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	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 11 – Worker Access and Assets

This procedure covers ISO 27001, Annex A, Controls A.9.1.2 and A.10.1.

Sections 2 and 3 cover ISO 27001, Annex A, Control A.9.1.2.

2 Procedure

(1) The following people are domain administrators.

Chief Technical Officer (CTO)
ICT Manager

(2) A firewall protects the company network.

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

(4) Passwords must comply with Section 3 - Password Policy.

(5) You MUST NOT disclose any of your passwords to anyone, including other workers.

(6) If you suspect that anyone else knows your network password, you MUST immediately do the following.

(a) Change the password(s).

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

3 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) 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.

4 Encryption Policy (Cryptography Policy)

This section covers ISO 27001, Annex A, Control A.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) Encrypting File System (EFS);

(b) BitLocker, using a password that complies with Section 3 - Password Policy;

(c) Microsoft Office, Open (and Edit) password protection, using a password that complies with Section 3 - Password Policy;

(d) A container utility, such as a compression utility, using a password that complies with Section 3 - Password Policy.

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

NOTES	(1)	EFS encryption is user specific; so one user cannot decrypt files encrypted by another user.
	(2)	Domain Recovery Agents can decrypt files encrypted by Encrypting File System (EFS). [All encryption MUST be accessible to more than one person.]
	(3)	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.