1. **Scope**

*{OrganisationName}*’s network(s), as *[specified/described]* in network map *ISMS-C REC [ ]*.

1. **Responsibilities**
   1. The *{NetworkManager}* is responsible for the network architecture and infrastructure, and for the security of systems, applications and information using the network.
   2. The *{NetworkManager}* /other specified *[owner]* is responsible for managing the *[in-house/outsourced]* network services in line with Clause 4 of this procedure.
   3. The *{HeadIT}* is responsible for information processing facilities that communicate by means of the network.
   4. The *{InfoSecManager}* is responsible for risk assessment.
   5. The *[owners]* (see 9.1.2 and 13.1.2 in the SoA of the [Manual](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/InfoSecManual.docm)) of network service relationships are responsible for managing those relationships.
2. **Network controls**
   1. Risk assessments are carried out for each network within the scope of this procedure, to ensure that all information security risks have been identified and appropriate controls selected. The risk assessment is reviewed in line with the review requirements of the ISMS.
   2. The network architecture reflects the risk assessment, is designed to maximise security and business efficiency, and is kept under review.
   3. Remote equipment is managed in line with [ISMS-C DOC 6](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_6.docm)*.*
   4. Network access control is managed in line with the requirements of [ISMS-C DOC 11](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_11.docm).
   5. *[Confidential]* and *[restricted]* information is encrypted as required *[identify what and why this is required]* and in line with [ISMS-C DOC 10](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_10.docm).
   6. Network availability is maintained by *[ ]*.
   7. *{OrganisationName}* has deployed logging and monitoring controls, the configuration of which and reporting procedures are set out in *Work Instruction [ ].*
3. **Security of network services**
   1. *{OrganisationName}* uses the following network services *[ ]*.
   2. Risk assessments are carried out for each network service and appropriate controls *[including authentication, encryption and network connection controls]* are selected. The risk assessment is reviewed in line with the review requirements of the ISMS.
   3. The identified controls are included in the *[external party agreement/internal SLA].*
   4. External party agreements are managed in line with [ISMS-C DOC 15](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_15.docm).
   5. Work Instruction *[ ]* sets out the technical parameters and configuration requirements for connection with network services.
4. **Segregation in networks**
   1. [*Details of how you segregate your networks into separate security or logical domains, how you interlink them, what protocols, etc.*]
   2. [*Details of routers and firewalls, with references for their configuration work instructions.*]
   3. [*Details of other security controls deployed to reflect your risk assessment.*]
5. **Information transfer policies and procedures**
   1. Formal transfer policies, procedures and controls are in place to protect the transfer of information through the use of all types of communication facilities.
   2. *{OrganisationName}*’s Internet Acceptable Use Policy, its e-mail usage rules, its information classification procedures ([ISMS-C DOC 8](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_8.docm)), its anti-malware procedure ([ISMS-C DOC 12](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_12.docm)) and related procedures, and the technological controls implemented as required in all those procedures, protect exchanges of information from interception, unauthorised copying, modification, destruction or misrouting.
   3. *{OrganisationName}*’s use of cryptographic techniques is controlled under [ISMS-C DOC 10](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_10.docm).
   4. *{OrganisationName}* has procedures for handling (ISMS-C DOC 8), retention ([ISMS-C DOC 18](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_18.docm)) and disposal (ISMS-C DOC 11) of information and related media.
6. **Agreements on information transfer**
   1. Agreements are established in line with ISMS-C DOC 8 for the transfer of information, and address the secure transfer of business information between *{OrganisationName}* and external parties.
7. **Electronic messaging** 
   1. Information involved in electronic messaging is appropriately protected.
   2. User Agreements (see ISMS-C DOC 8) set out *{OrganisationName}*’s rules on e-mail usage, and ISMS-C DOC 8 sets out security requirements related to information classification, encryption and digital signatures and users are trained on correct use of e-mail, including the requirement to verify that e-mail addresses are correct prior to dispatch.
   3. The *{HeadIT}* is responsible for ensuring that *{OrganisationName}*’s e-mail system is set up and configured in line with Operations Work Instruction DOC [ ], which was drawn up to document the controls identified in the e-mail risk assessment [ ].
   4. The *{HeadIT}* is responsible for *{OrganisationName}*’s web mail service and for its protection by a firewall configured according to Operations Work Instruction DOC [ ] and for ensuring that it is only accessible to authorised and authenticated users.
   5. Instant messaging systems require specific authorisation from the *{HeadIT}*. Their configuration is subject to Operations Work Instruction DOC [ ] and the user requirements are set out in an addendum to the User Agreement.
8. **Confidentiality or non-disclosure agreements**
   1. A confidentiality and non-disclosure agreement [provide a link to the appropriate document] reflecting *{OrganisationName}*’s requirements for the handling of information is in place and is reviewed regularly

***Document Owner and Approval***

The *{NetworkManager}* 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 |
|  |  |  |  |
|  |  |  |  |