Information Management

Policy and Guidelines

Lotuss Stores (Malaysia) Sdn. Bhd. (“Lotus’s Malaysia”)

Contents

Information Management Policy and Guidelines

Lotus's Malaysia

1. Intent

Information is a vital asset to all companies' business operations, including Lotus's Malaysia . 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 Lotus's Malaysia 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 Lotus's Malaysia 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 Lotus's Malaysia, 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 Lotus's Malaysia 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 Lotus's Malaysia 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) Lotus's Malaysia 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 Lotus's Malaysia premises is forbidden.
3) Any unauthorized usage, reproduction, printing, public release and installing pirated or copyright infringed software on Lotus's Malaysia information systems is forbidden.
4) Lotus's Malaysia employees must be cautious of downloading any software on the internet, including updating any existing software. Any software used in Lotus's Malaysia information systems must not violate any existing copyrights or intellectual properties of other companies
5) Protect Lotus's Malaysia intellectual properties and do not reveal them without proper permission.
6) Whenever any intellectual property owned by Lotus's Malaysia 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 Lotus's Malaysia 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 Lotus's Malaysia 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 Lotus's Malaysia 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. Lotus's Malaysia information is classified into the following 4 categories:

1) **Special Control** [Purple] is information that can seriously affect business strategy and severely damage Lotus's Malaysia market competitiveness, in the event the information is leaked and could cause extensive damage to Lotus's Malaysia 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 Lotus's Malaysia and business units and potential growth if leaked, may subject business unit to lawsuits. Any leaks of this level can cause damage to Lotus's Malaysia 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 Lotus's Malaysia. These documents affect daily operations and can cause damage to Lotus's Malaysia 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 Lotus's Malaysia Information Systems and other devices containing Lotus's Malaysia 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 Lotus's Malaysia information unattended.
5) Report to the IT Department immediately when any of Lotus's Malaysia 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 Lotus's Malaysia.
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 Lotus's Malaysia. In addition, devices must not be left unattended on public premises.

4) Regularly backup all files on their device regarding any data related to Lotus's Malaysia.
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 Lotus's Malaysia 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 Lotus's Malaysia files upon termination of employment.
9) Lotus's Malaysia 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 Lotus's Malaysia 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 Lotus's Malaysia 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 Lotus's Malaysia 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. 2537

10.3 Lotus's Malaysia 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

COVER PAGE FOR SPECIAL CONTROL DOCUMENT

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

COVER PAGE FOR CONFIDENTIAL DOCUMENTS

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

COVER PAGE FOR INTERNAL USE ONLY DOCUMENTS

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

COVER PAGE FOR PUBLIC DOCUMENTS

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

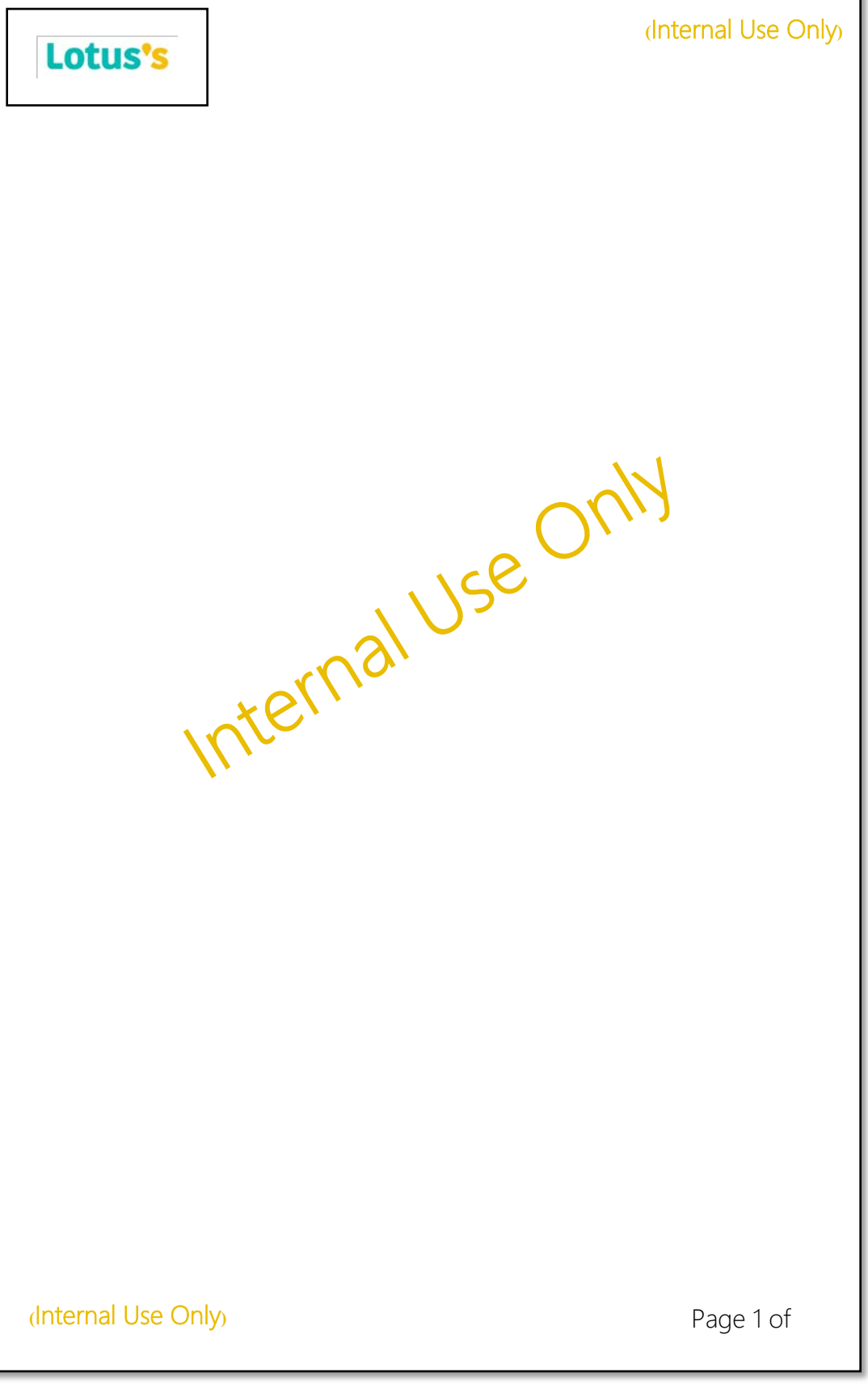
Examples of document prints based on confidentiality

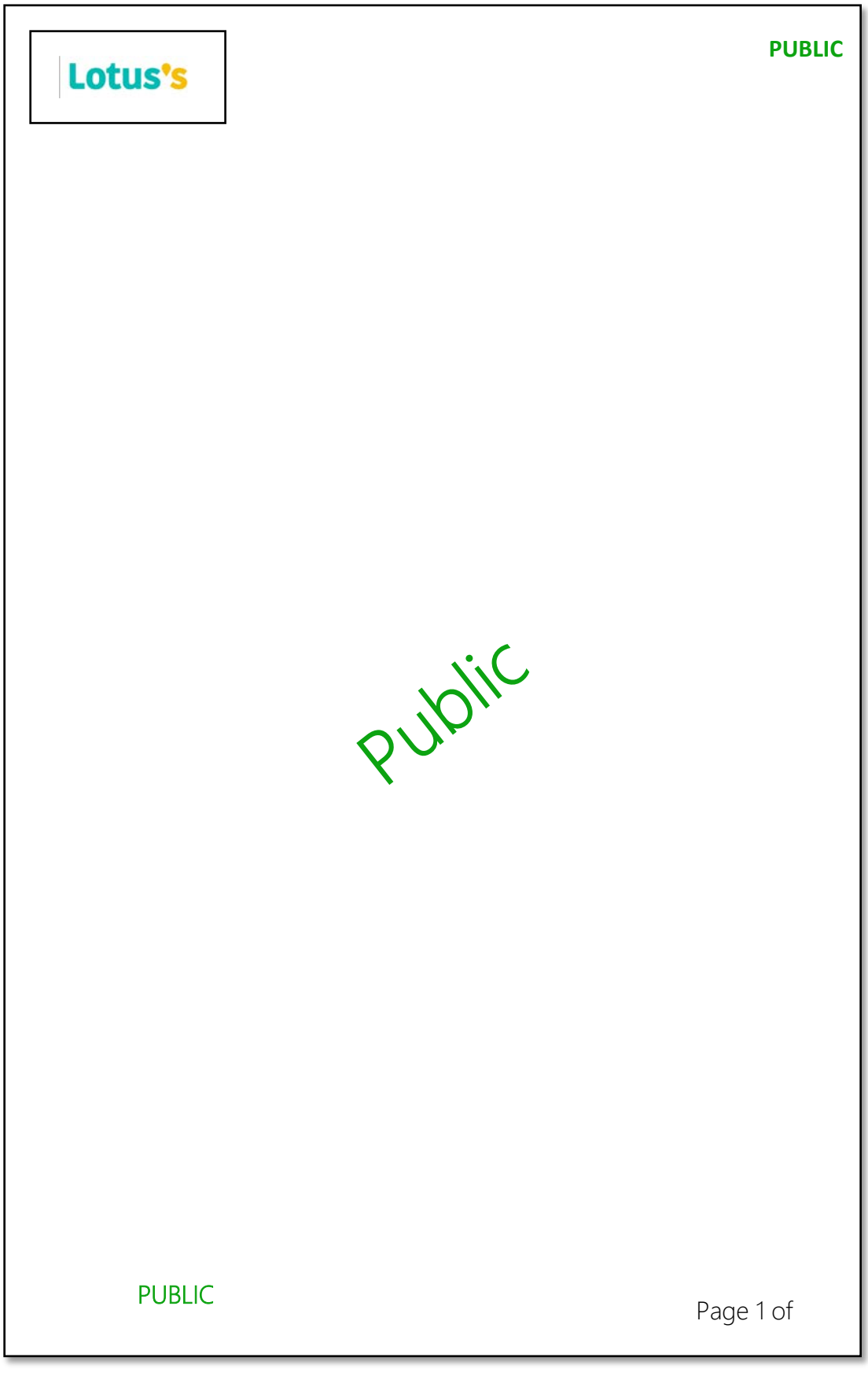
Lotus's

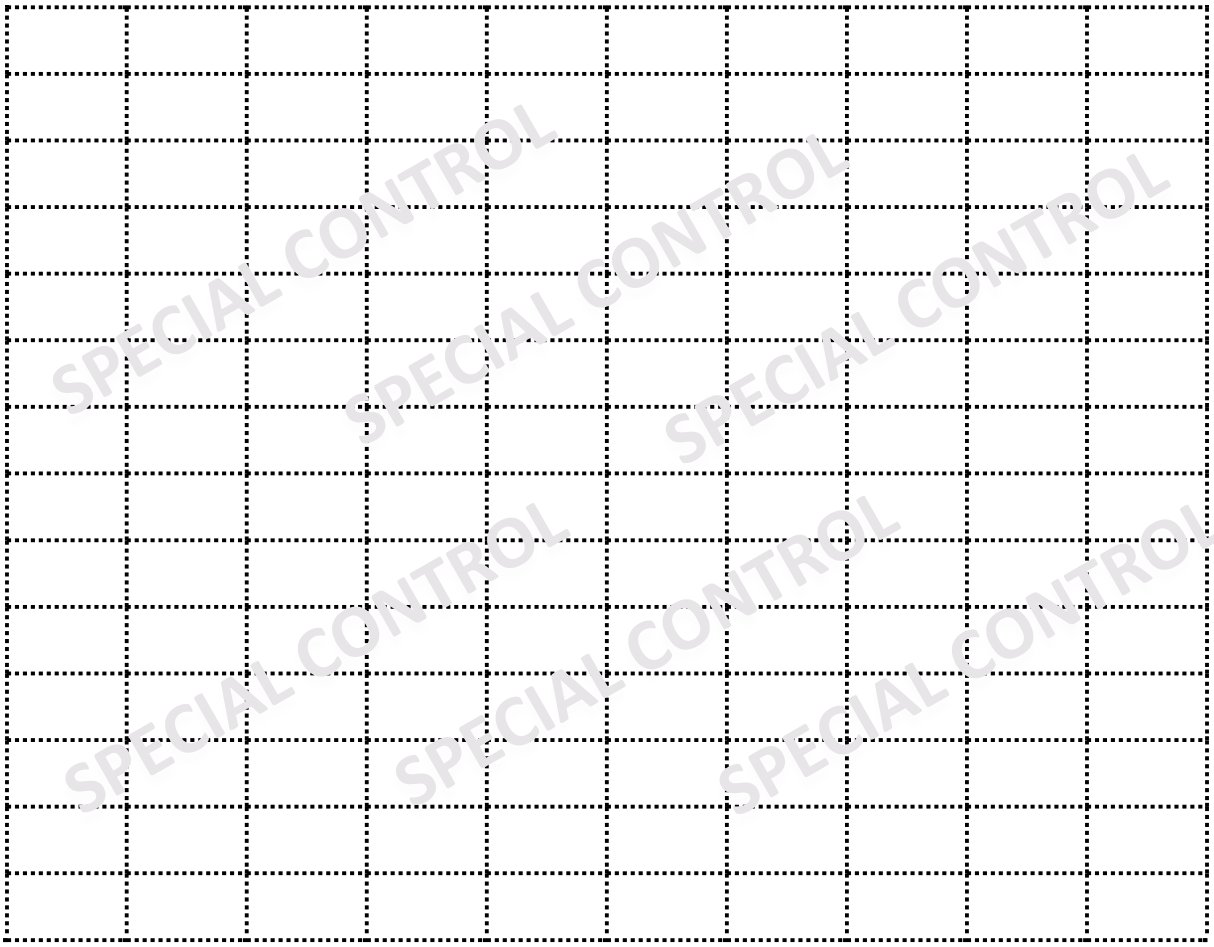
CONFIDENTIAL

CONFIDENTIAL

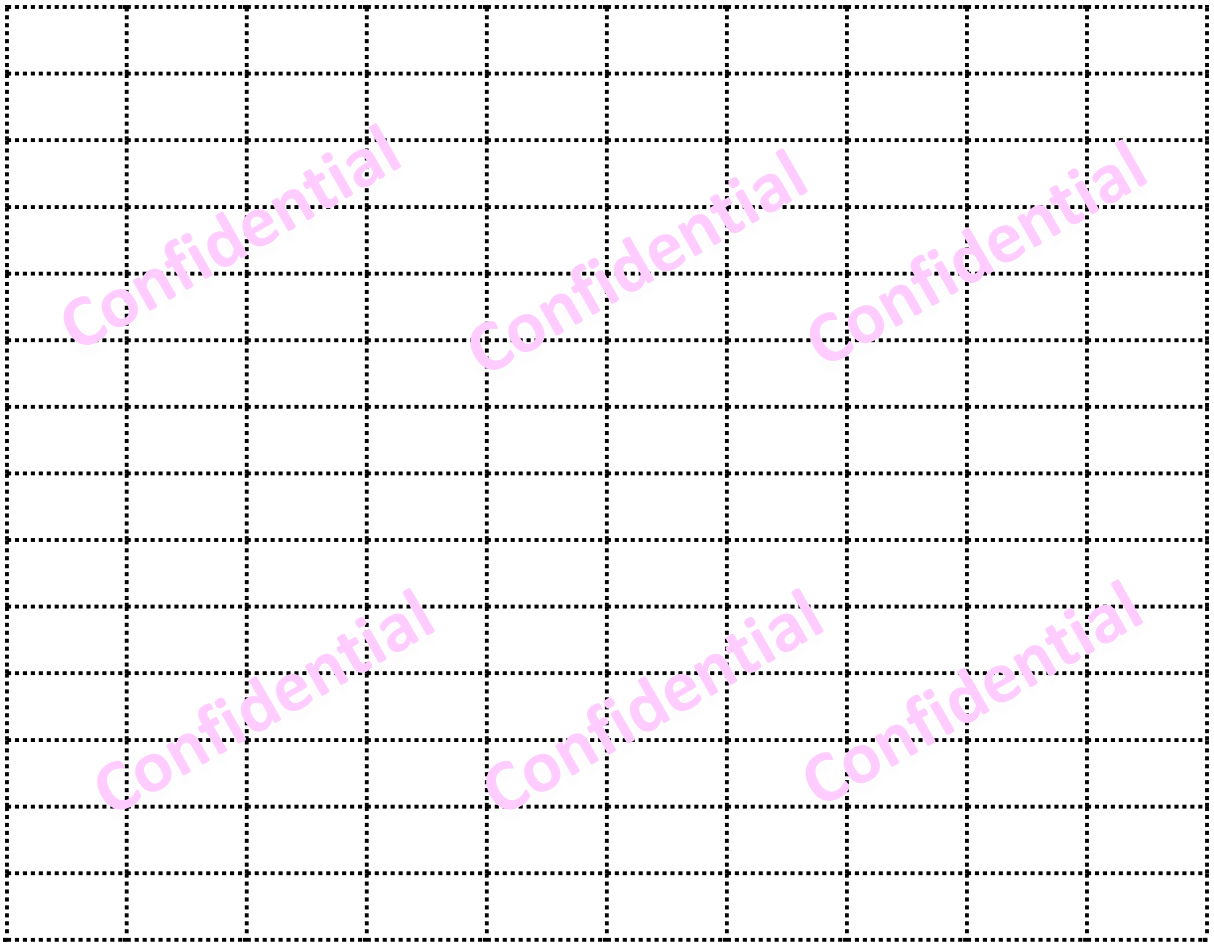
Page 1 of .....


Lotus's
(Internal Use Only)
Internal Use Only
(Internal Use Only)
Page 1 of

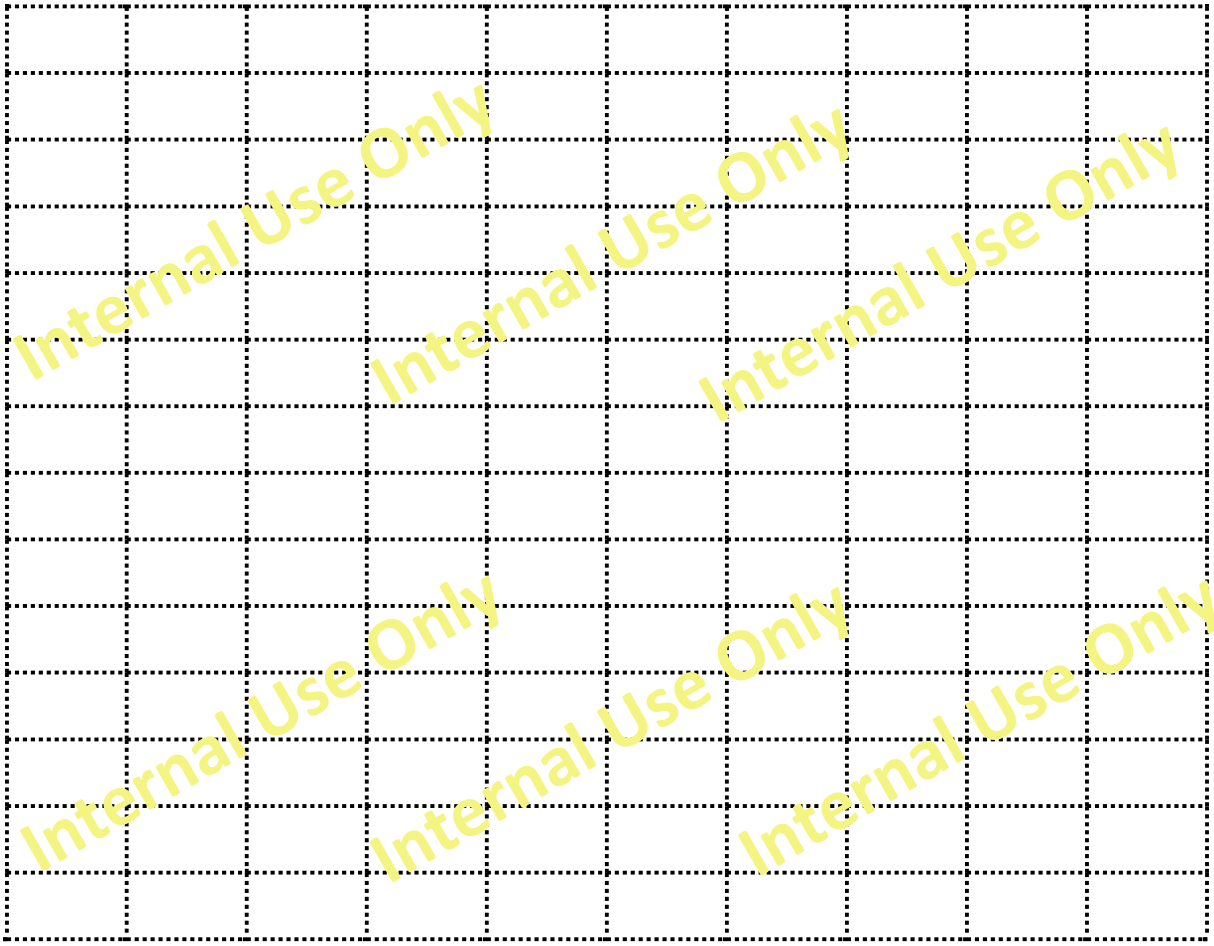

Lotus's
PUBLIC
Public
PUBLIC
Page 1 of



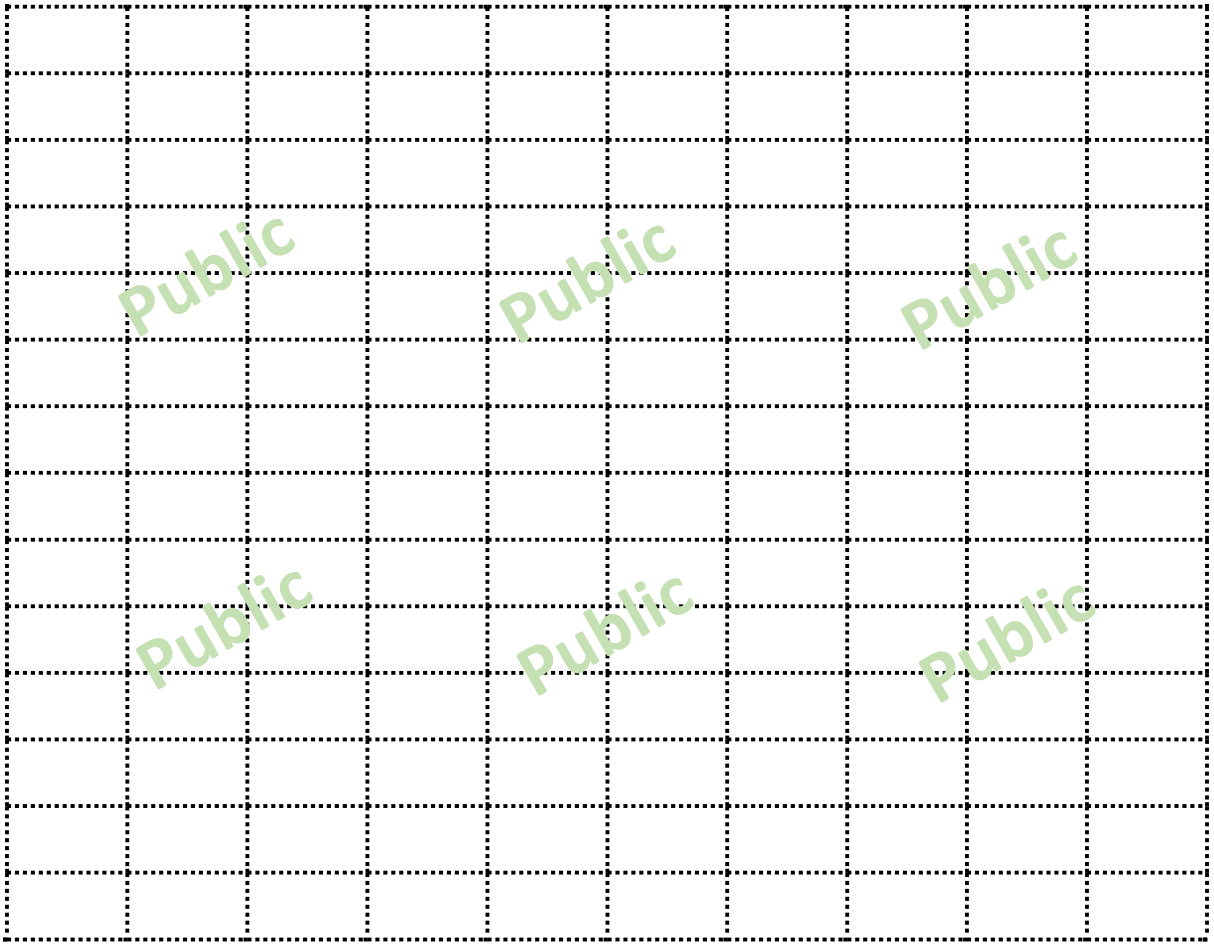
SPECIAL CONTROL



CONFIDENTIAL



Internal Use Only


Public
Public
Public
Public
Public
Public