ONE PLAN™

To make today better

Information Management Policy

POLICY NUMBER:	**25**
POLICY VERSION:	**1.0**
EFFECTIVE DATE:	**01 April 2019**

(010) 001 0141 www.oneplan.co.za
2nd Floor, South Tower, Nelson Mandela Square, Corner Maude & 5th Street, Sandton City, Johannesburg, 2196

Policy Area	**P01 (ONEPLAN) COMPLIANCE – INFORMATION POLICY**
Approved Date	1 April 2019
Current Version	1.0

This policy defines how we keep and file our business records securely and safely, how we protect our client information and the time periods we keep our records.

1. SCOPE

This policy is applicable to all staff, managers contractors, service providers and Executives of Oneplan.

All staff are responsible for *their own compliance* with this policy and for ensuring that it is consistently applied. All staff should ensure that they take the time to read and understand their roles and responsibilities in respect of it. Breach of this policy will be dealt with under our "Disciplinary Procedure"[1] and may be treated as gross misconduct which could result in dismissal.

2. REVIEW OF THIS POLICY

The policy shall be reviewed *annually* to ensure that it meets legal requirements and reflects best practice.

3. POLICY

More than virtually any another industry, the financial services industry has strict requirements to retain records, including electronic content of all types. Oneplan must retain records that relate to a wide range of activities in the business. This is not an option for any business in the financial services industry and likewise, should be implemented in all industries.

Records include

- e-mails and their attachments,
- voice-logging,
- financial reports,
- general business documentation,
- employee records,
- internal policies and procedures,
- client files,
- health information of clients
- claims
- social media posts, instant messaging conversations (Whatsapp, FB Messenger and the likes); and
- other information.

While many of the regulations that specify data-retention are not necessarily clear about exactly what types of records to retain and which can safely be deleted, and while some may not be completely clear about the length of

time that records should be retained, it is critical to retain relevant business records for long periods. *Data storage must satisfy long-term content retention goals in the context of storage space and speed of search across large data stores.*

A *failure* to implement appropriate systems and processes can result in significant financial penalties, as well as legal sanctions, loss of reputation and other negative consequences.

4. RECORDS TO BE MAINTAINED

4.1 Comprehensive and complete records must be kept of all:

4.1.1 Transactions such as, sales applications and sales calls, client files, financial and employment matters, claims, complaints and marketing and all records on OPA.

4.1.2 Verbal and written communications in respect of all financial and other services (this includes cellphone discussions (managers only) whatsapp and other social media platforms) and evidence of compliance with the requirements of the General Code of Conduct and other applicable legislation.

5. REASONS WHY IT IS IMPORTANT TO DOCUMENT AND MAINTAIN PROPER RECORDS

The importance of keeping accurate records cannot be overemphasised. Records tell us what, where and when something was done and why a decision was made. They also tell us who was involved and under what authority. They provide evidence of Oneplan, individual and/or client, contractor or independent broker and service provider activity and promote accountability and transparency.

Quality Records will provide the primary data source for many uses. These include:

5.1 *Improve Efficiency And Productivity* – when a colleague is off sick or on leave, it will not be too difficult to establish client and service history and a client can be helped without delay.

5.2 *Meet Legal And Internal Obligations And To Ensure Regulatory Compliance* - In terms of recordkeeping requirements, South Africa is one of the most heavily regulated country's in the world. Making and keeping valuable records depends on the co-operation of everyone. The only way Oneplan can be reasonably sure that it is in full compliance with laws and regulations is by operating a good records management program which takes responsibility for "regulatory compliance"[2]. Failure to comply with laws and regulations could result in severe fines, penalties or other legal consequences. Cases are won and lost based on facts, and records are the only evidence of this.

5.3 *Accountability* - Documentation and record keeping are important to establish accountability. Different roles require different requirements, and documentary evidence is the only way to prove who said or did what, and by what date. In this way, the responsible person/ party can be identified, and therefore accountability identified.

5.4 *Protect The Interests Of The Client* - The interests of our clients are protected by keeping record of disclosures done, transactions entered into (sale and/or claim), instructions and claims requirements and/or documents provided to the client or received from the client, and the regulatory provision e.g. Product information, the process for doing certain things, and dates and times to show that proper process has been followed. ***Supplying the client with records of what has happened, or has been discussed, allows him or her to review and decide any further actions going forward (TCF OUTCOME 1, 3 & 6 - Culture)***. In the event of there being a query, complaint or compliment, the client can refer to the records as evidence.

5.5 *Protect Each Individual's Rights* - Good records provide evidence of Oneplanners properly following process and ensuring that they are fulfilling their functions. In the event of a query or complaint, these records serve as an indemnification.

5.6 *Preserve Oneplan's Memory*

5.7 *Research And Development* - Every business day, records are created which could become background data for future management decisions and planning. These records document the activities of the people within Oneplan which can be used to improve processes, advance client service and build and advance Oneplan and its people.

5.8 *Consistency And Continuity In Oneplan* - Good records permit the building and monitoring of standard operating procedures, which allow for consistency and continuity in Oneplan. Where a process is followed, and each of the steps is documented, and recorded, should there be a change in personnel, someone who is ill or on leave, the internal operations can still continue to function seamlessly as all the steps in the process will have been recorded (Oneplan SOP's)[3].

Thus, rather than viewing documentation as tedious and time-consuming, it should be viewed in the light of it being an essential element of professional practice to deliver successful outcomes for the business and clients alike.

6. CONTROLS

As an FSP Oneplan must ensure that its internal controls are effective. Effective controls reduce the risk of loss, and help ensure that information is complete and accurate, information provided is reliable, and laws and regulations are complied with.
Internal controls protect in two ways:

- By minimising opportunities for unintentional errors or negligence
- By discovering small errors before they become big problems.

7. ELECTRONIC OR HARD COPY RECORDS

Oneplan supports a paperless environment and have put processes and procedures in place to effectively fulfil this outcome. Oneplan however understand that human and social resources will require some concession to operate a paper environment i.e. HR

8. RECORD STORAGE

Records are Oneplan's assets and do not belong to you. You may not remove them unnecessarily, or without the required authorisation and process. It is important they remain available to all staff.

Oneplan must take reasonable steps to ensure that records are stored in a secure location and are not available to others who are not authorised to have access.

A policy on backing up of soft-copy data, access rights and security must be implemented and maintained.[4]

Records may be stored both at "internal"[5] and registered "external storage providers"[6]. The area must be safeguarded by security, with access determined to prevent access from individuals that do not have clearance. When stored, there must be a system for location of records to allow for ease of access by authorised persons.

Records must be transported in a safe and confidential manner ensuring that access is only given to authorised persons. This includes both physical and electronic transporting.

File records according to the correct filing protocol - Oneplan has systems for managing its records, whether they are created and received in paper or electronically. Failure to capture records into the internal records systems makes them difficult or impossible to locate when needed. They may even end up lost or destroyed.

No person may store or "hoard" records in their own private store, separate from Oneplan's official records system. This also applies to e-mails: those you send or receive in the course of your employment are business records. If an e-mail needs to be kept documenting a transaction or decision, then it must be correctly filed timeously and correctly.

B. INFORMATION SECURITY

Security is an essential part of Oneplan's overall security plan. It forms the basis for all other security efforts, including data security. Security ensures that Oneplan's Information Resources are protected by physical security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

Physical security refers to the protection of building sites and equipment (and all other information and software contained therein) from theft, vandalism, natural disaster, man-made catastrophes, and accidental damage (e.g. electrical surges, extreme temperatures, spilled liquids). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders.

All Information Resources must be protected from physical tampering, damage, theft, or unauthorised physical access. Precautions should be made to protect soft copy records from electronic viruses or technical failure, and written records from damage due to fire, water or even rodents. All records must be stored in a secure, safe area where there is no possibility of damage by pests, vermin or environmental factors.

Access to areas containing confidential or protected data information must be physically restricted to authorised persons only. Physical and environmental security controls protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation.

Oneplan's security program prevents interruptions in online services, physical damage, unauthorised disclosure of information, loss of control over system integrity, and theft.

Physical access controls restrict the entry and exit of staff and visitors (and often equipment and media) from an area, to any place containing or holding sensitive data or equipment. Equipment must be protected to reduce risks from environmental threats and hazards, and opportunities for unauthorised access.

Physical access controls address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media, and any other elements required for the system's operation.

It is important to review the effectiveness of physical access controls in each area, both during normal business hours and at other times -- particularly when an area may be unoccupied.

Fires are a particularly important security threat because of the potential for complete destruction of both hardware and data as well as the risk to human life. Smoke, corrosive gases and high humidity from a localised fire can damage systems throughout an entire building. Security personnel must evaluate the fire safety of buildings that house systems. Oneplan has an **internal no smoking policy**.

Access to restricted IT areas such as the IT Office, computer rooms, network router and hub rooms, voice-mail system rooms, and similar areas containing IT resources must be restricted.

Physical access to records containing confidential or protected data, and storage of records and data in locked facilities, storage areas or containers must be restricted. Sensitive IT resources located in unsecured areas must be secured to prevent physical tampering, damage, theft, or unauthorised physical access to confidential or protected data.

IT equipment **must be marked with some form of identification that clearly indicates it is the property of Oneplan**.

The Head of Department must ensure that the following are implemented:

1. Procedures to safeguard the facility and equipment from unauthorised physical access, tampering, and theft.
2. Controls such as locked doors, signs and/or warning of restricted areas, surveillance cameras[7], alarms, property controls (property asset tag, engravings), and personnel controls (ID badges, visitor sign-in identification and escorts), security service or patrol of the facility are in place.
3. Procedures control and validate a person's access to facilities based on his/her role or function, including visitor control, and control of access to software programs for testing and revision.
4. Management reviews the list of individuals with physical access of sensitive facilities.
5. Procedures specify how to document facility repairs and modifications.
6. Procedures identify special circumstances when repairs or modifications to physical security components are required such as when special staff members with special access (e.g. application administrators) are terminated.
7. Workstation physical safeguards restrict access only to authorised users.
8. Physical safeguards for workstations that access sensitive information are in place
9. Procedures identify devices (e.g. desktops, laptops, tablets, PDA's, etc.) that are allowed to access systems containing sensitive information.
10. Physical safeguards are effective at protecting workstations with sensitive information.
11. Procedures identify when additional physical safeguards are needed to protect workstations.

B1 WORKSTATIONS

1. Computer workstation users must consider the sensitivity of the information that may be accessed and reduce the possibility of unauthorised access.

2. Physical access to workstations shall be restricted to only authorised personnel. Staff must prevent unauthorised viewing of information on a screen:

   - Monitors must be positioned away from public view. If necessary, install privacy screen filters or other physical barriers to prevent public viewing.
   - Manually activate a password protected screen saver when they leave their desk.
   - Systems must have a password protected screen saver activated within a short timeout period to ensure that workstations that were left unsecured are protected.

3. Before leaving for the day, staff must:
   . Exit running applications and close any open documents.
   . Ensure workstations are logged off

4. Staff must use workstations for authorised business purposes only and only approved personnel may install pre-approved software on workstations.

5. All sensitive information must be stored in a secure place, such as on network servers. Laptops containing sensitive information must have the hard drives encrypted and laptops shall be secured through the use of cable locks or locking laptops up in drawers or cabinets.

6. Workstations can use a surge protector (not just a power strip) or a UPS battery backup[8]. Workstations shall have vendor-issued critical security updates and patches installed when due.

B2. INFORMATION SYSTEMS SECURITY PROCEDURES

Oneplan implements common-sense protective measures to reduce the risk of loss, damage, or disclosure of information. The following guidelines identify Information Systems controls that assure that the system is properly used, resistant to disruptions, and reliable.

1. Access to information

- Users are a first line of defense and shall follow safe computing practices.
- Only legitimate software may be loaded on business computers.
- All anti-virus, firewalls etc. must be tested and updated regularly.
- Passwords – passwords are a key component to system security.
- Logon attempts – users shall be locked out after three consecutive invalid logon attempts.
- Inactivity – users shall be automatically logged off after 5 minutes of inactivity.
- Screen savers - protected screen savers are required and shall be activated after 5 minutes of inactivity.
- Clear desk – Staff shall lock up sensitive reports and computer media containing sensitive data when they leave their work areas. Staff who work with sensitive information should have lockable space available for storage when information is not in use. Staff must check with their immediate supervisor or Company management if an employee is not sure what information must be locked up or what lockable storage is available.
- Data storage – computers and handheld devices contain hard drives and non-destructive memory that may contain sensitive information.
- Third party access – prior to granting individuals physical or logical access to information resources, agreements with staff, third party users, and clients shall be in place and include responsibility for information security. Refer to “Non-Disclosure Ageements”[9].

B3. PASSWORD POLICY

Passwords are an important aspect of computer security and are the front line of protection for user accounts. A poorly chosen password may result in the compromise of our entire network. As such, all employees including contractors and vendors with access to systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The Responsible person shall ensure:

1. Manage the process of creating, changing, and safeguarding passwords.
2. Procedures prevent staff from sharing passwords with others.

3. Staff must not write passwords down.
4. Passwords are not stored in a file on ANY computer system or handheld devices without encryption.
5. If an account or password is suspected to have been compromised, report the incident and change all passwords
6. IT govern the password change frequency.
7. Passwords must be changed every 40 days
8. Passwords must not be inserted into e-mail messages or other forms of electronic communication.
9. Passwords must not be stored or transmitted in clear (unencrypted) text.

Password Guidelines

Passwords are used to restrict access to systems, software applications, and data. Some of the more common uses of passwords include user-level accounts, Web accounts, e-mail accounts, screen saver protection, voice mail passwords, and device passwords (e.g. firewalls, routers, Smartphones, Wearable Computing Devices).

When selecting a password, remember that the longer and stronger the password, the more likely it will help keep Information Systems, and the data contained with the systems, secure.

Where possible, make sure that the passwords:

i Contain both upper and lower case characters (e.g., a-z, A-Z).
ii Include both numbers and special characters (e.g. @, #, $, *).
iii Are at least eight alphanumeric characters long and is a passphrase.

Passwords should not include words based upon your personal information, names of family members, pets, cars, etc.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks." A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. A good passphrase is easy to remember but also secure. The phrase “We're off to see the wizard, The Wonderful Wizard of Oz” can be converted to WotstwTWWoO. Then add some numbers and special characters to make it even more secure.

Password Protection Standards

It is our policy that our people do not use the same password for business accounts as for other non-business access (e.g., personal e-mail, on-line banking, social media) and where possible, do not use the same password for various Oneplan access needs. For example, select one password for e-mail systems and a separate password for access to systems that store sensitive or confidential data. Persons are not permitted to share passwords with anyone,

including administrative assistants and/or QA, Sales, Care or Claims and all other staff. All passwords are to be treated as sensitive, confidential information.

1. Rules
   - Do not reveal a password over the phone to ANYONE.
   - Do not reveal a password in an e-mail message.
   - Do not reveal a password to the boss.
   - Do not talk about a password in front of others.
   - Do not hint at the format of a password (e.g., "my family name").
   - Do not reveal a password on questionnaires or security forms.
   - Do not share a password with family members.
   - Do not reveal a password to co-workers while on vacation.
   - Be careful when using social media so that you don't compromise your password.

If someone demands a password, refer them to this document. Do not use the "Remember Password" feature (e.g. browsers, software applications).

B4. RECORD REVIEW

It is good practice to review records so that service improvements can be made. Records should be reviewed periodically to establish whether internal requirements are being adequately complied with, and Oneplan's vision and mission is being followed

B5. ARCHIVING

Records must be **reviewed annually** in December of each year and where required, must be properly archived, stored and the record register updated accordingly.

B6. RECORD DESTRUCTION

Records must be current, and complete, and only destroyed with written consent from management by authorised personnel to make sure that information of a sensitive nature is not made public. Disposing of records should be conducted in a manner that protects is consistent with government, contractual and any other regulation.

Oneplan's records, whether paper or electronic, generally cannot be destroyed without proper authority. Routine records that only have temporary value can be destroyed when no longer needed.

Failing to maintain records for the length of time they are needed puts the individual and Oneplan at risk of being unable to account for what has happened or been decided. This can result in problems for clients, monetary losses from penalties or litigation, embarrassment or, in extreme cases, disciplinary action.

Action : Any confidential or sensitive paperwork must be shredded (at the appropriate POPI shredding station) prior to being sent for recycling.

B7. ENFORCEMENT

Any person found to have violated this policy may be subject to disciplinary action, up to and including termination.

1. David Milton – Sanction to be confirmed
2. Irene Willis - Compliance
3. \\onefile1\info\2019 COMPLIANCE (Irene Willis)\Operational SOP's\SOP'S 2019
4. IT Policy
5. Your desk area; the storage room in the basement
6. Metrofile
7. Not Implemented
8. Only Generator?
9. Non-Disclosure Agreement

ANNEXURE 1 - **RECORDS RETENTION PERIODS**

The FAIS and FIC act requires records of all documentation and advice to be kept in a safe place for a minimum period of five years after the service was rendered (where only a once-off transaction occurs) or five years after the relationship with the client ends.

Records must be securely stored for the period required in terms of any prevailing legislation.
Records are kept for as long as they have value, which in the case of our Oneplan's records varies.

COMPANIES ACT, NO 71 OF 2008

The Companies Act, No 71 of 2008, consolidates and amends the law that relates to companies. This Act became effective on 1 May 2011 and should be read with the Companies Amendment Act, No 3 of 2011, and the Companies Regulations, 2011. The Act expressly provides that records must be kept "in written form, or other form or manner that allows that information to be converted into written form within a reasonable time".

Document Retention Period - Reference: Section 24

3.1 General rule for company records: Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act and other public regulation
PERIOD OF RETENTION - 7 years or longer (as specified in other public regulation)

3.2 Notice of Incorporation (Registration certificate)
PERIOD OF RETENTION - Indefinite

3.3 Memorandum of Incorporation and alterations or amendments
PERIOD OF RETENTION - Indefinite

3.4 Rules
PERIOD OF RETENTION - Indefinite

3.5 Register of company secretary and auditors
PERIOD OF RETENTION - Indefinite

3.6 Regulated companies (companies to which chapter 5, part B, C and Takeover Regulations apply) - Register of disclosures of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued
PERIOD OF RETENTION - Indefinite

3.7 Notice and minutes of all shareholders meeting including:

- Resolutions adopted
- Document made available to holders of securities

PERIOD OF RETENTION - 7 years

3.8 Copies of reports presented at the annual general meeting of the company
PERIOD OF RETENTION - 7 years

3.9 Copies of annual financial statements required by the Act
PERIOD OF RETENTION - 7 years

3.10 Copies of accounting records as required by the Act
PERIOD OF RETENTION - 7 years

3.11 Record of directors and past directors, after the director has retired from the company
PERIOD OF RETENTION - 7 years

3.12 Written communication to holders of securities
PERIOD OF RETENTION - 7 years

3.13 Minutes and resolutions of directors' meetings, audit committee and directors' committees
PERIOD OF RETENTION - 7 years

3.14 Securities register and uncertificated securities register
PERIOD OF RETENTION - Indefinite

CONSUMER PROTECTION ACT, NO 68 OF 2008

The Consumer Protection Act, No 68 of 2008, seeks to promote a fair, accessible and sustainable marketplace, to provide for improved standards of consumer information and to prohibit certain unfair marketing and business practices. The Act became effective on 31 March 2011 and should be read with the Consumer Protection Act Regulations. There are specific requirements for information to be kept by intermediaries, for auctions and promotional competitions.

Document Retention Period - Reference: Section 27(3)(b) and Regulation 10

Disclosure by intermediary

4.1 Information provided to a consumer by an intermediary -

i. Full names, physical address, postal address and contact details;
ii. Id number and registration number;

iii. Contact details of public officer in case of a juristic person;
iv. Service rendered;
v. Intermediary fee;
vi. Cost to be recovered from the consumer;
vii. Frequency of accounting to the consumer;
viii. Amounts, sums, values, charges, fees or remuneration specified in monetary terms

PERIOD OF RETENTION - 3 years

4.2 Disclosure in writing of a conflict of interest by the intermediary in relevance to goods or service to be provided

PERIOD OF RETENTION - 3 years

4.3 Record of advice furnished to the consumer reflecting the basis on which the advice was given

PERIOD OF RETENTION - 3 years

4.4 Written instruction sent by intermediary to the consumer

PERIOD OF RETENTION - 3 years

Reference: Section 36(11)(b) and Regulation 11(6)

Promotional competitions

4.5 A person who conducts a promotional competition must retain:

- full details, including identity or registration numbers, addresses and contact numbers of the promoter;
- rules of promotional competition;
- copy of offer to participate in promotional competition;
- names and identity numbers of persons responsible for conducting the promotional competition;
- full list of prizes offered in promotional competition;
- a representative selection of materials marketing the promotional competition;
- list of all instances when the promotional competition was marketed, including dates, medium used and places where marketing took place;
- names and identity numbers of persons responsible for conducting the selection of prize winners in the promotional competition;
- acknowledgement of receipt, identity number and the date of receipt of the prize by the prize winner;
- declarations or afOneplanation that prize winners are not employees, directors, agents, or consultants who directly or indirectly controls or is controlled by the promoter or marketing service provider in respect of the promotional competition, or the spouses, life partners, business partners or immediate family members;
- basis of determining the prize winners;
- summary describing the proceedings to determine the winners;
- whether an independent person oversaw the determination of the prize winners;
- the means by which the prize winners were announced and frequency;

- list of names and identity numbers of prize winners;
- list of dates when prizes were handed over to the prize winners;
- steps taken by the promoter to contact the winner;
- reasons for prize winner not receiving or accepting the prize and steps taken by promoter to hand over the prize

  PERIOD OF RETENTION - 3 years

Document Section 45 and Regulation 31 - Auctions

4.6 Written agreement that contains the terms and conditions upon which the auctioneer accepts the goods for sale.

PERIOD OF RETENTION - 3 years

PROTECTION OF PERSONAL INFORMATION ACT, 4 OF 2013

The Protection of Personal Information Act, No 4 of 2013, aims to give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations.

Section 14 of the Protection of Personal Information Act states that personal information must not be retained for any longer than is necessary to achieve the purpose for its collection. If there is no legal requirement to keep the information, it should be deleted. The Act therefore places an obligation on the person collecting the data to delete or remove it at a certain time. Records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless:

(a) retention of the record is required or authorised by law;
(b) the responsible party reasonably requires the record for lawful purposes related to its functions or activities;
(c) retention of the record is required by a contract between the parties thereto; or
(d) the data subject or a competent person where the data subject is a child has consented to the retention of the record.

ELECTRONIC COMMUNICATION AND TRANSACTION ACT, NO 25 OF 2002

The Electronic Communication and Transaction Act, No 25 of 2002, regulates electronic communication and prohibits the abuse of information. Certain principles are stated for the electronic collection of personal information and also the timeframe in which this information must be kept.

Document Retention Period - Reference: Section 51

6.1 Personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information

PERIOD OF RETENTION - as long as information is used, and at least 1 year thereafter

6.2 A record of any third party to whom the information was disclosed must be kept for as long as the information is used

PERIOD OF RETENTION - As long as information is used and at least 1 year thereafter

6.3 All personal data which has become obsolete

PERIOD OF RETENTION - Destroy

FINANCIAL ADVISORY AND INTERMEDIARY SERVICES ACT, NO 37 OF 2002

The Financial Advisory and Intermediary Services Act, No 37 of 2002, seeks to regulate the rendering of certain financial advisory and intermediary services to clients and to provide for matters incidental to these services.

Document Retention Period - Reference: Section 18

7.1 An authorised financial services provider must maintain the following records regarding-

- known premature cancellations of transactions or financial products by clients of the provider;
- complaints received together with an indication whether or not any such complaint has been resolved;
- the continued compliance with the requirements referred to in section 8;
- cases of non-compliance with this Act, and the reasons for such non-compliance; and
- the continued compliance by representatives with the requirements referred to in section 13(1) and (2).

PERIOD OF RETENTION - 5 years (except to the extent exempted by the registrar)

GENERAL CODE OF CONDUCT FOR AUTHORISED FINANCIAL SERVICES PROVIDER AND REPRESENTATIVES Section 3(2)

7.2 Specific duties of provider

A provider must have appropriate procedures and systems in place to-

- record such verbal and written communications relating to a financial service rendered to a client as are contemplated in the Act, this Code or any other Code drafted in terms of section 15 of the Act;
- store and retrieve such records and any other material documentation relating to the client or financial service rendered to the client; and
- keep such client records and documentation safe from destruction.

All such records must be kept for a period after termination, to the knowledge of the provider, of the product concerned or, in any other case, after the rendering of the financial service concerned.

Providers are not required to keep the records themselves but must ensure that they are available for inspection within seven days of the registrar's request.

Records may be kept in an appropriate electronic or recorded format, which are accessible and readily reducible to written or printed form.

PERIOD OF RETENTION - 5 years From termination of business relationship
PERIOD OF RETENTION - 5 years From the date the transaction is concluded

SHORT TERM INSURANCE ACT, NO. 53 OF 1998)

POLICYHOLDER PROTECTION RULES (SHORTTERM INSURANCE), 2004

RULE 16

RECORD KEEPING

16.3 An insurer must have appropriate systems, processes and procedures in place to

(a) record all policy related communications with a policyholder;
(b) store and retrieve transaction documentation (including the policy) and all other material documentation relating to the policy and the policyholder; and
(c) keep the policy and policyholder records and documentation safe from destruction.

16.4 Records referred to in rule 16.3

(a) may be kept in an appropriate electronic or recorded format, which is accessible and readily reducible to written or printed form;
(b) must be kept for a period of at least five years after the policy came to end, or where the record does not relate to a particular policy, five years after the communication concerned; and
(c) must on request, timeously be made available to the Registrar, policyholder, former policyholder or, where the beneficiary is entitled to the information, to the beneficiary on request.

PERIOD OF RETENTION - 5 years From termination of business relationship
PERIOD OF RETENTION - 5 years From the date the transaction is concluded

FINANCIAL INTELLIGENCE CENTRE ACT, NO 38 OF 2001

The Financial Intelligence Centre Act, No 38 of 2001, established a Financial Intelligence Centre and a Money Laundering Advisory Council in order to combat money laundering activities and the financing of terrorist and related activities. The Act imposes certain duties on institutions and people who might be used for money laundering purposes and the financing of terrorist and related activities. The Act became effective on 1 February 2002.

Document Retention Period - Reference: Section 22 and 23

8.1 Whenever an accountable institution establishes a business relationship or concludes a transaction with a client, the accountable institution must keep record of:
- the identity of the client;

If the client is acting on behalf of another person,

- the identity of the person on whose behalf the client is acting; and
- the client's authority to act on behalf of that other person;

If another person is acting on behalf of the client—

- the identity of that other person; and
- that other person's authority to act on behalf of the client;

- the manner in which the identity of the persons referred to above was established.
- the nature of that business relationship or transaction;

In the case of a transaction—

- the amount involved; and
- the parties to that transaction;
- All accounts that are involved in—
  • transactions concluded by that accountable institution in the course of that business relationship; and
  • that single transaction;

- the name of the person who obtained the identity of the person transacting on behalf of the accountable institution; and
- any document or copy of a document obtained by the accountable institution

The records may be kept in electronic format.
Records must be kept:
PERIOD OF RETENTION - 5 years From termination of business relationship
PERIOD OF RETENTION - 5 years From the date the transaction is concluded

HEALTH AND SAFETY

COMPENSATION FOR OCCUPATIONAL INJURIES AND DISEASES ACT, NO 130 OF 1993

The Compensation for Occupational Injuries and Diseases Act, No 130 of 1993, provides for compensation for disablement caused by occupational injuries or diseases sustained or contracted by employees in the course of their employment or for death by these injuries at their place of work. The Act states that certain records that relate to the earnings should be retained.

Document Retention Period - Reference: Section 81(1) and (2)

9.1 A register or other record of the earnings and other prescribed particulars of all the employees
PERIOD OF RETENTION - 4 years

Occupational Health and Safety Act, No 85 of 1993

The Occupational Health and Safety Act, No 85 of 1993, was enacted to provide for the health and safety of employees at work and for people using plant and machinery and working in other hazardous employment conditions. Certain documents have to be kept based on the Administrative Regulations.

Document Retention period - Reference: Section 20(2)

9.2 A health and safety committee shall keep record of each recommendation made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation
PERIOD OF RETENTION - 3 years

9.3 Records of incidents reported at work (Ann 1 of the General Administration Regulations, 2003)
PERIOD OF RETENTION - 3 years
Reference: Asbestos Regulations, 2001, Regulation 16(e) and (f)

9.4 Records of assessments and air monitoring, and the asbestos inventory
PERIOD OF RETENTION - Min of 40 years

9.5 Medical surveillance records
PERIOD OF RETENTION - Min of 40 years
Reference: Hazardous Biological Agents Regulations, 2001, Regulation 9(1) and (2)

9.6 Records of risk assessments and air monitoring results
PERIOD OF RETENTION - 40 years

9.7 Medical surveillance records
PERIOD OF RETENTION - 40 years
Reference: Hazardous Chemical Substance Regulations, 1995, Regulation 9

9.8 Records of assessments and air monitoring
PERIOD OF RETENTION - 30 years

9.9 Medical surveillance records
PERIOD OF RETENTION - 30 years
Reference: Lead regulations, 2001, Regulation 10

9.10 Records of assessments and air monitoring
PERIOD OF RETENTION - 40 years

9.11 Medical surveillance records
PERIOD OF RETENTION - 40 years
Reference: Noise Regulations (MOSA) Regulation 11

9.12 All records of assessments and noise monitoring
PERIOD OF RETENTION - 40 years

9.13 All medical surveillance records, including the baseline audiogram of every employee
PERIOD OF RETENTION - 40 years

LABOUR
BASIC CONDITIONS OF EMPLOYMENT ACT, NO 75 OF 1997

The Basic Conditions of Employment Act, No 75 of 1997, states that various documents relating to employees should be kept for future reference.

Document Retention Period - Reference: Section 29(4)

11.1 Written particulars of employee must be kept after termination of employment
PERIOD OF RETENTION - 3 years from the date of the last entry in the record.
Reference: Section 31

11.2 Employee's name and occupation
11.3 worked by each employee
11.4 Remuneration paid to each employee
11.5 Date of birth of any employee under 18 years of age
11.6 Any other prescribed information
PERIOD OF RETENTION - 3 years from the date of the last entry in the record

A reference exists that an employer who keeps records in terms of this section is not required to keep any other record of time worked and remuneration paid as required by any other employment law.

EMPLOYMENT EQUITY ACT, NO 55 OF 1998

The Employment Equity Act, No 55 of 1998, provides for employment equity and applies to employers and employees. The Act has certain requirements with regard to the retention of certain documents.

Document Retention Period - Reference: Section 26

11.7 An employer must establish and maintain records in respect of its workforce, its employment equity plan and other records relevant to its compliance with this Act.

PERIOD OF RETENTION - 5 years after expiry of plan

Employment Equity Regulations, 2014 Reference: Regulation 9(3)

11.8 A designated employer must retain their Employment Equity Plan Reference: Section 21

Employment Equity Regulations, 2014 Reference: Regulation 10(9)

PERIOD OF RETENTION - 5 years after expiry of plan

11.9 A designated employer must submit a report to the Director General once every year. This report should be retained after submission to the Director General

PERIOD OF RETENTION - 5 years

LABOUR RELATIONS ACT, NO 66 OF 1995

The Labour Relations Act, No 66 of 1995, applies to employees, employers, trade unions and employers' organisations and provides a framework where the parties can collectively bargain regarding remuneration, basic conditions of service and other matters of importance. Various records relating to the structures created in this Act have to be kept for future reference.

Document Retention Period - Reference: Section 53(4)

11.10 Every Council must preserve the following documents in original or reproduced form:

- books of account
- supporting vouchers
- income and expenditure statements
- balance sheets
- auditor's reports
- minutes of its meetings (Reference: Section 54)

PERIOD OF RETENTION - 3 years from the end of the financial year to which they relate
Reference: Section 98(4)

11.11 Registered trade unions and registered employers' organisation must preserve the following documents in original or reproduced form:

- books of account
- supporting vouchers
- records of subscriptions or levies paid by its members
- income and expenditure statements
- balance sheets
- auditor's reports

PERIOD OF RETENTION - 3 years from the end of the financial year to which they relate.

(a) Reference: Section 99

11.12 Registered trade unions and registered employers' organisation must keep a list of its members Indefinite

11.13 Minutes of its meetings, in an original or reproduced form from the end of the financial year to which they relate
PERIOD OF RETENTION - 3 years

11.14 Registered trade unions and registered employers' organisation must keep the ballot papers for a period of three years from the date of every ballot
PERIOD OF RETENTION - 3 years
Reference: Section 205(1) and (2)

11.15 Every employer must keep the records in their original form or a reproduced form that an employer is required to keep in compliance with any applicable:
- collective agreement;
- arbitration award;
- determination made in terms of the Wage Act
PERIOD OF RETENTION - 3 years from the date of the event or end of the period to which they relate
Reference: Section 205(3)

11.16 Employer must keep prescribed details of any strike, lock-out or protest action involving its employees
PERIOD OF RETENTION - Indefinite
Schedule 8, Section 5

11.17 Employers should keep records for each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions
PERIOD OF RETENTION - Indefinite
Schedule 3, Section 8(a)

11.18 The Commission must keep the following records:
Books of accounts
Records of income, expenditure, assets and liabilities
PERIOD OF RETENTION - Indefinite

UNEMPLOYMENT INSURANCE ACT, NO 63 OF 2002

The Unemployment Insurance Act, No 63 of 2002, applies to all employers and workers, but not to –

- Workers working less than 24 hours a month for an employer;
- Learners;
- Public servants;
- Foreigners working on contract;
- Workers who get a monthly State (old age) pension; or
- Workers who only earn commission.

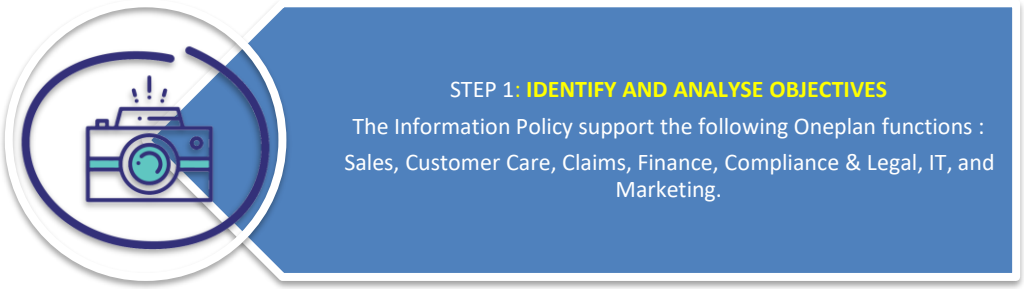
Domestic employers and their workers have also been included under the scope of the Act since 1 April 2003.

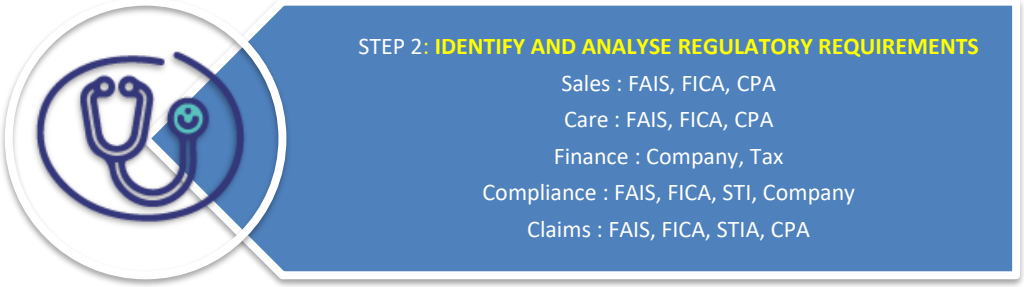
Document Retention Period - Reference: Section 56(2) (c)

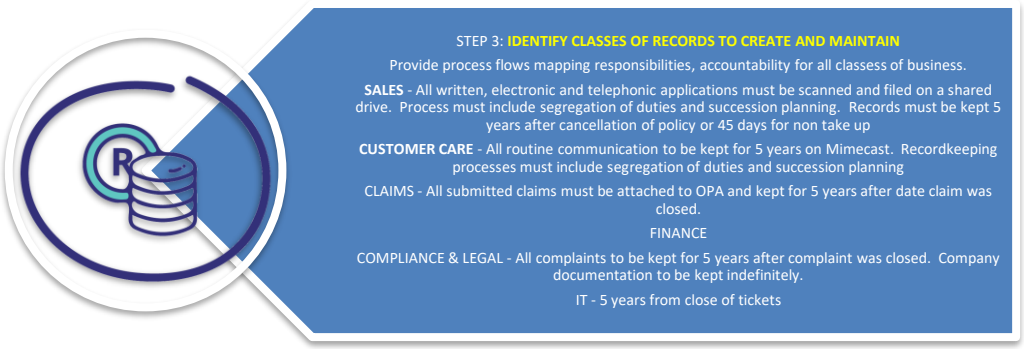
11.19 Employers must maintain personal records of each of their current employees in terms of
- names;
- identification numbers;
- monthly remuneration; and
- address where the employee is employed

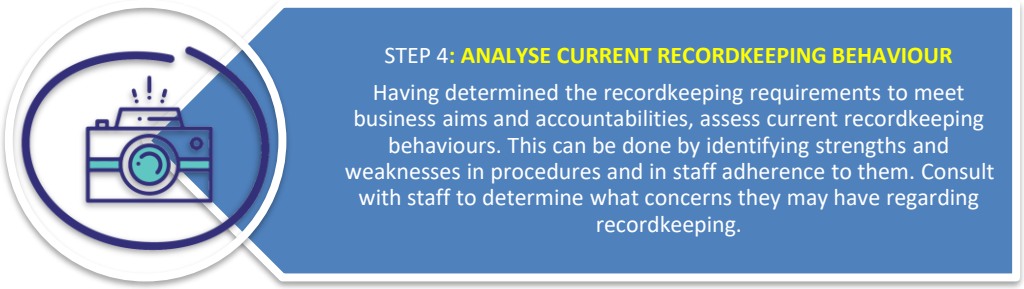
PERIOD OF RETENTION - Refer to 13.6 under Income Tax Act

C. PROCEDURE


STEP 1: IDENTIFY AND ANALYSE OBJECTIVES
The Information Policy support the following Oneplan functions :
Sales, Customer Care, Claims, Finance, Compliance & Legal, IT, and Marketing.


STEP 2: IDENTIFY AND ANALYSE REGULATORY REQUIREMENTS
Sales : FAIS, FICA, CPA
Care : FAIS, FICA, CPA
Finance : Company, Tax
Compliance : FAIS, FICA, STI, Company
Claims : FAIS, FICA, STIA, CPA


STEP 3: IDENTIFY CLASSES OF RECORDS TO CREATE AND MAINTAIN
Provide process flows mapping responsibilities, accountability for all classess of business.
SALES - All written, electronic and telephonic applications must be scanned and filed on a shared drive. Process must include segregation of duties and succession planning. Records must be kept 5 years after cancellation of policy or 45 days for non take up
CUSTOMER CARE - All routine communication to be kept for 5 years on Mimecast. Recordkeeping processes must include segregation of duties and succession planning
CLAIMS - All submitted claims must be attached to OPA and kept for 5 years after date claim was closed.
FINANCE
COMPLIANCE & LEGAL - All complaints to be kept for 5 years after complaint was closed. Company documentation to be kept indefinitely.
IT - 5 years from close of tickets


STEP 4: ANALYSE CURRENT RECORDKEEPING BEHAVIOUR
Having determined the recordkeeping requirements to meet business aims and accountabilities, assess current recordkeeping behaviours. This can be done by identifying strengths and weaknesses in procedures and in staff adherence to them. Consult with staff to determine what concerns they may have regarding recordkeeping.