EXAMPLE – Procedure IS-4 – Mobile Computing

1 People and Purpose

This procedure applies to the Chief Technical Officer (CTO), ICT Manager and all workers (employees and contractors). It specifies how to configure and use mobile computing and portable storage devices, to protect the security of information that they hold.

This procedure covers ISO 27001, Annex A, Controls A.6.2.1, A.6.2.2 and A.11.2.6.

2 Set Up and Configuration of Mobile Computing Facilities

2-1 Mobile Devices – Laptops, Tablets and Smartphones

This sub-section covers ISO 27001, Annex A, Control A.6.2.1.

2-1-1 Policy

(1) We shall provide one or more of the following mobile devices, to roles that require them, to enable staff to work remotely, for routine business operations and for business continuity.

Laptop
Phone
Tablet
USB Removable Memory

(2) Our company network shall not have Wi-Fi, so that any mobile device can only be directly connected to our company network by physical wire (Ethernet) connection.

(3) Only mobile devices provided by the company may be connected to our company network.

No personal mobile device may be connected to our company network.

NOTE	A personal mobile device may be connected to our completely separate Wi-Fi which we make available for personal use by workers and visitors.

(4) If a worker has a smartphone (or tablet), the smartphone (or tablet) must require a password (to access email through Outlook) that is different to the worker's network login password.

2-1-2 Procedure

(1) The ICT Manager sets the local Administrator password to comply with Procedure IS-3 – Network Management, Section 3 - Password Policy.

(2) The ICT Manager configures the operating system to require a password for local (non-domain) accounts that complies with Procedure IS-3 – Network Management, Section 3 - Password Policy.

(3) The ICT Manager configures the operating system to require a password to resume from power saving standby mode.

2-2 Working Remotely – Secure Remote Connection to our Network

This sub-section covers part of ISO 27001, Annex A, Control A.6.2.2 (see also Section 3 below).

2-2-1 Policy

(1) Where possible, a worker must use Virtual Private Network (VPN) to work remotely.

(2) A worker that does not possess a company mobile device to work remotely must not use a shared public computer (such as in a library) to use Microsoft Outlook Web Access.

2-2-2 Procedure

(1) The ICT Manager configures a Windows laptop or tablet to enable the worker to securely connect to our network through a VPN using Secure Socket Layer (SSL).

(2) The ICT Manager configures a smartphone or tablet to access email through Outlook using Active Sync.

3 Use of Mobile Devices, Storage and Computing Facilities

This section covers the following:

Part of ISO 27001, Annex A, Control A.6.2.2 (see also Section 2-2 above);
ISO 27001, Annex A, Control A.11.2.6.

3-1 Guidelines

Take care of mobile computing and portable storage devices provided to you. Observe the following.

(1) Only use the devices for work. Do NOT allow family, relatives or friends to use them.

(2) Take care when travelling to prevent the theft or loss of mobile devices. For example:

- (a) Carry a smartphone as securely as possible, such as in a fastened inside pocket;
- (b) Carry a laptop or tablet in a distinctively coloured case, not a black one, to dissuade an opportunist thief from taking yours;
- (c) Carry a laptop in a case with the strap over your neck, and across your body, not just on your shoulder, so that a thief cannot easily snatch it;
- (d) Do not leave a laptop or tablet in your car boot, in a public place for a long period;
- (e) Never leave a laptop or tablet unattended;
- (f) Always carry a laptop or tablet in its case, to avoid accidental damage.

3-2 Encryption

If a mobile computing or portable storage device does not encrypt all files stored on it, encrypt any documents assigned the classification **PAROLA-Confidential** (that Procedure IS-1 specifies) in accordance with Procedure IS-3 – Network Management, Section 4 – Encryption Policy.