# Sentien Printing Works Co., Ltd

# "Information Security Management System"
# Information Security Policy

**Classified Class: Fair**

**ID: IS-01-001**

**Version number: 1.0**

**Revised: 2024.07.15**

If you have any questions about the version before using this document, please check with the reviser for the latest version.

Changelog of previous documents :

| edition | Revision date | Revisers | illustrate | Approver |
|---|---|---|---|---|
| 1.0 | 2024.07.15 | Information Security Enforcement Team | Revision of the first draft | convener |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

This program is maintained by the Information Security Enforcement Team.

Directory:

1 objective

1.1 Sentien Printing Co., Ltd. (hereinafter referred to as the Company) has specified this policy in order to strengthen information security management, ensure the confidentiality, integrity and availability of its information assets, provide an information environment for the continuous operation of the Company's information business, and comply with the requirements of relevant laws and regulations, so that it is protected from internal and external deliberate or accidental threats.

2 Scope of application

2.1 All units of the Company.

3 definition

3.1 All personnel: the company's personnel and outsourced manufacturers.

4 Vision & Goals

4.1 Information Security Policy Vision:

4.1.1 Strengthen the knowledge of personnel

4.1.2 Avoid data leakage

4.1.3 Implement daily maintenance

4.1.4 Make sure the service is available

4.2 In line with the vision of the information security policy, the proposed information security objectives are as follows:

4.2.1 Conduct information security education and training, promote personnel's awareness of information security and strengthen their awareness of relevant responsibilities.

4.2.2 Protect the information of the company's business activities from unauthorized access and modification, and ensure its accuracy and integrity.

4.2.3 Conduct regular internal and external audits to ensure that relevant operations are properly implemented.

4.2.4 Ensure that the Company's business-critical systems maintain a certain level of system availability.

4.3 In view of the above-mentioned information security objectives, the annual to-do list, required resources, responsible personnel, estimated completion time, and result evaluation methods and evaluation results shall be formulated, and the relevant supervision and measurement procedures shall be handled in accordance with the Company's "Supervision and Measurement Management Procedures".

4.4 The Information Security Implementation Team shall report to the convener of the Information Security Committee on the results of the measurement of the effectiveness of the information security objectives at the management review meeting.

5 liability

5.1 This policy is established and reviewed by the management of the Company.

5.2 The Information Security Executive Team adopts standards and procedures to implement this policy.

5.3 All personnel are required to maintain information security policies in accordance with relevant security management procedures.

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

5.5 Any behavior that endangers information security will be investigated for civil, criminal and administrative liabilities or punished in accordance with the relevant regulations of the company.

5.6 The information security policy shall be communicated to internal and external personnel, and may be communicated through internal announcements, meetings, education and training, official websites, e-mails, etc.

6 censor

6.1 This policy shall be reviewed at least once a year to reflect the latest developments in government laws and regulations, technology and business, so as to ensure the company's sustainable operation and information security practical capabilities.

7 implement

7.1 The information security policy for the next fiscal year will be reviewed in conjunction with the management review meeting of the current year.

7.2 Each unit of the Company implements information security management work based on differences in business attributes and supports each other. Please refer to the attached table "ISMS Process and Organization Correspondence Table" for the projects responsible for each unit.

7.3 If each unit needs to make changes to the following items when performing information security management operations, it shall implement the changes in accordance with the planned method:

7.3.1 Changes to the information security management system.

7.3.2 A major information security incident occurred.

7.3.3 There are additions, changes, or deletions of information assets.

7.3.4 Changes in the operating environment.

7.4 If you need to make changes to your information security management system, you should consider the following:

7.4.1 The purpose of the change and its potential impact.

7.4.2 Integrity of the management system.

7.4.3 Availability of resources.

7.4.4 Assignment or reassignment of duties and authority.

7.5 This Policy shall be reviewed by the Information Security Committee and approved by the convener for implementation, and the same shall apply when it is revised.

Appendix ISMS Process and Organizational Mapping Table

| Provisions | procedure | Manage files | Department of Management | Information Section | Audit Office |
|---|---|---|---|---|---|
| 4 | Organize the panorama | Handbook of Organizational Panorama Analysis | ● | ○ | ○ |
| 5 | Leadership acts | Information Security Policy | ● | ○ | ○ |
|  |  | Information Security Organizational Procedures | ● | ○ | ○ |
| 6 | planning | Information Security Policy | ● | ○ | ○ |
|  |  | Risk assessment and management procedures | ○ | ● | ○ |
|  |  | Declaration of Applicability | ○ | ● | ○ |
| 7 | In the tank | Information Security Organizational Procedures | ● | ○ | ○ |
|  |  | Human Resource Management Procedures | ● | ○ | ○ |
|  |  | Document management programbook | ○ | ● | ○ |
| 8 | Operation | Risk assessment and management procedures | ● | ○ | ○ |
| 9 | Performance evaluation | Information Security Organizational Procedures | ● | ○ | ○ |
|  |  | Information security audit operating procedures | ○ | ○ | ● |
| 10 | improve | Correction Management Procedures | ○ | ○ | ● |
| A.5 | Organizational controls | Information Security Policy | ● | ○ | ○ |
|  |  | Document management programbook | ○ | ● | ○ |

| | | | | | |
|---|---|---|---|---|---|
| | | Information Security Organizational Procedures | ● | ○ | ○ |
| | | Information Asset Management Procedures | ○ | ● | ○ |
| | | Access control management program | ○ | ● | ○ |
| | | Communication and Operational Safety Procedures | ○ | ● | ○ |
| | | Supplier Management Procedures | ● | ○ | ○ |
| | | Information Security Incident Management Procedures | ○ | ● | ○ |
| | | Business Continuity Management Procedures | ○ | ● | ○ |
| A.6 | Personnel control measures | Information Security Organizational Procedures | ● | ○ | ○ |
| | | Human Resource Management Procedures | ● | ○ | ○ |
| A.7 | Entity controls | Entity Security Management Procedure Book | ○ | ● | ○ |
| A.8 | Technical controls | Information Security Organizational Procedures | ● | ○ | ○ |
| | | Information Security Audit Procedures | ○ | ○ | ● |
| | | Information Asset Management Procedures | ○ | ● | ○ |
| | | Access control management program | ○ | ● | ○ |
| | | Entity Security Management Procedure Book | ○ | ● | ○ |
| | | Communication and Operational Safety Procedures | ○ | ● | ○ |

| | | | | | |
|---|---|---|---|---|---|
| | | System development and maintenance program book | ○ | ● | ○ |
| ●: Responsibility ○: Support | | | | | |