INFORMATION SECURITY

Information Handling Policy

Version 1.3

Status	DRAFT
Classification	Restricted
Date Updated	31/08/2026
Version	1.3

This document is classified as RESTRICTED

Document Control

Revision history

Date	Version	Author	Summary of changes
19/04/2017	1.0	Rahim Hankin	Version 1 issued
06/02/2026	1.1	Reuben Njoku	Complete review by VCISO
17/06/2026	1.2	Muji Ali	Amended applicability
31/08/2026	1.3	Muji Ali	Information classification scheme and handling requirements aligned with the FDM ISMS and current Information Security training; classification decision flow added.

Approvals

Date	Version	Approver name	Approver title
13/02/2026	1.1	Rahim Hankin	Technical Director
17/06/2026	1.2	Muji Ali	Information Security Lead
31/08/2026	1.2	Muji Ali	Information Security Lead

Table of Contents

1	**Purpose**
2	**Scope**
3	**Policy Statement**
4	**Information Classification**
4.1	Classification Levels
5	**Information Ownership and Responsibility**
6	**Information Handling Requirements**
6.1	Creation and Collection
6.2	Storage and Processing
6.3	Access Control
6.4	Transmission and Sharing
6.5	Email and Collaboration Tools
6.6	Remote Working and Public Environments
6.7	Printing and Physical Records
6.8	Removable Media and Local Storage
6.9	Retention
6.10	Secure Disposal
7	**Information Incidents and Breaches**
8	**Training and Awareness**
9	**Exceptions**
10	**Compliance and Enforcement**
11	**Review and Continual Improvement**

1. Purpose

This policy defines how information must be classified, handled, stored, accessed, transmitted, retained, and disposed of within FDM CCS Insight.

Its objectives are to:

- protect the confidentiality, integrity, and availability of information
- prevent unauthorised disclosure, loss, or misuse of information
- support compliance with ISO/IEC 27001:2022, data protection legislation, contractual commitments, and client expectations
- provide clear and consistent handling rules for all forms of information.

2. Scope

This policy applies to:

- all employees, contractors, temporary staff, and third parties working for or on behalf of FDM CCS Insight
- all information, regardless of:
  - format (electronic, paper, verbal, visual)
  - location (office, home, client site, cloud, mobile);
  - system or medium (email, collaboration tools, databases, notebooks, recordings).

This includes information relating to:

- clients and partners
- employees and contractors
- research, analysis, and market insight outputs
- financial, legal, and commercial operations
- internal management and strategic activities.

3. Policy Statement

FDM CCS Insight information is a critical business asset and must be handled responsibly and securely throughout its lifecycle.

All information must:

- be classified appropriately
- be accessed only by authorised individuals for legitimate business purposes
- be protected against unauthorised access, disclosure, alteration, or destruction
- be retained only for as long as required and disposed of securely.

Information is not Public simply because it is unmarked. When unsure, use the higher applicable classification and contact Information Security.

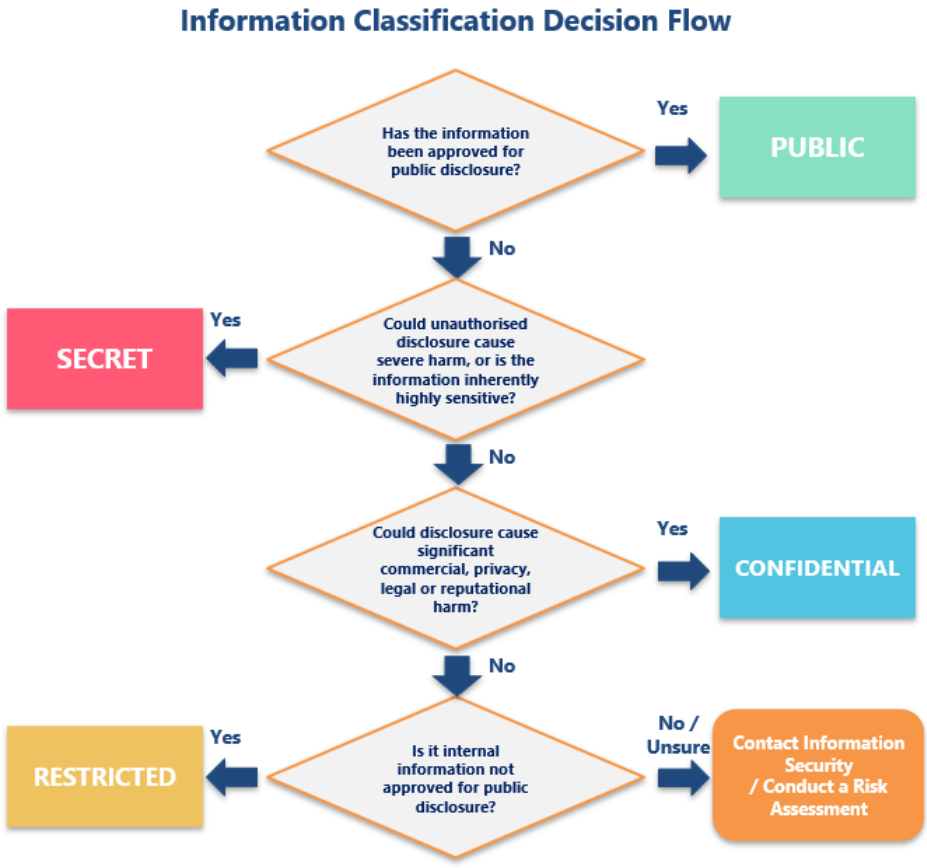
4. Information Classification

Classification is based on the sensitivity of the information and the potential impact of unauthorised disclosure. The classification may be increased where contractual, legal, regulatory or other specific obligations require it.

- Apply the highest classification present.
- Extracts, screenshots, summaries, emails, attachments and derived outputs inherit the classification of the information they contain.
- Label PowerPoints, spreadsheets and other information visibly - either in the document title when saving, in the document itself or, where appropriate, in the email subject.

Use the decision flow below when determining the appropriate classification.

- Classification hierarchy (highest to lowest): Secret, Confidential, Restricted, Public.



Classification rules

- Contractual, legal or regulatory requirements can require a higher classification
- Where information contains more than one classification, apply the highest classification present
- If unsure, use the higher classification and contact Information Security. Secret is the highest:
    1. Secret
    2. Confidential
    3. Restricted
    4. Public

Classification is based on sensitivity and the potential impact of unauthorised disclosure. The classification may be increased where specific obligations require it.

4.1 Classification Levels

a) Public

Information approved for public disclosure and which would not cause harm to FDM, its clients or individuals if shared externally.

Examples:

- published website content
- approved marketing material, public job adverts, published press releases and publicly available company information.

Handling requirements:

- use only approved/final versions and maintain the integrity of published information
- do not include Restricted, Confidential or Secret information; confirm approval before publishing new or amended content.

b) Restricted

Internal information that is not intended for the public and could cause limited harm, disruption or embarrassment if disclosed.

Examples:

- internal policies, procedures and training material
- internal contact lists, organisation charts, project documents, routine internal emails and meeting notes.

Handling requirements:

- share only for a legitimate business need and keep within approved corporate systems
- do not publish or forward externally without authority; check recipients and permissions before sharing.

c) Confidential

Information which, if lost or wrongly disclosed, could cause significant commercial, privacy, legal or reputational harm or cause distress to clients or individuals.

Examples:

- client contracts, pricing and commercial terms
- employee, payroll, sickness, performance or other personal data
- board papers, financial forecasts, risk registers, audit findings and supplier-security assessments
- internal financial information.

Handling requirements:

- need-to-know access only
- use approved FDM systems, verify recipients and apply appropriate protection
- external sharing only when authorised; secure retention and disposal rules apply
- Confidential information must not be printed.

d) Secret

Information where unauthorised disclosure or loss could cause severe harm to FDM, a client, an individual, a contract, the organisation's legal position, strategic objectives or security.

Examples:

- raw Sales Panel data and any related reference or derived output
- passwords, privileged credentials, recovery codes, encryption keys or sensitive system configuration details
- special category personal data, protected characteristics, highly sensitive client material or active incident/forensic information.

Handling requirements:

- named, explicitly authorised recipients only; approved secure storage and transmission
- no external sharing without prior written approval; encryption in transit and at rest where technically feasible; do not copy to personal email, devices or unapproved services
- Secret information must not be printed.

5. Information Ownership and Responsibility

- Each information asset should have an identified owner responsible for:
  - classification
  - access authorisation

  - ensuring appropriate protection and retention.
- Users are responsible for handling information in accordance with this policy and associated standards.

6. Information Handling Requirements

6.1 Creation and Collection

- Collect and create information only where there is a legitimate business need
- Avoid unnecessary duplication of sensitive information
- Apply classification at creation where possible

6.2 Storage and Processing

- Information must be stored only in FDM-approved systems and repositories
- Storing business information in personal email accounts or personal cloud storage is prohibited
- Restricted, Confidential and Secret information must:
  - be protected by access controls
  - not be stored on unmanaged or unencrypted devices

6.3 Access Control

- Access must be granted on a least privilege and need-to-know basis
- Users must not attempt to access information beyond their role
- Access rights must be reviewed periodically and revoked when no longer required

6.4 Transmission and Sharing

When sharing information:

- verify recipient identity and contact details
- share only the minimum information necessary
- use approved secure communication channels
- ensure appropriate contractual protections (e.g NDA, DPA) are in place for external parties

Restricted, Confidential and Secret information must not be shared via:

- personal email accounts
- consumer messaging applications
- unapproved file-sharing platforms.

6.5 Email and Collaboration Tools

- Care must be taken to avoid mis-sending information.
- Sensitive attachments should be encrypted or shared via secure links where available.
- Distribution lists must be used cautiously.

6.6 Remote Working and Public Environments

When working remotely or in public places:

- prevent unauthorised viewing (screen positioning, privacy filters where appropriate)
- avoid discussing sensitive matters in public areas
- ensure devices are locked when unattended.

6.7 Printing and Physical Records

- Confidential and Secret information must not be printed. Restricted information may be printed only where operationally necessary.

- Where Restricted information is printed, materials must be:
  - collected immediately from printers
  - stored securely when not in use
  - not left unattended on desks or in meeting rooms
- Clear desk and clear screen principles must be followed.

6.8 Removable Media and Local Storage

- Use of removable media is restricted and requires authorisation in line with A.7.10 - Storage Media.
- Where permitted, Restricted, Confidential or Secret information must be encrypted.
- Loss or theft of media must be reported immediately.

6.9 Retention

- Information must be retained only for as long as required by business, legal, or contractual obligations.
- Retention periods must follow applicable legal, contractual, business and ISMS retention requirements, including A.5.33 - Protection of Records and approved retention schedules.
- Information that is no longer required must be securely disposed of.

6.10 Secure Disposal

- Paper records: use approved confidential waste or shredding services.
- Electronic records: use secure deletion or approved IT disposal processes.
- Devices must be securely wiped before reuse or disposal. Disposal of Secret information must be appropriately authorised and recorded where required.

7. Information Incidents and Breaches

All users must immediately report:

- accidental or unauthorised disclosure of information
- loss or theft of devices or documents
- suspected data breaches or security incidents

Incidents will be managed in line with the Incident Response Plan and may trigger regulatory or client notifications where required

8. Training and Awareness

All personnel must:

- complete mandatory information security and data protection training
- acknowledge understanding of this policy
- apply its requirements in day-to-day work

9. Exceptions

Any exception to this policy:

- must be formally requested
- must include a documented risk assessment
- requires approval from the Head of Information Security
- must have a defined expiry and review date

10. Compliance and Enforcement

Failure to comply with this policy may result in:

- disciplinary action
- removal of system access
- contract termination
- legal or regulatory action where applicable

11. Review and Continual Improvement

This policy will be reviewed:

- at least annually
- following significant incidents, audits, or changes to business operations, technology, or regulation