Appendix No.1
to Order of CEO
AO Severstal Management
No. ОРД/СМ/П-15-0000224 dated 24.06.2015

POLICY OF AO SEVERSTAL MANAGEMENT IN INFORMATION SECURITY

Revision 1

Goals of the Policy

To avoid and minimize losses of AO Severstal Management and its controlled companies caused by:

- Confidential information leaks;
- Usage of incorrect, corrupted information;
- Violations in information processing.

Our commitments

Information of value for business and customers is protected irrespective of means of its processing.

Areas of activities

- Establishment, maintenance and development of Information Security Management System (ISMS) which shall satisfy the requirements of business, comply with the legislation requirements and the best global practices.
- Prediction, prevention, detection, countermeasures and neutralization of both external and internal hazards to information security, as well as minimization of damage caused thereby.
- Implementation of package of measures to ensure security of information systems, personnel, infrastructure, data transfer networks and data media.
- Ensuring compliance and monitoring compliance with the legislation requirements and local regulations in the sphere of information security.
- Improvement of staff awareness in matters related to information security.
-

Our principles

- **Business focus.** ISMS shall serve the business targets and business values and protect its interests.

  Consistency. Organizational measures, hardware and software shall be developed and applied within the unified security system that takes into account all possible actual hazards and is free of any security gaps at junction of its individual components.

- **Continuity.** Processes related to information security shall be carried out at all stages of the information life cycle - from its creation to destruction. Every employee at his/her level must be engaged in these processes.
- **Timeliness.** Information security measures shall be pre-emptive.
- **Continuous improvement.** ISMS shall be developed and improved following the new emerging vectors for spread of hazards, changes in the corporate information system and regulations. ISMS shall take into account the legislation requirements and be based on the results achieved and best global practices in the field of information security.
- **Economic expediency.** ISMS maintenance and improvement costs shall not exceed the amount of damages caused by disclosure, loss, destruction, corruption and unauthorized access to the information.
- **Minimization of authorization.** Access to information resources and technologies shall be limited, justified and provided for performance of official duties only.
- **Control.** Information resources and communication media shall provide for mechanisms to audit the confidential information handling.
- **Legality.** ISMS shall comply with the legislation requirements.