C-ISMS-DOC-07-3

[Internal]

Version 1.0

7th February 2025

CBL Procedure for the Control of Documented Information

CBL Procedure for the Control of Documented Information

[Internal]

Document Reference

Document Code:	C-ISMS-DOC-07-3
Document title:	CBL Procedure for the Control of Documented Information
Filename:	C-ISMS-DOC- 07-3 CBL Procedure for the Control of Documented Information
Author:	Consultant
Owner:	CBL
Date:	7th February 2025
Version:	1.0
Status:	Final

Revision Record

Version	Date	Summary of Changes	Revision Author
1.0 Draft 1	11th December 2024	Establishment of Procedure for the Control of Documented Information.	Consultant
1.0 Draft 2	7th February 2025	Inclusion of document classification, document reviewers, approvers, records retention period and records storage medium, exclusion of some naming conventions.	CBL
	6th February 2026	Next Version	

Distribution

Name	Title
Alex Iwobi	Chairman
Francisca Ordega	Chief Executive Officer
Sopade Adeola	Chief Information Security Officer
Ngozi Okobi	Chief Technology Officer

Rasheedat Ajibade	ISMS Manager

Approval

Name	Position	Signature	Date
Alex Iwobi	Chairman		11 February, 2025
Sopade Adeola	Chief Information Security Officer		11 February, 2025

CBL Procedure for the Control of Documented Information

[Internal]

Contents

CBL Procedure for the Control of Documented Information

[Internal]

1. Introduction

1.1 Definition and Scope of Documented Information

ISO defines “documented information” as information that an organisation must control and maintain, including the medium on which it is stored. This includes what was previously referred to as “documents and records”; for clarity, this procedure distinguishes between the two.

1.2 Importance of Documented Information in the ISMS

Documented information is a critical component of CBL’s ISMS, providing guidance on how processes should be performed, conveying management intent, and serving as evidence of completed activities.

1.3 Requirement for Control of ISMS Documentation

ISO/IEC 27001 requires that all ISMS documented information be controlled to ensure it is available, suitable, and adequately protected whenever and wherever needed. Proper control ensures that CBL’s processes and procedures remain appropriate and effective.

1.4 Standards for Managing Documented Information

All documented information at CBL must be:

- Readily identifiable and accessible.
- Dated and authorised by a designated individual.
- Legible and clear.
- Maintained under version control and available at all relevant locations where ISMS activities are performed.
- Promptly withdrawn when obsolete, with retention in archives where legally or operationally required.

1.5 Purpose of the Document Control Procedure

This procedure defines how CBL achieves consistent control, maintenance, and protection of all ISMS documented information.

2. Document Control Procedure

This procedure applies to documents (distinct from “records”) which are typically created using office applications (e.g., Word, Excel) and convey management intent, including policies, plans, procedures, and guidelines.

2.1 Overview

2.1.1

The overall process for controlling documents at CBL ensures documents are created, reviewed, approved, distributed, and maintained in a controlled manner.

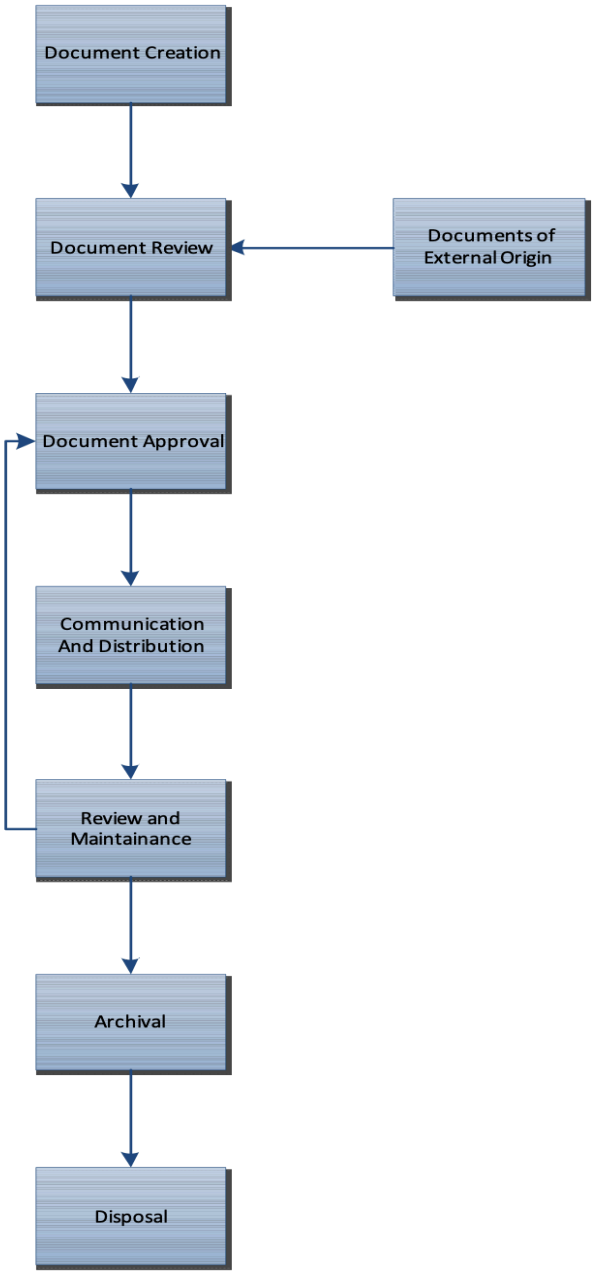

Figure 1 – Document control procedure

2.1.2

Each of these steps is described in detail in the following sections.

2.2 Creation of Documents

Documents within CBL's ISMS are created at the request of management and may be developed by any competent individual with the appropriate knowledge of the subject and document level. All document creation must comply with defined rules to ensure consistency, traceability, and control.

2.2.1 Naming Convention

2.2.1.1 ISMS documents at CBL follow this naming format:

O-ISMS-DOC-xx-yy Document Title

Where:

- ISMS = Information Security Management System
- DOC = Document
- xx = Subject area reference (see Table 1)
- yy = Unique document number
- Document Title = Clear, descriptive title of the document

2.2.1.2 Each document is assigned a unique number, with an index maintained in the Information Security Management System Documentation Log.

2.2.1.3 Subject area references correspond to ISO/IEC 27001 sections.

Subject Area Reference	ISO/IEC 27001 Subject Area
00	Introduction and project resources
01	Scope
02	Normative references
03	Terms and definitions
04	Context of the organisation
05	Leadership
06	Planning
07	Support
08	Operation
09	Performance evaluation

10	Improvement
A05	Organizational controls
A06	People controls
A07	Physical controls
A08	Technological controls

Table 1 – Document Subject Area References

2.2.2 Version Control

Document version numbers consist of a major number (e.g., V2 = Version 2).

2.2.2.1 A new document starts at V1 Draft 1. Each draft iteration increments the draft number. Once approved, the document becomes V1 Final.

2.2.2.2 Major revisions increase the major version, while minor edits increment the draft number until approval.

2.2.2.3 Revision History Table

Version	Date	Author	Summary of Changes
V1.0	YYYY-MM-DD	ISMS Manager	1. Updated 'ISMS' to 'Information Security'. 2. 'Information Governance' changed to 'Digital Governance'.

2.2.2.4 Only approved versions are retained in the revision history.

2.2.3 Document Status

- **Draft** – Document under development or discussion; not approved.
- **Final** – Approved by management and released for use.

2.2.4 Documents of External Origin

External documents that are part of the ISMS are assigned a reference and a header page, including:

- Document reference
- Version
- Date

- Status
- Distribution

2.2.4.1 These external documents are controlled in the same way as internal documents.

2.3 Document Review

Draft ISMS documents at CBL are reviewed by personnel with the appropriate authority, knowledge, and experience, based on the document's purpose and impact.

2.3.1 Review Guidelines

Document Type	Reviewers
Strategy	Top Management
Policy	Top Management
Procedure	Top Management
Plan	Top Management

Table 2 – Document Review Guidelines

2.3.2 Scheduled Reviews

2.3.2.1 All ISMS policies and procedures shall be reviewed at least annually or earlier where significant organisational, regulatory, or technological changes occur.

2.3.2.2 Following approval, the next scheduled review date shall be recorded in the ISMS Documentation Log.

2.4 Document Approval

2.4.1 All ISMS documents at CBL must undergo formal approval to confirm they are accurate, fit for purpose, and compliant with document control requirements.

2.4.2 Approval Authorities

Document Type	Approvers
Strategy	Chairman
Policy	Chairman
Procedure	Chief Executive Officer

Plan	Chief Executive Officer

Table 3 – Document Approval Authorities

2.4.3 Approval Record

Name	Position	Signature	Date

2.4.4 Approved documents must be electronically signed or printed and signed by the approver and stored in a centralised, controlled repository.

2.4.5 Once a new version is approved, it is released for use, and all previous versions are archived in accordance with the document retention and archiving procedure.

2.5 Communication and Distribution

Each controlled document shall include a distribution list identifying individuals or roles to whom the document applies.

Distribution List

Name	Title

2.5.1 The distribution list must be accurate, as it forms the basis for notifying relevant users when a new or updated version of the document is released.

2.5.2 All ISMS policies and procedures shall be communicated electronically, primarily via corporate email and made available through CBL's centralised document repository.

2.6 Review and Maintenance of Documents

All approved ISMS documents at CBL shall be stored electronically, with physical copies made available only where required. Documents must remain accessible, legible, and protected throughout their lifecycle.

2.6.1 ISMS documents are stored in a centralised electronic repository and organised by ISO 27001 subject areas. Access is granted in accordance with the Access Control Policy.

2.6.2 Access to ISMS documents is restricted to authorised users based on role and need-to-know, as defined in the approved distribution list.

2.7 Archival of Documents

Approved ISMS documents that are no longer in active use are retained in an Archive folder within the centralised repository. Archived documents must be clearly labelled with the suffix "_Archive".

2.8 Disposal of Documents

Physical copies of ISMS documents that are obsolete or no longer required shall be securely disposed of by shredding, in line with CBL's Asset Handling and Information Disposal Procedures.

3. Records Lifecycle

This section describes the control of records, which provide evidence of activities performed within CBL's ISMS.

3.1 Identification

3.1.1 ISMS records at CBL include:

- Security incident records
- Change requests
- Access request and approval forms
- Security and system event logs

3.1.2 General records, such as management review and committee meeting minutes, may apply across multiple ISMS processes.

3.1.3 Naming Rules

1. Meeting minutes: Meeting subject and date
2. Reports: Report subject and reporting period
3. Logs: Log title and date or time period covered

3.1.4

For other records, the creator must apply clear and descriptive naming and store the record in an appropriate location.

3.2 Storage

ISMS records are stored primarily in electronic format within secure systems and repositories.

3.2.2 Electronic ISMS records are stored in centralised systems with role-based access controls.

3.2.3 Paper records shall be scanned and stored electronically where an original electronic copy is not available.

3.3 Protection

3.3.1 ISMS records are backed up regularly in accordance with CBL's Backup and Recovery Policy.

3.3.2 Access to ISMS records is restricted to authorised individuals only.

3.4 Retrieval

3.4.1 ISMS records are retrieved using the systems or applications in which they were created.

3.4.2 Reporting and analysis tools may be used to aggregate and present records.

3.5 Retention

3.5.1 ISMS records are retained based on operational, legal, regulatory, and contractual requirements.

3.5.2 Security-related records are retained for a minimum of six (6) years.

3.5.3 Records with contractual or commercial relevance are retained for the same period.

3.5.4 Short-term operational records are retained only as long as there is a defined need.

3.5.5 Detailed retention periods are defined in the Records Retention and Protection Policy.

3.6 Disposal

3.6.1 Where supported, records should be archived rather than deleted. When disposal is approved, records shall be securely deleted using approved methods.

3.6.2 Storage media scheduled for disposal must be securely destroyed or sanitised.

3.6.3 Paper records approved for disposal shall be shredded in accordance with the Asset Handling Procedures.