SeAH Steel

Last Edited	November 6, 2025
Managed by	DX Team

Information Security Policy

Rev. 0

Chapter 1. General Provisions

Article 1. Objectives

This Information Security Policy (hereinafter referred to as “this Policy”) is established to protect the information assets of SeAH Steel Corporation (hereinafter referred to as the “Company”) and to define the requirements necessary for conducting security tasks. By applying the standards mentioned in this Policy to business operations, the Company aims to ensure the confidentiality, integrity, and availability of information assets.

Article 2. Scope of Application

① This Policy applies to all information assets owned by the Company and is extended to all employees as well as employees of external companies engaged in the Company’s business.

② However, within the scope of this Policy, external visitors and other individuals with contractual relations with the Company may also be liable, depending on the circumstances and operational needs.

③ This Policy applies to all tangible and intangible assets (hereinafter referred to as “Assets”) held by the Company, and all information assets, including trade secrets (hereinafter referred to as “Information Assets”). The term “Company Assets” collectively refers to both Assets and Information Assets.

Article 3. Approval and Effectiveness

This Policy takes effect throughout the Company upon review and approval by the Chief Information Security Officer (CISO).

Article 4. Information Protection Roles and Responsibilities

① All employees within the Company are responsible for complying with and maintaining information security.

② All employees who use Information Assets are responsible for complying with information security regulations and must immediately report any information security incidents.

③ Employees who manage or provide Information Assets to other users bear full responsibility for the confidentiality, integrity, and availability of those Information Assets.

④ The Chief Information Security Officer (CISO) holds ultimate responsibility for information security management.

⑤ External individuals or organizations that use the Company's Information Assets are responsible for protecting such Information Assets and complying with relevant regulations.

Article 5. Penalties for Violations

In the event that employees and outsourced personnel, or other contracted employees violate this Policy and adversely affect the security level of services provided by the Company, they shall be subject to disciplinary action in accordance with the HR policy and guidelines, and legal penalties may be imposed.

Chapter 2. Information Security Management System

The Company operates an information security management system, establishes an information security organization, and lays the foundation for information security activities.

Article 6. Responsibilities and Roles of the Information Security Organization

The responsibilities and roles of the information security organization are as follows.

Organization	Responsibilities and Roles
Chief Information Security Officer (CISO)	- Oversee the management of information security - Organize the information security organization - Implement and review the information security policy - Establish directions for information security strategies and provide support - Propose, consult, and coordinate the implementation of information security controls
Information Security Manager	- Define authorities and responsibilities related to protecting Information Assets and executing security processes outlined in information security policies and guidelines - Acquire security-related consultations and recommendations and report outcomes of implemented actions - Manage communication channels with external security-related organization - Review risk analysis and internal audit results
Information Security Officer	- Support the duties of the Information Security Manager - Verify compliance with information security policies and guidelines - Record and review the implementation of technical protections - Perform risk assessments and inspections of information systems

Article 7. Information Security Organization Structure

① The Company appoints a Chief Information Security Officer (CISO) responsible for overall information security operations, and may, if necessary, establish additional management or operational units to support this role.

② All members must have a clear understanding of their respective responsibilities and roles.

Chapter 3. Management of Information Assets

The Company establishes and operates standards to ensure appropriate levels of protection of Information Assets based on their importance and characteristics, safeguarding them from risks such as damage, tampering, theft, and leakage.

Article 8. Classification and Management of Information Assets

① All Information Assets shall be identified and listed for management.

② The importance of each Information Assets is assessed, classified by grade, and regularly reviewed for appropriateness.

③ Critical Information Assets are periodically inspected and analyzed, and vulnerabilities identified shall be addressed with appropriate improvement measures.

④ Important data and documents are disposed of in a manner that ensures they cannot be recovered.

Article 9. Risk Management of Information Assets

① The Company shall assess risks based on the importance, vulnerabilities, and threat levels of Information Assets, and establish corresponding management plans.

② Factors such as urgency, required resources, and feasibility shall be comprehensively considered to determine priorities when formulating risk management plans.

③ The risk management procedures shall be regularly reviewed and improved in accordance with the Company’s security management system.

Chapter 4. Management of Information Devices

The purpose is to enhance the safety and reliability of using PCs and other information devices by proactively preventing potential information protection vulnerabilities that may arise from their use, removal, or entry.

Article 10. Management of Information Devices

① Company-issued work PCs must be used and managed in accordance with the Company's information security policies.

② Work PCs shall not be used for purposes other than their intended business use, and measures shall be established to prevent security incidents caused by poor management.

③ Only approved and registered applications may be installed or operated on work PCs.

④ Personal storage devices shall not be used for business purposes unless authorized and registered in advance.

⑤ Procedures must be established for the usage of storage devices, and an inventory of storage devices must be maintained.

⑥ Countermeasures must be prepared against information leakage resulting from disposal, reuse, or loss of storage devices. If prevention is not possible, all data stored on the storage device must be permanently deleted before its removal from Company premises.

Chapter 5. Information System Security Management

The Company establishes requirements necessary for the security of the information system. By ensuring the application and operation of such requirements, Information Assets are safely and efficiently preserved and managed.

Article 11. User Authentication and Identification

① In order to control access to information systems by unauthorized users, all users, including employees and external personnel, must be authenticated before accessing applications, servers, network devices, and databases, and shall be granted only the minimum necessary permissions.

② Authentication methods shall be applied differentially based on the importance of the user, task, and resource, as well as the risks involved in the access process.

Article 12. Account and Access Rights Management

① Management standards for the registration, modification, and deletion of information system accounts (IDs) shall be established and maintained, and change logs shall be retained for a defined period.

② When granting permission for accessing major information systems, only the minimum necessary permissions should be granted based on the type of information handled, the user, and the role associated with the job. These permissions should be reviewed

regularly.

③ Each individual must use a unique account, and shared accounts are prohibited. In exceptional cases requiring shared account use, prior approval must be obtained from the information security organization, and usage must be limited to the approved purpose.

Article 13. Password Management

① Passwords shall be at least ten characters long and include uppercase letters, lowercase letters, numbers, and special characters, and must be securely managed to prevent exposure.

② Separate password criteria may be applied under the Company's system-specific security policy, with prior approval from the information security organization.

Article 14. Server Security Management

① A security review must be conducted, and appropriate security settings must be applied when implementing a new server.

② To ensure server security, important patches for the OS and software must be applied continuously. Before applying a patch, it must be tested in advance to verify its safety and compatibility with the existing system.

Article 15. Network Security Management

① Network areas must be separated according to the nature and importance of the respective task, and access control must be enforced in between separated network areas.

② Access rules, security reviews, and protection measures for network use must be established, reviewed, and applied.

③ Without approval from the information security organization, it is prohibited to connect wireless AP (Access Point) devices to the internal network to establish a wireless network.

Article 16. Database Security Management

① To ensure integrity, direct user access to the database must be restricted.

② Access rights to the database must be granted based on user job roles, and specific commands such as update and delete must be controlled so that only authorized personnel can use them.

Article 17. Information Security System Management

① Technical measures such as firewalls, intrusion prevention systems, and virtual private networks (VPNs) must be installed and operated to prevent intrusions through the network.

② Any changes to the security policies of information security systems must be performed only after obtaining approval from the information security organization, and the relevant details must be recorded and managed.

Chapter 6. Application Security Management

The purpose is to define information security requirements in the development, operation, and use of the Company's applications, and to ensure the security of applications and data.

Article 18. Application Security Management

① New or modified applications must be designed and developed according to security requirements and must undergo a security review prior to operation.

② Security must be considered at all stages of a development project — including analysis, design, development, testing, and transition to operation — and detailed standards shall follow separate secure development guidelines.

Article 19. Secure Application Development Management

① As a general rule, the system development and testing environments must be separated from the operational environment.

② Procedures must be established to control major changes to production applications, and change records must be maintained and managed to determine causes in case of incidents or failures.

③ To prevent leakage or exposure of operational data during application testing, dummy test data should be created and used, or operational data shall be processed for use. The use of actual operational data is strictly prohibited.

④ When migrating an application to the operational phase, the following security requirements must be adhered to:

1) Assign migration personnel other than the developer

2) Conduct the migration only after testing

3) Conduct a security inspection before the migration

4) Prepare countermeasures for any issues that may arise during the migration

Chapter 7. Physical Security Management

The purpose is to protect Company Assets by establishing and operating physical protection measures for facilities and Information Assets, based on their level of importance, and by managing access by employees, external personnel, and visitors.

Article 20. Classification Criteria for Protected Areas

① Physical areas, such as offices that require information protection considering the importance of Information Assets, must be designated as protected areas and categorized into general, restricted, and controlled zones for operation.

② A general zone refers to areas where no critical Company Assets are stored and where external visitors are permitted to enter, such as reception rooms and information desks.

③ A restricted zone refers to areas where some important Company Assets are stored and where access by external personnel is limited, such as offices, meeting rooms, document storage rooms, and situation rooms.

④ A controlled zone refers to areas where access by external personnel is strictly prohibited, and only a minimum number of employees may enter based on business necessity. Examples include data centers, network equipment rooms, and server rooms.

Article 21. Access and Monitoring of Protected Areas

① Access records of employees and external personnel entering protected areas must be logged and maintained, and the appropriateness of access records for major restricted and controlled zones must be periodically reviewed.

② To prevent the illegal removal or leakage of Information Assets within controlled zones, control procedures must be established so that approval from the information security organization is obtained prior to bringing Company Assets in or out of the area.

Article 22. Facility Protection

① Buildings and facilities must be maintained in optimal condition by implementing fire prevention, disaster prevention, temperature and humidity control, cable protection, rack installation management, and emergency power systems to safeguard them from environmental and natural threats.

Chapter 8. Incident Response

The purpose is to prevent security incidents proactively and to minimize damage by providing methods and procedures for systematic response when incidents occur.

Article 23. Incident Response Plan

① The company shall establish an incident response system to ensure prompt and systematic handling of security incidents.

② To prevent security incidents, the Company shall establish and operate a preemptive monitoring, detection, and response system, and respond to illegal information leakage and security breach attempts.

③ In the event of a security incident, the Company shall respond swiftly to minimize damage, analyze the circumstances and causes of the incident, and take necessary corrective actions.

Article 24. Incident Response Procedures

① In the event of a security incident, the information security organization shall cooperate with relevant departments to promptly investigate and analyze the cause and impact, and carry out response and recovery measures to minimize further damage.

② After completing the incident response, relevant records shall be analyzed to establish preventive measures against recurrence, and additional training or drills may be conducted if necessary.

Chapter 9. Disaster Recovery Management

The purpose is to establish systematic response procedures for disaster recovery to ensure effective action and minimize damage in the event of a disaster.

Article 25. Establishment of a Disaster Recovery Plan

① A disaster recovery plan must be developed as an emergency response measure to sustain core operations during disasters, accidents, or failures. This plan should define priorities based on risk impact and urgency based on processing time.

② Effective recovery strategies and plans shall be developed, taking cost factors into account, to achieve the target recovery time objectives (RTO) and recovery point objectives (RPO) for key services and IT assets.

Article 26. Activation of the Disaster Recovery Plan

① In accordance with the disaster recovery plan, relevant information such as the cause and scope of the crisis must be collected and analyzed when a crisis situation occurs.

② Response actions shall follow the disaster recovery plan based on the defined business recovery and recovery objectives, as determined by the business impact analysis.

③ After the crisis has ended, the response results shall be analyzed to identify and improve deficiencies in the recovery plan.

Addendum

This Policy is enacted and takes effect as of November 6, 2025.