Information Security Policy and Guidelines

Siam Land Flying Co., Ltd.

SIAM LAND FLYING

Contents

Information Security Policy and Guidelines

Siam Land Flying Co., Ltd.

1. Intent

Siam Land Flying Co., Ltd. (SLF) 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, the Company 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, the Company 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.

The Company 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, the Company 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.

นโยบายและแนวปฏิบัติ
ด้านความมั่นคงปลอดภัยสารสนเทศ
บริษัท สยามแลนด์ ฟลายอิ้ง จำกัด

สารบัญ

นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ

บริษัท สยามแลนด์ ฟลายอิ้ง จำกัด

1. ความสำคัญ

บริษัท สยามแลนด์ ฟลายอิ้ง จำกัด ตระหนักว่าสารสนเทศทั้งที่อยู่ในรูปแบบของเอกสารและอิเล็กทรอนิกส์ถือเป็นสินทรัพย์ที่มีค่าที่ใช้ในการดำเนินธุรกิจ ซึ่งอาจถูกจัดเก็บ รวบรวม ประมวลผลและส่งต่อผ่านระบบและเทคโนโลยีสารสนเทศควรได้รับการปกป้องจากการเข้าถึงที่ไม่ได้รับอนุญาต การเปิดเผย การดัดแปลงหรือการทำลายทำให้ไม่สามารถใช้งานต่อไปได้ และรักษาความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ บริษัทจึงให้ความสำคัญในการกำกับดูแลความมั่นคงปลอดภัยสารสนเทศและไซเบอร์อย่างเป็นระบบ มีประสิทธิภาพ ถูกต้อง สมบูรณ์และพร้อมใช้งาน เพื่อปกป้องสินทรัพย์ สารสนเทศ ป้องกันความเสี่ยงและลดความเสียหาย อันเกิดจากเหตุละเมิดความมั่นคงปลอดภัย รวมทั้งส่งเสริมให้เกิดความสามารถด้านการเตรียมพร้อมในการตอบสนองต่อภัยคุกคามทางไซเบอร์และการกู้คืนกระบวนการทางธุรกิจให้กลับมาดำเนินการได้ตามปกติ (Cyber Resilience) ตลอดจนตอบสนองความต้องการทางธุรกิจและกลุ่มผู้มีส่วนได้เสียทั้งภายในและภายนอกตลอดห่วงโซ่อุปทานภายใต้การบริหารจัดการความเสี่ยงตามระดับความเสี่ยงที่ยอมรับได้ของบริษัท

บริษัทจึงได้กำหนดนโยบายและแนวปฏิบัติฉบับนี้ขึ้น เพื่อรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ให้มีการบริหารความเสี่ยง การปกป้องดูแล การติดตาม การเฝ้าระวัง การตรวจสอบและการควบคุมเป็นไปตามกฎหมาย กฎระเบียบ และมาตรฐานที่เกี่ยวข้อง โดยยึดหลักการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ความพร้อมใช้งานของสินทรัพย์สารสนเทศ (Availability) และความปลอดภัย (Safety) เพื่อสร้างความต่อเนื่องในการดำเนินธุรกิจ ให้พนักงานทำงานด้วยความปลอดภัย สร้างวัฒนธรรมด้านความมั่นคงปลอดภัยที่เข้มแข็งและเพิ่มขีดความสามารถทางการแข่งขันอย่างยั่งยืน

2. ขอบเขตนโยบาย

นโยบายและแนวปฏิบัตินี้ใช้บังคับกับเครือเจริญโภคภัณฑ์ ต่อไปนี้เรียกว่า “เครือฯ” หมายถึง บริษัท เครือเจริญโภคภัณฑ์ จำกัด และบริษัทในเครือทุกบริษัทที่บริษัท เครือเจริญโภคภัณฑ์ จำกัด มีอำนาจบริหาร ซึ่ง “บริษัท” ที่จะกล่าวถึงในเอกสารฉบับนี้ให้หมายถึง บริษัทหนึ่ง ๆ ที่นำเอาเอกสารฉบับนี้ไปบังคับใช้ ทั้งนี้จะมีการทบทวนโยบายฉบับนี้อย่างน้อยปีละหนึ่งครั้ง หรือกรณีมีเหตุอันสมควร

3. วัตถุประสงค์

3.1 เพื่อให้กรรมการ ผู้บริหาร และพนักงานมีแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ

3.2 เพื่อปกป้องการเข้าถึงและใช้งานสินทรัพย์สารสนเทศให้มีความมั่นคงปลอดภัยจากความเสี่ยงด้านสารสนเทศที่อาจส่งผลกระทบต่อการดำเนินธุรกิจของบริษัท

4. หน้าที่และความรับผิดชอบ

4.1 คณะกรรมการบริษัท

4.1.1 พิจารณาอนุมัตินโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ

4.1.2 กำกับดูแลให้การดำเนินธุรกิจเป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ มาตรฐานและนโยบายและแนวปฏิบัติที่เกี่ยวข้อง

4.1.3 ติดตามดูแลให้เกิดการนำนโยบายไปปฏิบัติอย่างเป็นรูปธรรม

4.2 ผู้บริหาร

4.2.1 กำหนดกฎ ระเบียบ และขั้นตอนการดำเนินงานที่เหมาะสมกับบริบทของแต่ละบริษัท โดยให้สอดคล้องกับกลยุทธ์ นโยบายและแนวปฏิบัติ

4.2.2 จัดให้มีโครงสร้างองค์กรที่มีผู้รับผิดชอบ และบทบาทหน้าที่ที่เหมาะสม

4.2.3 กำหนดแผนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ รวมทั้งแผนบริหารความต่อเนื่องทางธุรกิจ

4.2.4 จัดให้มีระบบบริหารจัดการความเสี่ยง และการควบคุมภายใน

4.2.5 สื่อสารนโยบายและแนวปฏิบัติเพื่อสร้างการตระหนักรู้ให้กับผู้บริหารและพนักงานทุกระดับ

4.2.6 บริหารจัดการ และสนับสนุนให้มีการปฏิบัติตามกฎ ระเบียบ ขั้นตอนการดำเนินงานและมาตรฐานที่เกี่ยวข้อง

4.2.7 จัดให้มีช่องทางติดต่อหน่วยงานหรือบุคคลผู้รับผิดชอบ เพื่อรับแจ้งเหตุในกรณีที่เกิดเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

4.2.8 ส่งเสริมให้เกิดวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ทั่วทั้งองค์กร

4.2.9 พิจารณารายงานผลการดำเนินงานและแนวทางในการปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์อย่างสม่ำเสมอ

4.3 หน่วยงานหรือบุคคลผู้รับผิดชอบ

4.3.1 ประเมินและบริหารจัดการความเสี่ยงที่ครอบคลุมภัยคุกคาม (threat) ช่องโหว่ (vulnerability) ความเป็นไปได้ (likelihood) และผลกระทบ (impact) ต่อสินทรัพย์ด้านสารสนเทศ และผู้มีส่วนได้เสียทั้งภายในและภายนอกตลอดห่วงโซ่อุปทาน

4.3.2 กำหนดมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ให้สอดคล้องตามนโยบายและแนวปฏิบัติ รวมทั้งขั้นตอนการดำเนินงานและมาตรฐานที่เกี่ยวข้อง

4.3.3 เฝ้าระวังและบำรุงรักษาสินทรัพย์สารสนเทศให้อยู่ในสภาพพร้อมใช้งาน และมีความมั่นคงปลอดภัยอย่างต่อเนื่อง

4.3.4 ติดตามกฎหมาย ระเบียบ ข้อกำหนดและมาตรฐานต่าง ๆ ที่เกี่ยวข้องและนำมาปรับปรุงมาตรการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ รวมทั้งติดตามดูแลการปฏิบัติตามมาตรการที่กำหนดอย่างสม่ำเสมอ

4.3.5 กำหนดเกณฑ์และวิธีการรายงานเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

4.3.6 สร้างความตระหนักรู้และให้คำแนะนำแก่บุคลากร และผู้มีส่วนได้เสียทั้งภายในและภายนอก ตลอดห่วงโซ่อุปทาน

4.3.7 จัดทำรายงานผลการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

4.4 พนักงาน

4.4.1 เรียนรู้ ทำความเข้าใจและปฏิบัติตามกฎ ระเบียบ ข้อบังคับ นโยบายและแนวปฏิบัติ

4.4.2 ดำเนินการและรายงานเหตุการณ์ความผิดปกติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ที่ส่งผลกระทบต่อการปฏิบัติหน้าที่หรือเหตุการณ์ที่เกิดขึ้นตามช่องทางที่บริษัทกำหนด

4.4.3 ร้องเรียนหรือแจ้งเบาะแสเมื่อพบกรณีกระทำผิดหรือการกระทำที่อาจเข้าข่ายฝ่าฝืนนโยบายฉบับนี้

5. แนวปฏิบัติ

5.1 ประเมินและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ตามบริบททางธุรกิจและครอบคลุมความเสี่ยงที่เกิดจากผู้มีส่วนได้เสียทั้งภายในและภายนอกตลอดห่วงโซ่อุปทาน

5.2 จัดทำกลยุทธ์การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ที่สอดคล้องกับวิสัยทัศน์ พันธกิจ วัตถุประสงค์ และระดับความเสี่ยงที่ยอมรับได้ของบริษัท

5.3 กำหนดแผนและมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์โดยครอบคลุมการระบุบริบทสภาพแวดล้อมขององค์กร (identification) การปกป้องสินทรัพย์สารสนเทศ (protection) การตรวจจับเหตุการณ์ผิดปกติ (detection) การรับมือเหตุการณ์ผิดปกติ (response) และการกู้คืนสินทรัพย์สารสนเทศจากความเสียหาย (recovery)

5.4 บริหารจัดการสินทรัพย์สารสนเทศของบริษัทที่ดำเนินการทั้งโดยบุคลากรภายในและบุคคลภายนอกให้มีความมั่นคงปลอดภัยในทุกขั้นตอนของวัฏจักรการพัฒนาระบบสารสนเทศ/ซอฟต์แวร์ (secure system / software development life cycle)

5.5 ปกป้องสารสนเทศและข้อมูลที่ส่งผ่านระบบและเทคโนโลยีสารสนเทศ ซึ่งรวมถึงข้อมูลส่วนบุคคลของบุคลากร ลูกค้า คู่ค้า และบริษัทที่รับจัดเก็บประมวลผล ให้ปลอดภัยจากการเข้าถึง นำไปใช้ ส่งต่อ แก้ไข ทำซ้ำ ดัดแปลง ลบ หรือทำลายโดยไม่ได้รับอนุญาต

5.6 ตรวจประเมินและปิดช่องโหว่ (vulnerability management) ของระบบและเทคโนโลยีสารสนเทศ รวมถึงดำเนินการปรับปรุงระบบให้มีความมั่นคงปลอดภัย (patch management) อย่างสม่ำเสมอ

5.7 เฝ้าระวัง (monitoring) และตรวจจับเหตุการณ์ความผิดปกติหรือเหตุการณ์ที่ละเมิดความมั่นคงปลอดภัยสารสนเทศและไซเบอร์หรือเหตุการณ์ที่ส่งผลต่อความต่อเนื่องในการดำเนินธุรกิจ รวมทั้งตรวจสอบมาตรการที่เกี่ยวข้องให้มีประสิทธิภาพอย่างต่อเนื่อง

5.8 จัดให้มีกระบวนการบริหารจัดการเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ รวมทั้งปรับปรุงกระบวนการให้มีประสิทธิภาพอย่างสม่ำเสมอ สามารถจำกัดขอบเขต แก้ไขบรรเทาผลกระทบและเยียวยา รวมถึงการกู้คืนการดำเนินธุรกิจและสินทรัพย์สารสนเทศอย่างทันท่วงที มีความมั่นคงปลอดภัย

5.9 สนับสนุนและร่วมมือกับองค์กรภาคเอกชน ภาครัฐ และภาคประชาสังคมทั้งในประเทศและต่างประเทศในด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

5.10 ส่งเสริมและสนับสนุนการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์แก่บุคลากร ลูกค้า คู่ค้า พันธมิตรและผู้มีส่วนได้เสียทั้งภายในและภายนอกตลอดห่วงโซ่อุปทาน

6. การฝึกอบรม

จัดให้มีการสื่อสารและถ่ายทอดนโยบายและแนวปฏิบัติด้านด้านความมั่นคงปลอดภัยสารสนเทศ ผ่านการฝึกอบรม การประชุม หรือกิจกรรมในรูปแบบต่าง ๆ ที่เหมาะสมให้แก่ กรรมการ ผู้บริหาร พนักงานและผู้มีส่วนได้เสียภายนอก ซึ่งรวมถึงคู่ค้า พันธมิตรทางธุรกิจ และสาธารณชน ตลอดห่วงโซ่อุปทาน รวมถึงจัดให้มีการประเมินประสิทธิผลหลังการฝึกอบรมทุกครั้ง

7. การแจ้งเบาะแส

ร้องเรียนหรือแจ้งเบาะแสเมื่อพบเห็นการกระทำที่เชื่อได้ว่าเป็นการละเมิดนโยบายและแนวปฏิบัตินี้ โดยปฏิบัติตามแนวทางของนโยบายและแนวปฏิบัติด้านการแจ้งเบาะแส ทั้งนี้ผู้ร้องเรียนหรือผู้แจ้งเบาะแสจะได้รับความคุ้มครองและข้อมูลจะถูกเก็บเป็นความลับ โดยไม่มีผลต่อตำแหน่งงาน ทั้งในระหว่างดำเนินการสอบสวนและหลังเสร็จสิ้นกระบวนการ

8. การขอคำแนะนำ

ในกรณีที่มีข้อสงสัยว่าการกระทำนั้นอาจฝ่าฝืนกฎหมาย ระเบียบนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ สามารถขอคำแนะนำจากผู้บังคับบัญชา หน่วยงานหรือบุคคลผู้รับผิดชอบ ด้านกำกับการปฏิบัติตามกฎเกณฑ์ ด้านระบบและเทคโนโลยีสารสนเทศ และด้านงานกฎหมายก่อนตัดสินใจหรือดำเนินการใด ๆ

9. บทลงโทษ

ในกรณีที่เกิดการสอบสวน พนักงานทุกคนต้องให้ความร่วมมือกับหน่วยงานภายในและภายนอกอย่างเต็มที่ ทั้งนี้หากผู้บริหารและพนักงานกระทำการใด ๆ ที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายฉบับนี้ไม่ว่าทางตรงหรือทางอ้อม ผู้บริหารและพนักงานจะถูกพิจารณาโทษทางวินัยตามระเบียบข้อบังคับการทำงาน

10. กฎหมาย กฎระเบียบและนโยบายที่เกี่ยวข้อง

10.1 กฎหมายที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

10.2 กฎหมายที่เกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

10.3 กฎหมายที่เกี่ยวกับคุ้มครองข้อมูลส่วนบุคคล

10.4 กฎหมายที่เกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

10.5 มาตรฐานด้านความปลอดภัย ISO 27001 (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

10.6 กรอบความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Framework : CSF) ของ National Institute of Standards and Technology (NIST)

10.7 กรอบ Control Objectives for Information and Related Technologies (COBIT) ของ ISACA และ IT Governance Institute

10.8 CIS Controls ของศูนย์รักษาความปลอดภัยอินเทอร์เน็ต (Center for Internet Security: CIS)

10.9 กรอบการประเมินด้านไซเบอร์ (The Cyber Assessment Framework : CAF) ของศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติของสหราชอาณาจักร (National Cyber Security Centre : NCSC)

11. ภาคผนวก

นโยบายและแนวปฏิบัตินี้ ประกอบด้วยภาคผนวก ดังต่อไปนี้

11.1 ภาคผนวก ก คำนิยาม

ภาคผนวก ก
คำนิยาม

1. **การควบคุม (Control)**

   วิธีการจัดการ การปฏิบัติงาน หรือเทคนิคใด ๆ ที่ใช้ในการจัดการความเสี่ยง ซึ่งถูกออกแบบมาเพื่อติดตามและวัดผลตามมาตรฐานเฉพาะด้านนั้น ๆ เพื่อให้บริษัทสามารถบรรลุเป้าหมายหรือวัตถุประสงค์ที่กำหนดไว้

2. **ความปลอดภัย (Safety)**

   การลดความเสี่ยงที่เกี่ยวกับเทคโนโลยี ซึ่งอาจมีความผิดพลาดหรือถูกควบคุมโดยผู้ประสงค์ร้ายที่ก่อให้เกิดความเสียหายต่อบุคคลและสินทรัพย์

3. **ความมั่นคงปลอดภัย (Security)**

   กระบวนการและการกระทำใด ๆ เช่น การป้องกัน การเข้มงวดกวดขัน การระมัดระวัง การเอาใจใส่ในการใช้งาน และการดูแลรักษาสินทรัพย์สารสนเทศที่สำคัญให้พ้นจากความพยายามใด ๆ ทั้งจากบุคลากรภายในและจากบุคคลภายนอก ในการเข้าถึงเพื่อโจรกรรม ทำลาย ทำให้เสียหาย หรือแทรกแซงการทำงานจนเป็นเหตุให้การดำเนินธุรกิจของบริษัทได้รับความเสียหาย โดยมีหลักการดังนี้

   - ความลับ (confidentiality) การปกป้องความลับของสินทรัพย์สารสนเทศ โดยป้องกันการเข้าถึงและการเปิดเผยจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลที่เป็นกรรมสิทธิ์ของบริษัท
   - ความถูกต้องครบถ้วน (integrity) การทำให้มั่นใจว่าสินทรัพย์สารสนเทศต้องไม่มีการแก้ไขดัดแปลง หรือทำลายโดยผู้ที่ไม่ได้รับอนุญาต
   - ความพร้อมใช้งาน (availability) การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงสินทรัพย์สารสนเทศและบริการผ่านระบบทั้งออนไลน์และออฟไลน์ได้อย่างรวดเร็วและเชื่อถือได้
   - ภาระรับผิดชอบ (accountability)
     การรับผิดชอบในผลของการกระทำ การสั่งการ การมอบหมาย และการตัดสินใจตามบทบาทหน้าที่ของตนเอง

- การพิสูจน์ตัวตน (authentication) การทำให้มั่นใจว่าสิทธิในการเข้าใช้งานสินทรัพย์สารสนเทศต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น
- การกำหนดสิทธิ (authorization) การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานสินทรัพย์สารสนเทศเป็นไปตามความจำเป็น (least privilege) และสอดคล้องกับความต้องการขั้นพื้นฐาน (need to know basis) ตามที่ได้รับอนุญาต
- การห้ามปฏิเสธความรับผิดชอบ (non-repudiation) การทำให้มั่นใจว่าผู้มีส่วนร่วมที่เกี่ยวข้องในการทำธุรกรรมไม่สามารถปฏิเสธได้ว่าไม่มีส่วนเกี่ยวข้องกับการทำธุรกรรมที่เกิดขึ้น

4. **ความมั่นคงปลอดภัยในวัฏจักรการพัฒนาระบบสารสนเทศ/ซอฟต์แวร์ (Secure System/Software Development Life Cycle)**

   การกำหนดกระบวนการ มาตรการ และข้อกำหนดด้านความมั่นคงปลอดภัยให้เป็นส่วนหนึ่งของทุกขั้นตอนในวัฏจักรการพัฒนาระบบสารสนเทศ/ซอฟต์แวร์ ซึ่งครอบคลุมตั้งแต่การรวบรวมความต้องการ การออกแบบ การจัดหา การพัฒนา การทดสอบ การใช้งานและบำรุงรักษา รวมถึงการยกเลิกการใช้งาน

5. **ความเสี่ยง**

   ผลกระทบเชิงลบที่เกิดจากเหตุการณ์ไม่แน่นอนต่อการบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน

6. **ไซเบอร์**

   ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

7. **เทคโนโลยีสารสนเทศ (Information Technology)**

   การประยุกต์ใช้เทคโนโลยีด้านคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ เครือข่ายด้านโทรคมนาคม และการสื่อสาร เพื่อค้นหา จัดเก็บ วิเคราะห์ ประมวลผล จัดส่ง กระจายออก ติดตาม รวบรวม และจัดการสารสนเทศต่าง ๆ ของบริษัท

8. **ผู้มีส่วนได้เสีย (ภายในและภายนอก)**

บุคคล กลุ่มบุคคล หรือหน่วยงานที่ได้รับผลกระทบจากการดำเนินงานของบริษัท ประกอบด้วยผู้มีส่วนได้เสียภายใน ได้แก่ กรรมการ ผู้บริหารและพนักงาน และผู้มีส่วนได้เสียภายนอก ได้แก่ ลูกค้า ผู้บริโภค คู่ค้าธุรกิจ พันธมิตรทางธุรกิจ ผู้ถือหุ้น นักลงทุน ชุมชน สังคม ภาครัฐ องค์กรพัฒนาเอกชน สื่อมวลชน คู่แข่งการค้าและเจ้าหนี้

9. **พนักงาน (Employee)**

พนักงานในระดับรองลงมาจากระดับผู้บริหารของบริษัทที่ได้รับการว่าจ้างให้เป็นพนักงานประจำ พนักงานทดลองงาน หรือพนักงานสัญญาจ้างพิเศษที่อยู่ภายใต้สัญญาจ้างของบริษัท

10. **มาตรการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (Information and Cyber Security Measures)**

มาตรการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์แบ่งเป็น 5 ด้าน โดยครอบคลุมหัวข้อต่างๆ ดังนี้

- **การระบุสภาพแวดล้อมขององค์กร (identification)** ประกอบด้วย ธรรมาภิบาล (governance) การบริหารจัดการความเสี่ยง (risk management) การกำกับการปฏิบัติตามกฎเกณฑ์ (compliance) ความมั่นคงปลอดภัยด้านบุคลากร (human resource security) การบริหารจัดการความเสี่ยงในห่วงโซ่อุปทาน (supply chain risk management)
- **การปกป้องสินทรัพย์สารสนเทศ (protection)** ประกอบด้วย การบริหารจัดการสินทรัพย์สารสนเทศ (asset management) การควบคุมการเข้าถึงและการใช้งาน (access control) ความมั่นคงปลอดภัยในวัฏจักรการพัฒนาระบบสารสนเทศ/ซอฟต์แวร์ (secure system/software development life cycle) การจัดการเข้ารหัสลับ (cryptographic management) ความมั่นคงปลอดภัยในการปฏิบัติงาน (operations security) การบริหารจัดการการเปลี่ยนแปลง (change management) การบริหารจัดการขีดความสามารถด้านสารสนเทศ (capacity and performance management) ความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (physical and environmental security) การบริหารจัดการการสื่อสารและการใช้งานระบบเครือข่าย (communication and network management)
- **การตรวจจับเหตุการณ์ผิดปกติ (detection)** ประกอบด้วย การบันทึกและการเฝ้าระวัง (log monitoring) การบริหารจัดการภัยคุกคาม (threat management)

- **การรับมือเหตุการณ์ผิดปกติ (response)** ประกอบด้วย การบริหารจัดการเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (information and cyber security incident management)
- **การกู้คืนสินทรัพย์สารสนเทศจากความเสียหาย (recovery)** ประกอบด้วย การบริหารความต่อเนื่องทางธุรกิจ (business continuity management) และการกู้คืนสินทรัพย์สารสนเทศจากความเสียหายให้กลับมาดำเนินการได้ตามปกติ (disaster recovery)

11. ระบบ (System)

สินทรัพย์ประเภทระบบหรือเครือข่ายที่สามารถกำหนด จำกัดขอบเขต และจัดการได้ รวมถึง คอมพิวเตอร์ เวิร์กสเตชัน แล็ปท็อป เซิร์ฟเวอร์ เราเตอร์ สวิตช์ ไฟร์วอลล์ อุปกรณ์สื่อสารแบบพกพา และเทคโนโลยีสารสนเทศอื่น ๆ เป็นต้น

12. สารสนเทศ (Information)

ข้อมูลของบริษัทที่ผ่านการประมวลผล วิเคราะห์ คำนวณ และมีการแปลความหมายที่อาจสามารถเข้าถึง ค้นหา หรือเรียกใช้งานผ่านระบบเครือข่ายอิเล็กทรอนิกส์หรือเทคโนโลยีการประมวลผลข้อมูลอิเล็กทรอนิกส์ต่าง ๆ ซึ่งอยู่ในทั้ง 2 รูปแบบ คือ

1. ข้อมูลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ (Electronic information) ที่จัดเก็บอยู่ในระบบคอมพิวเตอร์ หรือเกิดจากการให้บริการและการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต โครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน เช่น เอกสารอิเล็กทรอนิกส์ ฐานข้อมูล สื่อหรือไดรฟ์ที่สามารถถอดออกได้ เครื่องมือที่ช่วยในการทำงานร่วมกัน เป็นต้น
2. ข้อมูลที่อยู่ในรูปแบบทางกายภาพ (Physical information) เช่น เอกสารที่พิมพ์ออกมา เป็นต้น

13. สินทรัพย์สารสนเทศ (Information Asset)

สารสนเทศ และระบบ รวมถึง ซอฟต์แวร์ แอปพลิเคชัน บริการ หรือทรัพยากรทางด้านสารสนเทศอื่น ๆ ที่สนับสนุนการดำเนินธุรกิจ และมีมูลค่าทางเศรษฐกิจต่อบริษัท

14. เหตุละเมิดความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (ทั้งภายนอกและภายใน)

สถานการณ์หรือเหตุการณ์ใด ๆ ที่อาจส่งผลกระทบในทางลบต่อการปฏิบัติการหรือ สินทรัพย์สารสนเทศของบริษัท บุคคล หรือองค์กรอื่นผ่านการเข้าถึงสินทรัพย์สารสนเทศ การทำลาย การเปิดเผย การแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต และ/หรือการทำให้ไม่สามารถให้บริการได้