1. **Scope**

Instructions for all IT and communications procedures must be documented in detail, so that *{OrganisationName}* can ensure that appropriate processes are applied consistently.

1. **Responsibilities**
   1. The *{InfoSecManager}* is responsible for the risk assessment that identifies the devices and processes that require documented work instructions.
   2. The *{HeadIT}* is responsible for coordinating creation of all the work instructions, and ensuring that they are followed.
   3. Asset *[owners]* are responsible for drafting work instructions for their assets, for ensuring they are kept up to date, and that the documented procedures are followed.
   4. Users are responsible for correctly following all relevant defined and documented work instructions, procedures and policies.
2. **Documented operating procedures** 
   1. Operating procedures have been documented, are maintained and are made available to all users who need them.
   2. The *{HeadIT}* is responsible for documenting all the IT working procedures for system activities related to information processing and communications facilities. The procedures required by *{OrganisationName}* are recorded in [generate a record to direct users to the appropriate work instructions].
3. **Change management**
   1. The following changes are considered routine or insignificant and are therefore not subject to this procedure:

Anti-virus updates

*[Vulnerability patching, hot fixes]*

*[Software upgrades]*

*[Others]*

* 1. The originator of a change request completes the change request form ([ISMS-C REC 12.1.2](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_REC_12.1.2.docm)) and obtains both *{Manager}* and *{HeadIT}* technical approvals for the change, taking into account the costs of the exercise, the potential benefits, etc.
  2. Copies of all change requests are retained to provide an audit trail.
  3. The *{InfoSecManager}* is then responsible for carrying out a risk assessment to identify potential risks, their impacts and to identify controls in line with *{OrganisationName}*’s risk management framework.
  4. A testing plan, complete with clear acceptance criteria *[including business, technical and load criteria]* must be documented prior to commencing change testing.
  5. Once the change is proved to be effective (working in line with the test criteria) the *{ChangeManager}* authorises its transfer to the operational environment.
  6. Software updates are version controlled *[describe how you do this]*, system documentation is updated and old documentation is archived.

1. **Capacity management**
   1. The capacity requirements of *{OrganisationName}* are defined as *[insert details, which may relate to bandwidth, server capacity, storage capacity, processor speed, software licenses, users, etc. and which should be assessed for each current or planned future information processing activity]*.
   2. *{OrganisationName}* requires available capacity sufficient to meet its *[peak]* demands *[plus a buffer percentage]* and this gives rise to the following capacity requirements schedule *[insert details or refer to a document that contains them]*.
   3. Capacity usage is recorded, measured and monitored *[insert details of how this is done]*, and the *{HeadIT}* is responsible for ensuring that current requirements stay within the planned upper limits.
   4. The *{HeadIT}* is responsible for identifying and implementing system improvements and tunings that will reduce the capacity requirements.
   5. Where there is evidence that requirements are higher than expected, the *{HeadIT}* investigates, identifies the cause(s) and proposes appropriate corrective action.
   6. The *{HeadIT}* assesses, on a *[quarterly]* basis, current and potential future capacity requirements and plans appropriate capacity increases or decreases to meet those changing requirements.
2. **Separation of development, test and operational environments**

* 1. The development, test and operational environments are different physical environments, configured and located as specified in *[ ]*. The test environment simulates the operational environment *[with exceptions detailed in the configuration document, together with details of impacts of these differences]*.
  2. All development tools *[describe which ones you have authorised for use]* are only accessible within the development environment.
  3. The development and test systems are not part of the network single sign-on system; developers and testers are issued with separate usernames and passwords for use in the development and test systems.
  4. Development and testing personnel *[do not have/are required to have special authorisation for]* access to operational systems.
  5. Operational software is only transferred from the test environment to the operational environment after completion of the system testing required by Clause 4 above.

1. **Controls against malware**
   1. The criteria for selection of the anti-malware software are that it must: *[set out your criteria, taking into account types of malware to be protected against, organizational hardware, robustness, reliability, updates (daily, not weekly), effectiveness, etc.]* and *{OrganisationName}*’s approved software is: *[insert name of software vendor and product selected]*.
   2. The anti-malware software is installed on all *{OrganisationName}* information systems and devices, including gateways and firewalls, with automatic updating enabled. The anti-malware software installed on the gateway(s) conducts automated scans of all attachments and deletes or quarantines suspect files.
   3. The firewall(s) are configured to halt download of software from the Internet.
   4. Software from external parties must be inspected by the *{ITDept}* and authorised as free of viruses before it can be loaded onto the network. A log [*Schedule ISMS-C REC 12.?*] is retained of all such software authorised for use, showing the originator of the request, the software details, and the date and time it was inspected, together with details of who carried out the inspection.
   5. *{OrganisationName}*’s gateway anti-spam filters must be set to exclude e-mails from unknown or bulk senders; the configuration requirements are in *WI 12.*?.
   6. *{OrganisationName}* allows the following mobile code *[none/Macros/ActiveX/Java/etc]* and the system configuration requirements are for all others to be banned from executing on any of *{OrganisationName}*’s information systems.
   7. User training on malware responses includes:
2. Identifying and responding to ‘hoax’ virus warnings, reporting them to the *{InfoSecManager}*, and not passing them on.
3. Not opening attachments to e-mails that are unexpected or where the sender is unknown.
4. How to respond if a virus does successfully install itself on their workstation or laptop.
5. What protective steps are necessary in respect of portable memory media.
6. *[Any special training in respect of wireless notebooks, PDAs, mobile phones, etc]*.
7. How to respond to screen and system alerts regarding viruses, spam, and mobile code.
8. Not to accept any file or folder execution requests while on the Internet.
9. **Information backup** 
   1. The required level (information, operational system, applications, etc.), extent (partial/full) and frequency of backup is: *[ ]*
   2. User backup requirements are stated in User Agreements and *users* are trained to perform backups as part of their induction.
   3. [*The procedure for remote storage of backups is: [ ] and the same level of control is applied at the remote site as within {OrganisationName} /the backup is protected by encryption in line with [ ].*]
   4. The retention period for backup information is [ ].
   5. The backup requirements for paper documents are: *[ ]*.
10. **Event Logging**
    1. *{OrganisationName}* has established a schedule/matrix of audit logging [location of file] and keeps logs of events in accordance with that.
    2. System administrators are prohibited from erasing or deactivating logs of their own activities *[and the technical configuration of this control is [ ]*.
    3. The schedule/matrix of audit log requirements and the audit log reports are classified as confidential information and must be handled in line with the requirements of this ISMS for handling confidential information.
11. **Protection of log information**
    1. Event logging is configured as set out above.
    2. *[Describe how system logs and event types are investigated; what tools might be used, etc]*.
    3. *[Describe how system logs are securely stored and archived, referencing control section 18.1.3 of the Manual]*.
12. **Administrator and operator logs**
    1. The *[servers/systems/devices]* for which administrator/operator activities are logged *[and the logging software that is deployed]* together with the schedule/matrix of administrator and operator activity log requirements *[and reporting regularity]* are set out in [establish a record of your requirements].
    2. The schedule/matrix of activity log requirements and the log reports are classified as confidential information and must be handled in line with the requirements of this ISMS for handling confidential information.
    3. The following data protection or privacy protection restrictions also apply
    4. *[Describe how administrator and operator logs and event types are investigated, what tools might be used, etc]*.
13. **Clock synchronization**
    1. The clocks of all information systems within *{OrganisationName} [or if necessary specify in a schedule different points of synchronisation for geographically dispersed systems]* are synchronised with *[specify what and how the synchronisation is performed across the network]*.
    2. The clocks on all servers and all organisational information processing devices (including laptops, PDAs) are checked on a *[regularity?]* basis *[how?]* and corrected where necessary. The record of completed checks and any necessary corrections is forwarded to the *{HeadIT}*.
14. **Installation of software on operational systems**
    1. {OrganisationName}’s operational software is listed in the asset inventory ([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 each item of operational software has an identified *[owner]*, who is the trained administrator of that item of software. Only the *[owner]* may perform software updates, and then only after the completion of satisfactory testing.
    2. Pre-implementation testing of operational software is carried out in the test environment.
    3. Previous versions of operational software are retained *[for how long, where, under whose control, and with what additional information?]* as a contingency.
    4. Physical or logical access is only given to suppliers *[under what conditions/against what criteria?]* and in line with the requirements of [ISMS-C DOC 13](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_13.docm).
15. **Management of technical vulnerabilities**
    1. {OrganisationName} has established the following timeline requirements for reacting to notifications of relevant vulnerabilities: *[insert details – classification and number of days]*.
    2. The required controls will be actioned through the change management procedure if they are *[what?*] or through the incident response procedure ([ISMS-C DOC 16](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_16.docm)) if they are only *[what?]*.
    3. Available patches must be risk assessed, taking into account the balance between risks in installing and not installing, before the final decision as to necessary controls can be made.
    4. Patches must be tested.
16. **Restrictions on software installation**
    1. Rules have been established governing the installation of software by users, as described in Clause 13 above.
    2. [Using externally evaluated and certificated products ]
    3. Malware, that might cause covert channels, is controlled through the anti-malware software (see Clause 7 above) and User Agreements.
17. **Information systems audit controls**
    1. [*Your procedure is determined by your software systems and by the requirements of your audit regime. The specific audit requirements need to be identified and documented here. You should refer to the guidance of ISO27002 Clause 12.7.1 in drafting your procedure for this activity. Many organisations will have little or no need for this procedure; others will have extensive procedures to deal with this area.*]

***Document Owner and Approval***

The *{HeadIT}* 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 |
|  |  |  |  |
|  |  |  |  |