used to generate, check the complexity and availability of compromised passwords in databases.

Requirements to user account passwords

Requirement	Value
Minimum password length	12 characters
Password complexity	Password must contain characters at least from **three** different categories listed below: • Upper case letters • Lower case letters • Numbers • "Special" characters ~!#$%^&*()_+=<>'?
Maximum password validity period	120 days
Minimum password validity period	1 day
Password unrepeatability	Password history length=12
Account lockout conditions	Lockout for 10 minutes, with 10 incorrect password entries in the last 10 minutes
Password generation	Password shall be generated by the user on his/her own or generated in a completely random order using specialized password autogenerators available via the IT catalog.

Requirements to user account passwords for privileged authorized users (including IT Department, Information Security Department, information system administrators, employees authorized to make changes in operation of information systems and equipment)

Requirement	Value
Minimum password length	15 characters
Password complexity	Password must contain characters from **each** category listed below: • Upper case letters • Lower case letters • Numbers • "Special" characters ~!#$%^&*()_+=<>'?
Maximum password validity period	120 days
Minimum password validity period	1 day
Password unrepeatability	Password history length=12
Account lockout conditions	Lockout for 10 minutes, with 10 incorrect password entries in the last 10 minutes
Password generation	Password shall be generated in a completely random order using specialized password autogenerators available via the IT catalog.

Requirements to password for printers, scanners, plotters, MFPs and other printing and copying equipment

Requirement	Value
Minimum password length	8 characters*
Password complexity	Password must contain characters at least from **one** category listed below: • Numbers • Upper case letters • Lower case letters
Maximum password validity period	Not limited. Password shall be changed in case of changing contractors who having access to the password.
Account lockout conditions	not specified.
Additional requirements	Password shall be generated in a completely random order using specialized password autogenerators available via the IT catalog.

*Number of characters depends on the technical restrictions.

Requirements to password for service accounts (including accounts for managed equipment: UPS, video cameras, media players, etc.)

Requirement	Value
Minimum password length	20 characters
Password complexity	Password must contain characters from **each** category listed below: • Upper case letters • Lower case letters • Numbers • "Special" characters ~!#$%^&*()_+=<>'?
Maximum password validity period	Not limited. Password shall be changed in case of termination of employees who have access to the password.
Password unrepeatability	Password history length=12
Account lockout conditions	Lockout for 10 minutes, with 10 incorrect password entries in the last 10 minutes
Additional requirements	Password shall be generated in a completely random order using specialized password autogenerators available via the IT catalog.

Requirements for one-time passwords used as a second factor of authentication

Requirement	Value
Minimum password length	6 characters*
Password complexity	Password must contain characters from **one** of the categories listed below: • Numbers
Maximum password validity period	|Not more than 5 minutes
Account lockout conditions	Lockout for 10 minutes, with 10 consecutive incorrect password entries. Time interval does not matter. Upon approval of the Information Security Department, other types of protection against brute force may be used.
Additional requirements	Each password can be used only once.
Additional requirements	Password shall generated in a completely random order using specialized cryptographically strong pseudo-random number generators.

*Number of characters depends on the technical restrictions.

Requirements to pin codes used to unlock mobile devices and mobile applications

Requirement	Value
Minimum code length	4 characters*
Code complexity	Code must contain characters from **one** of the categories listed below: • Numbers
Maximum validity period of pin code	Not specified.

Account lockout conditions	Lockout for 10 minutes, with 10 consecutive incorrect pin code entries. Time interval does not matter. Upon approval of the Information Security Department, other types of protection against brute force may be used.

*Number of characters depends on the technical restrictions.