

1. Policy: Document Control

1.1. PURPOSE

The purpose of this Policy is to ensure that documents containing Personal Information and the security and processing of Personal Information (policies, procedures, data subject forms, and templates, etc.) of the Company are appropriate, up-to-date, and controlled.

This Policy will define the procedure for establishing the controls needed for the identification, storage, protection, retrieval, and retention period of Documents, information, and records (Documents).

This Policy should be read in conjunction with all the Company's Information safety and security policies, as well as the *Acceptable Usage Policy*

1.2. INTRODUCTION AND SCOPE`

All Documents are stored electronically and controlled by the Information Officer, who will manage approval, publication, changes, and review, etc. of these documents. There are no controlled paper copy Documents. Once a Document is printed, it is no longer controlled.

1.3. APPROVAL

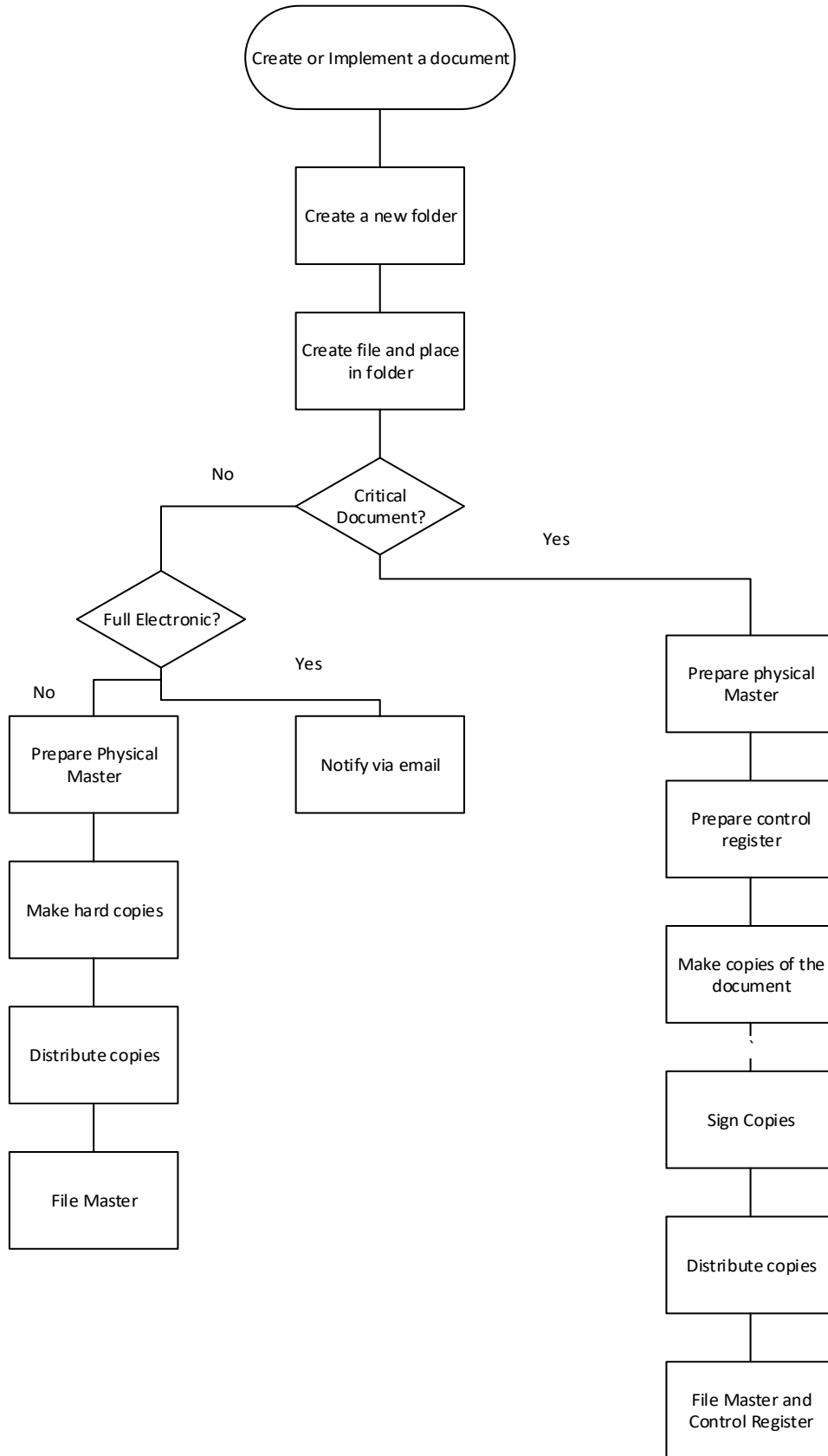
The Information Officer shall be responsible for controlling Documents and for ensuring that Documents are approved prior to issue, by submission to the CEO, and for ensuring that they conform to POPIA requirements.

The Information Officer is responsible for receiving all new and revised Documents, and for reviewing Documents.

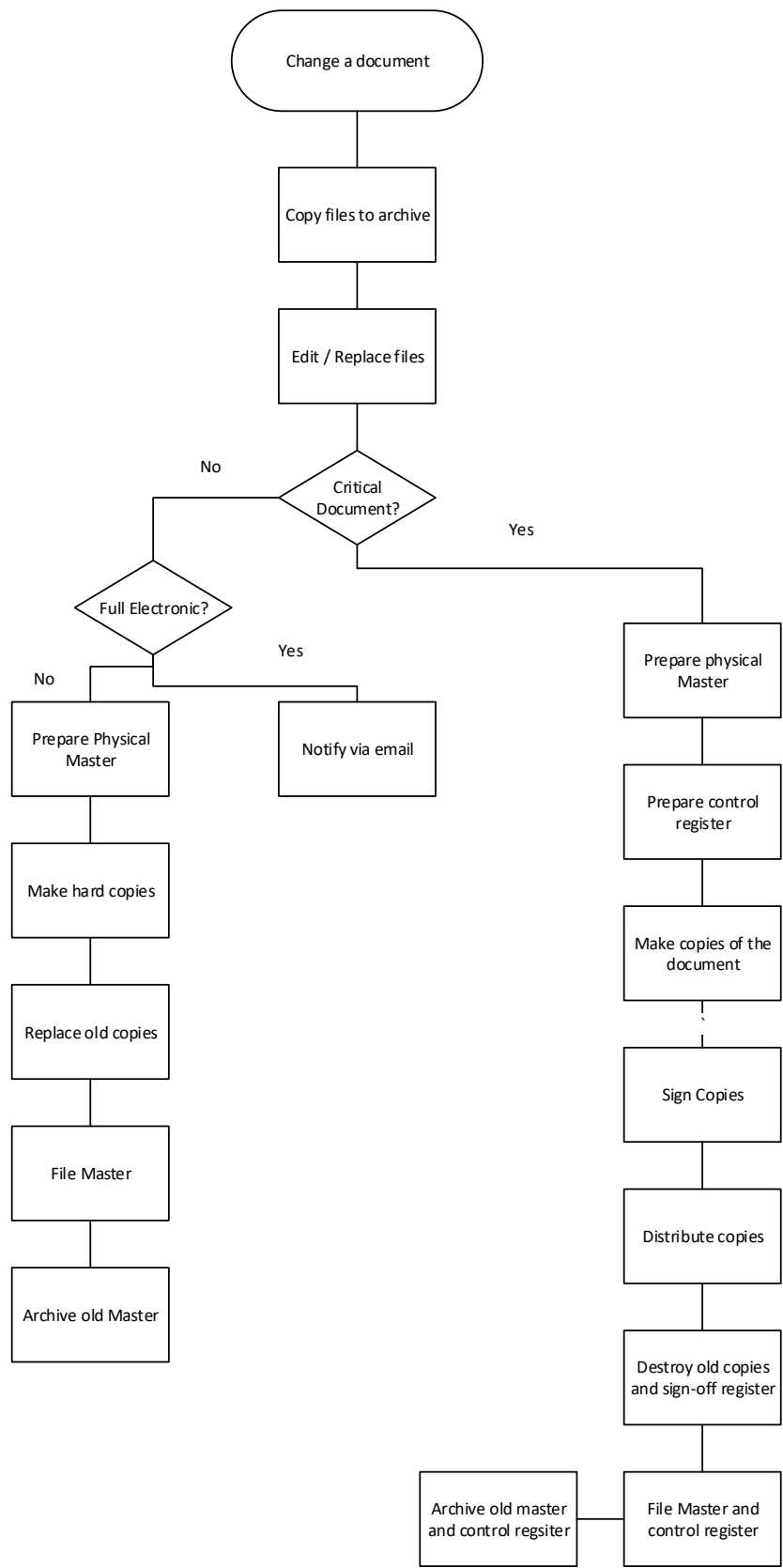
The CEO will approve all changes to Company Documents.

1.4. PROCESS

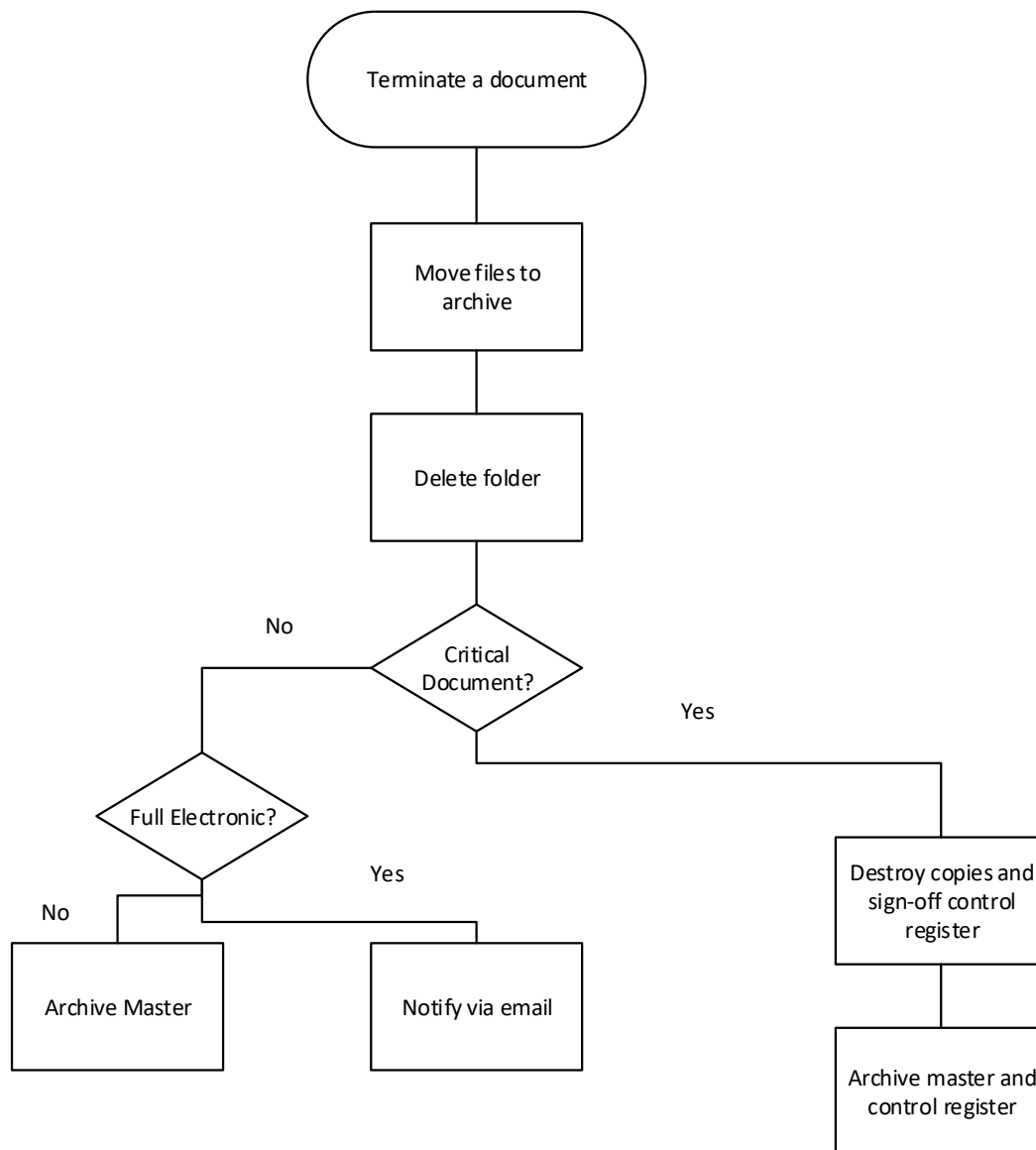
Implementation Process



Document Change Process



Documentation Termination Process



1.5. DOCUMENT STATUS, CHANGES, AND DISTRIBUTION

All Documents is kept in a controlled electronic location maintained by the Information Officer. Controlled copies are electronically distributed and may be read by all employees who have access to the system.

Individual documents may be reviewed, updated, and re-approved as often as necessary, whenever applicable legislation or other requirements change, at the discretion of the Information Officer. The whole system and all documents therein will be reviewed a minimum of once annually.

Every time a significant change is made to the Documents, or after 3 minor amendments have accumulated, an Amendment Email is prepared by the Information Officer as the basis for distribution/ publication and notifying all employees, Data Subjects (where applicable) and Data Operators.

Uncontrolled Copies

All printed copies of Documents are classed as “uncontrolled”. When documents must be sent electronically, especially to an external organisation or supplier, PDF format should be used, and all

applicable security protocols must be followed. Documents containing Personal Information must be password protected and encrypted.

When a Document has been superseded by a later revision, is withdrawn or becomes obsolete, it will be removed from the system to prevent further use. Copies will be retained by the Information Officer. Copies may be retained by others in private and restricted access server locations for reference purposes only, but if so the filename of electronic versions must contain SUPERSEDED or WITHDRAWN or OBSOLETE (likewise hard copies will be physically marked with the appropriate word).

1.6. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, to maintain compliance with these Policies and all relevant provisions of the Promotion of Access to Information Act 4 of 2013 (POPIA). Any distribution, unauthorised use, or benefit from Company information by an employee or user, in contravention of these Policies may result in disciplinary action being taken by the Company. The use of any system in such a way that breaches any of the provisions of these Policies, will be reported to the Information Officer at the Company, which may lead to further disciplinary action being taken.

1.7. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of these Policies may result in disciplinary action being taken against the employee or user in question. Such disciplinary action will be taken in accordance with the Company's disciplinary code and may include the termination of employment for employees of the Company, or cancellation of contractual relations in the case of other users, such as contractors or consultants.

1.8. POLICY AWARENESS AND UPDATE

Training and awareness:

The requirement for these Policies will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training regarding these Policies will be offered from time to time by the Company. The Company will specifically make users who are not employees of the Company aware of these Policies.


Dissemination:

These Policies will be made available on the Company's website, intranet, or notice boards.

Review:

These Policies will be reviewed from time to time to ensure ongoing compliance with POPIA. Such revisions will take place at least annually.

1.9. INTERNAL DOCUMENT APPROVAL

Information Officer Name	Signature	Date
Mrs Paula Gageiro		23 June 2021

1.10. DOCUMENT VERSION CONTROL

Version	Date	Summary of Changes