SuperAlloy Industrial Co., Ltd. Information Security Policy

1. Purpose
   1.1 This Policy is specifically established by SuperAlloy Industrial Company Ltd. to strengthen information security management and ensure the confidentiality, integrity, and availability of the information assets of employees to provide an information environment that supports the Company’s information business continuity and comply with the relevant legal requirements so as to prevent internal and external willful and accidental threats.

2. Scope
   2.1 This Policy shall apply to all units of the Company.

3. Terms and definitions
   3.1 N/A.

4. Objectives and targets
   4.1 Information security policy objectives
      4.1.1 Maintain the continuous operation of information systems.
      4.1.2 Prevent hackers and viruses from intrusion and destruction, ensure that the prototype is properly protected.
      4.1.3 Ensure routine maintenance and operation.
      4.1.4 Ingrain the basic information security and prototype protection concept and correct information security behavior in all employees.
   4.2 Set the following information security targets in accordance with the policy objectives.
      4.2.1 Ensure that the Company’s key and core systems are maintained at a certain level of system availability.
      4.2.2 Protect the information of the Company’s business activities (includes information security and prototype protection) against unauthorized access and alteration to ensure information accuracy and integrity.
      4.2.3 Periodically implement internal audits to ensure that all operations are unfailingly implemented.
      4.2.4 Organize information security and prototype protection education and training to enhance the awareness in information security and prototype protection responsibility of employees.
   4.3 Plan the to-do-list, required resources, responsible persons, estimated time of completion, and performance assessment method of the year based on the said information security objectives and assess their outcomes. The relevant measurement and monitoring procedures are subject to the Company’s “DOC00065739 Measurement and Monitoring Management Procedures.”
   4.4 During the management review, the Information Security Working Team shall report the results of

effectiveness assessment of the information security objectives to the convener of the Information Security Committee.

5. Responsibility

5.1 Management shall establish and review this policy.

5.2 The Information Security Working Team shall implement this policy through the standards and procedures.

5.3 All employees and contractors shall follow the relevant management procedures to maintain the information security policy.

5.4 It is the responsibility of all employees to report information security incidents and any identified vulnerabilities.

5.5 Any behavior endangering information security shall be held accountable for the civil, criminal, and administrative liabilities or punished according to the Company’s relevant regulations.

6. Review

6.1 This Policy shall be reviewed at least once a year at the management review to reflect the latest development status of government regulations, technology, and business to ensure the Company’s sustainable operations and capacity in information security practice.

7. Implementation

7.1 Any agencies and/or units obtaining the Company’s confidential and sensitive information or personal data due to business needs shall ensure their confidentiality and proper use and abide by the relevant national laws and regulations and the Company’s relevant information security regulations.

7.2 Agencies and/or units compromising such data or causing information security incidents shall take the relevant legal liabilities.

7.3 This Policy shall be implemented after the review of the “Information Security Committee” and the approval of the convener. The same shall apply to the amendments hereto.

7.4 If the Company decides to make changes to the Information Security Management System, the changes shall be implemented in a planned or projected manner.

7.5 If the following items need to be changed when performing information security management operations, the changes should be performed in a planned manner:

7.5.1 Information Security Management System (ISMS) changes.

7.5.2 A major information security incident occurs.

7.5.3 Changes in the information security organization structure.

7.5.4 More than 50% of the members of the Information Security Committee change at the same time.

7.5.5 When more than 3 information assets of key business processes are changed at the same time.

8. Communication and Transmission

8.1 Information security policy and objectives should be communicated and disseminated to all personnel of the company, including:

8.1.1 Announcement of Information Security Policies and Objectives.

8.1.2 For direct personnel without information system accounts, communication and dissemination should be conducted through printed announcements. If there are direct personnel who are not of the local nationality, announcements should be made in a language readable by foreign migrant workers.

8.1.3 The printed announcement should include the official seal of the issuing department, the announcement date, and the version of the announcement policy.

8.2 Information security policy and objectives should be communicated and transmitted to external stakeholders, including:

8.2.1 Suppliers and business partners providing services to the Company.

8.2.2 Non-specific third parties will be announced through external platforms, such as the Company's global website.

8.2.3 If there are changes to the information security policy vision or objectives, the Information Working Group should assess whether the changes are relevant to employees and external business partners. If the assessment indicates relevance, the changes should be communicated and transmitted to employees and external business partners.

Released: 2025/12/08 REV.005

Announcement: IT Division

Information Security Event Report:isms@superalloy.tw