

ISO / IEC 27001:2022 Lead Implementer Course

Exercise 17:

Instructions:

- Create a policy and a process of document control
- Considering your company as a case study for ISO 27001:2022 implementation
- Take a blank piece of a white paper, write (by-hand). Do not copy or review; trust your memory.
- Take a clear snapshot of the paper, create a folder on Google Drive 'ISO 27001:2022 Lead' and save the snapshot (If you did not create in Exercise A)
- Send me the link to access the snapshot file on your Google drive via Facebook Messenger.
- Facebook link: facebook.com/profile.php?id=61556175711538

Follow me on my social media platforms to learn more about ISO / IEC 27001:2022 via my posts:

- LinkedIn: linkedin.com/in/john-kimani-13831329b
- Facebook: facebook.com/profile.php?id=61556175711538
- Quora: quora.com/profile/The-Cyber-Hackers-Diary
- Pinterest: pinterest.com/hackersdiary
- YouTube: www.youtube.com/@CyberHackersDiary



@ The Cyber Hacker's Diary

Document Control Policy and Process

Stoopid Boy Animations Inc.

• [ISO/IEC 27001:2022 Implementation]

• Policy :- Document Control

1. Purpose:-

To ensure all information security documents are created, reviewed, approved, and maintained in a controlled manner.

2. Scope:-

This policy applies to all information security documents within Stoopid Boy Animations Inc.

3. Responsibilities:-

The Information Security Manager is responsible for implementing and maintaining this policy.

4. Document Identification:-

Each document will have a unique identifier, title and version number.

5. Review and Approval:-

Documents must be reviewed and approved by authorized personnel before distribution.

6. Distribution and Access:-

Documents will be distributed to relevant personnel and access controlled based on roles and responsibilities.

7. Document Revision:-

Any changes to documents must be reviewed approved following the same process as initial approval.

8. Archiving and Disposal:-

Obsolete documents will be archived and retained for a specified period before secure disposal.

Process :- Document Control:

1. Creation:-

The document author drafts the document and assigns a unique identifier and version number.

2. Review:-

The draft document is reviewed by designated reviewers for accuracy, relevance, and completeness.

3. Approval:-

The reviewed document is submitted to the Information Security Manager for final approval.

4. Distribution:-

Approved documents are distributed to relevant personnel through the document management system, ensuring access controls are in place.

5. Storage:-

Documents are stored in a secure, centralized repository with appropriate access controls.

6. Revision:-

Proposed changes are documented, reviewed, and approved as per the initial approval process. The document version number is updated accordingly.

7. Archiving:-

Superseded versions of documents are archived and retained for a period of five years.