# Information Classification and Handling Policy

# Introduction

## Purpose

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

## Scope

This policy applies to all COMPANY NAME employees and all information held within the business, including Personal Data as defined by GDPR.

## Responsibilities

It is the responsibility of all COMPANY NAME employees to ensure that their information is correctly classified and handled in line with this policy.

# Information Classifications

Information classification helps us to identify the level of information we are dealing with at COMPANY NAME and how it should be handled and protected.

Information is classified as either:

* In Strictest Confidence
* In Confidence
* Internal Use Only
* Public

# Types of information to be classified

It is not possible to list out all types of information that is used within COMPANY NAME, but these are some examples of information you may deal with on a daily basis and the category it would fall into, whether the information is verbal, electronic or on paper.

Classified information can be in different forms and types of media, e.g.:

* electronic documents
* information systems / databases
* paper documents
* storage media (e.g., disks, memory cards, etc.)
* information transmitted verbally
* email

# Why a classification label should be used

The confidentiality notices allow us to quickly see what category of information we are handling and what appropriate steps should be taken to protect that information. Information owners are responsible for the classification labelling of their documents when they are created. This determines how the owner and recipients should store and share (if applicable) the information.

If in doubt of which classification to use, take a cautious approach and default to the higher category under consideration.

The classification should be clearly visible on the top of the document to ensure compliance with this policy.

Where templates are created within the business, these should include the classification option.

# Sharing of Information

For each category, we have defined how we can share information, if at all, and security measures to implement.

Refer to International and third party data transfer policy and General data transfer policy for more information.

# Document Classification Matrix

The table below provides guidance for each level of classification with example of the kinds of information which would fall into each category and how they should be handled.

Further guidance can be provided by the ISO if required.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Classification | In Strictest Confidence | In Confidence | Internal Use Only | Public |
| Summary | High sensitivity | Medium sensitivity | Low sensitivity | Not sensitive |
| How do we label information? | In Strictest Confidence | In Confidence | Internal Use Only | Public |
| Risk & impact of information breach | Breach of legal / regulatory obligations threatens business survival or significantly affects our reputation  Damages customer confidence or leads to loss of competitor advantage and/or loss in revenue. | Limited impact – may cause some harm if the information is accessed / and or shared by an unauthorised external source. | Minimal impact to the business. | Will NOT cause any risk to the business. |
| Is further sharing possible | No, unless specifically authorised by the information owner and then security precautions to be taken when sharing (see below).  | No, unless authorised by the information owner.  To third parties (including contractors or consultants) where authorised and if relevant confidentiality agreement in place (e.g. in written contract, or separate NDA) (see below) | Yes, to employees only | Yes |
| Security precautions (sharing of information) | Electronic documents: * Password protection of files
* Encryption of documents
* Do not download to personal devices
* Store in an access-controlled folder
* Do not print unless necessary and collect from printer asap
* Not to be transmitted over public networks.

 Paper documents: * Store in a lockable cabinet.
* Ensure confidential shredding/place in confidential waste bins after use
 | Electronic documents: * Password protection of files
* Store in access-controlled files
* Do not print unless necessary and collect from printer asap
* Not to be transmitted over public networks.

 Paper documents: * Store in a lockable cabinet
* Ensure confidential shredding or place in confidential waste bins after use
 | Electronic documents: * Store in relevant electronic department folders/systems

 Paper documents: * Store in a lockable cabinet
* Ensure confidential shredding or place in confidential waste bins after use
 | Electronic documents: * Store in relevant folders and/or systems

 Paper documents: * Discard in general waste/recycling bins
 |
| Information Examples | * Significant incidents
* Annual/half year financial reports prior to publication
* Strategy under development
* Grievance & disciplinary records
* Information held under NDA
* New contract negotiations prior to execution
 | * Published company strategy/plans
* Audit reports
* Employee personal data
* Customer personal data
* Customer Pricing
* Business Continuity Plans
 | * Policies, Procedures & logs
* Template documentation
* Training Material
* KPIs
* Employee Photos
* Internal Communications
 | * Sales and Marketing collateral
* Our website information
* Press releases and publications
* Records published on companies’ house
 |

# Policy Compliance

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.

# Exceptions

Any exception to the policy must be approved by the policy owner in advance.