[Company]

DOCUMENTS AND RECORDS POLICY

The control of the Information Security Management System documents and records.

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Documents and Records Policy

3.1 Purpose

The purpose of this policy is the control of documents and records in the information security management system.

3.2 Scope

The documented information security management system.

Documented information required by ISO 27001.

Documented information determined by the company as being necessary for the effectiveness of the Information Security Management System.

All employees and third-party users.

3.3 Principle

Documents required for the information security management system are controlled, managed and available.

3.4 Creating and Updating

When creating and updating documented information, the company ensure appropriate

- identification and description (e.g., a title, date, author, or reference number),
- format (e.g., language, software version, graphics) and media (e.g., paper, electronic), and review and approval for suitability and adequacy.

3.5 Availability of documents

The latest approved version of document is presented to the appropriate users and are available and suitable for use, where and when it is needed.

3.6 Document Storage

Documents are stored in the document management technology implemented at the company.

Working documents for the information security management system are stored in the information security project / team folder.

Live documents and records are held within the relevant departments folder in a secure environment.

All stored documents are subject to access controls and adhere to the access control policy.

Documents and records are available to those that require them for their role.

3.7 Version Control and Approval

3.7.1 Policy documents

Policy documents are subject to change as a result of the continual improvement process.

Changes to policy documents are done by the information security management team.

Policy documents are approved by the Management Review Team.

Policy documentation version control history is maintained which captures as a minimum the author, the date, the change, the new version number.

Policy version controls follows an x.y numbering system where x is the release and y is the iteration. The release number is updated periodically as part of a periodic review for all policies and the policies issued as a release set.

3.7.2 Operational Documents and Records

Operational documents and records are updated by the document and / or process owner as part of day-to-day operations and as required.

Changes to operational documents and records are done by the process owner.

Operational documentation version control history is maintained which captures as a minimum the author, the date, the change, the new version number.

Records may have version control history which is maintained which may capture as a minimum the author, the date, the change, the new version number.

3.8 Example of Records

Records are evidence of an event and used for operational management and auditing. They include but are not limited to

- Meeting minutes
- Training records
- Audit Reports
- Incident Reports

3.9 Preservation of legibility

Documents are created and available in electronic format using standard, supported office applications or in native operational systems.

3.10 Obsolete documents and records

Obsolete documents and records **required** for audit and/or legal and regulatory purposes are archived in line with the data retention policy and removed from general accessibility.

Obsolete documents and records that are **not required** for audit and/or legal and regulatory purposes are deleted in line the data retention policy.

3.11 Documents of External Origin

Documented information of external origin determined by the company to be necessary for the planning and operation of the Information Security Management System are identified, as appropriate, and controlled.

3.12 Document Classification

Documents are classified in line with the Information Classification and Handling policy.

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.