1. **Scope**

All of *{OrganisationName}*’s information assets are within the scope of this procedure.

1. **Responsibilities**
   1. The *{FinanceDirector}* is responsible for implementing and maintaining the asset inventory.
   2. All asset *[owners]* (as defined below) are responsible for providing the information required under this procedure and for ensuring that it is maintained and kept up to date.
   3. The *{HeadIT}* is responsible for device configuration in line with the requirements of this procedure.
   4. The *{PremisesManager}* is responsible for the security of removable media on the site, for authorisation of their removal and for spot checks to ensure this procedure is being followed.
2. **Inventory and ownership of assets** 
   1. {OrganisationName} maintains an inventory of information assets ([ISMS-C REC 8.1.1](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_REC_8.1.1.docm))
   2. *[This inventory is the asset inventory that is used in the risk assessment process (see* [*ISMS DOC 6*](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Section_4-10/ISMS_DOC_6.docm)*).]*
   3. For each asset, *{OrganisationName}* documents sufficient information to identify the asset (type or category of asset, make or manufacturer, model, serial number), identifies the physical (or logical) location of the asset, information security classification of each asset, the *[purchase cost/current written down value/insurance value/all three]* for each asset, and the security processes or controls (including access controls, backups, etc.) associated (following a risk assessment) with each asset.
   4. For each asset, *{OrganisationName}* identifies the business unit or business role that ‘owns’ the asset. The *[owner]* is responsible for ensuring that the asset is correctly classified, for the day to day maintenance of the identified controls, that access controls are defined and periodically reviewed, and that vulnerabilities are identified and patched in line with [ISMS-C DOC 12](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_12.docm).
   5. *{OrganisationName}* groups some assets together into composite information ‘systems’, in which case it identifies the assets within the system and the *[owner]* is the business unit or role responsible for the system.
   6. All new information assets are added to the appropriate schedule as and when they are acquired, together with details of the required security processes/controls, and removed from the schedule when they are disposed of (in line with [ISMS-C DOC 11](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_11.docm)).
3. **Acceptable use of assets**
   1. Rules for the acceptable use of information and assets associated with information and information processing facilities have been identified, documented and implemented.
   2. The *{HeadIT}* is responsible for ensuring that all users sign User Agreements that set out requirements for acceptable use of information assets and in which they also explicitly accept *{OrganisationName}*’s Internet Acceptable Use Policy.
   3. These User Agreements also explicitly accept *{OrganisationName}*’s Rules for Use of E-mail.
   4. The Information Security Manager is responsible for monitoring compliance.
4. **Return of assets**
   1. All employees and contractors are required to return all *{OrganisationName}* assets in their possession upon termination of their employment, contract or agreement.
   2. Upon termination of employment, complete a termination checklist ([ISMS-C REC 7.3.1](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_REC_7.3.1.docm)) to confirm that assets have been returned.
5. **Classification of information**
   1. *{OrganisationName}* 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 and in the asset inventory.
   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.
   4. Information received from outside *{OrganisationName}* is reclassified by its recipient (who becomes its *[owner]*) so that, within *{OrganisationName}*, it complies with this procedure.
   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.
   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.

|  |  |
| --- | --- |
| **Classification** | **Definition** |
| Confidential | Applies to information that is specifically restricted to the *{BoardDirectors}* and specific professional advisers. |
| Restricted | Information of this category is restricted to *{Employees/Staff}* above the level of:  [] |
| Private | This classification covers all information assets that have value but which do not need to fall within either of the other categories. |
| Public | This is information which can be released outside *{OrganisationName}*. |

* 1. Confidential information 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.]*
  2. Confidential information sent by e-mail must be encrypted and digitally signed, and sent only to the e-mail box of the identified recipient.
  3. Confidential information can only be sent by fax if the nominated recipient is available to receive it directly from the fax machine.
  4. Confidential information can only be processed or stored on facilities which have been assessed as providing adequate security for such information. This classification is recorded on the asset inventory.
  5. Restricted information sent by e-mail must be encrypted and digitally signed, and sent only to the e-mail box of individuals known to be allowed to receive such information.
  6. 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.
  7. Restricted information can only be processed or stored on facilities which have been assessed as providing adequate security for such information. This classification is recorded on the asset inventory.
  8. Everyone employed by *{OrganisationName}* is entitled to access information classified ‘private’.
  9. This information has no restrictions in terms of how it is communicated, other than that it is not cleared for release outside *{OrganisationName}*.

1. **Labelling**
   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 *[describe any colour-coded systems used to indicate classification levels].*
   3. Electronic documents and information assets are labelled by *[insert mechanism]*.
   4. Information processing facilities are labelled *[describe how, if this clause is relevant]*.
   5. All e-mails have a standard disclaimer *[set out where]* to the effect that the views expressed in the e-mail are those of the sender alone and do not reflect the views of *{OrganisationName}*.
2. **Handling**
   1. Information assets can only be handled by individuals that have appropriate authorisations or on facilities that *[meet what requirements?]*.
   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.
   3. *{OrganisationName}* requires that confidential documents are only circulated *[in secure pdf format] / [as read-only documents]*.
   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, and are *[protected appropriately]* while being recorded.
   5. Agreements with external organisations that include information sharing include a matrix for translating their security classifications into this one.

1. **Management of removable media**
   1. Removable media drives *[are/are not]* enabled and this is contained in the device configuration specification in work instruction *[ ].*
   2. Removable media are labeled as described in Clause 7 above.
   3. Removable media may only carry information that is required for a specific purpose.
   4. The requirement for the authorisation of the removal of media from site(s), and the requirement for their physical protection, is set out in ISMS-C DOC 11.
   5. Long term storage of information must be on media, the manufacturer’s specification of which indicates that it will not degrade during the required storage period.
   6. Media (including spooled media) are stored *[identify where]* and in accordance with the manufacturer’s instructions.
   7. Media are disposed of securely and as required by ISMS-C DOC 11.
2. **Physical media transfer**
   1. ISMS-C DOC 11 sets out how [{OrganisationName}] ensures that media are protected against unauthorised access, misuse or corruption during transportation.

***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/specified]* members of staff on the *[corporate intranet]* and is published *[ ]*.

This procedure was approved by the *{ChiefInfoSecOffiecer}* on *[date]* and is issued on a version controlled basis under his/her signature.

Signature: Date:

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | <Manager> | Xx/yy/zz |
|  |  |  |  |
|  |  |  |  |