Document Management Policy

Overview

Who the policy affects

The policy applies to all members or representatives of the organisation.

Purpose

This policy supports employees and representatives of Dewi Development Ltd to manage the storage, review, retention, disposal and confidentiality of the corporate documents.

The policy sets standards for defining and marking documents with Document Management Criteria. The policy is supported by Document Management Guidance which provides the latest implementation guidance.

Scope

The policy includes all people representing the organisation from director to employee, temporary staff, sessional staff, agency staff, contractors and volunteers. All employees are included whether full time, part time, office based or home worker.

The policy covers all documents produced by Dewi Development Ltd.

The policy does not form part of the terms and conditions of employment with Dewi Development Ltd.

Effective Date

This policy applies from the 29 January 2019.

The company holds the right to update the policy at any time.

Policy

1. Marking

1.1. Documents will have an Identification Mark on the front page, making it quickly visible to the user the confidentiality and therefore management requirements of the document.

1.2. Documents developed for marketing of Dewi Development Ltd to the general public do not have to have an Identification Mark, although this can be displayed on the inside page or rear cover.

1.3. The document Identification Mark will include the Confidentiality Level, Confidentiality Classification, Document Type and the Document Version.

2. Document information

2.1. Documents will include Document Management Information. This information will include:

- 2.1.1. Document Control
- 2.1.2. Authors
- 2.1.3. Retention
- 2.1.4. Disposal

2.2. Large reports with covers should have the document information on the first page, while one-page documents should have the document information at the back.

3. Document ownership

3.1. Documents will be provided a document owner, which will usually be assigned as a job role.

3.2. The owner is responsible for ensuring document reviews take place.

3.3. The owner is responsible for reviewing when the retention dates are due and ensuring document are removed from circulation when required.

3.4. The owner is responsible for identifying who the authoriser is for new versions or acting as the authoriser themselves.

4. Document status

4.1. Documents will be provided with workflow status. These statuses will be:

- 4.1.1. Draft
- 4.1.2. Review
- 4.1.3. Awaiting Approval
- 4.1.4. Published
- 4.1.5. Removed

4.2. All documents requiring an approval process should not be marked as published until they have moved through workflow.

4.3. Communication documents that do not need approval can go direct to published.

4.4. Documents that are no longer current, no longer applicable or have been superseded should be marked as removed.

5. Document Versioning

5.1. All documents will have a version number and the version number will be added to the end of the electronic file name.

5.2. Documents in draft format will begin 0, for example 0.1.

5.3. Documents that have been approved will start 1 or above, for example 1.0.

5.4. Documents needing a major revision may need to go through the document workflow and get approval.

5.5. Documents that need grammatical corrections or updated figures that do not need authorising, can be updated as minor revision, for example 1.1.

6. Document types

6.1. Documents will be classified by the nature of their content, this can include Policy, Procedure, Risk Assessment, Process, Project Plan, Business Case, Communication, Report or Form. See Guidance for full list.

6.2. Documents will be stored linked to their project, client or document type.

7. Confidentiality

7.1. Document confidentiality level will be defined and accordingly managed based on who can access the documents. The levels will be defined based closely on the Data Management Body of Knowledge and are:

- 7.1.1. General audience
- 7.1.2. Protected
- 7.1.3. Confidential
- 7.1.4. Restricted Confidential
- 7.1.5. Registered Confidential

7.2. Documents confidentiality classification will be applied to provide an indication as to why the confidentiality level has been applied and the potential legal or regulatory frameworks that apply. A full list of classifications are in the guidance, but include:

- 7.2.1. Internal
- 7.2.2. Personal
- 7.2.3. Client
- 7.2.4. Investigation
- 7.2.5. Legal

7.3. Documents defined as Registered Confidential will need to have a signed legal agreement and received clearance to view documents. Individuals issued with a document will have responsibility for the secrecy of the document.

7.4. Documents defined as Restricted Confidential and Registered Confidential must have their distribution managed and recorded.

7.5. Documents marked Protected and above should not be left lying around and should be stored securely.

7.6. Document marked Protected and above should be disposed of appropriately.

8. Storage

8.1. Documents should be stored on secure corporate servers.

8.2. Protected and confidential documents should be transferred through corporate File Transfer Sites.

8.3. If a protected or confidential document needs to be transferred on a USB memory stick, the memory stick must be encrypted with password access.

8.4. Protected and confidential documents that have been printed, must be stored in locked cabinet or locked case during transfer.

8.5. Protected and confidential printed documents must not be left on the desk. If an individual leaves their desk while working on document, it must be stored securely.

9. Disposal

9.1. Documents will have defined disposal requirements, linked to their confidentiality level. These classifications are:

- 9.1.1. Not controlled
- 9.1.2. Locally destroyed
- 9.1.3. Securely destroyed

9.2. Document defined as Locally Destroyed or Securely Destroyed must not be thrown in general waste, whether in paper or electronic format.

9.3. Documents defined as Securely Destroyed should be handled by an approved disposal carrier of Dewi Development Ltd.

9.4. Documents that are Securely Destroyed should be logged and collection notes logged.

9.5. Hardware which contained sensitive information, must be logged when it is destroyed and by what methods.

10. Retention

10.1. At the time of production all documents will be considered as to their retention time frame and this date will be added to the document.

10.2. The retention time frame will depend on the document and what contractual, regulatory or legal requirement it pertains. See retention policy.

10.3. All documents should be reviewed at the retention date and appropriately disposed of where extension is not required, or destruction hold is not in place.

11. File naming

11.1. Files will be named with the company name, topic category, document type, document name, and version all separated by '~'. If the document is for Dewi Development Ltd, it does not have to have company name at the start.

12. Transferring documents electronically

12.1. Confidential documents should not be transferred by e-mail, but uploaded to the corporate FTP site where access can be managed.

12.2. Documents that are transferred by e-mail, should have the Confidentiality Level and Confidentiality Classification in the subject or start of the message.

12.3. Protected documents that are posted, should have the envelopes marked appropriately.

12.4. Confidential documents that are posted and it should not be easily recognised as confidential, should be placed in two envelopes, with no markings on the out envelop.

12.5. Registered restricted documents should only be sent by registered courier with documents signed for on receipt.

Compliance

The inappropriate sharing of confidential documents may lead to disciplinary action or possible dismissal within the laws of the employing country.

Related Legislation

- General Data Protection Act (GDPR) 2018

Definitions

Term	Definition
Document	Covers, but is not limited to, text files, desktop publishing files, pictures, video and audio.

Document Information

Document Control

Document Confidentiality	General Audiences
Confidentiality Classification	Internal
Document Owner	Information Officer
Approved By	David Husband
Approval Date	29/01/2019
First Published	29/01/2019
Review Date	01/02/2021
Related documents	Document Management Procedure Data Retention Policy Data Retention Schedule
Status	Published

Version

Version	Author	Date	Summary Changes
0.1	David Husband	26/01/2019	
1.0	David Husband	29/01/2019	Approval
1.1	David Husband	12/03/2019	Formatting definitions Legislation added
1.2	David Husband	16/05/2019	Review and change file naming convention Review of transfer of documents

Authors

Author	Company	Job Title	Department
David Husband	Dewi Development	Director	Management

Retention

Retention date	N/A
Retention details	Document is appropriate until replaced.

Disposal

Disposal classification	Not Controlled
Disposal details	Document does not contain commercially sensitive information. Paper copies should be recycled.