Demo Limited		
Asset Classification Procedure		
ISO/IEC 27001:2013		
Issue 7	**A8.2.1 Classification of information** **A8.2.2 Labelling of information** **A8.2.3 Handling of Assets**	**Authorised By :- Directors of Demo Limited**
Page 1 of 8	**Effective Date: 25th October 2021**	**Classification :- Internal**
Issue Date: 25th October 2021	**Last Review Date: 25th October 2021**	

Scope

This controlled procedure defines the process for the classification of information assets such classification assigns the appropriate handling, processing, storing and communicating information.

Responsibility and Authority

The appointed information security representatives are responsible for the overall management of this process including its correct implementation and regular review.

Control and Distribution

This procedure is issued as a controlled document and can only be updated by the authorised information management representatives and must include a revision status and traceability of the change process.

A master is retained as part of the information security management system with uncontrolled copies issued at point of use.

The procedure

The information that Demo Company holds in an asset. All information is assigned an owner and is protected in a manner commensurate with its value to the organisation and its customers.

In order to preserve the confidentiality, integrity and availability of Demo Company's information assets, Demo Company must ensure they are protected against unauthorised access, disclosure or modification.

Demo Limited		
Asset Classification Procedure		
ISO/IEC 27001:2013		
Issue 7	**A8.2.1 Classification of information** **A8.2.2 Labelling of information** **A8.2.3 Handling of Assets**	**Authorised By :- Directors of Demo Limited**
Page 2 of 8	**Effective Date: 25th October 2021**	**Classification :- Internal**
Issue Date: 25th October 2021	**Last Review Date: 25th October 2021**	

Different types of information require different security measures, depending on their value to Demo Company, and Demo Company's customers. This asset classification procedure is intended to provide guidance on how to classify information assets correctly.

A.8.2.1 Classification of information

A rating is used to classify documents and information. This is detailed within this procedure in line with the access control policy see 9.1.1 and the application of CIA.

The Inventory of Assets also details the classification of different types of information assets.

Classification

CLASSIFICATION	RESTRICTED	CONFIDENTIAL	INTERNAL	PUBLIC
Description	Information which, if disclosed to an unauthorised individual , could cause significant damage to Demo Company , for instance, where compromise could: • Breach legal or regulatory requirements • Cause adverse and material financial	Information which, if disclosed to an unauthorised individual, could cause moderate damage to Demo Company's reputation, or have a moderate, adverse financial	Information intended for access by all Demo Company personnel.	Information available in the public domain.

	damage to Demo Company • Cause Demo Company to lose competitive advantage (e.g. market sensitive information) • Allow other users to subvert security measures put in place to secure Demo Company's information or that of our customers. Information that can be used on its own or with other information to identify an individual.	impact. Confidential information is intended for access by specific personnel within Demo Company and access will be restricted on a need-basis by role function.		
Examples	Financial Reporting Security Information Name and Address	Player data	Company policies	Press releases and information on websites

Responsibilities

Information Owners:

- Identify the information assets owned by them that need to be controlled, and ensure that they are correctly classified and labelled.
- Ensure that the information media items i.e. CDs, DVDs, USB devices or flash drives, hard drives, magnetic tapes, floppy disks, memory cards etc. that have been used to store sensitive information are managed appropriately throughout their lifecycle.
- Ensure that methods for exchanging information with third parties are consistent with Demo Company's requirements for information handling.

Information Users:

- Understand the classification of the information that they are processing or handling and ensure it is handled in the appropriate manner, commensurate with the classification of the information.
- Report any incidents of non-compliance with the information owner as soon as possible.

Labelling

A.8.2.2 Labelling of information.

Information is classified as per the Information Classification and Handling Procedure and includes both physical and electronic formats. The classification is documented within the Inventory of Assets.

Labelling is used, where applicable, and documented within the Inventory of Assets.

All information should be labelled with the correct classification when created. Documents should contain the classification. Media should be labelled with the highest classification of information it contains.

If classification of the information changes the information owner is responsible for updating the label on the information.

Information Handling

A.8.2.3 Handling of assets.

Demo Company requires difference classifications of information to be handled in a manner commensurate with its value to the organisation and our customers. Information must be handled in the prescribed manner throughout its lifecycle.

Information Handling – Collect or Create

Information collected must comply with Privacy legislation: especially information deemed Personally Identifiable Information (PII).

Information either created or collected must be assigned an information owner.

The information owner is responsible for assessing the criticality and sensitivity of the information and this will provide the requirements for the secure handling, storage and disposal of the information.

Information must be classified by the owner of the information and clearly labelled as prescribed by this procedure, whether that is a physical label, or included in the document or metadata.

Information must be placed in an appropriate Demo Company location, with adequate security and access controls, whether electronic or paper-based.

Information Handling – Store

Depending on the classification of information, Demo Company uses different measures to protect information during storage. These may include:

- Encryption
- Access control
- Physical controls

When using Demo Company information, especially company sensitive, personally identifiable information (PII) or transactional information, personnel must ensure that copies of information in e-mail or other form, is protected in a way which is at least equivalent to the security measures in place.

Information Handling – Modify

Controls must be in place to ensure that the integrity of the information is maintained and access to modify information must be provided on a needs-basis.

Information Handling – Destroy

Demo Company takes the security of information disposal seriously and employs the following controls to:

- Secure wipe/destruction of media or hard drives
- Certified destruction of electronic media by an approved supplier.

In all cases, throughout the information lifecycle the appropriate combination of controls must be selected and applied for all information and this is especially important during the sanitisation and destruction of information. For guidance, please refer to the Demo Company Secure Disposal of Media procedure.

Maintaining Security of Information

All Demo Company personnel, contractors and third parties with access to the Demo Company information must be aware of, and comply with all information security standards.

Information must not be transferred to unauthorised individuals regardless of whether the information is still in its original form. Care must be taken, especially when:

- E-mailing information – are the recipients authorised to receive the information? Does the e-mail contain any information that should be removed before sending?
- Faxing information – are the recipients authorised to receive the information? If the information is sensitive is someone waiting to collect the fax? Is the fax number confirmed as correct?

- Copying information from a secure repository – e.g. a database into another file or format. Information must be protected in a manner at least equivalent to the controls applied to the source of information.
- Physically moving information, whether hard copy or electronic format. Laptops and portable storage must not be left unattended and should be protected using encryption where possible.
- Destroying information – the Demo Company secure disposal of media procedure describes the manner in which information that is no longer required must be destroyed. Have all copies of the information been destroyed? Has electronic information been appropriately sanitised to ensure the information is not recoverable?

Also refer to documents:

Removable media 8.3.1
Asset management 8.1.3
HR Security section 7.1.2

Demo Limited		
Asset Classification Procedure		
ISO/IEC 27001:2013		
Issue 7	**A8.2.1 Classification of information** **A8.2.2 Labelling of information** **A8.2.3 Handling of Assets**	**Authorised By :- Directors of Demo Limited**
Page 8 of 8	**Effective Date: 25th October 2021**	**Classification :- Internal**
Issue Date: 25th October 2021	**Last Review Date: 25th October 2021**	

Example of handling requirements for different types of handling

Example	RESTRICTED	CONFIDENTIAL	INTERNAL	PUBLIC
Meetings and Conversations	Avoid talking in public places and ensure you are not overheard. Do not leave voicemail messages containing restricted information.	Avoid talking in public places and ensure you are not overheard. Do not leave voicemail messages containing restricted information.	No restriction	No restrictions.
Storage	Encrypted storage. Hard copies to be stored in locked containers.	Appropriate access control to ensure access on needs-only basis. Hard copies to be stored in locked containers.	Access restricted to Demo Company Only. Hard copies to be kept secure when off-premises.	No restrictions.
E-mail	Encrypted only.	Encryption recommended. Care taken to ensure distribution to authorised personnel only.	Care taken to ensure distribution to authorised personnel only.	No restrictions.
Removable Media	Prohibited unless authorised. Must be encrypted and on Demo Company media only.	Must be encrypted and on Demo Company media only.	Care taken to ensure distribution to authorised personnel only.	No restrictions.
Post or Courier	Recorded delivery, hand to hand or secure courier only.	Recorded deliver, hand to hand or secure courier only.	Care taken to ensure distribution to authorised personnel only.	No restrictions.
Publication	Prohibited – only to approved recipients.	Prohibited – only to approved recipients.	Care taken to ensure distribution to authorised personnel only.	Public distribution following approval and at an agreed time.