Document & Records Management

Aim

The aims of this procedure are:

- To define how the Management System of the Organisation is documented and system records are maintained.
- To ensure that records that verify Work, Health & Safety, Environmental and Quality activities of the Organisation are collected and maintained for a suitable period.

Scope

This procedure applies to:

- The development, distribution, control and continuous improvement activities related to all management system documentation.
- The identification, collection, indexing, accessing, filing, storage, maintenance and disposal of system records.
- All documentation (including records) that is/are created, distributed and retained for information and action in managing PWT.

Documentation

This procedure applies to controlled documents (including data) in the Management System, including:

- Manuals (Management System Document)
- Procedures (Management System Document)
- Work Method Statements & Instructions and Forms (Management System Document)
- Action Plans (Management System Document)
- International and local standards (External Document)
- Government regulations (External Document)
- Equipment operating manuals (External Document)
- Design drawings, layout plans and manufacturing drawings (External Document)
- Customer documentation

Method

Internal Documents

The internal documents listed above are marked with a title, document owner and date of issue. This information is controlled by the system software.

External Documents

The external environmental documents listed in the scope above will be identified by the Organisation with a title, and where possible, a revision number (or some other means of determining revision status) and date of issue.

An external document is any document that is relevant to the management system that cannot be modified by Elliam electronically.

International and Australian Standards are examples of external documents as are customer issued documents such as contract requirements.

External documents issued by customers are kept in the relevant contract folder.

Issuing Management System Documents

All Management System Documents, as nominated above, are stored electronically. Access to the Management System is controlled by the network security system. With the exception of the Directors and the Management Representative all access is read only. All hard copies are defined as uncontrolled.

Copies of System documents may be issued to persons outside the company with the Management Representative's approval.

Changes

Any person can propose changes to documentation by raising a Corrective Action. The Management Representative reviews the proposed changes with other relevant personnel to determine whether the change is appropriate. The document is then actioned as needed, approved by the Management Representative and reissued.

Obsolete Documents

A copy of the previous version of a document is stored within the individual document as part of the revision process.

Obsolete documents are stored electronically and may be maintained indefinitely.

Control of Documents

Each document contains the date issued in the document footer.

Electronic Data

Documents and data kept in electronic form will be backed up regularly, as follows:

- Cloud servers - backed up weekly to alternating external hard drives, stored off-site.

Version Control

The Management System software displays the current version of all System documents.

Control of Records

Responsibility

Management Representative - Determination of suitable retention periods

Method

Among others, the system records include following:

- Management Review results.
- Legal compliance records.
- Internal audit results.
- Records of meetings.
- Records of communication with interested parties.
- Inspection, maintenance and calibration records.
- Contractor & supplier records.
- Process monitoring records.
- Staff training and performance records.

General

Throughout the term of a contract, we will maintain a records management program. All records will be kept in compliance with the State Records Act and AS ISO 15489.1:2017.

Records (both hard copy and electronic media) are identified, collected, indexed and filed as required by the relevant procedure and or process.

Access to records is controlled by personnel defined in the body of the relevant procedure with specific details recorded in the records section of each procedure.

As a default, all other records are managed by the Management Representative.

Indexing, Accessing, Filing, Storage and Maintenance

Records listed above will generally make reference to the Management System and be filed with other documents relating to that section of the System. All documents are stored electronically in accordance with the process outlined above.

Disposal of Records

Electronically stored documents are retained indefinitely. Unless otherwise stated, the minimum retention period for all records is five years.

Records that are retained for legal and business purposes must not be destroyed without the approval of the Directors.

Record	Location	Duration	From
Qualifications	Personnel Files	7 Years	End of Employment
Management Reviews	Cloud Storage	7 Years	After Date of Meeting
WHS Meetings	Employee file - HR Manager Office	7 Years	After date of meeting
Accident/Incidents	Cloud Storage	7 Years	After date of incident
Induction/Training	Cloud Storage	30 Years	After date of training
Hazardous Substances	Hazardous Substances Register	30 Years	After Date of Use
Equipment Maintenance	Cloud Storage	7 Years	After item is sold
Confined Space Entry Records	Client Archived	7 Years	After Entry
Emergency Testing Records	Archived	7 Years	After Testing Date
Incident Analysis	Accident / Incident Folder	7 Years	After Incident Date
Accident Statistics	Accident / Incident Folder	7 Years	After Incident Date
Calibration & Testing	Cloud Storage	7 Years	After calibration date
WHS Audit Reports	Cloud Storage	7 Years	After audited date

Record	Location	Duration	From
Pre Employment Medicals	Employee File – HR Manager	7 Years	End of Employment
Toolbox Meeting	Cloud Storage	7 Years	After date of meeting
Safety Inspections	Cloud Storage	7 Years	Date of inspection
Committee Meeting Records	Cloud Storage	7 Years	After date of meeting
Asset Register Records	Accounts Department	7 years	Date of Purchase