[Company]

INFORMATION CLASSIFICATION AND HANDLING POLICY

Classifying and handling information

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Information Classification and Handling Policy

3.1 Purpose

The purpose of this policy is ensuring the correct classification and handling of information based on its classification.

The information contained in the policy is summarised in the accompanying document:

Information Classification Summary.xlsx

3.2 Scope

All employees and third-party users.

Personal Data as defined by GDPR.

Information that forms part of systems and applications deemed in scope by the ISO 27001 scope statement.

3.3 Principle

Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

3.4 Information Storage

Company information is not to be stored on personal equipment or systems including personal email and cloud-based storage unless approved by senior management and recorded in a register of approved users.

Company information is to be protected by access control as recorded in the Access Control Policy.

3.5 Confidential Information Storage

Confidential information is encrypted at rest and in transit when stored inside and outside company primary systems.

Confidential Information and Internal Information is not stored or processed in development or test environments.

Confidential Information physical storage is recorded in the asset register.

Physical transfer of devices containing confidential information is via recorded, secure courier.

Confidential Information is not transmitted over public networks.

3.6 Control of Devices and Media Containing Information

All electronic and paper media containing confidential information is physically secured from unauthorised access by securing in locked draws, cabinets and / or rooms.

Information Asset Registers are in place a reviewed at least annually.

3.7 Information Back Up

Company information is backed up, retained, and tested in line with the backup schedule.

Company backups are encrypted using strong vendor encryption.

All backups are stored in secure locations.

Backups are tested on a periodic basis.

3.8 Information Destruction

3.8.1 Destruction of Hard copy paper records

Hard copy paper records containing internal and confidential information are shredded to a standard no less than DIN32757 Level 4 or placed within the confidential waste bins provided.

Public hard copy paper records can be recycled or placed in general waste.

3.8.2 Destruction of Electronic Information

All media and devices that may contain internal or confidential information are wiped of electronic information prior to destruction or reuse to a minimum of the DoD 5220.22-M 3-Pass method or equivalent.

Logs of the wipe are maintained by the application where possible.

3.8.3 Destruction of Electronic media / devices

Electronic media and devices that may contain internal or confidential information are destroyed by approved, specialist third party contract suppliers.

Destruction certificates are sought and kept for complete audit trail.

An inventory of devices, including those destroyed, is maintained.

4 Information Classification

Information is classified as either Confidential, Internal or Public. The following pages give further guidance for each level of classification.

4.1 Confidential Information

4.1.1 Confidential Information Guidance

Confidential information is information where:

- Disclosure has a significant short-term impact on operations or tactical objectives
- Disclosure has a serious impact on long term strategic objectives or puts the survival of the organization at risk.

4.1.2 Confidential Information and GDPR

'Confidential' information has significant value for the company and unauthorized disclosure, or dissemination could result in severe financial or reputational damage to the company, including fines of up to 4% global turnover from the Information Commissioner's Office, the revocation of contracts and the failure to win future bids.

Data defined by the GDPR as Special Categories of Personal Data falls into this category.

4.1.3 Confidential Information Examples

GDPR defined Special Categories of personal data:

- racial/ethnic origin
- political opinion
- religious beliefs

- trade union membership
- physical/mental health condition
- sexual life
- criminal record

Also

- salary information
- individuals' bank details
- passwords
- large aggregates of GDPR defined Personal Data (>1000 records) including elements such as name, address, telephone number
- HR system data

Company specific propriety information unique to and fundamental to the operation of the company.

4.1.4 Confidential Information Document Marking

Documents containing confidential information are marked with the word Confidential.

4.1.5 Confidential Information Controls

Only those who explicitly need access must be granted it, and only to the least degree in order to do their work (the 'need to know' and 'least privilege' principles).

When held outside the company, on mobile devices such as laptops, tablets, or phones, or in transit, 'Confidential' information must be protected behind an explicit

logon and by AES 256-bit encryption at the device, drive, or file level, or by other controls that provide equivalent protection.

4.1.6 Confidential Information Destruction

Confidential waste bins,

Shred, erase permanently or degauss magnetic media

Use specialist third party destruction companies with records of destruction.

4.2 Internal Information

4.2.1 Internal Information Guidance

Internal information is information where:

Disclosure causes minor embarrassment or minor operational inconvenience

4.2.2 Internal Information and GDPR

‘Internal’ information is open to groups of people within the company.

Information defined as Personal Data by the GDPR falls into this category, such as names, email addresses, phone numbers, photos. If information does not fit into the ‘Confidential’ or ‘Public’ categories, then it is ‘Internal’ information.

Public disclosure or dissemination of this information is not intended and may incur fines from the ICO and negative publicity for the company.

4.2.3 Internal Information Examples

The majority of company information falls into this category. Policies, procedures, logs, plans, training materials, management reports, internal communications, customer lists, order history all not otherwise marked as 'Confidential'.

Name, email, work location, work telephone number, photographs

Other information:

- reserved committee business

- draft reports, papers, and minutes
- systems
- internal correspondence
- information held under license
- company policy and procedures

4.2.4 Internal Information Document Marking

Documents containing internal information are marked with the word Internal.

Unmarked documents are classified as INTERNAL

4.2.5 Internal Information Controls

It is subject to controls on access, such as only allowing valid logons from groups of staff, but it does not have the stricter controls required by ‘Confidential’ information. ‘Internal’ information must be held in such a manner that prevents unauthorised access i.e., on a system that requires a valid and appropriate user to log in before access is granted.

4.2.6 Internal Information Destruction

Confidential waste bins,

Shred, erase permanently or degauss magnetic media

Consider specialist third party destruction companies

4.3 Public Information

4.3.1 Public Information Guidance

Disclosure causes no harm

4.3.2 Public Information and GDPR

‘Public’ information can be disclosed or disseminated without any restrictions on content, audience, or time of publication.

4.3.3 Public Information Examples

Information already in the public domain, websites, marketing materials, records published on companies’ house, policies marked as 'Public’.

4.3.4 Public Information Document Marking

Public documents are marked with the word Public unless published on public platforms where no marking will be required.

4.3.5 Public Information Controls

Disclosure or dissemination of the information must not violate any applicable laws or regulations, such as privacy rules. Modification must be restricted to individuals who have been explicitly approved by information owners to modify that information, and who have successfully authenticated themselves to the appropriate computer system.

4.3.6 Public Information Destruction

General Waste/ Recycling

5 Policy Compliance

5.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.