EXAMPLE – Procedure IS-1 – Information Security Basics

1 People and Purpose

This procedure applies to all workers (employees and contractors) and specifies the following:

(a) How to classify information;

(b) How to label information (according to its classification);

(c) How to handle information (according to its classification);

(d) How to store information (according to its classification) on removable media;

(e) How to transfer information (according to its classification);

(f) How to leave communications and computing devices unattended;

(g) When you must clear your computer desktop and physical desk.

It covers the following ISO 27001, Annex A, Controls.

KEY	*Italics signifies Required Policy*
	Bold Italics signifies Required [Policy and] Procedure

A.8.2.1	Classification of information
A.8.2.2	***Labelling of information***
A.8.2.3	***Handling of assets***
A.8.3.1	***Management of removable media***
A.13.2.1	***Information transfer policies and procedures***
A.13.2.3	Electronic messaging
A.11.2.8	Unattended user equipment
A.11.2.9	*Clear desk and clear screen policy*

2 Information Classification Policy

This section covers ISO 27001, Annex A, Control A.8.2.1.

All information must be assigned ONE of the following three classifications.

(1) PAROLA–Public

This is information that does not require protection. The following are examples of information that may be assigned this classification:

(i) Marketing material;
(ii) Product specification or data sheets.

(2) PAROLA–Restricted

This is information that may be available to all PAROLA workers. A Manager may authorise disclosure of the information to other people outside PAROLA that require it. The following are examples of information that may be assigned this classification:

(i) Organisation Chart;
(ii) Information Security Management System (ISMS) Manual;
(iii) Statement of Applicability.

NOTE	Information such as the above items may be required by a (potential) customer or as part of a submission for a tender. Information about specific workers may be required if one or more worker(s) will be required to work for a period onsite and/or exclusively towards a contract.

(3) PAROLA–Confidential

This is information that must ONLY be available to (PAROLA workers and other) people that require it. A Director, or the Chief Executive Officer (CEO), Chief Operating Officer (COO), Chief Technical Officer (CTO) or Chief Compliance Officer (CCO), may authorise disclosure of the information to other people outside PAROLA that require it (such as the following):

Partner organisations;
Consultants;
(Potential) Customers.

The following are examples of information that may be assigned this classification:

(i) Customers' information that we are legally and contractually obliged to protect;
(ii) Other organisations' information from that we must handle as confidential;
(iii) Technical details of products and services;
(iv) Tender documentation;
(v) Information security and business continuity risk register.

IMPORTANT	(1)	ALL research and development, accounts and payroll, and personnel (human resources) information has this classification.
	(2)	An auditor may require access to information with this classification. For example, an auditor auditing against ISO/IEC 27001 will require access to our Risk Register and Statement of Applicability.

3 Information Labelling Procedure

This section covers ISO 27001, Annex A, Control A.8.2.2.

When you create or modify a computer file and/or document you MUST do the following:

(1) Assign the appropriate classification, which Section 2 describes;

(2) Do (a), (b) or (c).

(a) If you assign the classification **PAROLA-Confidential**, make the last four characters of the filename a SPACE, a HYPHEN or an UNDERSCORE, followed by the letters "**CON**" in capitals, as in the following examples.

PAROLA SecurityProposals CON.doc
PAROLA-SecurityProposals-CON.doc
PAROLA_SecurityProposals_CON.doc

If it is also a document, put the classification in the header, at the top of each page.

NOTE	It is not necessary to label software source code and Sage data files. ALL source code and Sage data is assigned the classification **PAROLA-Confidential** without exception.

(b) If you assign the classification **PAROLA-Restricted**, make the last characters of the filename a SPACE, a HYPHEN or an UNDERSCORE, followed by the letters "**RES**" in capitals, as in the following examples.

PAROLA OrganisationChart 2013-04-01 RES.doc
PAROLA-OrganisationChart-2013-04-01-RES.doc
PAROLA_OrganisationChart_2013-04-01_RES.doc

If it is also a document, put the classification in the header, at the top of each page.

(c) If you assign the classification **PAROLA-Public**, do NOT add anything to the filename.

If it is also a document, do NOT put the classification in the header.

4 Information Handling Procedure

This section covers ISO 27001, Annex A, Control A.8.2.3 and Control A.8.3.1.

4-1 Computer files

4-1-1 Encryption

(1) Encrypt a computer file that has the classification **PAROLA-Confidential**.

NOTE	If the file is a computer aided design (CAD) or technical illustration file, or a normal office document, you can password protect it, to encrypt it. Otherwise, use an encryption utility or (an) Encrypting Filing System (EFS).

4-1-2 Storage

(1) Only store a computer file on one or more of the following:

The PAROLA network;
A computer or laptop that PAROLA provides to you;
A portable storage device that PAROLA provides to you.

(2) Only store a computer file that has the classification **PAROLA-Confidential** on an encrypted portable storage device.

NOTE	Use BitLocker to encrypt the removable storage device, if it does not have integral (hardware) encryption. The encryption of the portable storage device is additional to the encryption of individual files (that have the classification **PAROLA-Confidential**).

4-1-3 Use

(1) Close a computer file that has the classification **PAROLA-Confidential** or **PAROLA-Restricted**, after you view, edit, or print it.

4-1-4 Attachment to an Email

To send a computer file that has the classification **PAROLA-Confidential** or **PAROLA-Restricted** as an attachment to an email, do the following procedure, in the specified order.

(1) Open a blank email.

(2) Specify the recipient(s). If you wish to send the email to a group, do the following:

(a) Expand the group;
(b) Examine the individual members of the group;
(c) Delete any members of the group, to which you do NOT wish to send the email.

(3) Specify the subject and message.

(4) If the file has the classification **PAROLA-Confidential**, and you will send the email to one or more recipients outside PAROLA, encrypt it (if it is not already encrypted).

(5) Attach the file.

(6) Send the email.

(7) If the attached file has the classification **PAROLA-Confidential**, inform the recipient of the decryption key in a separate type of communication, such as a text message or phone call.

4-2 Paper Documents

4-2-1 Storage

(1) Store a paper document that has the classification **PAROLA-Confidential**, in a **locked** container (drawer, cupboard).

(2) Store a paper document that has the classification **PAROLA-Restricted**, in a **closed** container (drawer, cupboard).

4-2-2 Use

(1) If you use a paper document that has the classification **PAROLA-Confidential**, and you leave your desk unattended, do one or both of the following.

(a) Remove the document from your desk and store it.

IMPORTANT	You MUST do this if you share an office with other workers.

(b) Lock the door to your office.

IMPORTANT	You MUST do this if: (i) You CAN lock the door to your office; (ii) You are the only person working in your office; (iii) You choose to leave the document on your desk.

(2) After you use a paper document that has the classification **PAROLA-Confidential** or **PAROLA-Restricted**, remove it from your desk and store it.

4-2-3 Post or Courier, and Fax

(1) If you send a paper document that has the classification **PAROLA-Confidential** or **PAROLA-Restricted** by post or courier, mark the envelope ***PRIVATE***.

(2) Obtain authorisation from a Director or Chief Officer {Chief Executive Officer (CEO), Chief Operating Officer (COO), Chief Technical Officer (CTO) or Chief Compliance Officer (CCO)} to send or fax a document that has the classification **PAROLA-Confidential**.

(3) Obtain authorisation from a manager to send or fax a document that has the classification **PAROLA-Restricted**.

EXCEPTION	You may send or fax a document that has the classification **PAROLA-Restricted** if the recipient (organisation) operates appropriate controls to ensure that the received document will only be available to people that require it: for example, (routine) communications with a bank. If you are not sure, obtain authorisation from a manager.

4-2-4 Disposal

Shred a document that has the classification **PAROLA-Confidential** or **PAROLA-Restricted**.

5 Information Transfer Policy and Procedure

This section specifies how to communicate with third parties.

It covers ISO 27001, Annex A, Controls A.13.2.1 and A.13.2.3.

5-1 Information Transfer Policy

(1) Use email and telephone where possible. Only use fax or post if unavoidable.

(2) Where possible, send an email to named individuals.

(3) All communications must conform to any applicable agreements.

5-2 Information Transfer Procedure

5-2-1 Email

This sub-sub-section covers ISO 27001, Annex A, Control A.13.2.3.

Observe the following when you use email to communicate with third parties (partners, customers and suppliers, government etcetera).

(1) Do not put any information in the message of an email that meets the criteria for the classification **PAROLA-Confidential**.

(2) If possible, send an email to named individuals, such as **johann.strauss@musical-composers.com**.

Where possible, do not send an email to a group or a shared email address, such as **classical-composers@musical-composers.com**.

NOTE	A third party may require you to use an impersonal (shared) email address, such as **support@musical-composers.com**, for example, where you communicate with a team, not a specific individual.

(3) Conform to Section 4-1-4, if you attach any files to an email.

5-2-2 Partners, Providers and Potential Customers

This applies to communications with the following:

Research and Development Partners;
Product and Service Delivery Partners;
Outsource Providers including Suppliers and Sub-Contractors;
Reseller Partners;
Potential Customers.

Do the following.

(1) Use email and telephone where possible. If appropriate, use video communication, with suitable security controls.

(2) Ensure that all communications and disclosures of information conform to any applicable (confidentiality and/or non-disclosure) agreements.

5-2-3 Communications between Account Management and Customers

Do the following.

(1) Use email and telephone where possible. If appropriate, use video communication, with suitable security controls.

(2) Ensure that all communications and disclosures of information conform to any applicable (confidentiality and/or non-disclosure) agreements.

5-2-4 Communications between Technical Support and Customers

Do the following.

(1) Use email and telephone where possible. If appropriate, use video communication, with suitable security controls.

(2) If necessary, use appropriate remote connection, with suitable security controls.

e.g. Virtual Private Network (VPN)

Microsoft Remote Desktop Connection

NOTE	Some customers may require you to conform to specific remote connection protocols.

(3) Ensure that all communications and disclosures of information conform to any applicable (confidentiality and/or non-disclosure) agreements.

6 Clear Desk and Screen Policy

This section covers ISO 27001, Annex A, Controls A.11.2.8 and A.11.2.9.

6-1 Clear Desk Policy

At the end of the day, do the following.

(1) Remove from your desk any portable storage device and either store it (in a closed container) or take it with you, if you work remotely (at home or on-site).

(2) Remove from your desk all paper documents that have the classification **PAROLA-Confidential** or **PAROLA-Restricted** and store them (as Section 4-2-1 specifies).

6-2 Clear Screen Policy

(1) If you leave your computer for any period, do both (a) and (b).

- (a) Save any unsaved work.
- (b) Lock your computer, so that you must key in your network password to unlock it.

(2) At the end of the day, do either (a) or (b).

- (a) Shut down (turn off) your computer.
- (b) Do the following.
  - (i) Save any unsaved work.
  - (ii) Lock your computer, so that you must key in your network password to unlock it.

6-3 How to Lock Your Computer

Whenever you leave your computer or laptop unattended, lock it (so that you must enter your network password to unlock it) as follows.

(1) Press the **[WINDOWS]** and **[L]** keys simultaneously.

(2) The computer is now locked and displays a prompt for you to enter your log in (network) password, to unlock it.

6-4 Lock Your Smartphone

Whenever you leave your smartphone unattended, lock it.

Summary of Procedure IS-1

How to Classify Information

PAROLA–Public	Information that does not require protection.
PAROLA–Restricted	Information that may be available to all PAROLA workers.
PAROLA–Confidential	Information that must ONLY be available to people that require it.

How to Label Information

PAROLA–Public	Do not label.
PAROLA–Restricted	Filename ends with space, hyphen or underscore and the text **RES**. The header must contain the text **PAROLA–Restricted**.
PAROLA–Confidential	Filename ends with space, hyphen or underscore and the text **CON**. The header must contain the text **PAROLA–Confidential**.

How to Store Computer Files

PAROLA–Restricted	Only store on: (1) The PAROLA network; (2) A computer or laptop that PAROLA provides to you; (3) A portable storage device that PAROLA provides to you.
PAROLA–Confidential	As above plus (1) ENCRYPT the file [using password protection, an encryption utility or (an) Encrypting Filing System (EFS)] and (2) Only store on an ENCRYPTED portable storage device.

How to Use Computer Files

PAROLA–Restricted	After you view or edit a file, close it.
PAROLA–Confidential	As above.

How to Send Computer Files

PAROLA–Restricted	Open a blank email. Specify the recipient(s). If you wish to send the email to a group, expand the group and delete any members as appropriate. Specify the subject and message. Attach the file and send the message.
PAROLA–Confidential	As above plus – Encrypt the attachment if you send the email to one or more recipients outside PAROLA.

How to Store Paper Documents

PAROLA–Restricted	In a closed cupboard or drawer.
PAROLA–Confidential	In a locked cupboard or drawer.

How to Use Paper Documents

PAROLA–Restricted	After use, remove from your desk and store.
PAROLA–Confidential	After use, remove from your desk and store. If you leave your desk unattended, remove from your desk and store. [See also Section 4-2-2.]

How to Send Paper Documents

PAROLA–Restricted	Obtain authorisation from a Manager. [See Section 4-2-3.] Mark envelope PRIVATE.
PAROLA–Confidential	Obtain authorisation from a Director. Mark envelope PRIVATE.

Information Transfer

Comply with any applicable non-disclosure or confidentiality agreements.
Use email and telephone where possible.
Do not put any information in the body of an email that you would classify as PAROLA-Confidential.
Where possible send an email to named individuals, not an email group.
Refer to Section 5 for full details.

Clear Desk

At the end of the day:
(1) Remove any portable storage device and either store it, or take it with you if you work remotely;
(2) Remove and store PAROLA-Confidential and PAROLA-Restricted documents.

Clear Screen

If you leave your computer, save any unsaved work, and
lock your computer so that you must enter your network password to unlock it.
At the end of the day either, (a) shut down your computer, or (b) save any unsaved work, and
lock your computer so that you must enter your network password to unlock it.

How to Lock Your Computer

Press the **[WINDOWS]** and **[L]** keys simultaneously.