1. **Scope**

All the networks, public and private, to which Retirement Capital connects or over which organisational information assets are transmitted, and as identified in the policy [ISMS-C DOC 13.1.3](ISMS-C_DOC_13.1.3.docx), are within the scope of this procedure.

1. **Responsibilities**

The Network Manager is responsible for the network architecture and infrastructure, and for the security of systems, applications and information using the network.

The Network Manager is responsible for managing the in-house/outsourced network services in line with Clause 4 of this procedure.

The Director (CISO) is responsible for information processing facilities that communicate by means of the network.

The Director (CISO) is responsible for risk assessment.

The owners (see control section 8.1.2 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx)) of network service relationships are responsible for managing those relationships.

1. **Segregation in networks** [ISO27002 Clause 13.1.3]

Retirement Capital only uses two physical/logical networks.

The office VPN and the live environment and segregated by Firewalls at each end, which are linked via a secure, permanent VPN. Specific static routes are used to connect the two firewalls.

1. **Network connection control** [ISO27002 Clause 13.1.2]

Network Access Control is defined in [ISMS-C DOC 9.1.1](../Control%20A9%20-%20access%20control/ISMS-C_DOC_9.1.1.docx)) with reference to device configuration Work Instructions. All staff have access to the company network when in office.

1. **Network routing control** [ISO27002 Clause 13.2.1]

Retirement Capital defines its users either as Corporate Users or Technical Users, although a Technical User may also be a Corporate User.

Corporate Users will normally access the company documentation through Google G-Suite and therein Google Drive, however through secure interconnection to the company VPN, such users can access the company fileserver.

Technical Users are the only classification of user that can connect to the live environment that is hosted by XXX. They will do this via manual connection from the Corporate Network across the VPN to the static IP address of the firewall in the data centre.

1. **User authentication for external connections** [ISO27002 Clause 9.4.2]

XXX manages single-sign-on connectivity to the Corporate Network and to Google G-Suite.

Connection to the Google G-Suite is via two-factor authentication or username/password and Google Authenticator App on a mobile device.

Devices that can gain access to the Corporate network are limited to those entered into the device list of the firewall. Access to this network is via Username/Password and machine authentication.

Users who wish to access the live environment (Technical Users) will connect from the Corporate Network to the Data Centre over the secure VPN by manual connection to the server IP Address. Once they have reached the server, username/password authentication is used.

1. **Limitation of connection time** [ISO27002 Clause 9.4.2]

Bit Defender manages connection time, and this is set to automatically disconnect the user after five minutes of inactivity. Adherence to the policy is confirmed following the monthly firewall Syslog analysis.

1. **Equipment identification** [ISO27002 Clause 13.1.1]

Any unrequired access methods are disabled where the facility exists. Initial connectivity to any of the company servers will be to a Command Line Interpreter (CLI) which is configured to give the company and system name in the prompt of the CLI, enabling any user to confirm that the session is connected to the correct system.

1. **Remote diagnostic and configuration port protection**

XXX are used to provide remote diagnostics, The policy is to not use port-based authentication and any unrequired port is to be disabled.

***Document Owner and Approval***

The Network 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 members of staff on the corporate intranet.

This procedure was approved by the Director (CISO) on 214th November 2020 and is issued on a version-controlled basis under his/her signature.

Signature:

Date: 14/11/2020

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 14/11/2020 |
|  |  |  |  |
|  |  |  |  |