

Profusion Administrators

# Record Keeping Policy

Version 1: Creation Date 12/11/2020

A handwritten signature or mark in blue ink, located in the bottom right corner of the page. It appears to be a stylized, cursive signature.

## Table of Contents

Introduction .....	2
Receipt and classification of documentation .....	2
Storage and maintenance of records.....	2
Email Record Management .....	3
Telephonic Record Management.....	3
Clean Desk Practices .....	3
Access and Security.....	3
Disposal of records.....	4
Period of Retention and the Request of Documentation .....	4
Roles and Responsibilities .....	4
Non-Compliance .....	5

A handwritten signature or mark, possibly a stylized 'A' or similar character, located in the bottom right corner of the page.

## Introduction

This record keeping and management policy outlines the requirements and processes for Profusion employees to follow with respect to the management of records, documentation and information. This policy has been drafted in line with the following Acts and their applicable provisions:

- Financial Advisory and Intermediary Services Act, 2002
- Short-Term Insurance Act, 1998 (Policyholder Protection Rules)
- Financial Advisory and Intermediary Services Act, 2002 (Fit and Proper Requirements)
- Protection of Personal Information Act, 2013
- Companies Act, 2008

The objectives of this policy are:

- Establish the internal record keeping management processes and practices and align them with the relevant legislation.
- Establish the rights, duties and responsibilities of employees at all levels regarding effective record keeping and management.
- Ensure confidentiality, privacy, security, integrity, accessibility and retrievability of records, documentation and information received.

Through effective record keeping management, Profusion will enhance its strategic goals and objectives of rendering services of the highest quality and professionalism.

## Receipt and classification of documentation

1. Any documentation received by Profusion must be identified and classified by its nature and confidentiality. Documents, records, and information must be uploaded to Profusions electronic administrative system Easy Broker and stored under the policyholder's profile identified by a unique policy ID.
2. Documentation, records and communication related to the general policy details such as banking details, contact information and general matters are uploaded under the "Policy Document List" section of the policyholders' profile.
3. Any records, documentation and communication related to a policyholder's claim must be uploaded under the claim file itself.
4. Any documentation or record uploaded must be categorised and correctly referenced with a description allowing for easy referral when required.
5. In the rendering of services and administrative functions, such as the uploading of policyholder data, debit order collections and recording of policyholder payments, all data and records must be uploaded to the local shared server and its corresponding file. No data, records or documentation is to be stored on an employee's individual laptop or desktop itself.
6. All paper and hard copy documentation must be filed and stored within the corresponding product files and cabinets.
7. All paper and hard copy documentation and records must be scanned to an electronic format and uploaded to either the local server or administrative system depending on the nature and classification of the record.

## Storage and maintenance of records

1. Hard copy and paper passed documentation and records need to be preserved and the integrity and originality of the record must be maintained.
2. Hard copy documentation must be identified by its nature and stored within the applicable file or storage area.
3. Files, records and documentation which are no longer deemed necessary or are a year older are transferred and stored within steel cabinets and storage containers.
4. It is the employee's responsibility to ensure that all relevant documentation, records, and communication are correctly stored and/or uploaded as required within a reasonable time from receipt thereof.



## Email Record Management

1. All emails and electronic communications received or provided serve as a historical record of business transactions. It is therefore required that emails be stored for as long as they are required for functional and/or historical purposes.
2. Emails which are a year old or no longer deemed necessary are to be transferred from one's inbox and stored under the employees archived email inbox allowing for retrieval and access when required.
3. Emails and communication between employees, management and/ or policyholders which approve an action, authorise an action, contain guidance, advice or direction related to claims and administrative functions need to be uploaded to the administrative system.
4. Employees are required to maintain their email inboxes and archives, ensuring that all non-business-related emails are cleaned up and separated.

## Telephonic Record Management

1. All telephonic communications are automatically recorded and stored via the service provider.
2. Access to call recordings is restricted to the partners of Profusion, and it is their responsibility to ensure the functionality of the call recording system and storage.
3. Retrieval of telephonic communications is actioned and authorised by the Partners of Profusion.

## Clean Desk Practices

1. All employees at every level must ensure that they maintain and keep a clean desk by filing/ uploading and storing documentation and records when unattended or no longer required for the performance of their functions.
2. Where possible one must minimise the printing of hard copy documents and should use electronic formats preferably.
3. All employees must at all times be aware of their responsibilities and procedures with regards to record keeping management.
4. Disposal of documentation and records must be performed in accordance with this policy and in a manner which protects the confidentiality of the documentation and prevents its reconstruction.

## Access and Security

1. Employees shall at all times protect and safeguard records, documentation and information from unauthorised destruction, access, movement and tampering with.
2. Employees shall at all times protect and maintain the authenticity, confidentiality and quality of records, documentation and data.
3. Employees shall not share or disclose information and records which are confidential with anyone without the prior written consent of the Partners and/or the data subject concerned.
4. Employees shall at all times adhere to the provisions of the Protection of Personal Information Act when processing personal information.
5. Employees shall at all times adhere to the provisions of all governing legislation regarding the maintenance of records.
6. All laptops, desktops, servers and devices will remain password protected and update the password on the first day of each month.
7. Storage areas and cabinets shall remain securely locked and protected at all times, preventing unauthorised access.
8. Retrieval of historical records, telephonic recordings and data shall only be made available upon request and approval by the Partners of Profusion.
9. Profusion shall at all times, maintain and update anti-virus software, encryption and firewalls on electronic devices.
10. Laptops and desktops will be shut down and locked up at the end of each business day.
11. Profusion will maintain data back-ups on a daily basis.
12. Profusion will effectively implement internal controls to ensure that they are operating effectively to deter, and detect areas of non-compliance.



### Disposal of records

1. No records, documentation, information, data and communications will be destroyed, deleted, erased or disposed of without the prior consent from the Partners of Profusion.
2. Deletion of electronic data, records, and information shall be disposed of in a manner which prevents its reconstruction and duplication.
3. Hard copy records shall be disposed of through the use of a paper shredding machine and shall be done in a manner which prevents its reconstruction.
4. No records, data, documentation and information shall be disposed of, deleted or destroyed prior to the completion of the period of retention.
5. Records needed for the purpose of litigation, promotion of administrative actions and promotion of access to information purposes shall not be disposed of without the prior written consent of the Partners of Profusion.

### Period of Retention and the Request of Documentation

1. All records, documentation, data and information shall be stored for a minimum of 5 years, unless otherwise stated.
2. Profusion retains the view that historical records of business transactions be retained indefinitely or until such time that the Partners of Profusion provide consent for the disposal thereof.
3. Request for the transfer or disclosure of records, documentation, data and information may not be actioned without the consent of the Partners of Profusion or whereby required by law an authorised authority.
4. Approved requests for the disclosure or transfer of records will be done so within 7 days.

### Roles and Responsibilities

<b><u>Responsibility</u></b>	<b><u>Responsible Party</u></b>
Establishing appropriate information governance structures and overall information governance processes	Key Individual & Partners
Manage and review: <ul style="list-style-type: none"> <li>• IT risks and controls,</li> <li>• Business continuity and data recovery related to IT,</li> <li>• Information security and privacy,</li> <li>• Information and Record Management</li> </ul>	Key Individual
Supervision and monitoring of compliance with provisions, responsibilities and processes of the record keeping policy.	Key Individual & Partners
Approval of requests regarding the disclosure, transfer, deletion, amendment and access of records and information	Key Individual & Partners
Approving the development, implementation and maintenance of processes, procedures, standards and information security in support of this policy	Partners
Establishing appropriate controls and processes to ensure compliance	Key Individual

Training of employees with the provisions, requirements and processes of the record keeping policy	Key Individual
Identification, uploading and storage of records, data and documentation	Employees at all levels
Clean desk practices	Employees at all levels
Complaints and issues of non-compliance	Key Individual & Partners

### Non-Compliance

Any failure by the employees of Profusion or its Partners to adhere to this policy, the processes and provisions shall be viewed as a situation of misconduct which may result in disciplinary action being taken.

Handwritten signatures in blue ink, appearing to be two distinct signatures, located in the bottom right corner of the page.