Information Security Policy and Guidelines

Charoen Pokphand Engineering Co.,Ltd.

Revision History

Information Security Policy and Guidelines

Charoen Pokphand Group

Version	Responsible Department	Description	Reviewer	Approver	Date of approval
1					
2					

Notice: This page is intended for internal use only

Revision History

Information Security Policy and Guidelines

Charoen Pokphand Engineering Co.,Ltd.

Version	Responsible Department	Description	Reviewer	Approver	Date of approval
1					
2					

Notice: This page is intended for internal use only

Contents

Information Security Policy and Guidelines

Charoen Pokphand Engineering Co.,Ltd.

1. Intent

Charoen Pokphand Engineering Co. ,Ltd. realizes that information, either in document and electronic form, is one of the most valuable assets to the business. Information, which may be stored, collected, processed, and transmitted through systems and information technology, shall be protected from unauthorized usage, including access, disclosure, alteration, or destruction that renders such information unusable, as well as cyber threats. For these reasons, Charoen Pokphand Engineering Co. ,Ltd. prioritizes the oversight of systematic information and cybersecurity to ensure that they are efficient, accurate, complete, and ready to use in order to safeguard company assets and information, as well as minimize risks and damages resulting from security breaches. Moreover, Charoen Pokphand Engineering Co. ,Ltd. fosters cyber resilience with risk management by considering the company's risk tolerance in order to respond to business requirements and the needs of both internal and external stakeholders across the supply chain.

Charoen Pokphand Engineering Co.,Ltd. has, therefore, established this Policy and Guidelines to ensure that information security and cybersecurity has risk management, prevention, monitoring, surveillance, audit, and controls in compliance with applicable laws, regulations, and standards. Furthermore, this Policy and Guidelines promotes business practices that adheres to the principle of confidentiality, integrity, availability, and safety. Ultimately, Charoen Pokphand Engineering Co.,Ltd. can maintain business continuity and working environment safety while building a robust information security culture and increasing sustainable competitive advantage.

2. Scope

This Information Security Policy and Guidelines apply to Charoen Pokphand Group (hereafter "the Group"), which includes Charoen Pokphand Group Co., Ltd., and all of its subsidiary companies that Charoen Pokphand Group Co., Ltd. has management control. The term "company" hereafter refers to any such company individually that has adopted this Information Security Policy and Guidelines. This document shall be reviewed at least once a year or as conditions require.

3. Objectives

3.1 To provide directors, management, and staff with guidelines for information security.

3.2 To secure the access and the use of information assets from information risks that may affect the company's business operations.

4. Roles and Responsibilities

4.1 Board of Directors

4.1.1 Consider and approve the Information Security Policy and Guidelines.

4.1.2 Oversee business operations and their compliance with related laws, rules, regulations, policies and guidelines.

4.1.3 Supervise to ensure the tangible implementation of this Policy and Guidelines.

4.2 Management

4.2.1 Establish rules, regulations, and procedures according to the company' s business context in line with its strategy, policy, and guidelines.

4.2.2 Determine the corporate structure and responsible persons with appropriate roles and responsibilities.

4.2.3 Establish information and cybersecurity action plans, including business continuity plans.

4.2.4 Establish risk management and internal control systems.

4.2.5 Communicate this Policy and Guidelines to promote awareness for managers and staff at all levels.

4.2.6 Manage and support employee compliance with related rules, operating procedures, and standards.

4.2.7 Establish whistleblowing and grievance channels to contact responsible department/persons regarding information and cybersecurity breaches.

4.2.8 Foster a culture of information and cybersecurity across the company.

4.2.9 Consider information and cybersecurity performance reports and areas for improvement on a regular basis.

4.3 Responsible Department/Persons

4.3.1 Evaluate and manage risks involving threat, vulnerability, likelihood, and impact on information assets, internal, and external stakeholders throughout the supply chain.

4.3.2 Establish information and cybersecurity measures in accordance with this Policy and Guidelines, including relevant operational procedures and standards.

4.3.3 Surveil and maintain information assets on an ongoing basis to ensure their operability and security.

4.3.4 Follow up on related laws, rules, regulations and standards in order to improve information and cybersecurity measures, together with monitoring compliance with measures on a regular basis.

4.3.5 Establish criteria and procedures for reporting information and cybersecurity breaches.

4.3.6 Promote awareness and advise employees on information and cybersecurity, as well as internal and external stakeholders throughout the supply chain.

4.3.7 Prepare information and cybersecurity performance reports.

4.4 Employees

4.4.1 Learn and comply with rules, regulations, policies, and guidelines.

4.4.2 Take action and report any abnormalities or incidents related to the company's information and cybersecurity that may affect business operations through the company's provided channels.

4.4.3 File complaints or blow the whistle related to any actual or potential misconduct on this Policy and Guidelines.

5. Guidelines

5.1 Assess and analyze information and cybersecurity risks of the business, together with risks associated with internal and external stakeholders throughout the supply chain.

5.2 Develop an information and cybersecurity risk management strategy in alignment with the company's vision, mission, objectives, and risk tolerance.

5.3 Determine information and cybersecurity plans and measures covering the identification of company's environment, the protection of information assets, the detection of unusual events, the response to security incidents, and the recovery of information assets from damages.

5.4 Manage the company's information assets operated by both internal and external parties to ensure security at all phases of the system/software development life cycle.

5.5 Protect information as well as data transferred through computer systems and information technology, including personal data of employees, customers, suppliers and third-party data processors, from unauthorized access, use, transfer, modification, reproduction, alteration, deletion, and destruction.

5.6 Assess and manage vulnerabilities in computer systems and information technology, as well as conducting patch management on a regular basis.

5.7 Monitor and detect unusual activities or violations of information and cybersecurity, or activities that can impact business continuity, as well as audit relevant measures to ensure their efficiency on an ongoing basis.

5.8 Establish the information and cybersecurity incident management process to contain, mitigate, remediate and recover from impacts, in addition to restoring information assets in a timely and secure manner. This also includes improving the process on an ongoing basis.

5.9 Support and collaborate with domestic and international organizations in private and governmental sectors, including civil society, on information and cybersecurity.

5.10 Promote and support information and cybersecurity awareness building with employees, customers, suppliers, and business partners along with internal and external stakeholders throughout the supply chain.

6. Training

The Company shall communicate and cascade the Information Security Policy and Guidelines through training programs, conferences, and other appropriate channels to its directors, management, staff, and external stakeholders, including suppliers and business partners throughout the supply chain. The effectiveness of training shall be evaluated after each session.

7. Whistleblowing

File complaints or blow the whistle related to this Policy and Guidelines according to the Whistleblowing Policy and Guidelines. All whistleblowers or reporters shall be protected from retaliation regarding their employment status, with their information to be kept confidential both during and after the investigation processes.

8. Policy Guidance

If there are any enquiries regarding possible violations of laws, regulations, and this Information Security Policy and Guidelines, employees can seek guidance from their supervisor, responsible department or persons, the Compliance Department, the Information Systems and Technology Department or Legal Department before carrying out any decision or action.

9. Penalties

All employees must fully cooperate with internal and external authorities in the event of an investigation. Any direct and indirect violations or failure to comply with this Policy and Guidelines by management and staff will be subject to disciplinary action in accordance with Company's regulations.

10. Related Laws, Regulations, and Policies

10.1 Relevant Information and Cybersecurity Laws

10.2 Relevant Computer Crime Laws

10.3 Relevant Personal Data Protection Acts

10.4 Relevant Electronic Transactions Laws

10.5 ISO/IEC 27001 - Information Security Management System by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

10.6 Cybersecurity Framework (CSF) by the National Institute of Standards and Technology (NIST)

10.7 Control Objectives for Information and Related Technologies (COBIT) Framework by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute

10.8 Center for Internet Security Controls by the Center for Internet Security (CIS)

10.9 The Cyber Assessment Framework (CAF) by the United Kingdom's National Cyber Security Center (NCSC)

11. Appendix

The following appendix is attached to this Policy and Guidelines:

11.1 Appendix A: Definitions

Appendix A

Definitions

1. **Control**

   Functions of managements, operations, or techniques in risk management that help a company to monitor and evaluate an area of interest according to relevant standards and achieve target goals and objectives.

2. **Safety**

   A principle for minimizing technology- related risks, in which technological failure or manipulation by malicious actors can cause damage to individuals and assets.

3. **Security**

   Any processes and actions, such as prevention, rigor, care, prudent usage, and maintenance, with the aim to protect information assets from theft, destruction, damage, or interference by internal and external parties that harms the company's business operations. The security principles are as follows:

   - **Confidentiality**: Protecting the confidentiality of information assets by preventing from unauthorized access and disclosure, including personal identifiable information that is proprietary to the company.
   - **Integrity**: Ensuring that information assets are not altered, modified, or destroyed by unauthorized persons.
   - **Availability**: Ensuring that information assets in online channels and offline forms are available to authorized users in a timely and reliable manner.
   - **Accountability**: Taking responsibility for the results of actions, orders, assignments, and decisions based on their roles and responsibilities.
   - **Authentication:** Ensuring that access to information assets is only granted after successful authentication.

- **Authorization:** Ensuring that access rights to information assets are only given for a subject to complete its task (least privilege) where its job function legitimately requires (need to know basis).
- **Non- repudiation:** Ensuring that an individual cannot deny having performed a transaction.

4. Secure System/Software Development Life Cycle

Implementation of information security processes, measures, and requirements at all phases of the system/ software development life cycle, including requirements gathering, design, procurement, development, testing, operation, maintenance, and decommissioning.

5. Risk

Negative effects of uncertain events on achieving monetary and non-monetary objectives and goals of the company.

6. Cyber

Information and communications arising from the use of services, computer networks, internet system, or telecommunication network including the regular service of satellites and similar networks connected in general.

7. Information Technology

Utilizing computer technologies, electronic equipment, and telecommunication networks to search, store, analyze, process, transfer, distribute, track, collect, and manage the company's information.

8. Stakeholder (internal and external)

An individual, group of individuals, or entity that are affected by the company's operations. This can be separated into internal stakeholders, composed of directors, management, and staff, and external stakeholders, composed of customers, consumers, suppliers, business partners, shareholders, investors, communities, societies, governments, nongovernmental organizations, competitors, and creditors.

9. Employee

Personnel hired by the company on a permanent or temporary basis at a level below management, as well as those who are hired to work under special contracts.

10. Information and Cyber Security Measures

Five areas of information and cyber security measures are as follows:

- **Identification** consists of governance, risk management, compliance, human resource security, and supply chain risk management.
- **Protection** consists of asset management, access control, secure system/ software development life cycle, cryptographic management, operations security, change management, capacity and performance management, physical and environmental security, and communication and network management.
- **Detection** consists of log monitoring and threat management.
- **Response** consists of information and cyber security incident management.
- **Recovery** consists of business continuity management and disaster recovery.

11. System

An asset including system or network that can be specified, scoped, and managed e.g., computers, workstations, laptops, servers, routers, switches, firewalls, mobile devices, etc.

12. Information

The company's processed, analyzed, calculated, or interpreted data that may be accessed, searched, or retrieved through electronic network systems or electronic data processing technologies, available in either of two formats:

1. Electronic information stored in computer systems or created from the usage of services and computer networks, internet systems, telecommunications networks, including satellite and similar network services, such as electronic documents, databases, media or portable drive, and collaboration tools, etc.
2. Physical information such as printed document, etc.

13. Information Asset

Information and systems, including software, applications, services, or other information resources that support business operations and has economic value to the company.

14. Information and Cyber Security Incident (Internal and External)

Any scenario or event that may have a negative impact on operations and information assets owned by the company, individuals, or other organizations through unauthorized access, destruction, disclosure, alteration and/or service disruption.