Information Classification and Handling Policy June 2014

Introduction

The Scottish Enterprise Information Classification and Handling policy has been developed to ensure that Information in, whatever form, is valued by the organisation and its employees. SE must be trusted by partners and clients as an organisation that will respect the information they share with us. Information classification is used to ensure that information assets receive an appropriate level of protection.

Scope of Policy

This policy applies to all employees within SE. Individuals who are seconded into SE from another organisation (or employed through an agency) will be required to comply with this policy in the absence of a similar policy with their employer. Any employee found to have breached this policy may be subject to disciplinary action

Scope of Information Assets

This policy covers all information assets:

- Electronic documents and files
- Hardcopy – printed material documents
- Verbal – phone conversation / voicemail
- Multi media – photos / video / pod cast

From whatever source:

- SE
- Clients
- Partners

Key principles

- All information is valuable and should be treated with care at all times
- Confidentiality must be maintained
- SE must comply with statutory regulation – Data Protection Act, Freedom of Information
- SE must be seen as a trustworthy organisation so that client, partners and colleagues can have confidence to share information
- Information must only be shared with those who have a legitimate need to see it
- Lock sensitive/confidential information away, following SEs 'Clear Desk' procedures
- Only store SE information on authorised IT systems/equipment
- Do not discuss sensitive/confidential issues in public places/on public transport
- Report stolen or lost information as soon as possible, following the reporting procedure below:
    - Non-confidential information – report to line manager – if electronic report to Service Desk
    - Confidential information – report to line manager and Information Asset Owner - if electronic report to Service Desk
    - Confidential Sensitive – same as Confidential plus Director and Senior Information Responsible Owner (Chief Financial Officer)

Classification Definitions

Public	Information that has been specifically approved for general publication.
Internal	Information whose unauthorised disclosure, particularly outside SE, would be inappropriate; this classification refers to the majority of information processed by SE and need not be marked on the document
Confidential	Information, the unauthorised disclosure of which, even within SE would cause significant harm to the interests of SE or other parties
Confidential Sensitive	This is a sub-classification of Confidential and may be applied to information where loss or disclosure would have damaging consequences for SE or causes significant distress for an individual or group of people.eg sensitive information such as organisational restructuring, sensitive personal information etc

How to identify and label Information Assets with an appropriate Classification

There is no need to label Public or Internal information.

SE does not prescribe a mandatory labelling system for sensitive and confidential information. The labelling of information with a 'Confidential' marker is at the discretion of the information owner/author based on the proportion of the information's sensitivity and on how the information is intended to be handled and shared.

It is recommended that all personal data (eg HR information) is labelled as Confidential but there may be occasions when information (eg legal correspondence) is always handled as confidential but the Confidential label may not be practical and is not always required. Information Asset Owners and line mangers should consider and agree what labelling is appropriate for their information, ensure that where labelling is not used for confidential information the information is still being handled/processed as confidential and communicate this to their teams.

If information is deemed to be confidential or sensitive and if labelling is required, labels should be applied 'as follows:

Document:

- At the top of the front/title page: **Confidential (*plus Optional Information Identifier*** – please see below)
- Within a document: Confidential should be clearly marked at the top of every page within the document
- Save your document on your team's shared folders

Email:

- 'Confidential' should be included in the subject line of the email
- All attachments deemed to be sensitive or confidential should be marked as above for documents.

Deciding on Information Classification

Has the information been approved for general publication?

NO / YES

Information is Public

Can the information safely be made available to, or be accessed by, anyone within SE but not anyone else?

NO / YES

Information is for internal use only

Should access to the information be restricted to those who have a legitimate need to know?

YES

Handle and share information as confidential and consider labelling if appropriate

Optional Information Identifiers

An optional information identifier may be used with **Confidential** to indicate the users/groups that have a need to know for that information. For example:

Information Asset	Optional Information Identifier
Personnel information	CONFIDENTIAL – SENSITIVE
Sensitive Partner information	CONFIDENTIAL – SENSITIVE [group/partner name] ONLY
Very Limited distribution – Named individuals	CONFIDENTIAL – A Smith & B Jones ONLY

Public	Internal	Confidential
Brochures Annual reports Information published on the Internet Advertising materials	Routine internal business email Routine work in progress Training materials Meeting agendas	Personnel information Personal information (as defined by the Data Negotiating positions Pre-release publications Draft Board Papers Commercially confidential information relatin potential suppliers

How to Handle Information

What you want to do with the information	What is the classification?	What are the handling rules?
I want to store electronic information in the office	Internal	Store on your team's shared folders or on the intranet
	Confidential	Store on your team's shared folders or on the intranet – ensure that file / folder permissions are set so that only those who 'need to know' have access
I want to store, copy, print or work on hardcopy in the office	Internal	Protect against accidental compromise to non SE personnel Clear away at the end of the day
	Confidential	Ensure hardcopy is cleared away when not in use When printing or copying ensure that all copies are picked up from printer promptly or, where available, set up a pin number for the printer. Secure documentation in locked drawer or filing system during out of office
I want to carry hardcopy outside of an SE office	Internal	Handle with due diligence Protect against accidental compromise to non SE personnel – carry in a folder or bag If lost or stolen report as soon as possible, following the reporting procedure below: ▪ Non-confidential information – report to line manager – if electronic report to Service Desk
	Confidential	Never leave unattended If lost or stolen report as soon as possible, following the reporting procedure below: ▪ Confidential information – report to line manager and Information Asset Owner - if electronic report to Service Desk

		▪ Confidential Sensitive – same as Confidential plus Director and Senior Information Responsible Owner (Chief Financial Officer)
I want to carry electronic information out of the office on a laptop, Blackberry, iPad, smart phone or memory stick	Internal	Only use SE provided device Do not let unauthorised people use your device When using in a public place be aware of being overlooked If lost or stolen report as soon as possible, following the reporting procedure below: ▪ Non-confidential information – report to line manager – if electronic report to Service Desk
	Confidential	Try to avoid having Confidential documents on portable devices. If unavoidable follow the SE Internal handling requirements plus: Ensure the information is only on the device for the minimum time necessary Obtain permission from the owner of the data If lost or stolen report as soon as possible, following the reporting procedure below: ▪ Confidential information – report to line manager and Information Asset Owner - if electronic report to Service Desk ▪ Confidential Sensitive – same as Confidential plus Director and Senior Information Responsible Owner (Chief Financial Officer)
I want to share or send hardcopy information to an SE	Internal	When possible avoid sending hardcopy by using the SE email or the intranet for sharing information with colleagues

colleague		Use post system If lost or stolen report as soon as possible, following the reporting procedure below: ▪ Non-confidential information – report to line manager – if electronic report to Service Desk
	Confidential	Obtain permission from the owner of the information prior to copying and / or distributing to other When possible avoid sending hardcopy by using the SE email or the intranet for sharing information with colleagues Use mail system – send in sealed envelope – consider using registered delivery service If lost in transit If report as soon as possible, following the reporting procedure below: ▪ ▪ Confidential information – report to line manager and Information Asset Owner ▪ Confidential Sensitive – same as Confidential plus Director and Senior Information Responsible Owner (Chief Financial Officer)
I want to share or send electronic information to an SE colleague	Internal	Use the SE email system, a secure file share or the intranet
	Confidential	Verify recipients prior to sending by email – Use Outlook Message options to set Sensitivity level to: Confidential. Check the folder permission - restricted to the 'need to know' individuals.
I want to share or send hardcopy information to someone outside of	Internal	Send to external recipient only where there is an approved business need or other justification (i.e. Freedom of Information Act request).

SE		External mail should be sealed. If lost or stolen report as soon as possible, following the reporting procedure below: ▪ Non-confidential information – report to line manager
	Confidential	Share with someone outside SE only on a 'need to know' basis where there is an approved business, contractual or legislative need and with the approval of the originator/information owner. No security marking should appear on the outer envelope. Double envelopes are required. Courier/registered mail is the recommended option. If faxing ensure the recipient is at the receiving end at the time of transmission If lost or stolen report as soon as possible, following the reporting procedure below: ▪ Confidential information – report to line manager and Information Asset Owner - if electronic report to Service Desk ▪ Confidential Sensitive – same as Confidential plus Director and Senior Information Responsible Owner (Chief Financial Officer)
I want to share or send electronic information to someone outside of SE	Internal	Email to external recipient only where there is an approved business need or other justification (i.e. Freedom of Informational request) Ensure that the external recipient is aware that the information must only be used for the declared purpose and forwarded only with the approval of the originator/information asset owner. If lost or stolen report as soon as possible,

		following the reporting procedure below: ▪ Non-confidential information – report to line manager – if electronic report to Service Desk
	Confidential	Send Confidential content as WinZip AES 256 encrypted attachments • Set a strong, complex encryption password. • Communicate password verbally after confirming receipt of encrypted files. • Do not reuse a previous password. Send to external recipient only on a 'need to know' basis where there is an approved business, contractual or legislative need and with the approval of the originator/information owner. Ensure that the external recipient knows the classification level and is aware of the protection requirements. If lost or stolen report as soon as possible, following the reporting procedure below: ▪ Confidential information – report to line manager and Information Asset Owner - if electronic report to Service Desk ▪ Confidential Sensitive – same as Confidential plus Director and Senior Information Responsible Owner (Chief Financial Officer)
I want to post information on a social networking or collaboration website	Internal	Do not post outside of a closed user group – ensure group membership is appropriate for the 'need to know'. Please see the SE Social Media Policy
	Confidential	Not allowed
I want to discuss	Internal	Ensure the conversation cannot be overheard

with someone (face to face / phone call)		by non-SE personnel
	Confidential	Ensure the conversation cannot be overheard by those with no 'need to know'. Do not leave confidential information on voicemail systems.
I want to dispose of hardcopy	Internal	Check to confirm that the information does not require to be retained - see SE Retention policy May be disposed of in the recyclable paper waste bins or shredded.
	Confidential	Check to confirm that the information does not require to be retained - see SE Retention policy Must be disposed of by shredding or via confidential waste bins.

Non SE classification

Partner organisations may share information with SE that is marked with their classification. This information must be handled in accordance with the contractual arrangement with the information owner. If the information owner has not defined any handling rules you should handle the information as if it had an SE classification.

The table below maps Government, Corporate and SE classification.

Government Protective marking	Common business terms	SE classification
Top Secret		***Not held by SE***
Secret	**Confidential**	**CONFIDENTIAL**
Official-Sensitive	**Confidential**	**CONFIDENTIAL**
Official	**For internal use only**	**INTERNAL**
Official	**Publicly Available**	**PUBLIC**

Review of policy

This policy will be reviewed as a minimum every 2 years or at times of significant legislative or organisational changes.