Information Management

Policy and Guidelines

Siam Land Flying Co., Ltd.

SIAM LAND FLYING

Contents

Information Management Policy and Guidelines

Siam Land Flying Co., Ltd.

1. Intent

Information is a vital asset to Siam Land Flying (SLF). Complete and reliable information could contribute to better business decision-making and to an increase in a company's competitiveness. Therefore, it is necessary to ensure that SLF systematically manage information controls in order to maximize the utility of all available data, while also reducing asset risk and loss of confidential information.

2. Scope

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

3. Objective

For directors, management and staff to understand their roles and responsibilities in preventing the misuse of information and information systems.

4. Roles and Responsibilities

For directors, management, and staff to use as a basic guideline for effective coordination between company functions.

4.1 Board of Directors

4.1.1 Ensure that the Information Management Policy and Guidelines are in place.

4.1.2 Ensure that the policy and guidelines are properly implemented.

4.2 Management

4.2.1 Establish rules and procedures to suit the nature of business while remaining consistent with the Policy and Guidelines of SLF in addition to the laws and regulations in countries where the company operates.

4.2.2 Ensure that the organizational structure and related functions are in place.

4.2.3 Delegate users' access rights to information and information systems.

4.2.4 Ensure that there is effective information risk management.

4.2.5 Ensure the reporting of policy compliance, as well as reporting of any information mismanagement

4.3 **Department/person designated as the information asset owner**

4.3.1 Comply with guidelines in Section 5.2 Risk Management.

4.3.2 Comply with guidelines in Section 5.3 Information Management.

4.3.3 Comply with guidelines in Section 5.4 Disclosure of Information to External Parties

4.3.4 Comply with guidelines in Section 5.8 Information Disposal.

4.3.5 Prepare policy compliance reports and compile any arising problems concerning the use information for management.

4.4 **Information Technology department**

4.4.1 Ensure that all information systems and devices are well maintained.

4.4.2 Maintain the company's information systems access controls.

4.4.3 Maintain the company's information security.

4.4.4 Ensure that data backup and data recovery procedures are correctly followed.

4.5 **Internal Audit department**

4.5.1 Audit information management procedures to ensure adherence to this policy.

4.5.2 Provide advice and guidance to management and staff to ensure compliance with this policy.

4.6 **Staff**

4.6.1 Protect the confidentiality of personal information as well as confidential information owned by SLF, customers, suppliers and business partners.

4.6.2 Prepare accurate and reliable information, records and reports.

4.6.3 Protect intellectual property ("IP") rights of SLF and not infringe on IP rights of others'.

4.6.4 Comply with this Policy and Guidelines, related international laws and standards.

5. Guidelines

5.1 All directors, management and staff are advised to follow Mason's Four Ethical Issues of the Information Age (PAPA: Privacy, Accuracy, Property and Accessibility) regarding the ethical use of information. The four components of this model are as follows:

5.1.1 Information Privacy

Personal information includes National Identification card number, date of birth, and account information (ID and passwords)

1) Maintain confidentiality and security of personal information of all directors, management, staff, customers, suppliers and business partners.
2) Do not use customer information from any source for marketing purposes, as well as selling customer databases to other companies.
3) All directors, management and staff are required to keep their account and password information related to SLF's information systems private and unique.
4) Passwords must not be written down in any manner that would allow anyone other than the authorized user access, as well as making passwords easy to decipher.
5) In instances when the authorized user needs to share their password, such as for information systems maintenance, the user must change his or her password at the earliest opportunity

5.1.2 Information Accuracy

1) In order for information to remain accurate and reliable, data should be validated for accuracy before adding into the database. This converted information should be updated for any new changes.
2) Source of information must be reliable and verifiable i.e. government agencies and other trusted organizations.

5.1.3 Information Property

1) SLF formally own all intellectual property created by directors, management and staff at and/or for the company over the course of work performed, whether partially or completed.
2) Any copyright and IP infringement or unauthorized disclosure of any work produced within SLF's premises is forbidden.
3) Any unauthorized usage, reproduction, printing, public release and installing pirated or copyright infringed software on SLF information systems is forbidden.
4) SLF's employees must be cautious of downloading any software on the internet, including updating any existing software. Any software used in SLF information systems must not violate any existing copyrights or intellectual properties of other companies
5) Protect SLF's intellectual properties and do not reveal them without proper permission.
6) Whenever any intellectual property owned by SLF is used, employees are required to use the seal or display the trademark service mark or copyright symbol. For example, using ®, ™, © (201X), etc.
7) Employees are required to inform their business unit/department of any new discoveries, inventions (such as computer programs, technological inventions and other innovations), as well as proprietary information.
8) Assist in acquiring patents, copyrights and protected trademarks for SLF's newly discovered or invented intellectual properties.

5.1.4 Data Accessibility

1) All individual information systems (include computers, applications, email servers, wireless LAN, internet) owned by SLF must have configured user access rights by the responsible manager in accordance to the employees' assigned tasks and responsibilities.
2) Review information and information system access rights annually, or when necessary access rights changes are made, such as promotions, where the promoted employee should have his or her access rights adjusted to match their new tasks and responsibilities.
3) Only management are authorized to make any changes within the information system access rights.
4) Record details of access to information and information systems, including any historical changes to access rights. Any authorized and

unauthorized access should be recorded for evidence and potential forthcoming investigations

5) Record and monitor SLF's information systems usage and remain wary of any potential unauthorized security breaches.

5.2 Information Risk Management

5.2.1 Identify and assess information risks.

5.2.2 Prioritize risks based on importance, and identify key risks that need to be addressed first.

5.2.3 Determine and implement risk management measures.

5.3 Information Management

5.3.1 Classification of Information: each batch of information, in the form of electronic files and printed documents, should be categorized by impact from any possible level of security risk. SLF's information is classified into the following 4 categories:

1) **Special Control** [Purple] is information that can seriously affect business strategy and severely damage SLF's market competitiveness, in the event the information is leaked and could cause extensive damage to SLF's international reputation.

Examples of information falling under this category include:

- Trade Secret
- Business strategies
- Market strategies / product development
- Merger plans

2) **Confidential** [Red] is information that may cause significant impact to SLF and business units and potential growth if leaked, may subject business unit to lawsuits. Any leaks of this level can cause damage to SLF's domestic reputation.

Examples of information falling under this category include:

- Yet to be published marketing information
- Personal information
- Customer information

3) **Internal Use Only** [Yellow] is information that can only be used internally within SLF. These documents affect daily operations and can cause damage to SLF if leaked.

Examples of information falling under this category include:

- Internal announcements / Policies
- Regulations / Operations Manual
- Daily records of activities

4) **Public** [Green] is information considered not having an impact on the organization if leaked, and can be disclosed to third parties.
Examples of information falling under this category include:
   - Sustainability reports
   - Public announcements
   - Marketing promotions

In addition, any full or partial reproductions of documents/prints shall have the same confidentiality level as the original.

5.3.2 Safe Storage of Information & Storage Devices

1) Management and information asset owners determine the duration of information storage based on their confidentiality levels.
2) Use removable media storage devices to back up information, and must be set up to record and display software type, date, backup time and person responsible for backing up.
3) Ensure the security and safekeeping of SLF's Information Systems and other devices containing SLF's information (mobile phones, laptops and tablets); particularly outside the workplace. In addition, portable information systems should be stored within provided lockers or cabinets.
4) Use a password-protected screen lock when leaving information systems containing SLF's information unattended.
5) Report to the IT Department immediately when any of SLF's information system and any removable storage device containing confidential information is lost or stolen.

5.3.3 Bring Your Own Device

Mobile devices are essential in business communications and improving staff productivity. In addition to the increased use of mobile devices, directors, management and staff are requesting the option of connecting their own mobile devices to their business unit network. Therefore, approving personal mobile devices and applications is at the discretion of each company.

Directors, management and staff utilizing personal mobile devices must agree to the following:

1) All intellectual property created within the devices resulting from work remains the property of SLF.
2) Present their laptops to the IT Department for configuration and installing of standard apps before being able to access the network.
3) All mobile devices must be password-protected in order to prevent unauthorized access to any files owned by SLF. In addition, devices must not be left unattended on public premises.
4) Regularly backup all files on their device regarding any data related to SLF.
5) Notify the respective Company when the device containing company information is lost or stolen.
6) Employees are personally responsible for all costs associated with his or her device.
7) Assume full liability for risks including, but not limited to, the partial or complete loss of SLF's files and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
8) Hand in or destroy all of SLF's files upon termination of employment.
9) SLF reserves the right to disconnect devices from the network or disable services without prior notice.

5.3.4 Backing Up Information

1) Ensure that there are data backup and recovery processes, both in software and physical forms. Procedures must be written to accommodate both forms.
2) Back up documents contained in SLF's information systems and hard drives in removable media storage devices, as well as steps to recover the files within them. Examples include universal serial bus drives (USB drives), external hard drives and CDs. Information contained in these devices should be up-to-date.
3) Ensure the security and safekeeping of removable media storage devices, must be examined for testing at least annually, in addition to maintaining back up files.

5.3.5 Use data encryption to prevent any unauthorized usage or access while exchanging Special Control and Confidential information between companies/ departments.

5.4 Disclosure of information to external parties

5.4.1 In the event where Special Control or Confidential information is to be disclosed to third parties or initially unauthorized persons, the information must be verified by the owner and approved by management, in addition to both parties signing a non-disclosure agreement (NDA).

5.4.2 Use data encryption to prevent any unauthorized usage or access while sending Special Control and Confidential information to external parties.

5.5 Internet Usage

5.5.1 Do not use corporate internet during work hours for personal business use.

5.5.2 Do not use corporate internet for any activities that may constitute copyright infringement. For example, downloading programs, music, films, photos or statements of others for monetary gain without the owners' permission.

5.5.3 Do not use corporate internet for any activities that violates SLF's Code of Conduct.

5.5.4 Do not use corporate internet in ways that may slow down corporate internet speeds of other users, i.e. downloading an excessively large number of files.

5.6 Email Usage

5.6.1 Do not send any email while faking sources, in a manner that interferes with the recipient's normal utilization of their information system.

5.6.2 Do not send any email in a manner that disturbs the recipient or contains inappropriate content (including illegal content, intimidation, harassment, abusive content, inciting violence, and supporting illegal activity).

5.6.3 Employees must be careful when opening email attachments. Spam mails can introduce malware or trick the recipient into giving up confidential information (phishing). This applies to emails from unfamiliar addresses. Immediately report any suspicious email sources to the IT Department.

5.6.4 Employees must be careful when opening links from any source of communication, which may contain malware such as viruses, spyware and trojans.

5.6.5 Do not use the 'Blind Carbon Copy' or Bcc function to conceal parts of the recipients when sending business emails.

5.6.6 Employees must use email signatures and include them in all outgoing business emails.

5.6.7 Use personal email accounts (Gmail, Yahoo Mail) outside working hours or during lunch breaks.

5.7 Social Media

For further details, please refer to SLF's Social Media Policy and Guidelines.

5.8 Information Disposal

5.8.1 Special Control, Confidential and Internal Use Only documents that are printed must be properly disposed when not needed through depositing in designated disposal bins. Public documents can be disposed in the garbage bins or through paper shredders.

5.8.2 When disposing of removable media storage devices, transfer confidential information out of them first, if possible.

5.9 Detecting and Tracing Information Leaks

In the event of Special Control and Confidential information leaks, the responsible manager must appoint an investigative committee. The committee is required to properly investigate the source and cause of the leaks, as well as make improvements to information management procedures to prevent similar cases from occurring, and finally report the investigation back to management.

6. Training

The Company shall communicate the Information Management Policy and Guidelines and cascade it through training programs, conferences, and other appropriate channels to its directors, management, and staff. The effectiveness of such training and communications programs shall be evaluated on a regular basis.

7. Whistleblowing

In case a violation of this Information Management Policy and Guidelines is found, a report must be filed by following the procedure stated in the Whistleblowing Policy and Guidelines. The

information of complainant or whistleblower will be protected and the information will be kept confidential during the investigation and after the completion of the investigation process.

8. Policy Advice

In case of suspicion on the action that may violate laws, regulations and this Information Management Policy and Guidelines, the employee can seek advice from her or his supervisors; team or persons responsible for information management within the Company, the Compliance Department or Legal Department before making any decision or carrying out any action.

9. Penalties

In the event of an investigation, all employees must fully cooperate with internal and external entities. If an employee violates or fails to comply with this Policy and Guidelines, either directly or indirectly, the employee will be subject to disciplinary action in accordance with Company's regulations.

10. Related Laws, Regulations and Policies

10.1 Thailand's Computer Crime Act, B.E. 2550

10.2 Thailand's Copyright Act, B.E. 2561

10.3 Charoen Pokphand Group's Social Media Policy and Guidelines

10.4 ISO/IEC 27001:2013 or the Information Security Management System (ISMS)

11. Appendices

The following appendices are attached to this Policy and Guidelines:

11.1 Appendix A: Examples of document covers based on confidentiality

11.2 Appendix B: Examples of document prints based on confidentiality

Appendix A

Examples of document covers based on confidentiality

SPECIAL CONTROL

SIAM LAND FLYING

Disclosure of this special control document will have an impact on the organization's business strategy, resulting in serious competitive disadvantage in business which will damage the organization's reputation on an international level.

Responsibilities of the holder of this special control document

1. The holder of this document is responsible for its safekeeping.
2. This document must be protected from unauthorized disclosure. It must not be left alone unattended except in a safe and secure place.
3. This document can only be disclosed to persons who have been authorized to know its contents.

Storage

When not in use, the document must be kept in a package or in a folder with "SPECIAL CONTROL" marked on the cover, and stored under lock and key in a safe that is located in a controlled area with restricted access except for authorized persons.

Duplication

This confidential document cannot be copied, separated, or reproduced in whole or in part without permission.

Disposal

This document can only be disposed of by using a document shredder. All other disposal methods are not allowed.

(THIS COVER PAGE WILL NOT BE TREATED AS CONFIDENTIAL WHEN SEPARATED FROM THE DOCUMENT)

CONFIDENTIAL

SIAM LAND FLYING

Disclosure of this confidential document will have an impact on the organization's business and future. It may result in a lawsuit for damages which will affect the organization's reputation on a national level.

Responsibilities of the holder of this confidential document

1. The holder of this document is responsible for its safekeeping.
2. This document must be protected from unauthorized disclosure. It must not be left alone unattended except in a safe and secure place.
3. This document can only be disclosed to persons who have been authorized to know its contents.

Storage

When not in use, the document must be kept in a package or in a folder with "CONFIDENTIAL" marked on the cover, and stored under lock and key in a filing cabinet that is located in a controlled area with restricted access except for authorized persons.

Duplication

This confidential document cannot be copied, separated, or reproduced in whole or in part without permission.

Disposal

This document can only be disposed of by using a document shredder. All other disposal methods are not allowed.

FOR INTERNAL USE ONLY

SIAM LAND FLYING

The disclosure of documents for internal use only will have an impact on the organization's daily operations which can result in reputational damage. The contents of this document are only permitted to be used internally within the work unit.

Responsibilities of the holder of this document

1. The holder of this internal use only document is responsible for its safekeeping.
2. This document must be protected from unauthorized disclosure. It must not be left alone unattended except in a safe and secure place.
3. This document can only be disclosed to persons who have been authorized to know its contents by nature of their work duties and/or responsibilities.

Storage

When not in use, the document must be kept in a package or in a folder with "CONFIDENTIAL" marked on the cover, and stored under lock and key in a filing cabinet

Duplication

This internal use only document can be copied, separated, or reproduced in whole or in part only with permission from an authorized person.

Disposal

This document can only be disposed of by using a document shredder. All other disposal methods are not allowed.

(This cover page will not be treated as confidential when separated from an internal use only document)

PUBLIC DOCUMENT

The contents of this document have been reviewed and can be disclosed to external parties without having an impact on the organization.

Responsibilities of the holder of this document
The holder of this document can disclose its contents to the public whenever deemed appropriate.

Storage
When not in use, the document must be kept in a package or in a folder with "PUBLIC DOCUMENT" marked on the cover and stored in a filing cabinet.

Duplication
This public document can be copied, separated, or reproduced in whole or in part whenever deemed appropriate.

Disposal
The document can be disposed of in the garbage or by using a document shredder

(THIS COVER PAGE IS NOT TREATED AS CONDIENTIAL)

Appendix B

Examples of document prints based on confidentiality

SPECIAL CONTROL

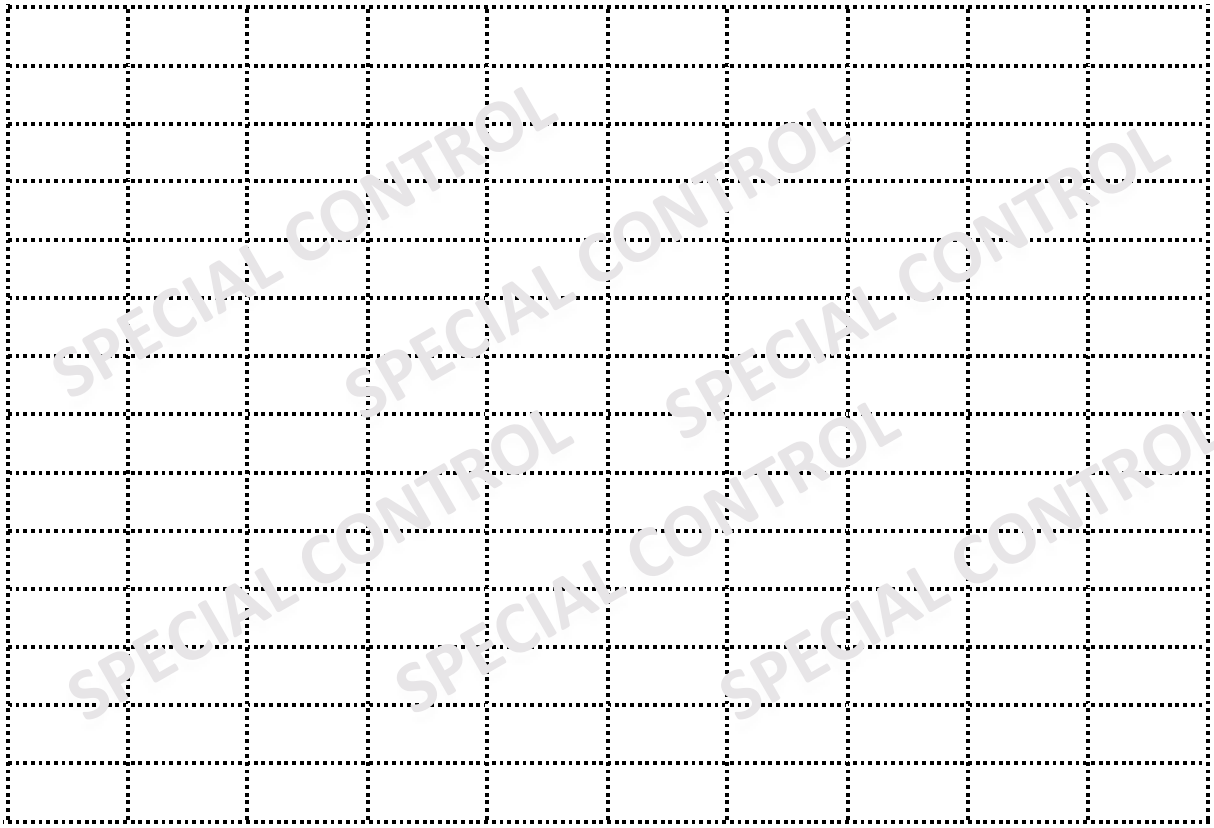
SPECIAL CONTROL

Page 1 of .....

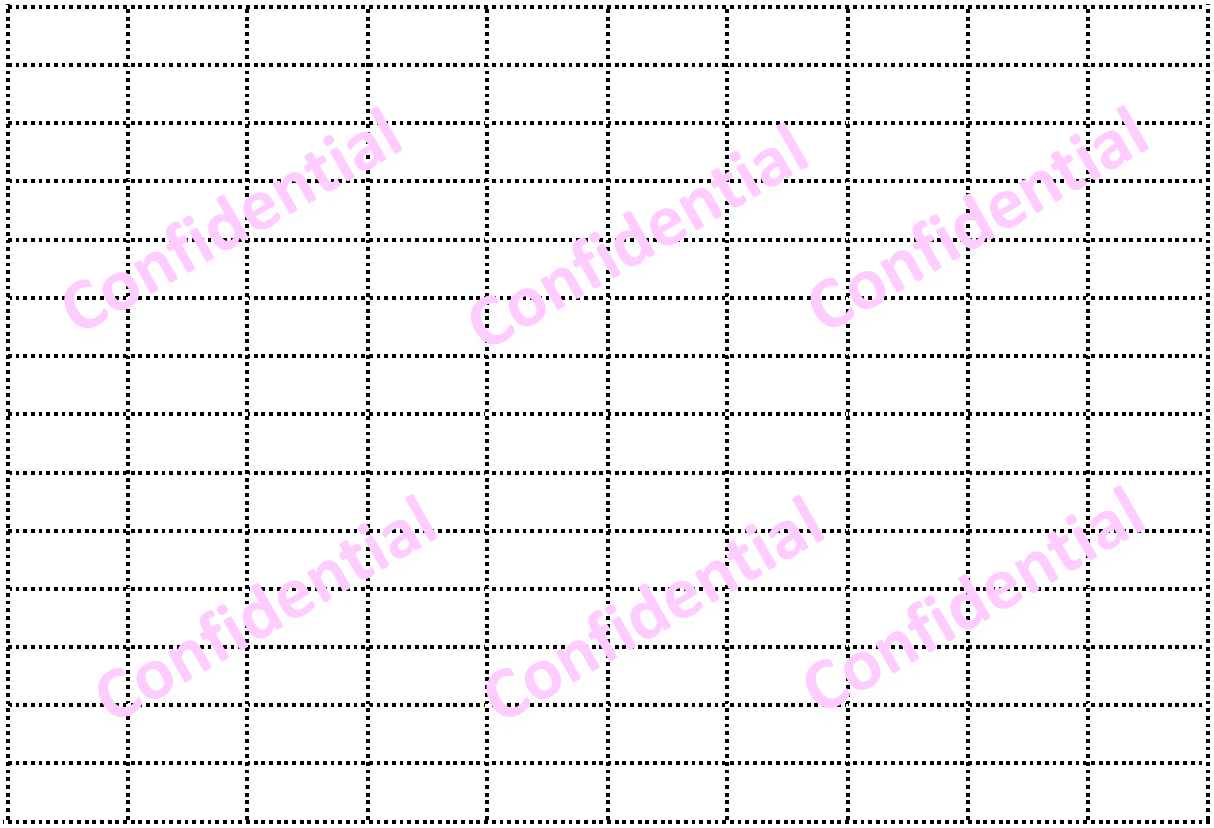
CONFIDENTIAL

CONFIDENTIAL

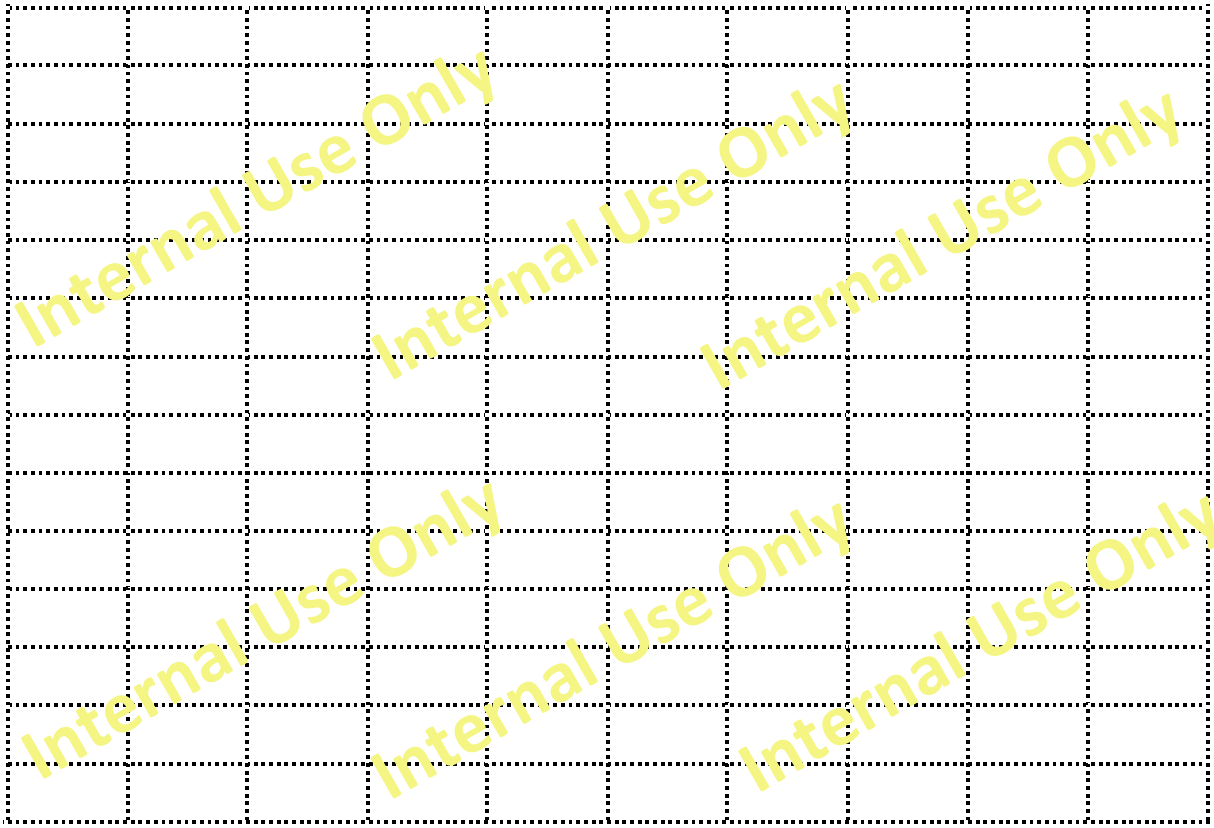
Page 1 of .....



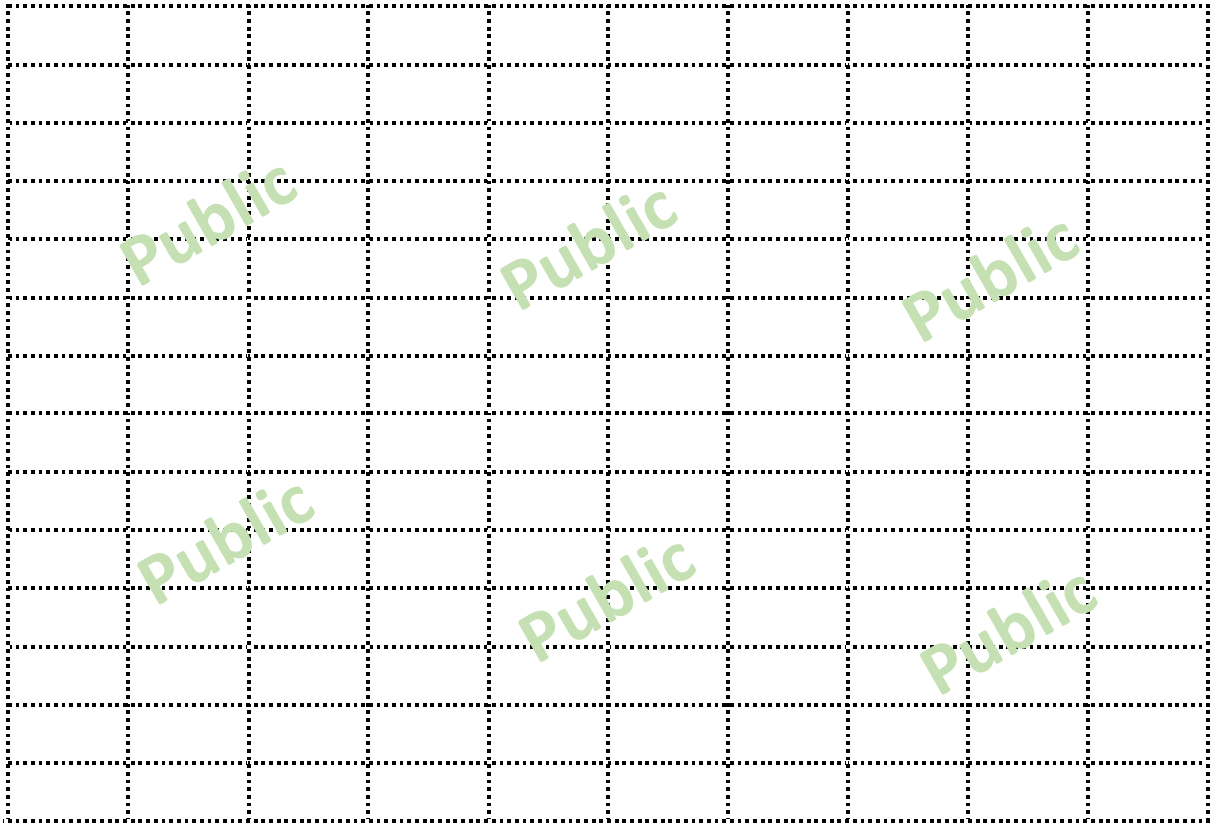
SPECIAL CONTROL



CONFIDENTIAL



Internal Use Only



Public

นโยบายและแนวปฏิบัติ
ด้านการบริหารจัดการข้อมูลสารสนเทศ
บริษัท สยามแลนด์ ฟลายอิ้ง จำกัด

สารบัญ

นโยบายและแนวปฏิบัติด้านการบริหารจัดการข้อมูลสารสนเทศ
บริษัท สยามแลนด์ ฟลายอิ้ง จำกัด

1. ความสำคัญ

ข้อมูลสารสนเทศถือเป็นสินทรัพย์ที่มีค่าของบริษัท สยามแลนด์ ฟล่ายอิ้ง จำกัด จึงต้องมีการกำกับดูแลข้อมูลสารสนเทศอย่างเป็นระบบและมีประสิทธิภาพ มีความน่าเชื่อถือถูกต้องสมบูรณ์ ซึ่งเป็นการป้องกันความเสี่ยงจากความเสียหาย ปกป้องทรัพย์สินของบริษัท และช่วยลดการสูญหายของข้อมูล ส่งผลให้การตัดสินใจทางธุรกิจมีประสิทธิภาพรวมถึงเพิ่มขีดความสามารถทางการแข่งขัน

2. ขอบเขตนโยบาย

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

3. วัตถุประสงค์

เพื่อให้บุคลากรเข้าใจบทบาทหน้าที่และร่วมกันปกป้องข้อมูลสารสนเทศของบริษัทมิให้รั่วไหลหรือนำข้อมูลไปใช้ในทางที่ผิด

4. หน้าที่และความรับผิดชอบ

สำหรับบุคลากรใช้เป็นแนวทางในการประสานงานภายในบริษัท

4.1 คณะกรรมการบริษัท

4.1.1 กำหนดให้มีนโยบายและแนวปฏิบัติด้านการบริหารจัดการข้อมูลสารสนเทศ

4.1.2 กำกับดูแลให้มีการนำนโยบายและแนวปฏิบัติไปปฏิบัติอย่างเป็นรูปธรรม

4.2 ผู้บริหาร

4.2.1 จัดให้มีระเบียบปฏิบัติให้เหมาะสมกับบริบทของแต่ละบริษัท โดยให้สอดคล้องกับบริบทของบริษัท และข้อกำหนดกฎหมายของแต่ละประเทศที่บริษัทดำเนินธุรกิจ

4.2.2 จัดให้มีโครงสร้างผู้รับผิดชอบ เช่น หน่วยงาน หรือบุคคลผู้รับผิดชอบเพื่อดูแลข้อมูลและระบบสารสนเทศ

4.2.3 กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศ

4.2.4 มั่นใจว่ามีการบริหารความเสี่ยงจากการใช้ข้อมูลสารสนเทศ

4.2.5 มั่นใจว่ามีการรายงานผลการปฏิบัติงานตามนโยบายฯ รวมถึงรายงานปัญหาจากการใช้ข้อมูลสารสนเทศ

4.3 **หน่วยงาน/บุคคลผู้รับผิดชอบดูแลข้อมูลและระบบสารสนเทศ**

4.3.1 ปฏิบัติตามแนวปฏิบัติ ข้อ 5.2 การบริหารจัดการความเสี่ยง

4.3.2 ปฏิบัติตามแนวปฏิบัติ ข้อ 5.3 การบริหารจัดการข้อมูลสารสนเทศ

4.3.3 ปฏิบัติตามแนวปฏิบัติ ข้อ 5.4 การแลกเปลี่ยนข้อมูลสารสนเทศกับบุคคลภายนอก

4.3.4 ปฏิบัติตามแนวปฏิบัติ ข้อ 5.8 การทำลายข้อมูลสารสนเทศ

4.3.5 รายงานผลการปฏิบัติงานตามนโยบายและแนวปฏิบัติ และระเบียบปฏิบัติ รวมถึงรายงานปัญหาจากการใช้ข้อมูลสารสนเทศ

4.4 **ฝ่ายเทคโนโลยีสารสนเทศ**

4.4.1 ดูแลรักษาเทคโนโลยีสำหรับระบบข้อมูลสารสนเทศ

4.4.2 ควบคุมการเข้าถึงระบบข้อมูลสารสนเทศและเครือข่าย

4.4.3 รักษาความปลอดภัยของข้อมูลสารสนเทศ

4.4.4 จัดให้มีการเก็บสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง

4.5 **หน่วยงานตรวจสอบภายใน**

4.5.1 ตรวจสอบให้มีการบริหารจัดการข้อมูลสารสนเทศตามนโยบายฯ

4.5.2 ให้คำแนะนำและให้ความรู้แก่บุคลากรเพื่อให้เกิดการปฏิบัติตามนโยบายฯ

4.6 **พนักงาน**

4.6.1 รักษาความลับและปกป้องความปลอดภัยของข้อมูลส่วนตัว รวมทั้งข้อมูลสารสนเทศของเครือเจริญโภคภัณฑ์ ลูกค้าและคู่ค้าธุรกิจและพันธมิตรทางธุรกิจ

4.6.2 จัดทำข้อมูลสารสนเทศ บันทึกและรายงานให้มีความถูกต้อง น่าเชื่อถือ

4.6.3 ปกป้องทรัพย์สินทางปัญญาของบริษัท และไม่ละเมิดสิทธิในทรัพย์สินทางปัญญาของผู้อื่น

4.6.4 ปฏิบัติตามนโยบายฯ กฎหมาย และมาตรฐานสากลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลสารสนเทศ

5. แนวปฏิบัติ

5.1 ให้ปฏิบัติตามแนวทางตามมาตรฐานสากลเกี่ยวกับการใช้เทคโนโลยีสารสนเทศซึ่งประกอบด้วยหลัก 4 ประการ คือ Privacy, Accuracy, Property และ Accessibility (PAPA) โดยมีรายละเอียด ดังนี้

5.1.1 ความเป็นส่วนตัวของข้อมูลสารสนเทศ (Information Privacy)
ลักษณะของข้อมูลที่เป็นส่วนตัว เช่น หมายเลขบัตรประจำตัวประชาชน วันเดือนปีเกิด ชื่อบัญชีผู้ใช้งาน (account) และรหัสผ่าน (password)

1) รักษาความลับและปกป้องความปลอดภัยของข้อมูลส่วนตัวของบุคลากร ลูกค้า คู่ค้าธุรกิจ และพันธมิตรทางธุรกิจ
2) ไม่ใช้ข้อมูลของลูกค้าจากแหล่งต่างๆ เพื่อผลประโยชน์ทางการตลาดหรือนำไปสร้างฐานข้อมูลประวัติลูกค้าขึ้นมาใหม่แล้วนำไปขายให้กับบริษัทอื่น
3) เก็บรักษาชื่อบัญชีผู้ใช้งาน (account) และรหัสผ่าน (password) ที่เกี่ยวข้องกับระบบข้อมูลสารสนเทศของบริษัทไว้เป็นส่วนตัวและสร้างให้เป็นเอกลักษณ์
4) ไม่จด password ไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่นที่ไม่ได้รับอนุญาต และง่ายต่อการถอดรหัสผ่าน
5) กรณีที่มีความจำเป็นต้องบอก password แก่ผู้อื่นเพื่อเข้าดำเนินการในระบบข้อมูลสารสนเทศ หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านทันที

5.1.2 ความถูกต้องของข้อมูล (Information Accuracy)

1) การจัดทำข้อมูลสารสนเทศให้มีความถูกต้องและน่าเชื่อถือนั้น ข้อมูลควรได้รับการตรวจสอบความถูกต้องก่อนที่จะนำเข้าฐานข้อมูล รวมถึงการปรับปรุงข้อมูลให้มีความทันสมัยอยู่เสมอ
2) แหล่งที่มาของข้อมูลต้องมีความน่าเชื่อถือและตรวจสอบได้ เช่น หน่วยงานภาครัฐ องค์กรอื่นที่เชื่อถือได้ เป็นต้น

5.1.3 ความเป็นเจ้าของ (Information Property)

1) บริษัท สยามแลนด์ ฟลายอิ้ง จำกัด เป็นเจ้าของในทรัพย์สินทางปัญญาที่บุคลากรได้พัฒนาหรือสร้างขึ้นไม่ว่าจะทั้งหมดหรือบางส่วน
2) ไม่ละเมิดหรือเปิดเผยโดยไม่ได้รับอนุญาตในทรัพย์สินทางปัญญาและลิขสิทธิ์ของงานที่ทำร่วมกัน
3) ไม่ใช้งาน ทำซ้ำ ตีพิมพ์หรือเผยแพร่รูปภาพ บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิด ลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของบริษัท
4) ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ตซึ่งรวมถึงการอัพเดทโปรแกรมต่างๆ ซอฟต์แวร์ที่ใช้ในระบบข้อมูลสารสนเทศของบริษัทต้องไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่น

5) ปกป้องทรัพย์สินทางปัญญาของบริษัทโดยไม่เปิดเผยก่อนได้รับอนุญาต
6) ปกป้องทรัพย์สินทางปัญญาโดยไม่ใช้ผิดวิธีหรือผิดกฎหมาย และเมื่อใช้ ต้องแน่ใจว่าได้ประทับตราหรือแสดงเครื่องหมายการค้า หรือเครื่องหมายบริการหรือสัญลักษณ์ลิขสิทธิ์ เช่น การใช้ ®, ™, © (20xx) เป็นต้น
7) แจ้งให้บริษัททราบถึงการค้นพบ การประดิษฐ์ เช่น โปรแกรมคอมพิวเตอร์ สิ่งประดิษฐ์ทางเทคโนโลยีและผลงานนวัตกรรม รวมไปถึงข้อมูลจำเพาะ
8) ให้ความช่วยเหลือบริษัทเพื่อให้ได้มาซึ่งสิทธิบัตร ลิขสิทธิ์ หรือปกป้องเครื่องหมายการค้าที่เป็นทรัพย์สินทางปัญญาของบริษัท

5.1.4 การเข้าถึงข้อมูล (Data Accessibility)

1) การใช้งานระบบสารสนเทศ เช่น ระบบคอมพิวเตอร์ แอปพลิเคชัน อีเมล ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น ผู้บริหารต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศก่อนเข้าใช้ระบบฯ ของผู้ใช้งานให้เหมาะสมกับงานและหน้าที่ความรับผิดชอบ
2) ผู้บริหารทบทวนสิทธิการเข้าถึงข้อมูลและระบบฯ ปีละหนึ่งครั้งหรือเมื่อต้องเปลี่ยนสิทธิของผู้ใช้งาน เช่น การเลื่อนตำแหน่ง โดยผู้บริหารต้องอนุมัติเลื่อนขั้นในระบบฯ
3) ผู้รับมอบอำนาจจากผู้บริหารเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบฯ
4) บันทึกรายละเอียดการเข้าถึงข้อมูลและระบบฯ รวมถึงการแก้ไขเปลี่ยนแปลงสิทธิต่างๆ ทั้งของผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น
5) บันทึกและติดตามการใช้งานระบบฯ และเฝ้าระวังการละเมิดความปลอดภัยที่มีต่อข้อมูลและระบบฯ ที่สำคัญ

5.2 การบริหารจัดการความเสี่ยง

5.2.1 ระบุและประเมินความเสี่ยง

5.2.2 จัดลำดับความสำคัญของความเสี่ยงและบริหารความเสี่ยงสำคัญที่ต้องดำเนินการก่อน

5.2.3 กำหนดมาตรการจัดการความเสี่ยงและดำเนินการตามมาตรการ

5.3 การบริหารจัดการข้อมูลสารสนเทศ

5.3.1 การจัดระดับความลับข้อมูลสารสนเทศ (Classification of Information) โดยพิจารณาจากระดับความเสี่ยงต่อความมั่นคงปลอดภัย ผลกระทบต่อมูลค่าผลกระทบต่อความเสียหายทางทรัพย์สินและภาพพจน์บริษัทโดยแบ่งตามประเภทดังต่อไปนี้

1) **เอกสารลับพิเศษ (Special Control)** [สีม่วง] เป็นข้อมูลสารสนเทศที่ส่งผลกระทบต่อการดำเนินยุทธศาสตร์ทางธุรกิจและก่อให้เกิดความเสียเปรียบในการแข่งขันเชิงธุรกิจอย่างร้ายแรง ถ้าเกิดการรั่วไหลของข้อมูลออกมาจะก่อให้เกิดความเสียหายต่อภาพพจน์ของบริษัทในระดับสากล เช่น
   - ข้อมูลความลับทางการค้า (Trade Secret)
   - แผนกลยุทธ์ทางธุรกิจ
   - แผนการตลาด / การพัฒนาผลิตภัณฑ์
   - แผนควบรวมกิจการ
2) **เอกสารลับ (Confidential)** [สีแดง] เป็นข้อมูลสารสนเทศที่ส่งผลกระทบต่อการดำเนินธุรกิจและความก้าวหน้าของธุรกิจ องค์กรอาจถูกฟ้องร้องเรียกค่าเสียหาย ถ้าเกิดการรั่วไหลของข้อมูลและก่อให้เกิดความเสียหายต่อภาพพจน์บริษัทในระดับประเทศ เช่น
   - เอกสารทางการตลาด (ที่ยังไม่เปิดเผยต่อสาธารณะ)
   - ข้อมูลส่วนบุคคล
   - ข้อมูลลูกค้า
3) **เอกสารใช้ภายในเท่านั้น (Internal Use Only)** [สีเหลือง] เป็นข้อมูลสารสนเทศที่อนุญาตให้ใช้ภายในบริษัทในเครือฯ เท่านั้น ส่งผลกระทบต่อการปฏิบัติงานประจำวันและอาจทำให้เกิดความเสียหายต่อภาพพจน์ เช่น
   - ประกาศภายใน/นโยบายต่างๆ
   - ระเบียบ/คู่มือปฏิบัติงาน
   - บันทึกการปฏิบัติงานประจำวัน
4) **เอกสารเปิดเผย (Public)** [สีเขียว] เป็นข้อมูลสารสนเทศที่พิจารณาแล้วเห็นว่าไม่มีผลกระทบต่อองค์กร สามารถเปิดเผยต่อบุคคลภายนอกได้ เช่น
   - ข้อมูลด้านความยั่งยืน
   - ข้อมูลประชาสัมพันธ์
   - โปรโมชั่นทางการค้าต่างๆ

ทั้งนี้ เอกสารหรือสิ่งตีพิมพ์ไม่ว่าจะทั้งหมดหรือบางส่วนที่พิมพ์หรือทำซ้ำขึ้นมาจากต้นฉบับ ซึ่งมีการกำหนดชั้นความลับไว้ ให้ถือว่ามีชั้นความลับเดียวกันกับต้นฉบับ

5.3.2 การจัดเก็บข้อมูลสารสนเทศและอุปกรณ์

1) ผู้บริหารและผู้รับผิดชอบดูแลข้อมูลสารสนเทศเป็นผู้กำหนดระยะเวลาจัดเก็บข้อมูลสารสนเทศตามระดับความลับ
2) จัดเก็บข้อมูลสำรองในสื่อบันทึกข้อมูลและจัดทำรายการบันทึกให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

3) รักษาความปลอดภัยของระบบสารสนเทศและอุปกรณ์ซึ่งบรรจุข้อมูลสารสนเทศของบริษัท เช่น โทรศัพท์มือถือ แล็ปท็อป แท็บเล็ต เป็นต้น และต้องระมัดระวังเป็นพิเศษในการใช้งานอุปกรณ์ดังกล่าวนอกสถานประกอบการ รวมทั้งจัดเก็บไว้ในที่ที่มีกุญแจล็อคหลังการใช้งาน
4) ตั้งรหัสผ่าน (password) ล็อคหน้าจอซึ่งบรรจุข้อมูลสารสนเทศของบริษัทเมื่อต้องการออกจากระบบสารสนเทศหรือเสร็จสิ้นงาน
5) รายงานฝ่ายเทคโนโลยีสารสนเทศทันทีเมื่อข้อมูลสารสนเทศหรืออุปกรณ์ ซึ่งบรรจุข้อมูลสารสนเทศของบริษัทสูญหายหรือถูกขโมย

5.3.3 การนำอุปกรณ์ส่วนตัวมาใช้ในสถานประกอบการ

อุปกรณ์สื่อสารไร้สายเป็นสิ่งสำคัญต่อการสื่อสารทางธุรกิจและช่วยเพิ่มประสิทธิผลการทำงาน นอกจากนี้การใช้อุปกรณ์สื่อสารไร้สายของพนักงานที่เพิ่มขึ้นทำให้ต้องมีการขออนุญาตเชื่อมต่อกับเครือข่ายของบริษัท การอนุมัติการใช้อุปกรณ์ส่วนตัวและแอปพลิเคชั่นให้เป็นไปตามแต่ละบริษัทกำหนด

บุคลากรที่ใช้อุปกรณ์สื่อสารไร้สายส่วนตัวต้องปฏิบัติ ดังต่อไปนี้

1) งานที่ได้พัฒนาขึ้นบนอุปกรณ์ส่วนตัวถือเป็นทรัพย์สินทางปัญญาของบริษัท
2) อุปกรณ์สื่อสารไร้สายส่วนตัวให้ฝ่ายเทคโนโลยีสารสนเทศตั้งค่าระบบและติดตั้งโปรแกรมพื้นฐานก่อนการเข้าถึงเครือข่าย
3) อุปกรณ์สื่อสารไร้สายจะต้องตั้งรหัสผ่านสำหรับการเข้าถึงข้อมูลของบริษัทเพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต และจะต้องไม่วางทิ้งไว้ในที่สาธารณะ
4) ต้องสำรองข้อมูลที่เกี่ยวข้องกับบริษัทเป็นประจำเพื่อป้องกันการสูญหาย
5) แจ้งให้บริษัทในเครือฯ ทราบในกรณีที่อุปกรณ์ที่เก็บข้อมูลของบริษัทสูญหายหรือถูกขโมย
6) รับผิดชอบค่าใช้จ่ายใดๆ ที่เกี่ยวข้องกับอุปกรณ์ส่วนตัว
7) รับผิดชอบต่อความเสี่ยงที่ข้อมูลส่วนตัวหรือข้อมูลของบริษัท บนอุปกรณ์ส่วนตัวจะสูญหายอันเกิดจากความล้มเหลวของระบบปฏิบัติการ ไวรัส โปรแกรมประสงค์ร้าย (malware) หรือข้อผิดพลาดใด ๆ ของซอฟต์แวร์และตัวอุปกรณ์
8) ส่งคืนหรือทำลายข้อมูลของบริษัทที่อยู่ในอุปกรณ์สื่อสารไร้สายส่วนตัวเมื่อสิ้นสุดการเป็นพนักงาน
9) บริษัทสงวนสิทธิ์ในการตัดสัญญาณการเชื่อมต่อเครือข่ายหรืองดให้บริการโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

5.3.4 การสำรองข้อมูล

1) จัดให้มีขั้นตอนการปฏิบัติการเก็บสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศโดยจัดทำเป็นลายลักษณ์อักษร
2) สำรองข้อมูลในระบบข้อมูลสารสนเทศและ Hard Drives ของบริษัทมาไว้ที่สื่อบันทึกข้อมูล เช่น USB Drives, External Hard Disk และแผ่นดิสก์ ให้เป็นปัจจุบันอย่างสม่ำเสมอ
3) ดูแลรักษาสื่อบันทึกข้อมูลโดยการสำรองข้อมูลลงในสื่อบันทึกข้อมูลใหม่และทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมออย่างน้อยปีละหนึ่งครั้ง เพื่อป้องกันการเสื่อมสภาพ รวมทั้งมีวิธีการนำข้อมูลกลับมาใช้งานใหม่

5.3.5 สร้างรหัสลับ (Encryption) เมื่อส่งข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษระหว่างหน่วยงาน/บริษัท

5.4 การแลกเปลี่ยนข้อมูลสารสนเทศกับบุคคลภายนอก

5.4.1 ในกรณีที่จำเป็นต้องให้ข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษแก่บุคคลภายนอกหรือบุคคลที่ไม่ได้รับอนุญาตต้องได้รับการตรวจสอบความถูกต้องของข้อมูลจากผู้รับผิดชอบดูแลข้อมูลสารสนเทศและต้องได้รับอนุญาตจากผู้บริหาร รวมทั้งบุคคลภายนอกจะต้องลงนามในข้อตกลงห้ามเปิดเผยข้อมูล (Non Disclosure Agreement หรือ NDA)

5.4.2 สร้างรหัสลับ (Encryption) เมื่อส่งข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษให้กับบุคคลภายนอก

5.5 การใช้อินเทอร์เน็ต

5.5.1 ไม่ใช้อินเทอร์เน็ตของบริษัทในเวลาทำงานเพื่อใช้ดำเนินธุรกิจส่วนตัวซึ่งไม่เกี่ยวกับงานของบริษัท

5.5.2 ไม่ใช้อินเทอร์เน็ตในทางที่ละเมิดกฎหมายลิขสิทธิ์ เช่น การดาวน์โหลดโปรแกรม ไฟล์เพลง ไฟล์ภาพยนตร์ รูปภาพหรือข้อความของบุคคลอื่นบนเว็บไซต์โดยไม่ได้รับอนุญาตและนำไปใช้เพื่อแสวงหาผลประโยชน์โดยไม่ได้รับอนุญาตจากเจ้าของ

5.5.3 ไม่ใช้อินเทอร์เน็ตเพื่อกระทำการใดๆ ซึ่งขัดต่อจรรยาบรรณธุรกิจของบริษัท

5.5.4 ไม่ใช้อินเทอร์เน็ตของบริษัทซึ่งทำให้การใช้งานอินเทอร์เน็ตของบุคคลอื่นช้าลง เช่น ดาวน์โหลดไฟล์จำนวนมากเกินไป

5.6 การใช้อีเมล

5.6.1 ห้ามส่งอีเมลแก่บุคคลอื่นโดยปลอมแปลงแหล่งที่มาของการส่งอีเมล อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น

5.6.2 ห้ามส่งอีเมลที่มีข้อความหรือรูปภาพ ซึ่งก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ มีเนื้อหาผิดกฎหมาย สร้างความอับอาย คุกคาม ก้าวร้าว สร้างความเกลียดชังหรือสนับสนุนให้มีการกระทำผิดกฎหมาย

5.6.3 ระมัดระวังเมื่อจำเป็นต้องเปิดอีเมลจากผู้ส่งที่ไม่รู้จักซึ่งอาจพบโปรแกรมประสงค์ร้าย (malware) การหลอกเก็บข้อมูลที่มาจากอีเมลหลอกลวง (phishing) รวมถึงระมัดระวังอีเมลจากผู้ที่ไม่รู้จักและแจ้งฝ่ายเทคโนโลยีสารสนเทศทันทีเมื่อพบอีเมลที่ต้องสงสัย

5.6.4 ระมัดระวังในการเปิดลิงค์ซึ่งอาจพบโปรแกรมประสงค์ร้าย (malware) เช่น ไวรัส spyware trojan เป็นต้น

5.6.5 ไม่ส่งอีเมลทางธุรกิจโดยใช้สำเนาลับ (Blind Carbon Copy: Bcc)

5.6.6 ตั้งค่าอีเมลทางธุรกิจที่ส่งออกทุกฉบับให้มี E-mail Signature

5.6.7 ใช้อีเมลส่วนตัว (Gmail, Yahoo Mail) นอกเวลางานหรือในเวลาพักกลางวัน

5.7 การใช้สื่อสังคมออนไลน์ (Social Media)

โปรดดูรายละเอียดในนโยบายและแนวทางปฏิบัติในการใช้สื่อสังคมออนไลน์ของบริษัท

5.8 การทำลายข้อมูลสารสนเทศ

5.8.1 ข้อมูลสารสนเทศที่จัดพิมพ์เป็นเอกสารในรูปแบบกระดาษหรือวัตถุใดๆ ซึ่งอยู่ในระดับเอกสารใช้ภายในเท่านั้น เอกสารลับและเอกสารลับพิเศษ เมื่อไม่ต้องการแล้วให้ทำลายโดยเครื่องทำลายเอกสารเท่านั้น ส่วนเอกสารเปิดเผยให้ทิ้งลงถังขยะหรือเครื่องทำลายเอกสาร

5.8.2 ย้ายข้อมูลสารสนเทศที่สำคัญแล้วจึงลบข้อมูลสารสนเทศเป็นการถาวรก่อนทำลายสื่อบันทึก

5.9 การตรวจสอบการรั่วไหลของข้อมูลสารสนเทศ

ในกรณีที่เกิดการรั่วไหลของข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษ ผู้บริหารที่รับผิดชอบต้องแต่งตั้งคณะกรรมการสอบสวนเพื่อสอบสวนและตรวจสอบหาสาเหตุความผิดพลาด พร้อมทั้งปรับปรุงวิธีจัดเก็บข้อมูลสารสนเทศไม่ให้รั่วไหลและระบบการป้องกันการรั่วไหลของข้อมูลสารสนเทศ ตลอดจนรายงานให้ผู้บริหารรับทราบ

6. การฝึกอบรม

จัดให้มีการสื่อสารและถ่ายทอดนโยบายและแนวปฏิบัติด้านการบริหารจัดการข้อมูลสารสนเทศผ่านการฝึกอบรม การประชุม หรือกิจกรรมในรูปแบบต่าง ๆ ให้แก่กรรมการ ผู้บริหารและพนักงานและให้มีการประเมินประสิทธิผลอย่างต่อเนื่อง

7. การแจ้งเบาะแส

ร้องเรียนหรือแจ้งเบาะแสเมื่อพบเห็นการกระทำที่เชื่อได้ว่าเป็นการละเมิดนโยบายและแนวปฏิบัตินี้ โดยขั้นตอนให้เป็นไปตามนโยบายและแนวปฏิบัติเกี่ยวกับการแจ้งเบาะแส ทั้งนี้ผู้ร้องเรียนหรือผู้แจ้งเบาะแสจะได้รับความคุ้มครองและข้อมูลจะถูกเก็บเป็นความลับ โดยไม่มีผลต่อตำแหน่งงานทั้งในระหว่างดำเนินการสอบสวนและหลังเสร็จสิ้นกระบวนการ

8. การขอคำแนะนำ

ในกรณีที่มีข้อสงสัยว่าการกระทำนั้นอาจฝ่าฝืนกฎหมาย ระเบียบ นโยบายและแนวปฏิบัติด้านการบริหารจัดการข้อมูลสารสนเทศสามารถขอคำแนะนำจากผู้บังคับบัญชา หน่วยงานหรือบุคคลผู้รับผิดชอบด้านการบริหารจัดการข้อมูลสารสนเทศ ด้านกำกับการปฏิบัติตามกฎเกณฑ์หรือด้านกฎหมายก่อนตัดสินใจหรือดำเนินการใด ๆ

9. บทลงโทษ

ในกรณีที่เกิดการสอบสวน พนักงานทุกคนต้องให้ความร่วมมือกับหน่วยงานภายในและภายนอกอย่างเต็มที่ ทั้งนี้หากผู้บริหารและพนักงานกระทำการใด ๆ ที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายฉบับนี้ไม่ว่าทางตรงหรือทางอ้อม ผู้บริหารและพนักงานจะถูกพิจารณาโทษทางวินัยตามระเบียบข้อบังคับการทำงาน

10. กฎหมาย กฎระเบียบและนโยบายที่เกี่ยวข้อง

10.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

10.2 พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537

10.3 นโยบายและแนวทางปฏิบัติในการใช้สื่อสังคมออนไลน์ของบริษัทในเครือเจริญโภคภัณฑ์

10.4 ISO/IEC 27001:2013 (Information Security Management System: ISMS)

11. ภาคผนวก

นโยบายและแนวปฏิบัตินี้ ประกอบด้วยภาคผนวก ดังต่อไปนี้

11.1 ภาคผนวก ก ตัวอย่างเอกสารปกตามระดับความลับของข้อมูล

11.2 ภาคผนวก ข ตัวอย่างการใช้กระดาษระดับความลับของข้อมูล

ภาคผนวก ก
ตัวอย่างเอกสารปกตามระดับความลับของข้อมูล

เอกสารลับพิเศษ

SIAM LAND FLYING

การเปิดเผยเอกสารลับพิเศษนี้ ส่งผลกระทบต่อยุทธศาสตร์การดำเนินธุรกิจและก่อให้เกิดความเสียเปรียบในการแข่งขันเชิงธุรกิจอย่างร้ายแรงทำให้เกิดความเสียหายต่อภาพพจน์ขององค์กรในระดับสากล

หน้าที่ความรับผิดชอบของผู้ครอบครอง

1. ผู้ถือครองมีหน้าที่รับผิดชอบความปลอดภัยของเอกสารลับพิเศษนี้
2. มีการป้องกันที่จำเป็นเพื่อไม่ให้เอกสารถูกเปิดเผยโดยไม่ได้รับอนุญาต โดยการไม่ทิ้งเอกสารไว้ลำพัง ยกเว้นเมื่อเก็บรักษาในสถานที่ปลอดภัย
3. การเปิดเผยเอกสารจะให้เฉพาะผู้ที่มีสิทธิรับรู้เท่านั้น

การเก็บ

เมื่อไม่มีการใช้งานจากเอกสารให้ใส่ในหีบห่อหรือแฟ้มเอกสารระบุด้านหน้าว่า **“SPECIAL CONTROL (เอกสารลับพิเศษ)”** และให้เก็บไว้ในตู้นิรภัยที่ตั้งไว้ในพื้นที่ที่มีการควบคุมการเข้า-ออก เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

การทำสำเนา

เอกสารลับพิเศษห้ามทำสำเนา แยกชิ้น หรือทำขึ้นมาใหม่ โดยไม่ได้รับอนุญาต

การทำลาย

ห้ามทิ้งถังขยะ ให้ทำลายโดยเครื่องทำลายเอกสารและเผาเท่านั้น

(ใบปะหน้านี้จะไม่เป็นความลับเมื่อถูกแยกจากเอกสารลับพิเศษ)

เอกสารลับพิเศษ
(SPECIAL CONTROL)

เอกสารลับ

การเปิดเผยเอกสารลับนี้ ส่งผลกระทบต่อการประกอบธุรกิจและความก้าวหน้าขององค์กรอาจถูกฟ้องร้องเรียกค่าเสียหาย เกิดความเสียหายต่อภาพพจน์ในระดับประเทศ

หน้าที่ความรับผิดชอบของผู้ครอบครอง

1. ผู้ถือครองมีหน้าที่รับผิดชอบความปลอดภัยของเอกสารลับนี้
2. มีการป้องกันที่จำเป็นเพื่อไม่ให้เอกสารถูกเปิดเผยโดยไม่ได้รับอนุญาต โดยการไม่ทิ้งเอกสารไว้ลำพัง ยกเว้นเมื่อเก็บรักษาในสถานที่ปลอดภัย
3. การเปิดเผยเอกสารจะให้เฉพาะผู้ที่มีสิทธิรับรู้เท่านั้น

การเก็บ

เมื่อไม่มีการใช้งานจากเอกสารให้ใส่ในหีบห่อหรือแฟ้มเอกสารระบุด้านหน้าว่า “**CONFIDENTIAL (เอกสารลับ)**” และให้เก็บไว้ในตู้เอกสารที่ปิดล็อกด้วยกุญแจที่มั่นคงที่ตั้งไว้ในพื้นที่ที่มีการควบคุมการเข้า-ออก เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

การทำสำเนา

เอกสารลับห้ามทำสำเนา แยกชิ้น หรือทำขึ้นมาใหม่ โดยไม่ได้รับอนุญาต

การทำลาย

ห้ามทิ้งถังขยะ ให้ทำลายโดยเครื่องทำลายเอกสารเท่านั้น

(ใบปะหน้านี้จะไม่เป็นความลับเมื่อถูกแยกจากเอกสารลับ)

เอกสารลับ
(CONFIDENTIAL)

เอกสารใช้ภายในเท่านั้น

SIAM LAND FLYING

การเปิดเผยเอกสารใช้ภายในเท่านั้น ส่งผลกระทบต่อการปฏิบัติงานประจำวัน อาจทำให้เกิดความเสียหายต่อภาพพจน์ เป็นข้อมูลที่อนุญาตให้ใช้ภายในหน่วยงานเท่านั้น

หน้าที่ความรับผิดชอบของผู้ครอบครอง

1. ผู้ถือครองมีหน้าที่รับผิดชอบความปลอดภัยของเอกสารใช้ภายในเท่านั้น
2. มีการป้องกันที่จำเป็นเพื่อไม่ให้เอกสารถูกเปิดเผยโดยไม่ได้รับอนุญาต โดยการไม่ทิ้งเอกสารไว้ลำพัง ยกเว้นเมื่อเก็บรักษาในสถานที่ปลอดภัย
3. การเปิดเผยเอกสารจะให้เฉพาะผู้ที่มีสิทธิรับรู้ตามหน้าที่ความรับผิดชอบเท่านั้น

การเก็บ

เมื่อไม่มีการใช้งานจากเอกสารให้ใส่ในหีบห่อหรือแฟ้มเอกสารระบุด้านหน้าว่า " INTERNAL USE ONLY **(เอกสารใช้ภายในเท่านั้น)**" และให้เก็บไว้ในตู้เอกสารที่ปิดล็อกด้วยกุญแจ

การทำสำเนา

เอกสารใช้ภายในเท่านั้น สามารถทำสำเนา แยกชิ้น หรือทำขึ้นมาใหม่ โดยต้องได้รับอนุญาตจากผู้มีหน้าที่รับผิดชอบเท่านั้น

การทำลาย

ให้ทำลายโดยเครื่องทำลายเอกสารเท่านั้น

(ใบปะหน้านี้จะไม่เป็นความลับเมื่อถูกแยกจากเอกสารใช้ภายในเท่านั้น)

เอกสารใช้ภายในเท่านั้น

(INTERNAL USE ONLY)

เอกสารเปิดเผย

เป็นข้อมูลที่พิจารณาแล้วเห็นว่าไม่มีผลกระทบต่อองค์กร สามารถเปิดเผยสู่บุคคลภายนอกได้

หน้าที่ความรับผิดชอบของผู้ครอบครอง
ผู้ครอบครองเอกสารสามารถเปิดเผยสู่สาธารณะได้ตามความเหมาะสม

การเก็บ
เมื่อไม่มีการใช้งานเอกสารให้ใส่ในหีบห่อหรือแฟ้มเอกสารระบุด้านหน้าว่า “PUBLIC (เอกสารเปิดเผย)” และให้เก็บไว้ในตู้เอกสาร

การทำสำเนา
เอกสารเปิดเผย สามารถทำสำเนา คัดลอก แยกชิ้น หรือทำใหม่ได้ ตามความเหมาะสม

การทำลาย
ให้ทำลายโดยทิ้งลงถังขยะให้เรียบร้อย หรือเครื่องทำลายเอกสาร

(ใบปะหน้านี้จะไม่เป็นความลับ)

เอกสารเปิดเผย

(PUBLIC)

ภาคผนวก ข
ตัวอย่างการใช้กระดาษระดับความลับของข้อมูล

เอกสารลับพิเศษ / **SPECIAL CONTROL**

เอกสารลับพิเศษ / **SPECIAL CONTROL**

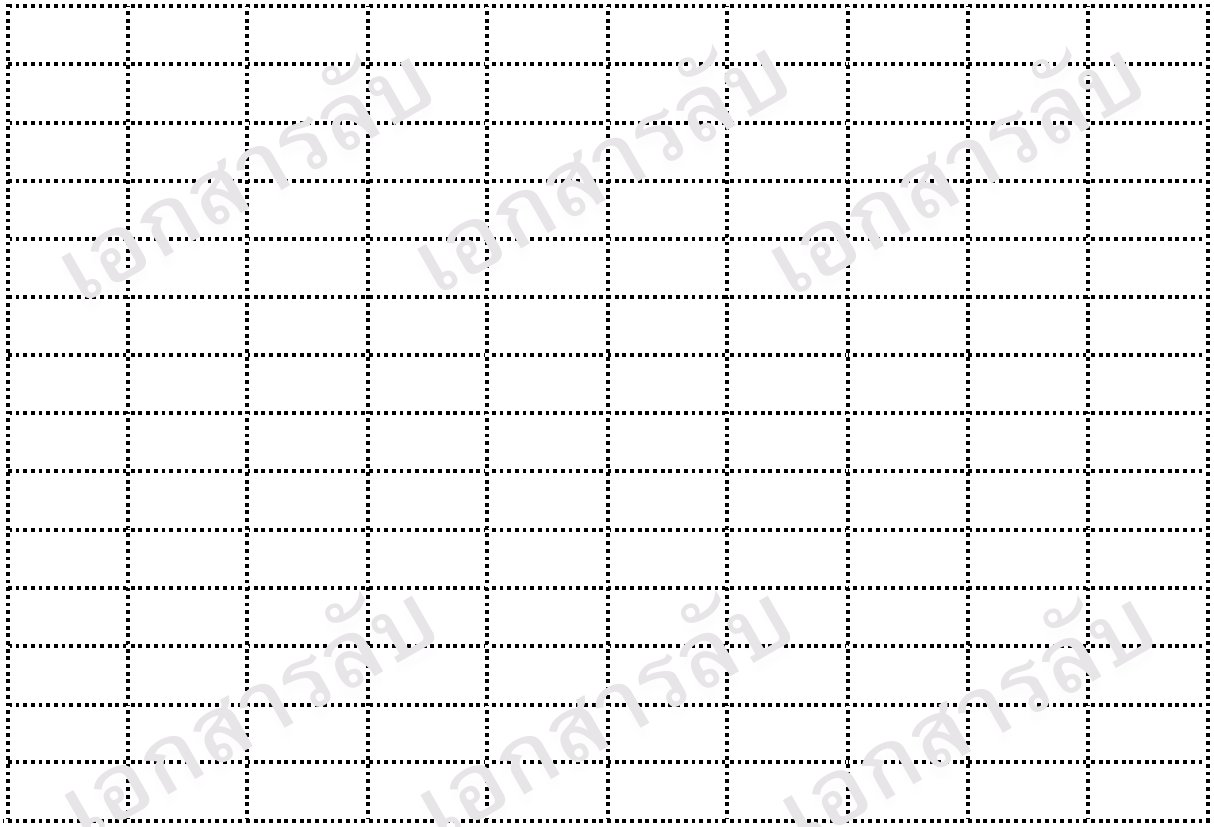
.....

ใช้ภายในเท่านั้น/ (Internal Use Only)

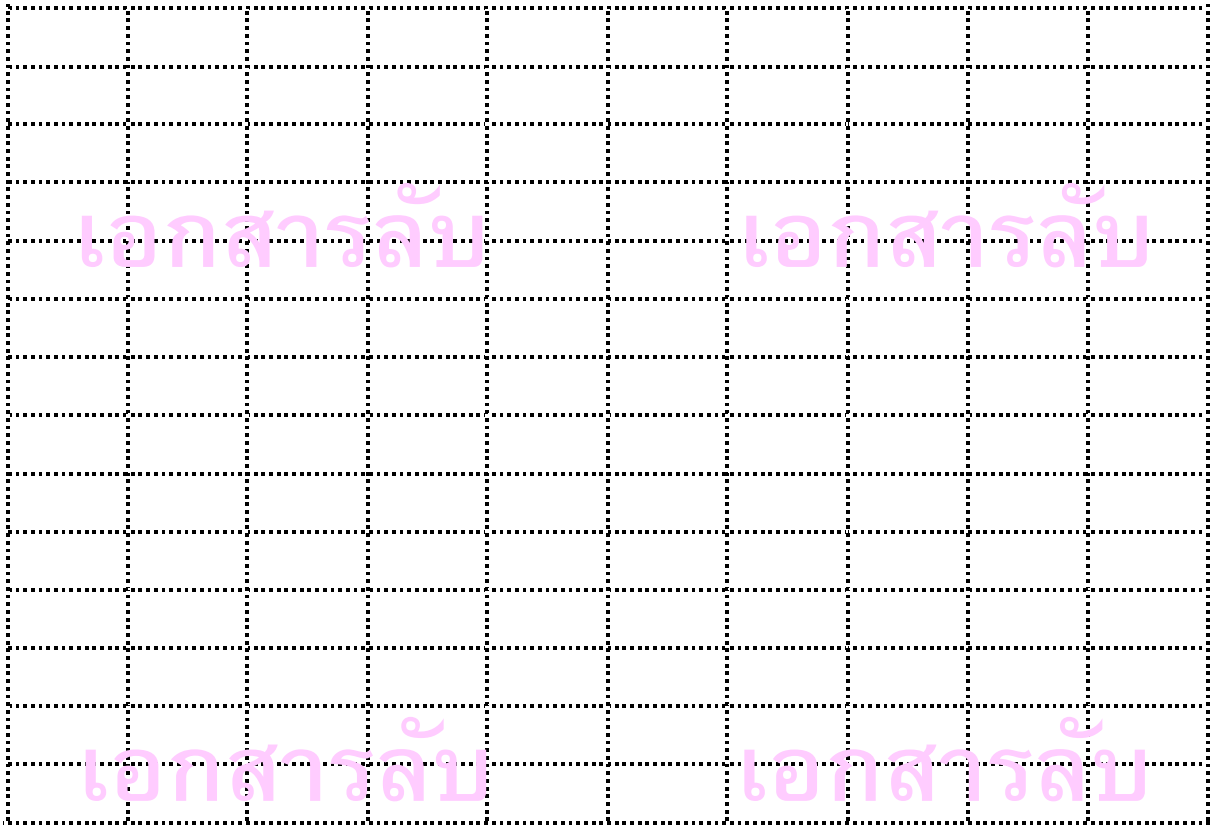
Page 1 of .....

เปิดเผย / **PUBLIC**

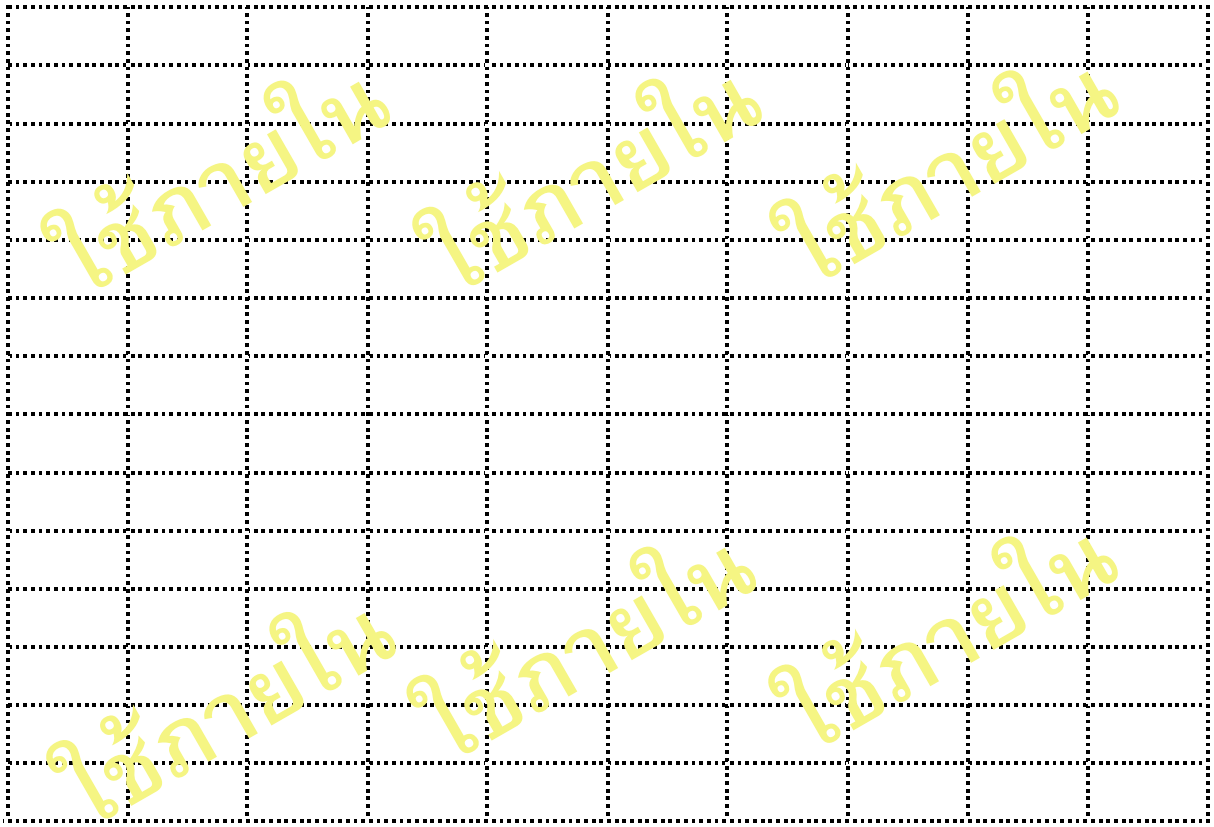
.....

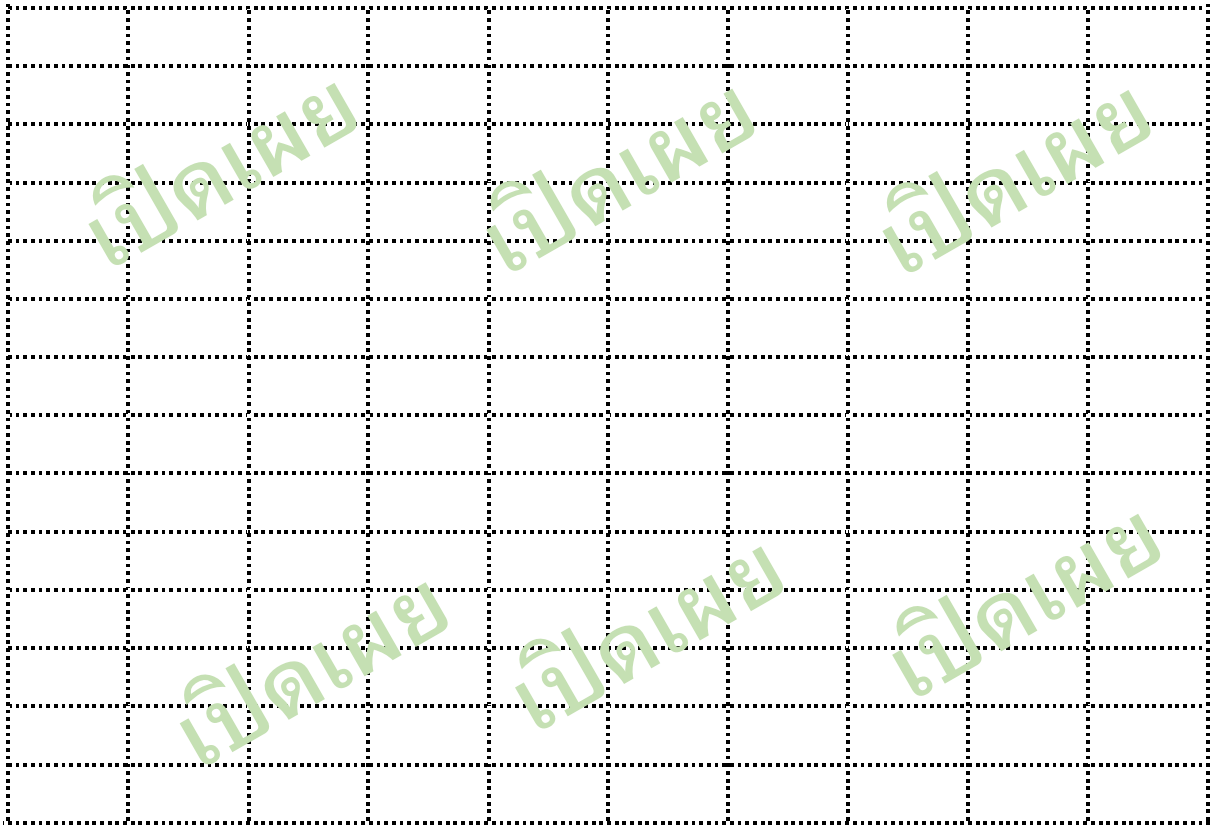


เอกสารลับพิเศษ / SPECIAL CONTROL



เอกสารลับ / **CONFIDENTIAL**


ใช้ภายใน
ใช้ภายใน
ใช้ภายใน
ใช้ภายใน
ใช้ภายใน
ใช้ภายใน



เปิดเผย / **Public**