Huali Industrial Group Co., Ltd.

Information Security Policy	Document number: HL-M-IT001	
	Effective Date : December 1 , 2021	
	Revision: 2022.1.1	Page: 1OF 9

Document Revision Record

Edition Revision	Revision Date Revise Date	Changes Description of Change	Proposed Editor Originator
1.0	2021/11/30	Initial version	Keith Jhou
Version number description: ab (a is the year of the version, b is the number of revisions in the year, and the version that is not revised and continued to be used across years is a.0			

Approval		Review		Audit		Write	

A. Purpose

Huali Group Co., Ltd. (hereinafter referred to as the Group) has established this policy to enhance information security management, ensure the confidentiality, integrity, and availability of information assets across its affiliated factories, provide the necessary infrastructure and framework for the Group's information operations, comply with relevant legal and regulatory requirements, and protect information assets from internal and external intentional or accidental threats..

B. Scope of application

1. The scope of this policy covers the Group's China headquarters and factories, Vietnam factories, Dominican Republic factory, Southeast Asia factories, and any subsequent companies or factories established in different countries to meet the Group's business needs, as well as the Hong Kong branch, Taiwan branch, Taipei IDC (Internet Data Center) data center, Kaohsiung data center, and related departments and operation and maintenance personnel, to fully manage information operations and meet security requirements.

2. Information Security Management System Scope

2.1 When establishing an information security management system, the Group shall consider information security concerns raised by internal and external stakeholders, including the security of system services and personal privacy protection, as well as stakeholders' expectations and requirements for the information security management system, and include them in the scope of objectives and effectiveness evaluation.

2.2 The above-mentioned information security concerns, expectations, or requirements shall be incorporated into risk assessment and risk management to ensure the information security management system achieves the expected outcomes and supports continuous improvement.

3. Information security management encompasses 14 management items to prevent improper use, leakage, tampering, or destruction of data due to human negligence, intentional acts, or natural disasters, which may pose various risks and hazards to the Group. The management items are as follows:

3.1 Security Policy

3.2 Information Security Organization

3.3 Human Resources Security

3.4 Asset Management

3.5 Access Control

3.6 Encryption

3.7 Physical and Environmental Security

3.8 Operations Security

3.9 Communication Security

3.10 Information System Acquisition, Development, and Maintenance

3.11 Supplier Relationship

3.12 Information Security Incident Management

3.13 Business Continuity Management Related to Information Security

3.14 Legal and Regulatory Compliance

The corresponding table of internal and external issues and concerns of the Group's information security is as follows:

Internal and external stakeholders	Expectations and issues (information security)	policy	Corresponding matters and documents	Goals and targets
1. Group Information HQ	Ensure information security of business systems and network operations	1. Information Security Policy 2. Information Security Organization Policy 3. Asset Management Policy 4. Human Resources Security Policy 5. Access Control Policy 6. Physical and Environmental Security Policy 7. Communications and Operations Management Policy 8. Information System Acquisition, Development, and	1. Information Security Policy 2. Information Security Organization Procedures 3. Information Asset Management Procedures 4. Personnel Security and Training Procedures 5. Access Control Management Procedures 6. Physical Security Management Procedures 7. Communications and Operations Management Procedures	A.1 Information Security Policy Formulation and Evaluation 1. Number of information security policy reviews 2. Number of information security policy awareness campaigns A.2 Information Security Organization 1. Confirmation of signed confidentiality agreements 2. Number of management review meetings A.3 Human Resources Security 1. Verify training hours for information security for new and current personnel 2. Verify training hours for personnel violating information security regulations 3. Ensure accounts of resigned personnel are deleted

		Maintenance Policy 9. Information Security Incident Management Policy 10. Business Continuity Management Policy 11. Compliance Policy	8. System Development and Maintenance Procedures 9. Security Incident Management Procedures 10. Business Continuity Management Procedures 11. Risk Assessment and Management Procedures 12. Information Security Audit Procedures 13. Corrective and Preventive Management Procedures 14. Supplier Management Procedures	A.4 Information Asset Management 1. Update information asset inventory 2. Ensure information asset inventory complies with classification and labeling regulations A.5 Access Control Security 1. Regularly review access permissions for critical systems 2. Number of unauthorized accesses to sensitive data on critical systems A.6 Encryption 1. Regularly update computer login passwords A.7 Physical and Environmental Security 1. Verify compliance with data center access control regulations 2. Verify regular maintenance of fire safety equipment 3. Verify UPS is under regular warranty or maintenance agreements

Internal and external stakeholders	Expectations and issues (information security)	policy	Corresponding matters and documents	Goals and targets
1. Group Information HQ	Ensure information security of business systems and network operations	1. Information Security Policy 2. Information Security Organization Policy 3. Asset Management Policy 4. Human Resources Security Policy 5. Access Control Policy 6. Physical and Environmental Security Policy 7. Communications and Operations Management Policy 8. Information System Acquisition, Development, and Maintenance Policy 9. Information Security Incident Management Policy	1. Information Security Policy 2. Information Security Organization Procedures 3. Information Asset Management Procedures 4. Personnel Security and Training Procedures 5. Access Control Management Procedures 6. Physical Security Management Procedures 7. Communications and Operations Management Procedures 8. System Development and Maintenance Procedures 9. Security Incident	A.8 Operations Security 1. Regularly monitor system capacity (e.g., CPU, RAM, hard disk) of critical network servers 2. Verify real-time updates of antivirus software 3. Regularly back up critical system data A.9 Communication Security 1. Number of internal network disconnections (per year) 2. Verify synchronization of critical system clocks 3. Verify firewall settings align with the firewall configuration record 4. Number of vulnerability scans A.10 Information System Acquisition, Development, and Maintenance 1. Test critical system updates before deployment 2. Update system documentation during critical system development or changes 3. Ensure critical systems have emergency recovery mechanisms

		10. Business Continuity Management Policy 11. Compliance Policy	Management Procedures 10. Business Continuity Management Procedures 11. Risk Assessment and Management Procedures 12. Information Security Audit Procedures 13. Corrective and Preventive Management Procedures 14. Supplier Management Procedures	A.11 Supplier Relationships 1. Confirm signed confidentiality agreements A.12 Information Security Incident Management 1. Number of unreported information security incidents 2. Review incident notification forms and count recurring incidents A.13 Business Continuity Management (Information Security) 1. Review execution of business continuity plan drills 2. Conduct risk assessment and operational impact analysis A.14 Legal and Regulatory Compliance 1. Ensure installation of licensed software 2. Complete corrective and preventive measures within specified timelines

Internal and external stakeholders	Expectations and issues (information security)	policy	Corresponding matters and documents	Goals and targets
2. Customer	1. Business information and network management security 2. Customer privacy protection	1. Physical Security Management Policy 2. Communications and Operations Management Policy 3. Business Continuity Management Policy	1. Physical Security Management Procedures 2. Communications and Operations Management Procedures 3. Business Continuity Management Procedures	A.7 Physical and Environmental Security 1. Verify compliance with data center access control regulations 2. Verify regular maintenance of fire safety equipment 3. Verify UPS is under regular warranty or maintenance agreements A.8 Operations Security 1. Regularly monitor system capacity (e.g., CPU, RAM, hard disk) of critical network servers 2. Verify real-time updates of antivirus software 3. Regularly back up critical system data A.9 Communication Security 1. Number of internal network disconnections (per year) 2. Verify synchronization of critical system clocks 3. Verify firewall settings align with the firewall configuration record 4. Number of vulnerability scans

				A.13 Business Continuity Management (Information Security) 1. Review execution of business continuity plan drills 2. Conduct risk assessment and operational impact analysis

C. Definition

Information assets: The infrastructure, hardware, software, data, and personnel that maintain the normal operation of the Group's information business.

D. Target

Maintain the confidentiality, integrity, and availability of the Group's information assets and protect the personal privacy of users. With the collective effort of all employees, the Group aims to achieve the following goals:

1. Implement standard operating procedures for the Group's business systems, related departments, and operation and maintenance personnel to ensure the confidentiality, integrity, and availability of the Group's IDC, factory data centers, and business system services, meeting the requirements and expectations of stakeholders.
2. Protect the Group's business activity information from unauthorized access and modification, ensuring its integrity.
3. Appoint a cross-departmental Information Security Officer or team to oversee the Information Security Department's promotion and evaluation of improvements in information security management, ensuring a robust information environment for business continuity.
4. Conduct information security education and training to enhance employees' awareness of information security and strengthen their understanding of related responsibilities.
5. Implement an information security risk assessment mechanism to enhance the effectiveness and timeliness of information security management.
6. Evaluate critical information security facilities and establish backup or failover infrastructure as necessary to ensure system availability.
7. Implement an information security internal audit system to ensure the execution of information security management.
8. Ensure the Group's business activities comply with relevant legal and regulatory requirements.
9. Control, inspect, and accept services provided by suppliers based on the items and content of their services.

10. Establish internal and external communication and coordination mechanisms.
11. Regularly review and continuously improve the Group's information security management system.
12. Properly plan and implement requirements for business system service information security.
13. Conduct proper risk management for internal authorized personnel of business system services.
14. Ensure proper separation between suppliers and customers, and between customers, in business system services.
15. Fully define and manage the rights and responsibilities of access control personnel for business system services.
16. Notify customers when changes in business system management or operational regulations affect services.
17. Properly preserve customer information provided by business system services.
18. Implement customer lifecycle management for business system services.
19. Establish clear investigation and handling regulations for incidents or accidents in business system services, notifying the competent authority and affected stakeholders.
20. Ensure personal data processing and management in business system services protect personal privacy.

E. Responsibility

1. The Group's Information Technology Office establishes and reviews this policy, with information security responsibilities of department heads and members stipulated in the "Information Security Organization Procedures."
2. Information security managers implement this policy through appropriate standards and procedures.
3. All personnel and suppliers are required to follow information security management procedures to maintain the information security policy.
4. All personnel have a responsibility to report information security incidents and any identified vulnerabilities.
5. Any behavior that endangers information security will be subject to legal liability or disciplinary action in accordance with the Group's relevant regulations, depending on the severity of the circumstances.