1. **Scope**

*{OrganisationName}*’s information assets and any information assets owned by a third party that *{OrganisationName}* encounters are within the scope of this procedure.

1. **Responsibilities**
   1. All *{Manager}* throughout *{OrganisationName}* are responsible for ensuring and checking for procedural compliance.
   2. *[Owners]* have responsibility for *{OrganisationName}* assets.
   3. *Users* have responsibility for any third-party assets.
2. **Identification of applicable legislation and contractual requirements**
   1. All relevant legislative, statutory, regulatory and contractual requirements and *{OrganisationName}*’s approach to meet these requirements have been explicitly defined, documented and are kept up to date for each information system and *{OrganisationName}*.
   2. All legislative, contractual, statutory and regulatory requirements that apply to *{OrganisationName}* and to its information assets are identified by {CompanySecretary} in a compliance database.
   3. The {CompanySecretary} is responsible for creating and maintaining the [multi-jurisdictional] database ([ISMS-C REC 18.1.1](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_REC_18.1.1.docm)) of *{OrganisationName}*’s statutory and regulatory information/data and computer-related compliance requirements. The controls and responsibilities necessary to meet these compliance requirements are also identified in this schedule.
3. **Intellectual property rights**
   1. Appropriate procedures have been implemented to ensure compliance with legislative, regulatory and contractual requirements relating to intellectual property rights and on the use of proprietary software products.
   2. [*You should set out here the procedures that will implement whatever Intellectual Property Rights policy that you adopt. As a minimum, in order to conform to ISO27002, you need to set out the procedures that are appropriate in your jurisdiction for ensuring that third-party copyright is not compromised and that software and software licence usage is controlled.*]
4. **Protection of records** 
   1. Every record established under this procedure must be identified by means of [*a sticker]* that identifies the object as being a record within the ISMS. This sticker must identify *{OrganisationName}*, the classification of the information contained in the record, the *[owner]* of the information and the date it was generated (or covers).
   2. The existence of the record must be referenced in the procedure or work instruction that leads to its existence.
   3. Where necessary, records can be given serial numbers in respect to the specific process to which they relate.
   4. Records are subject to the levels of protection appropriate to information of their classification level (i.e. at least the same as that of the asset to which they relate or the information they contain) and they are therefore protected, stored, maintained and disposed of in line with the requirements of the ISMS.
   5. The required retention periods,[[1]](#footnote-1) by record type, are below:

| **Record Type** | **Retention Period** | **Storage Media** | **Other Information** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. **Privacy and protection of personally identifiable information**
   1. *{OrganisationName}* ensures the privacy and protection of personally identifiable information as required in relevant legislation and regulation.
   2. *{OrganisationName}*’s Data Protection and Privacy policy is as below:  
        
      *{OrganisationName}***[[2]](#footnote-2)** is committed to compliance with all national *[and international]* maintaining appropriate procedures and work instructions. *[There are restrictions on the transfer of personal data from x to y, or outside x.]*

Personal data is classified as *[refer to classification levels in* [*ISMS-C DOC 8*](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_8.docm)*]*.

The policy applies to all personal data held by the company, including on wireless notebook computers, personal digital assistants and mobile telephones.

All *{Employees/Staff}* will be provided with training to ensure that they understand *{OrganisationName}*’s policy and the procedures it has put into place to implement that policy.

The disciplinary process will be invoked in circumstances where this policy may have been transgressed.

* 1. *{OrganisationName}* has appointed a [Data Controller] who is responsible for ensuring that the procedures set out in this document are implemented.
  2. *{OrganisationName}* has implemented specific technical measures to protect personal information.

1. **Regulation of cryptographic controls**
   1. Cryptographic controls are used in compliance with all relevant agreements, legislation and regulations, as set out in [ISMS-C DOC 10](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_10.docm).
2. **Independent review of information security**
   1. {OrganisationName}’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) is independently reviewed at planned intervals, and when significant changes to the security implementation occur.
   2. The {QualityManager} is responsible for organising independent audits of the ISMS. Where necessary, the {QualityManager}, in conjunction with the {InfoSecManager} engages expert (technical) external assistance.
   3. The ISMS is also subject to periodic reviews by external compliance auditors.
   4. Risk assessments are [independently] reviewed annually to ensure that they are still complete and up-to-date.
3. **Compliance with security policies and standards**
   1. *{Manager}* regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
   2. *{Manager}* are required, under their job descriptions, to carry out [monthly] checks to ensure that all security procedures and work instructions within their area of responsibility are being carried out, to identify shortfalls and to take action to ensure that shortfalls are immediately corrected. This action should involve identification of the causes of the non-compliance, an evaluation of the need for action to ensure non-recurrence of the shortfall, a determination of the appropriate action, followed by a review of the action to ensure that it has achieved its objectives.
   3. The details of the corrective actions, and confirmation of their successful implementation, should also be recorded in the *[review report]*.
   4. Review reports are made available to independent reviewers carrying out independent reviews in accordance with 8.6 above.
   5. *{Manager}* are also responsible for identifying non-conformances in the ordinary course of business and taking appropriate corrective action.
4. **Technical compliance review**
   1. The *{InfoSecManager}* has a schedule of *{OrganisationName}*’s 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)) and these are prioritised by *[value]* to *{OrganisationName}*.
   2. All assets that are *[what level?]* or above are checked for technical compliance with their documented configuration requirements on a *[what?]* basis. This includes periodic penetration testing of all websites and Internet-facing applications and connectivity.
   3. *{OrganisationName}* requires that any person/organisation who carries out technical compliance checking has [*specify required qualifications and experience – which will be determined by your technical set up and your information security environment*].
   4. The *{InfoSecManager}* approves the technical checking plan put forward by the [*contracted technical compliance checking team/organisation*] and authorises commencement of the check plan only when satisfied that the testing will not compromise the asset or system being checked.
   5. Nonconformities are identified and dealt with as described in 9, above.
   6. New weaknesses or vulnerabilities uncovered as a result of the technical compliance checking are reported and dealt with in line with [ISMS-C DOC 16](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_16.docm).

***Document Owner and Approval***

The *{CompanySecretary}* 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 *{ChiefInfoSecOfficer}* 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 |
|  |  |  |  |
|  |  |  |  |

1. Your local law will set minimum retention periods for different types of documentation. You will need to identify all of these (sometimes by authority – for instance, tax records may be required for a different period than other accounting records) and set these as your minimum retention periods – there may be circumstances where your risk assessment identifies that longer retention periods are required. Public sector organisations may also have Freedom of Information requirements that have to be taken into account here. [↑](#footnote-ref-1)
2. This is another complex area that requires competent legal advice. Organisations trading in a number of jurisdictions may be subject to more than one set of data protection and privacy regulation/legislation. If this is the case, you will need a matrix that shows, by country, the regulatory requirements, and that identifies any overlaps/conflicts. Public sector organisations may have conflicts with Freedom of Information legislation that need to be taken into account here. You probably already have most of this in place, and your key task will be to pull existing procedures into the ISMS format, fill any holes and tie it off. [↑](#footnote-ref-2)