AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Binte Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release

TABLE OF CONTENTS

PURPOSE

This document defines a way of classifying information to ensure identification and understanding of protection needs of information in accordance with its importance to the organisation, and to maintain the security of information transferred within an organisation and with any external interested party.

SCOPE

This control applies to all organisation's information and associated assets all throughout the information lifecycle.

REFERENCE

ISO/IEC 27001 standard	Annex A 5.12 Classification of information Annex A 5.13 Labelling of information Annex A 5.14 Information Transfer

RESPONSIBILITIES & AUTHORITIES

Top Management has the prime responsibility and approval authority for this control.

The user has a responsibility to protect the information it holds and processes using controls appropriate to the sensitivity of the information involved, and to carefully consider how the information they produce, handle, transferred or dispose of can remain effectively protected.

PROCEDURE

1. Information Classification

On creation, all information assets must be assessed and classified by the owner according to their content. The classification will determine how the document should be protected and who should be allowed access to it. Any system subsequently allowing access to this information should clearly indicate the classification.

The organisation's information classification scheme requires information assets to be protectively marked as per their classification (excluding "Public" which does not need to be marked). The way the document is handled, published, moved and stored will be dependent on this scheme.

The classes of information are:

Level	Classification	Description	Examples
1	Public (Unclassified)	Freely available outside of the organisation or is intended for public use. No classification mark required, and will not be assigned a formal owner or inventoried.	• Online public information • Website information • Public corporate announcements
2	Internal	May be freely shared within and among staff, but must not be shared with third parties unless a non-disclosure agreement has been signed.	• Internal policies and operating procedures • Interoffice memorandums • Internal meeting minutes
3	Confidential	Highest level of classification. Sensitive information that may be directly or indirectly damaging to the organisation or to the information owner, if disclosed.	• Personal data • Information about customer and the business that the company is obliged to protect, with local laws taking precedence • Product or system development information or marketing strategies • Information on mergers, acquisitions, or divestitures, prior to general or public disclosure • Identification and authentication information • Any form of cryptographic key

The following points should be considered when assessing the classification to use:

- Applying too high a classification can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of the organization's business.
- Applying too low a classification may lead to damaging consequences and compromise of the asset.
- The compromise of larger sets of information of the same classification is likely to have a higher impact (particularly in relation to personal data) than that of a single instance. Generally, this will not result in a higher classification but may require additional handling arrangements. However, if the accumulation of that data results in a more sensitive asset being created, then a higher classification should be considered.
- The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within it.

2. Information Labelling

In order to ensure that the correct controls are applied to the information, a system of protective marking will be used so that all employees and third parties (where applicable) are aware of how that information must be managed.

2.1 Documents

Physical and electronic documents that carries "internal" and "confidential" classification will display the security marking clearly visible on the document either in the header or footer or 1st page or even as a watermark (or stamp for physical documents). Folder-level labelling of classification will be implemented where it is more efficient to achieve this purpose.

Unless labelled otherwise, electronic documents housed within application systems (e.g., Help Files, Operations Guide) are classified as "internal" even if the classification label is not inherently obvious.

Note: Documents classified as "Public" do not require any classification label.

2.2 Emails

Email confidentiality disclaimer notice shall be appended to all company email users' signature. Any email attachments must state the classification clearly as per 2.1 above.

2.3 Personal Data

Physical and electronic documents with personal data shall be labelled as "Confidential". The DPO shall ensure that people under the organisation's control are made aware of the definition of personal data and how to recognize the information.

3. Information Handling

For each security classification, a set of handling controls must be in place to ensure that the information asset involved is appropriately protected at all times.

The following sections set out the main procedural components of these controls.

Considerations	Public	Internal	Confidential
Secure Processing	In general, there are no specific controls that must be placed on the processing of such information although, it should be borne in mind that items such as headed stationery and their electronic	Information at this level of classification will be subject to access controls involving either physical security or an authorised use logon or both. Access should not generally be granted in public areas and output	Information at this level of classification will be subject to strictest access controls involving both physical security and authorised use logon. Access should not generally be granted in public areas and output

Considerations	Public	Internal	Confidential
	equivalents should not be made freely available.	such as printouts should be to areas where public access is prevented.	such as printouts should be to areas where public access or unauthorized access is prevented.
Storage	Information may be stored in unsecured areas which may be accessible to the public. However, some controls should be placed on large quantities of such information such as leaflets which could still be subject to theft or misuse. Information of this classification may be stored electronically without encryption or other forms of protection.	May be stored electronically without the need for encryption or password-protection, or physical without lock and key within the organisation as long as public access can be prohibited.	When stored electronically, access restriction must be implemented. Hard copy format must be stored under lock and key. Encryption or password-protection must be implemented for personal data.
Transmission *(Refer to section 4 of this procedure for further details on information transfer)*	In general, information may be sent over unencrypted connections or distributed freely in hard copy or even verbally.	In general, information may be sent over unencrypted connections internally within the organisation. However, if the need to send to external parties arises, approval from the assigned owner shall be obtained. Conversations in public areas where other people might be able to hear should be avoided. Any hardcopy must not be left unattended in public areas.	Information may only be shared or disclosed with authorisation from the owner or in the case of personal data, with consent from the individual limited to the purpose notified to them unless an exception applies. Sharing / transmission must be through encrypted connections.
Declassification *(Refer to section 1 of this procedure in deciding declassification)*	Information will not be subject to declassification as it is considered unclassified.	Information may be declassified to “Public” with the permission of the asset owner at which time the controls specified for “Public” will apply.	No declassification is allowed.

Considerations	Public	Internal	Confidential
Destruction	Information falling may be disposed of via normal waste routes without need for controls such as shredding. Where possible, items should be recycled.	Information must be destroyed securely so that it cannot be reconstituted e.g., via shredding. In case of electronic files, it can be deleted by the assigned owner.	Information must be destroyed securely so that it cannot be reconstituted e.g., via shredding (using at least P3 cross cut shredder) for paper (reuse of paper is not allowed) or deletion for electronic files where the information will be irrecoverable. Where possible, secure destruction should be verified by a second authorised individual. For personal data, de-identification and anonymization will be considered, as it applies.
Chain of Custody	Information assets will be freely distributed amongst organization employees, customers and members of the public where required, without the need to keep records (unless for operational purposes).	No specific controls are placed on the chain of custody for information although reasonable precautions should be taken to ensure that it stays within the organization at all times.	Chain of custody must be tracked, and where necessary, recorded.
Logging of Security-related Events	There is generally no need to log security events unless subject to criminal activity such as large-scale theft of material.	Events where information has been compromised should be recorded and assessed in accordance with the organisation's procedure on events assessment.	Events where information has been compromised should be reported immediately and flagged as an incident. Such incidents will be recorded and investigated in accordance with the organisation's procedure on information security management. Where personal data is involved, it will be categorized as data breach and assessment has to be

Considerations	Public	Internal	Confidential
			made to determine if mandatory notification as per the applicable law (e.g., Singapore PDPA) is required.

4. Information Transfer

The organisation's *Information Transfer and Communications Security Policy* must be communicated to all relevant interested parties. Confidentiality clause in agreements or separate non-disclosure agreements will be maintained with the recipient to protect information in all forms in transit within the organisation (e.g., employee contract confidentiality clause / employee NDA) and when it is transferred to third parties (e.g., contractual requirements / NDA).

For all types of information transfer, the following must be ensured:

- Controls designed to protect transferred information from interception, unauthorized access, copying, modification, misrouting, destruction and denial of service, including levels of access control commensurate with the information classification and any special controls that are required to protect sensitive information (e.g., personal data), such as use of cryptographic techniques.
- Controls to ensure traceability and non-repudiation, including maintaining a chain of custody for information while in transit.
- Identification of appropriate contacts related to the transfer including information owners / custodians.
- Responsibilities and liabilities in the event of information security incidents, such as loss of physical storage media or data.
- Use of labelling system ensuring that the meaning of label is immediately understood by the recipient.
- Reliability and availability of the transfer service.
- Retention and disposal requirements.
- Consideration of any other relevant legal, regulatory and contractual requirements related to transfer of information.

4.1 Electronic Transfer

When using electronic communication facilities for information transfer, the following items must be considered:

- Detection and protection against malware that can be transmitted through the use of electronic communications;
- Protection of communicated sensitive electronic information that is in the form of email attachment;

- Prevention against sending documents and messages in communications to the wrong address or number;
- Use of only approved external public services such as instant messaging, social networking, file sharing or cloud storage;
- Stronger levels of authentication when transferring information via publicly accessible networks;
- Restrictions associated with electronic communication facilities (e.g., preventing automatic forwarding of electronic mail to external mail addresses);
- Advising personnel and other interested parties not to send short messaging service (SMS) or instant messages with critical information since these can be read in public access (and therefore by unauthorized persons) or stored in devices not adequately protected; and
- Advising personnel and other interested parties about the problems of using fax machines or services, namely:
    - Unauthorized access to built-in message stores to retrieve messages;
    - Deliberate or accidental programming of machines to send messages to specific numbers.

4.2 Physical Storage Media and Paper Transfer

When transferring physical storage media including paper, the following must be considered:

- Responsibilities for controlling and notifying transmission, dispatch and receipt;
- Ensuring correct addressing and transportation of the message;
- Packaging that protects the contents from any physical damage likely to arise during transit, for example protecting against any environmental factors that can reduce the effectiveness of restoring storage media such as exposure to heat, moisture or electronic fields. Depending on the classification of information, use tamper evident or tamper-resistant controls.
- A list of authorized reliable couriers with identification and tracking mechanisms; and
- Keeping logs for identifying the contents, the protection applied as well as recording the list of authorized recipients, the times of transfer to the transit custodians and receipt destination.

4.3 Verbal Transfer

To protect verbal transfer of information, personnel and other interested parties should be reminded that they must:

- Not have confidential verbal conversations in public places or over insecure communication channels since these can be overheard by unauthorized persons;
- Not leave messages containing confidential information on answering machines or voice messages since these can be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialling;
- Be screened to the appropriate level to listen to the conversation;
- Ensure that appropriate room controls are implemented (e.g., sound proofing, closed door); and

- Begin any sensitive conversations with a disclaimer so those present know the classification level and any handling requirements of what they are about to hear.