1. **Scope** [ISO27002 Clause 8.2.1]

All Retirement Capital’s information assets and services (see control section 8.2 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx)) are classified, taking into account their legality, value, sensitivity and criticality to Retirement Capital.

1. **Responsibilities**
   1. The owner of each asset (see Control A.8 Asset Management / 8.1.2 in 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. The intended recipient of any information assets sent from outside Retirement Capital becomes the owner of that asset.
   3. The Managing Director is responsible for maintaining the inventory of assets and services together with their classification levels.
   4. The IT Manager is responsible for the technical labelling mechanisms.
   5. The IT Manager is responsible for the creation, maintenance and review of electronic distribution lists and for ensuring that they conform to this security classification system.
   6. All users of organisational information assets (including mobile phones, PDAs and other peripherals) have specific responsibilities identified in their user agreements.
   7. Manager/owners are responsible for ensuring that mail/postal services (work instruction [ISMS-C DOC 8.1.3c](ISMS-C_DOC_8.1.3c.docx)), voicemail and voice communication (work instruction [ISMS-C DOC 8.1.3d](ISMS-C_DOC_8.1.3d.docx)), fax machines (work instruction [ISMS-C DOC 8.1.3e](ISMS-C_DOC_8.1.3e.docx)), photocopiers ([ISMS-C DOC 8.1.3f](ISMS-C_DOC_8.1.3f.docx)), couriers and sensitive documents (including cheques, invoices, headed notepaper) are handled in line with specific work instructions.
2. **Classification**
   1. Retirement Capital classifies information into four levels of classification (confidential, restricted, private and public).
   2. The classification level of all assets is identified, both on the asset (see Control A.8 Asset Management / 8.1.2) and in the asset inventory (see Control A.8 Asset Management / 8.1.1) in the Information Security Manual.
   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.
   4. Information received from outside Retirement Capital is re-classified by its recipient (who becomes its owner) so that, within Retirement Capital, it complies with this procedure.
   5. Information that is not marked with a classification level is deemed ‘Private’.
   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 de-classifying information.
   7. **Confidential: this classification applies to information that is specifically restricted to the Board of Directors and specific professional advisers.**
      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.
      2. Examples of confidential information might include information about potential acquisitions or corporate strategy, or about key organisational personnel, such as the Managing Director*.*
      3. Confidential information sent by e-mail must be encrypted and digitally signed, in line with the control section A10.1 of the Information Security Manual, and sent only to the e-mail box of the identified recipient.
      4. Confidential information CANNOT be sent by fax.
      5. Confidential information can only be processed or stored on facilities which have been assessed (in line with Section 6.4 of the 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 Manual.
      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 Retirement Capital.

* 1. **Restricted: information of this category is restricted to company managers only:**
     1. Examples of restricted 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 prior to their being rolled out.
     2. Restricted information sent by e-mail must be encrypted and digitally signed, in line with control section A.10 Cryptography, 10.1 of the Manual, and sent only to the e-mail box of individuals known to be allowed to receive such information.
     3. Restricted information can only be sent by fax if a recipient from the required level is available to receive it directly from the fax machine.
     4. Restricted information can only be processed or stored on facilities which have been assessed (in line with Control A.11 Physical and Environmental Security / 11.1.1) as providing adequate security for such information. This classification is recorded on the asset inventory drawn up in line with Control A.8 Asset Management / 8.1.1. (Refer the Information Security Manual for Controls).

* 1. **Private: this classification covers all information assets that have value but which do not need to fall within either of the other categories**.
     1. Everyone employed by Retirement Capital is entitled to access information with this classification.
     2. This information has no restrictions in terms of how it is communicated, other than that it is not cleared for release outside Retirement Capital.
  2. **Public: this is information which can be released outside Retirement Capital**.

1. **Labelling** [ISO27002 Clause 8.2.2]
   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.
   2. Removable and storage media (CD-ROMs, USB sticks, tapes, etc.) are labelled in Red for Confidential, Blue for Restricted, Yellow for Private and Green for Public.
   3. Electronic documents and information assets are labelled within the document.
   4. All e-mails have a standard disclaimer to the effect that the views expressed in the e-mail are those of the sender alone and do not reflect the views of Retirement Capital.
2. **Handling** [ISO27002 Clause 8.2.3]
   1. Information assets can only be handled by individuals that have appropriate authorisations or on facilities that have been approved to do so by the CISO (DIRECTOR).
   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 [ISMS-C DOC 8.3](ISMS-C_DOC_8.3.docx).
   3. Retirement Capital requires that confidential documents are only circulated in secure pdf format.
   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 [ISMS-C DOC 11.2.1](../Control%20A11%20-%20physical%20and%20environmental%20security/ISMS-C_DOC_11.2.1.docx), and are encrypted while being recorded.
   5. Agreements with external organisations (see control section 15.1.2 of the Manual) which include information sharing (see also control section 13.2.2 of the Manual) include a matrix for translating their security classifications into this one.

***Document Owner and Approval***

The Information Security Manager 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 on the corporate intranet

This procedure was approved by the Chief Information Security Officer (CISO (DIRECTOR)) on 14th November 2020 and is issued on a version-controlled basis under his/her signature.

Signature: Date: 14/11/2020

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 14/11/2020 |
|  |  |  |  |
|  |  |  |  |