Information Classification Policy

Change Control

Version	Created by	Owned by	Change date	Changes/Comments	Approved by
1.0	Stephen Houston	CTO	01/12/2022	Initial	CEO
1.1	Stephen Houston	CTO	27/02/2024	Reviewed by Management	CEO
1.2	Mark Kerr	CIO	06/04/2025	Annual Review	CEO
1.3	Mark Kerr	CIO	05/03/2026	Annual Review	CEO

Table of Contents

Information Classification Procedure

Roles and Responsibilities

Roles and responsibilities for managing information classification are defined as follows:

Role	Responsibility
1. Updating and maintaining an accurate information asset register	Information Security Officer
2. Classification of information assets	Information Security Officer
3. Accurate labelling of information assets	Asset owner
4. Secure and appropriate information handling	Any person with access rights to CONCEPT APPS LTD related information assets, in accordance with this Policy

If classified information is received from outside the organisation, CONCEPT APPS LTD *is responsible for its classification in accordance with the rules prescribed in this Policy, and the receiving person becomes the owner of such an information asset.*

Registering and Assigning Assets

It is the responsibility of the Information Security Officer to ensure that all new assets are registered with an Asset Tag before handing over to the newly assigned asset owner. The Asset Register must be updated with the Asset Tag ID, Serial Number (if applicable) and Asset Description.

All asset owners are also responsible for ensuring that their assigned information assets are registered accordingly. Any concerns should be raised with the Information Security Officer.

Classification of Information

Classification Criteria

The classification level is determined based on the following criteria:

- Value of information - based on impacts assessed during risk assessment
- Sensitivity and criticality of information - based on the highest risk calculated for each information item during risk assessment
- Legal and contractual obligations - based on the List of Legal, Regulatory, Contractual and other requirements.

Information Classification Matrix and Handling Guide

Classification category	Classification criteria	Example Information Assets	Information Labelling	Controls	Reproduction	Distribution and Storage	Destruction/ Disposal

Public	Information that may be broadly distributed without causing damage to the organisation, its employees and other interested parties. Senior Management or the Marketing Team must approve the use of this classification before publication or distribution. Information assets with Public classification	Materials authorised for public release such as webinars, web pages, blogs, job specs	No labelling necessary	Pre-approval from senior management before distribution Assess content for damage to reputation	Unlimited	No restrictions	Recycling

	may be disclosed or passed to persons outside the organisation.						

Internal Only	Unauthorised access/ disclosure, particularly outside the organisation, may cause minor damage and/ or inconvenience to the organisation.	Most corporate information falls into this category. Training materials, policies, procedures, guidelines, phone and email directories, SLA's, SharePoint pages.	Internal Use Apply to: • cover page, header or footer of word docs • footer of presentations • label on external storage media • All content in SharePoint or OneDrive unless otherwise specified, is classified for Internal Use Only.	Disclosure to anyone outside of CONCEPT APPS LTD requires senior management authorisation. Author: responsible for proper labelling. User: responsible for proper storage and document control.	Limited copies may be made only by employees or other interested parties who have signed a confidentiality agreement	Internal: • Hand to hand distribution to authorised persons External: • Sealed envelope, recorded delivery Electronic: • SharePoint and OneDrive but must only be shared with named users/groups and never publicly accessible Internal email system / communication channels.	Paper records: • must be shredded using the office secure document disposal wastebin Electronic data: • File erasure or • Media to be sent to CTO for appropriate disposal in accordance with the Disposal and Destruction Policy.

Highly Confidential	Highly sensitive or valuable information, both proprietary and personal. Must not be disclosed outside of the organisation without the explicit permission of C-level senior management.	Passwords/ account credentials, VPN tokens, credit card credentials, personal information (such as employee HR records) most accounting data, other highly sensitive or valuable proprietary information.	Confidential Client Confidential Apply to: • cover page, header or footer of word docs • footer of presentations • label on external storage media	Disclosure to anyone outside of CONCEPT APPS LTD requires C-level senior management authorisation. Author: responsible for ensuring that confidential information is distributed on a strict need-to-know basis. User: responsible for ensuring that confidential information is password	Limited copies if necessary but only with written permission from C-level senior management	Internal: • Hand to hand distribution to authorised persons External: • Sealed envelope, recorded delivery Electronic: • SharePoint but must only be shared with named users/groups and never publicly accessible Internal email system / communication channels, but must	Paper records: • must be shredded using the office secure document disposal wastebin Electronic data: • File erasure or • Media to be sent to CTO for appropriate disposal in accordance with the Disposal and Destruction Policy.

				protected/ kept under lock and key when not in use.		be password protected Storage: • Hard copies to be locked away when not in use Electronic copies to be stored on cloud restricted access folders in encrypted form.	

Handling Classified Information

All interested parties accessing classified information must follow the rules outlined in the matrix above.

CONCEPT APPS LTD must initiate disciplinary action each time these rules are breached or if information is communicated to an unauthorised person. Each incident related to handling classified information must be reported in accordance with the Incident Management Procedure.

Information assets may be taken off-premise only after obtaining authorisation in accordance with the Acceptable Use Policy.

The method for secure disposal and destruction of media is defined in the Disposal and Destruction Policy.

Authorised Access

Access to information assets, in particular those classified as 'Internal Use' or 'Highly Confidential', must follow the principle of least privilege. In other words, only those who need access to carry out their job function (or other defined interested parties) should have access in accordance with the Access Control Policy.

Reclassification

Information asset owners must review the confidentiality level of their information assets every 2 years and assess whether the confidentiality level can be changed. If possible, the confidentiality level should be lowered.

Communication

This policy and all major changes will be communicated to CONCEPT APPS LTD staff and other interested parties as appropriate.

If any employee feels that they require clarification on any part of this policy, please contact the Information Security Officer to discuss further.

Continual Improvement and Review

The Information Security Officer has overall responsibility for the review and update of this policy at the beginning of each year or at regular intervals as required.