EXAMPLE – Procedure IS-3 - Network Management

1 People and Purpose

This procedure applies to the Chief Technical Officer (CTO), ICT Manager and all workers (employees and contractors). It specifies what they must do to maintain the security of our network and information and communications technology resources.

NOTE This procedure implements the following controls:

ISO/IEC 27002:2022, 5.15 (ISO/IEC 27002:2013, 9.1.1 and 9.1.2);
ISO/IEC 27002:2022, 8.24 (ISO/IEC 27002:2013, 10.1).

2 Policies

2-1 Access Control Policy

NOTE This sub-section implements ISO/IEC 27002:2022, 5.15 (ISO/IEC 27002:2013, 9.1.1).

(1) We will provide to each worker, only the access to ICT resources required, to do their work.

> **NOTE** The following procedure and form, control the allocation and removal, of access and assets, to and from, a worker.
>
> Procedure BM-1 - Starting and Finishing a Role
> Form 10 - Worker Access and Assets

(2) A worker must only access our ICT resources with administrator access when necessary.

(3) A worker must NOT access the internet when logged in with administrator access.

2-2 Password Policy

(1) Network Administrator passwords must be at least 20 characters, including at least one capital, one lowercase and one number and must differ from all Network User and Local Administrator passwords that the user uses.

(2) Network User passwords must be at least 12 characters, including at least one capital, one lowercase and one number and must differ from any Local Administrator passwords that the user uses.

(3) Local Administrator passwords must be at least 12 characters, including at least one capital, one lowercase and one number.

(4) The initial, supplied password of a new device (e.g. an Internet router or hardware firewall), must be changed, and conform to the requirements for a network administrator password.

(5) All passwords for application software (such as accounts) and web (subscription) services (such as online purchasing) must conform to the following, where possible.

(a) Conform to the requirements for a Local Administrator password.

NOTE	An application or web service may enforce more stringent or different criteria for passwords.

(b) Differ from all Network Administrator, Network User and Local Administrator passwords that the user uses.

2-3 Encryption Policy (Cryptography Policy)

NOTE	This sub-section implements ISO/IEC 27002:2022, 8.24 (ISO/IEC 27002:2013, 10.1).

(1) Encrypt any documents assigned the classification **PAROLA-Confidential** (that Procedure IS-1 specifies) using one or more of the following methods:

(a) Manufacturer’s encryption facility provided with a (removable USB) hard drive;

(b) BitLocker, using a password that complies with Section 2-2 - Password Policy;

(c) Encrypting File System (EFS);

(d) Microsoft Office, Open (and Edit) password protection, using a password that complies with Section 2-2 - Password Policy;

(e) A container utility, such as a compression utility, using a password that complies with Section 2-2 - Password Policy.

(2) At least two people must know the details of any encryption.

NOTES	EFS encryption is user specific; so one user cannot decrypt files encrypted by another user. Domain Recovery Agents can decrypt files encrypted by Encrypting File System (EFS). [All encryption MUST be accessible to more than one person.] A portable storage device MUST be formatted as NTFS to utilise EFS. If you do not know how to do this, ask the ICT Manager, or Helpdesk.

3 Procedure

NOTE	This section implements ISO/IEC 27002:2022, 5.15 (ISO/IEC 27002:2013, 9.1.2).

3-1 General

(1) The following people are domain administrators.

Chief Technical Officer (CTO)
ICT Manager

(2) Network passwords comply with Section 2-2 - Password Policy.

(3) Security software protects all machines connected to the company network.

(4) A firewall that meets our security and capacity requirements protects the company network.

3-2 Change Initial, Supplied (Default) Passwords (of New Devices)

NOTE	This applies to the ICT Manager.

(1) Change the initial, supplied (default) password, of a new device (e.g. an Internet router or hardware firewall).

IMPORTANT	The new password must conform to the requirements for a network administrator password, as specified in Section 2-2 – Password Policy.

3-3 Periodically Review Firewall Rules

NOTE	This applies to the ICT Manager.

(1) Review the firewall rules every 6 months.

(2) Report on each review to the next ICT Systems Security Review Meeting.

3-4 Administrator Access

NOTE	This applies to all workers that have Local Administrator access and/or Domain Administrator access.

(1) Only log in to our network or other ICT resource(s) with (local or domain) administrator access to do work that requires administrator access.

(2) Do not access either email or the internet while logged in with administrator access.

(3) Log out after completing any task(s) that require administrator access and, if necessary, log in again with user (non-administrator) access.

3-5 Backlog of Updates

NOTE	This applies to all workers.

(1) If you start a (physical or virtual) computer after a period of inactivity, ensure that all operating system and application updates are applied before you use the computer.

3-6 Network Password Security

NOTE	This applies to all workers.

(1) Do NOT disclose your network password to anyone, including other workers.

If you suspect that anyone else knows your password, you MUST immediately do the following:

(a) Change the password;

(b) Notify the ICT Manager and/or Chief Technical Officer (CTO).

(2) If either of the following occur:

(a) The anti-malware software on your computer detects malware;

(b) The ICT Manager informs you that your computer may have malware on it,

after the malware has been removed, change your network password.

3-7 Unused Software

NOTE	This applies to all workers.

If you have any software application installed on your computer, laptop, tablet or smartphone that is no longer used, it must be uninstalled. Do either of the following.

(1) If you have local administrator access, uninstall it.

(2) If you do NOT have local administrator access, ask the Network Manager to uninstall it.