**Company Information Classification & Handling Policy**

**Doc A8.2**

**Version: 1.0**

Publication Date: January 01, 2019

Current Status: Published

Author(s): Michael Woolard

Last Reviewed: Michael Woolard

**Table of Contents**

1 Information Classification and Handling Policy 3

1.1 Scope 3

1.2 Responsibilities 3

1.3 Classification 3

1.4 Labelling 4

1.5 Confidentiality Agreements and Non-Disclosure Agreements (NDA’s) 4

1.6 Storage 4

1.7 Cloud Storage and sharing services 5

1.8 Storage on Personal Equipment 5

1.9 Communication & Transmission 5

1.10 Reclassification 5

1.11 Destruction 5

1.12 Exchange of Information and Transport of information 5

1.13 System Documentation 5

2 Document Control and Approval 6

2.1 Distribution 6

2.2 Version Information 6

Annex A: Classification and Handling Guidelines Summary 7

# Information Classification and Handling Policy

## Scope

This document outlines the policies and procedures relating to the classification of information assets within Wacky Widget.

## Responsibilities

All employees and contractors share the responsibility for ensuring that information Assets are assigned an appropriate level of protection by following this classification policy.

Customer provided data, processed by Wacky Widget systems, must be re-classified by the asset owner and handled in accordance with this policy. Staff working at a customer site, with customer data, and on customer computing equipment, must follow the customer classification procedures.

## Classification

The organization classifies information into 5 levels of classification: -

* Company Secret
* Personal Data, Personally Identifiable Information (PII) and Payment Data (PCI)
* Confidential
* Company Sensitive
* Public

Assets holding information are protected in line with the highest classification of information held or processed on the asset wherever this is practicable.

Information that is classified as Company Secret must identify the individuals or roles to whom the information is restricted.

Company Secret and Personally Identifiable data must not be revealed by mistake or otherwise to unauthorized personnel.

The classification information must be included in the document footer, which must be manually set to appear on all pages of the document, or on the media on which it is recorded.

Information received from outside the organization should be re-classified by its recipient so that it complies with Wacky Widget classification.

Information sent and received internally that is not marked with a classification level is treated as Company Sensitive. Any unmarked information sent externally is classified as public information.

If any Confidential, Personal, PCI, or Company Secret data is sent externally without the correct classification or protective controls, then that action is classed as mis-conduct.

The information asset owner is responsible for re-classifying information.

## Labelling

From the date of issue of this policy, all information should be labelled as follows:

Electronic documents are labelled with the appropriate classification set in the document footer. Documents that do not have footers are marked accordingly.

## Confidentiality Agreements and Non-Disclosure Agreements (NDA’s)

The organization’s confidentiality agreement, which requires the maintenance of confidentiality for a set period, includes clauses that:

* Define the information to be protected, its ownership and its classification
* Set out the expected duration of the agreement
* Describe the required actions on termination of the agreement
* Identify the various responsibilities and actions required of signatories in order to avoid unauthorized information disclosure
* Identify the permitted use of the information, and the signatories’ rights in respect of that information
* Clarify rights to audit and monitor use of that information
* Describe the process for notification and reporting of unauthorized disclosure or breaches of confidentiality
* Set out the terms for the information to be returned or destroyed at agreement cessation
* Describe the actions that are to be taken if the agreement is breached

The agreement is reviewed by the organization’s legal department as required and whenever they identify a relevant change in the law.

The agreement is also reviewed whenever there are significant changes to contracts of employment and contracts for services with third parties.

Third parties are required to sign an NDA prior to being given access to sensitive and above data.

## Storage

All media should be stored in a safe, secure environment.

All paper media declared Company Secret, Confidential or Personally Identifiable Information must be stored in lockable cabinets with owners identified.

All electronic data files that have been declared as Company Secret, Confidential, or Personally Identifiable Information must be stored in a secured directory / folder with strict access restrictions. In addition, wherever possible such files are password protected. Encryption at rest of database structures and full disk encryption of file storage drives should be implemented where possible. Backup copies of all such files / are taken in a secured folder / directory.

Other forms of information whether digital or paper should have access rights based on Need-To-Know and it is the individual’s responsibility to store these securely.

Only company issued encrypted USB sticks, external hard drives and flash drives may be used for storing confidential company data. Data stored on removable and storage media must be encrypted if used for the storage of Company Sensitive, Confidential, Company Secret or Personal Data.

## Cloud Storage and sharing services

Staff requiring access to such a service should approach the Internal IT team to discuss their requirements so that an appropriate solution can be found. Only solutions on the approved technology list may be used.

## Storage on Personal Equipment

Do not store company data on any personal media

## Communication & Transmission

Communication of digital or paper information classified as Company Sensitive, Confidential, Company Secret or Personal Data, must be done on a ‘Need-To-Know’ basis and through a secure mode of communication and to suitable recipients only.

Company Sensitive, Confidential, Company Secret and Personal Data must not be discussed in non-secure environments.

## Reclassification

The decision to change classification shall be taken by the relevant information asset owners.

Once the level of classification has changed, the method of handling, storage, communicating must be changed as per guidelines defined above.

## Destruction

All paper media that has been declared Company Secret, Confidential and Personally Identifiable Information that is deemed ready for destruction, is cross cut shredded for secure disposal.

Hard drives, removable media and any similar items which may have contained Personally Identifiable, Confidential or Company Secret information and such are shredded beyond use.

## Exchange of Information and Transport of information

Any information transmitted externally is protected from unauthorized access by the controls established within Wacky Widget. See Annex A for guidance.

Any Company Secret, Confidential or Personally Identifiable Information sent externally is protected from unauthorized access by either being sent only to the intended recipient or if physically sent by sealing the protective container or being hand carried by a member of staff.

## System Documentation

System documentation is classified as Confidential or Company Sensitive depending on the nature of the documentation and must be protected accordingly.

# Document Control and Approval

The Chief Information Security Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff and is the published version.

Signature: Executive Manager Signature Date: 01.01.2019

## Distribution

|  |  |
| --- | --- |
| **Name** | **Role** |
| *Intranet* | *Distribution to all staff* |

## Version Information

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author(s)** | **Details** |
| 0.1 | 11/28/18 | M.Woolard | First draft |
| 0.2 | 12/07/18 | M.Woolard | Second draft |
| 1.0 | 01/01/19 | M.Woolard | First published |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Annex A: Classification and Handling Guidelines Summary

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Classification** | **Public** | **Company Sensitive** | **Confidential** | **Personal Data, PII or PCI** | **Company Secret** |
| **Description** | Information that can be disclosed to the general public without concern for harming the company, employees, customers or business partners. | Information that can be disclosed within the company but may cause harm to the company if disclosed externally | Anything that provides a competitive advantage and if disclosed would create severe problems for the organization. | Personal Data, Personally Identifiable Information (PII) or payment data such as credit card details covered by Payment Card Industry Data Security Standard  (PCI DSS) | Information usually available to Board members only and if disclosed could cause irreparable harm to the company. |
| **Examples** | Company brochure or web-site.  Business contact information. | Policies and procedures, Intranet content, system and software in use, contracts, offers, other company data that isn’t commercially sensitive. | Customer Confidential Data, Passwords, Pricing, executed contracts, technical design data, customer details, safety information etc. | Individuals name and address, IP Addresses, VIN, usernames, bank account number, credit card number. | Board papers, takeover plans, confidential financial data etc. |
| **Labelling** | Optional | Optional | Mandatory  Printed records must be numbered sequentially as part of a set | Mandatory  Printed records must be numbered sequentially as part of a set | Mandatory  Printed records must be numbered sequentially as part of a set |
| **Storage Encryption** | Not required | Optional | Mandatory | Mandatory | Mandatory |
| **Logging** | No Restrictions | Logs are for internal use only and should not be shared externally without consent from asset owner | Information may be logged. Access is limited to a “need to know basis” down to record level, and access controls should be implemented on the log access (both directly and through tools) | Only IP Address, VIN, and Username may be logged. Requirements:   * Logged information can be removed upon request * Access controls - “need to know” * Obfuscate where possible to eliminate PII (0 of last 5 of VIN) | Never |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Classification** | **Public** | **Company Sensitive** | **Confidential** | **Personal Data, PII or PCI** | **Company Secret** |
| **Reproduction** | No restrictions | Due care and custody | Due care and custody based on Access Control requirements. | None permitted except for any backups necessary to meet business continuity needs | Copies must be limited and returned to the originator or designated representative. |
| **Transmit Encryption** | Not required | Optional | Mandatory for transmission across open public networks using Company approved technology | Mandatory for transmission across open public networks using Company approved technology | Mandatory for transmission across open public networks using Company approved technology |
| **Physical Transmit** | Not required | Retained within company premises or addressed to intended recipient | Retained within company premises or addressed to intended recipient | Secure courier if sent outside company or hand delivered. | Secure courier if sent outside company or hand delivered. |
| **Access Control** | Not required | Staff and trusted contractors only | Discretionary access as determined by owner.  Principle of least access should be followed. | Strictly need to know only enforced by both physical and logical controls | Strictly need to know only enforced by both physical and logical controls |
| **Access Auditing** | Not required | Not required | Optional | Track and monitor all access | Optional |
| **Secure Disposal** | Optional | Mandatory using Company approved method | Mandatory using Company approved method | Mandatory using Company approved method | Mandatory using Company approved method |
| **Transmit approval** | Not required | Not required | Data owner or Document Creator | Data owner or Document Creator | Executive data owner |
| **Retention requirements** | Disposal must be authorized by the data owner | Disposal must be authorized by the data owner | Disposal must be authorized by the data owner | Disposal must be authorized by the data owner | Disposal must be  authorized by a data owner |
| **Classification** | **Public** | **Company Sensitive** | **Confidential** | **Personal Data, PII or PCI** | **Company Secret** |
| **Classification Review** | After any major change and every three years | After any major change and every two years | After any major change and annually | Annually | After any major change and annually |
| **Sharing of information** | Internal: Free to share  External: Free to share | Internal: Free to share  External: Need to know | Internal: Need to know  External: Need to know with NDA in place | Internal: Need to know  External: Rare occasion. Legal approval. NDA and Contract in place | Internal: Strict need to know  External: Strict need to know with NDA in place |
| **Stored on Public Cloud or File Sharing Service** | Allowed | Temporary | Temporary. Must be encrypted.  Never exposed in plain text on 3rd party system | Limited to need. Must be encrypted.  Never exposed in plain text on 3rd party system | Limited to need. Must be encrypted.  Never exposed in plain text on 3rd party system |