1. **Scope**

This procedure addresses the operation of information security within the scope of the ISMS. This includes defining information security roles and responsibilities, segregation of duties, requirements for contacting authorities and critical suppliers, information security in project management, the use of mobile technologies (laptops, notebooks, etc.) and teleworking protocols.

1. **Responsibilities**
   1. *{OrganisationName}* has clearly defined and allocated all information security responsibilities, as documented in each ISMS document and in individual job descriptions.
   2. Each body listed in Clauses 4 and 5 below has a nominated *{Owner}* (see [ISMS-C DOC 8](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_8.docm)) who is responsible for managing the relationship with the body. This responsibility includes initiating and maintaining the relationship, and ensuring that the contact information in the schedule to which this work instruction relates (Schedule [ISMS-C REC 6.1.3](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_REC_6.1.3.docm)) is current and complete.
   3. The *{HeadIT})* is responsible for specifying and/or providing the firewalls, anti-malware software, automatic updating, connectivity and backup facilities required for wireless technologies under this procedure. This person is also responsible for the configuration of all required computing equipment.
   4. All users have specific responsibilities in terms of their User Agreements.
   5. The *{PremisesManager}* is responsible for site surveys and implementation of necessary physical improvements and controls.
2. **Segregation of duties**

*[As far as is practicable and possible]*, *{OrganisationName}* segregates duties and areas of responsibility. In particular, the following functions are segregated:

|  |  |
| --- | --- |
| Risk assessment | *{InfoSecManager}* |
| Authorisation of controls | {*ChiefInfoSecOfficer}* |
| Change initiation | *[Functional Managers]* |
| Change management | *[Program Change Manager]* |
| Network management | *{NetworkManager}* |
| Network administration | *{NetworkManager}* |
| IT operations | *{HeadIT}* |
| Software development | *{HeadSoftwareDevel}* |
| System testing | *{HeadSystemTest}* |
| Employee administration | *{HeadHR}* |
| Asset purchase | *{ProcurementManager}* |
| Site/Secure area security | *{SiteManager}* |
| Security audit | *{QualityManager}* |
| Other | *[]* |

1. **Contact with authorities**

Relationships with these authorities are owned by the *{InfoSecManager}:*

Local/Regional police/law enforcement

Fire department

Anti-Phishing Working Group

Business Software Alliance

Federation against Software Theft

1. **Contact with special interest groups**

These relationships are owned by the business roles identified in ISMS-C REC 6.1.3:

Internet service provider(s)

Telecommunications provider(s)

Water authorities

Power, heating and lighting suppliers

Air-conditioning suppliers

Etc.

The *{InfoSecManager}* and the *{BusinessContinuityManager}* have version controlled copies of this document with their personal copies of the business continuity plan.

1. **Information security in project management**
   1. The project management methodology is [ ].
   2. The *{InfoSecManager}*, in conjunction with the *{ProjectManager}* is required to ensure that information security objectives are included in project objectives.
   3. The project is subject to an information security risk assessment at the initiation of the project, in order to identify necessary controls.
2. **Wireless technologies**
   1. *{OrganisationName}* requires mobile device-level deployment of *[the company’s specified]* firewalls, anti-malware software, and automatic updating facilities that are all up to date [and meet the corporate minimum standards, which are specified in [ ] and in the User Agreement.
   2. *{OrganisationName}* requires mobile device-level deployment of the corporate policy on usernames and passwords, to have a password protected screensaver, and to *[password protect/encrypt]* all folders containing *[confidential]* corporate information, and to disable folder and printer sharing, all of which is specified in the User Agreement.
   3. *{OrganisationName}* requires that mobile devices are physically protected against theft and damage while in transit, in storage or in use and that, in cases of loss or theft, the specified corporate policy (see User Agreement) for dealing with such incidents is followed.
   4. *{OrganisationName}* requires *users* (in the User Agreement) to ensure that all the most recent operating system and application security-related patches, fixes and updates have been installed.
   5. *{OrganisationName}* requires (in the User Agreement) that mobile devices are backed up in line with corporate specification *[set out where?]*.
   6. *{OrganisationName}* requires *users* of mobile devices to carry with them at all times the chargers and spare batteries specified in the User Agreement.
   7. *{OrganisationName}* requires *users* to comply with the corporate requirements *[set out where?]* on the means of connecting to public access points, *[and accessing corporate information, both]* as described in the User Agreement.
   8. *{OrganisationName}* requires *users*, in the User Agreement, to act with care in public places so as to avoid the risk of screens and *[confidential]* mobile device activity being overlooked by unauthorised persons.
   9. *{OrganisationName}* carries out regular and ad hoc audits of all mobile devices to ensure that they are configured in compliance with this procedure.
   10. *{OrganisationName}* provides *users* with appropriate training and awareness to ensure that they understand the risks of wireless on-the-road computing and that they understand and can carry out their agreed security obligations.
3. **Teleworking**
   1. {OrganisationName}’s policy on teleworking is that it provides teleworking facilities in order to improve the productivity, flexibility, responsiveness and effectiveness of its operations. *{OrganisationName}*’s policy is to authorise and control teleworking facilities to ensure that information is secure. It carries out a risk assessment ([ISMS DOC 6](file:///Users/NEW%20ISMS/ISMS%20Development/ISO27001-FastTrackToolkit-v1.0/ISMS_DOC_6.docm)) to ensure that each teleworking site is secure (ensures that there is adequate equipment and connectivity) physical and logical protection, access controls, cryptography, backups and malware protection for equipment installed in teleworking locations and will also ensure that teleworkers receive appropriate training before they are allowed to commence working. Teleworkers are required to accept in writing ([ISMS-C REC 6.2.2A](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_REC_6.2.2A.docm)) specific responsibilities with regard to teleworking activity, including physical protection, backups, malware protection and their use of *{OrganisationName}*’s equipment, particularly with regard to allowing unauthorised access by third parties.
   2. The proposed site for teleworking must be surveyed and the risks assessed before a decision can be made as to whether or not to authorise creation of a teleworker facility and, if it is to be authorised, to decide what controls will be necessary.
   3. The findings of the site survey and the details of the requirements gathered in [ISMS-C REC 6.2.2B](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_REC_6.2.2B.docm) are used as input into a risk assessment. The risk assessment determines the controls that are necessary for each teleworking location. The *{InfoSecManager}* documents the required controls in the output from the risk assessment.
   4. The teleworking site is brought into conformity with the required specification, in terms of any necessary physical security improvements, and the provision of home network and connectivity infrastructure.
   5. Any necessary changes to the network are made to ensure that *{OrganisationName}*’s access control policy ([ISMS-C DOC 9](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_9.docm)) is not breached by the teleworker. Once these steps have all been accomplished, the teleworker facility can be authorised.
   6. The teleworker undergoes necessary training and then signs a teleworker User Agreement (ISMS-C REC 6.2.2A) which sets out all the obligations and requirements in respect of the teleworking facility.

***Document Owner and Approval***

The *{InfoSecManager}* is the owner of this document and is responsible for ensuring that this work instruction 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 work instruction 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 |
|  |  |  |  |
|  |  |  |  |