

Information Security and Privacy Classification Guidelines

Reference: ISMS-C DOC 8.2

DocumentKits Issue No: 2.0

Organisation Issue No:

DocumentKits Issue Date: 01/06/2020

Organisation Issue Date:

1. Scope [ISO 27002 Clause 8.2.1]

All Organisation Name's information assets and services (see control section 8.2 of the [Information Security Manual](#)) are classified, taking into account their legality, value, sensitivity and criticality to Organisation Name.

2. Responsibilities

2.1 The
"owner"

of each asset (see control section 8.1.2 of the [Information Security Manual](#)) is responsible for its classification, for ensuring it is correctly labelled and for its correct handling in line with its classification.

2.2 The intended recipient of any information assets sent from outside Organisation Name becomes the
"owner"

of that asset.

2.3 The Finance Director (CFO) is responsible for maintaining the inventory of assets and services together with their classification levels.

2.4 The Head of IT (CIO) is responsible for the technical labelling mechanisms.

2.5 The Head of IT (CIO) is responsible for the creation, maintenance and review of electronic distribution lists and for ensuring that they conform to this security classification system.

2.6 All Users of organisational information assets (including mobile phones, PDAs and other peripherals) have specific responsibilities identified in their user agreements.

2.7 Every Manager/Executive (generic/line) /
"owners"

is responsible for ensuring that mail/postal services ([Mail/Postal Services Work Instruction](#)), voicemail and voice communication ([Voicemail Work Instruction](#)), fax machines ([Fax Machine Work Instruction](#)), photocopiers ([Photocopier Work Instruction](#)), couriers,
"other services"

and sensitive documents (including
"cheques, invoices, and headed notepaper")

are handled in line with specific work instructions.

3. Classification

3.1 Organisation Name classifies information into an appropriate number of levels for their structure. It could be
"five"

levels of classification: confidential, restricted,
"personally identifiable information (PII)"

, private and public.

"Enter the classification levels you intend to use in your organisation."

3.2 The classification level of all assets is identified, both on the asset (see control section 8.2.2 of the [Information Security Manual](#)) and in the asset inventory (see control section 8.1.1 of the [Information Security Manual](#)).

3.3 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, in line with Clause 8, below.

3.4 Information received from outside Organisation Name is re-classified by its recipient (who becomes its "owner"

) so that, within Organisation Name, it complies with this procedure.

3.5 Information that is not marked with a classification level is returned to its sender for classification; if it cannot be returned, it is destroyed.

3.6 The classifications of information assets are reviewed every "six months"

by their "owners"

and if the classification level can be reduced, it will be. The asset "owner"

is responsible for declassifying information.

3.7 Confidential: this classification applies to information that is specifically restricted to the Board of Directors and specific professional advisers.

3.7.1 Information that falls into this category must be marked 'Confidential', and its circulation is kept to a minimum

"with the names of the people to whom it is limited identified on the document."

"Each copy of a document that has this level of classification is numbered and a register is retained identifying the recipient of each numbered copy."

3.7.2 Examples of confidential information might include information about potential acquisitions or corporate strategy, or about key organisational personnel, such as the Chief Executive Officer (CEO).

3.7.3 Confidential information sent by email must be encrypted and digitally signed, in line with the [Policy on Use of Cryptographic Controls](#), and sent only to the email box of the identified recipient.

"Depending on your risk assessment, you may want to insert the restrictions about wireless handling and PDAs."

3.7.4 Confidential information can only be sent by fax if the nominated recipient is available to receive it directly from the fax machine.

3.7.5 Confidential information can only be processed or stored on facilities which have been assessed (in line with section 6.4 of the [Information Security Manual](#)) as providing adequate security for such information. This classification is recorded on the asset inventory drawn up in line with control section 8.1.1 of the [Information Security Manual](#).

3.7.6 The amount of information that falls into this category should be carefully limited; the cost and operational inconvenience of protecting it properly is such that it needs only to be information whose release can significantly damage Organisation Name.

3.8

"Enter Restricted, or enter the name of the level of classification in your organisation that will have this level of restriction..."

Information of this category is restricted to Employees/Staff above the level of:

"Identify here the levels of staff that should have access to this level of information; remember that their PAs and assistants are also likely to see this information, so take this into account in your procedure."

3.8.1

"Enter 'Examples of Restricted', or enter the name of the level of classification in your organisation that will have this level of restriction..."

information include draft statutory accounts, which might be available to everyone in senior management, or implementation plans for corporate restructuring, which senior managers need to work through before they are rolled out.

3.8.2

"Enter Restricted, or enter the name of the level of classification in your organisation that will have this level of restriction..."

information sent by email must be encrypted and digitally signed, in line with the [Policy on Use of Cryptographic Controls](#), and sent only to the email box of individuals known to be allowed to receive such information.

"Depending on your risk assessment, you may want to insert restrictions about wireless handling and PDAs."

3.8.3

"Enter Restricted, or enter the name of the level of classification in your organisation that will have this level of restriction..."

information can only be sent by fax if a recipient from the required level is available to receive it directly from the fax machine.

3.8.4

"Enter Restricted, or enter the name of the level of classification in your organisation that will have this level of restriction..."

information can only be processed or stored on facilities which have been assessed (in line with Section 6.4 of the [Information Security Manual](#)) as providing adequate security for such information. This classification is recorded on the asset inventory drawn up in line with control section 8.1.1 of the [Information Security Manual](#).

3.9

"[Personally identifiable information (PII) . This information is available to the majority of employees within Organisation Name, but is subject to more stringent controls than information classified as 'Private'.

3.9.1 Examples of PII include names, addresses, usernames and other online identifiers that could be used to identify a person.

3.9.2 PII sent by email must be...

3.9.3 Any PII transmitted over untrusted networks (including the Internet) must be...

3.9.4 PII may may/not be sent by fax...

3.9.5 PII can only be processed or stored on facilities that have been assessed (in line with section 6.4 of the [Information Security Manual](#)) as providing adequate security for such information. This classification is recorded on the asset inventory drawn up in line with control section 8.1.1 of the [Information Security Manual](#)."

3.10

"Enter Private, or enter the name of the level of classification in your organisation that will have this level of restriction..."

This classification covers all information assets that have value but which do not need to fall within either of the other categories.

3.10.1 Everyone employed by Organisation Name is entitled to access information with this classification.

3.10.2 This information has no restrictions in terms of how it is communicated, other than that it is not cleared for release outside Organisation Name.

3.11

"Enter Public, or enter the name of the level of classification in your organisation that will have this level of restriction..."

This is information which can be released outside Organisation Name.

4. Labelling [ISO 27002 Clause 8.2.2]

4.1 Documents are labelled as set out above, in the document footer. Documents that do not have footers are marked by addition of a physical, stick-on label.

4.2 Removable and storage media (CD-ROMs, USB sticks, tapes, etc.) are labelled "describe any colour-coded systems used to indicate classification levels."

4.3 Electronic documents and information assets, including assets stored in Cloud services, are labelled by "insert mechanism."

4.4 Information processing facilities are labelled "describe how"

4.5 All emails have a standard disclaimer "set out where?"

to the effect that the views expressed in the email are those of the sender alone and do not reflect the views of Organisation Name.

"Detail how you will implement this."

5. Handling [ISO 27002 Clause 8.2.3]

5.1 Information assets can only be handled by individuals who have appropriate authorisations or on facilities that

"meet what requirements?"

5.2 The requirements for transmission, receipt, storage and declassification of classified and restricted information are described above. Destruction of information media can only be carried out by someone who has an appropriate level of authorisation and in line with the requirements of [Media and Information Handling Procedure](#).

5.3 Organisation Name requires that confidential documents are only circulated

"in secure PDF format/as read-only documents."

5.4 Portable and storage media (including spooled media) must be moved, received and stored on the basis of the highest classification item recorded on them, and are subject to the physical security controls specified in [Equipment Security](#), and are protected appropriately while being recorded.

"Set out how this is to be done in your organisation."

5.5 Agreements with external organisations (see control section 15.1.2 of the [Information Security Manual](#)) which include information sharing (see also control section 13.2.2 of the [Information Security Manual](#)) include a matrix for translating their security classifications into this one.

5.6 Where it is necessary to create hard copy materials containing PII, the creator shall

ensure that only such materials as are necessary to fulfil the purpose are created.

"6. Customer assets in Cloud services [ISO 27017 Clause 8.2.2]

6.1 Organisation Name provides the following functionality to customers of its Cloud service(s) to enable them to classify and label information assets stored within those service(s):

Describe the mechanism(s) you provide to customers of your Cloud service in respect of classification and labelling."

Document owner and approval

The Information Security Manager is the owner of this document and is responsible for keeping it up to date.

The current version of this document is available to

"Specify which members of staff this document is intended for"

and is published

"Describe the location(s) – electronic and physical – where this document is available"

Its approval status can be viewed in [Master List of Document Approval](#).