Retention Destruction Policy POPI

1. Purpose

1.1. This policy defines, the company's obligations regarding the retention of personal information and data collected, held, and processed by Trade Link (Pty) Ltd in accordance with POPI and other relevant legislation.

1.2. The company only maintains records and information for legal business reasons and always adheres to the laws, standards, and best practices of SA.

1.3. The question of how long personal information should be kept from a specific entity is not clear in South Africa. This policy therefore describes the types of personal data held by the company, the period(s) for which that personal information is to be retained, the criteria for determining and reviewing such period, and when and how it was removed or otherwise disposed of.

2. Scope of the Policy

This policy applies to all the company's employees, contractors, vendors, and agents' company-owned or personally owned computer or workstation used to connect to the network. This policy applies to remote access connections used to do work on behalf of the company including reading or sending email and viewing intranet web resources. This policy covers all technical implementations of remote access used to connect to the company networks.

3. Principles

- The company must collect personal information about employees, workers, or individuals that we have a business relationship within order to conduct our daily business functions and activities efficiently and with satisfaction, and to provide the services determined by our business type. This information may include, but is not limited to, name, address, email address, date of birth, identification number, private and confidential information, sensitive information, and banking details.
- It may sometimes be necessary for the company to collect certain types of personal information to comply with the requirements of the law and/or regulations.
- The company is committed to the secure processing and retention of any confidential and information assets in accordance with contractual and legal obligations and that Trade Link (Pty) Ltd does so in an ethical and consistent manner. The company confirms that its approach and procedures comply with POPI laws and regulations, and that staff are trained and advised accordingly on the procedures and controls in place.

3.1. Retention of Personal Information

- POPI obliges companies as a data controller to process personal data fairly and not to hold the data for a longer period than is necessary to achieve those goals.
- Furthermore, records will be retained to provide information on, and proof of the company's transactions, customers, employment, and activities.
- Trade Link (Pty) Ltd.'s data retention objectives and principles are to:
  - Set boundaries for retaining personal data and ensuring compliance.
  - Ensure that the company fully meets its obligations and rights of data under POPI.

- Secure protection of confidential data and its information assets.
- Ensure that records and documents are retained for the legal, contractual, and regulatory periods set in accordance with the rules of terms of each body.

- The company systematically maintains data records in a manner that meets POPI's requirements. This policy is widely disseminated to ensure a standardized approach to data retention and record management.
- Records will be retained to provide information on, and proof of, the company's transactions, customers, employment, and activities. Schedules will determine the period that records will be retained and for how long. See the schedule at the end of the policy.
- Documents are always stored in a secure platform and server with authorised personnel being the only people who have access to it.

RETENTION AND DISPOSAL OF RECORDS

RETENTION AND DISPOSAL OF RECORDS

RETENTION

- Trade Link (Pty) Ltd retains all information for up to seven years after the conclusion of an agreement to comply with legislative requirements. Data subjects are notified, and non-consenting individuals' data will default to the prescribed legislative retention period and be flagged for timely destruction. After the applicable retention period has reached its maturity date, all documents will be disposed of by shredding physical copies and deleting electronic copies from the server.
-

DISPOSAL

An efficient records management system should include arrangements for archiving or destroying dormant records to make space available for new records, particularly in the case of paper records. Records held electronically are covered by the Electronic Communications and Transactions Act, which specifies that personal information must be deleted or destroyed when it becomes obsolete.

A policy for disposal of records should include clear guidelines on record retention and procedures for identifying records due for disposal. The records should be examined first to ensure that they are suitable for disposal and an authority to dispose should be signed by a designated member of staff.

THE RECORDS MUST BE STORED OR DESTROYED IN A SAFE, SECURE MANNER.

If records are to be destroyed, paper records should be shredded or incinerated. USB Drives and other forms of electronic storage should be overwritten with random data or physically destroyed.

If you use an outside contractor to dispose of patent-identifiable information, it is crucial that you have a confidentiality agreement in place and that the contractor provide you with certification that the files have been destroyed.

You should keep a register of all records that have been destroyed or otherwise disposed of. The register should include the reference number (if any), the employee/customer/suppliers name, address and date of birth, the start and end dates of the record's contents, the date of disposal and the name and signature of the person conducting or arranging for the disposal.

3.2. Destruction of personal Information

Retention and destruction rules apply to both hard copies/documents, as well as electronic versions Practices must consciously evaluated, and in some instances completely overhauled, how and in what manner they destroy or delete personal information and whether such processes meet muster as required by the test established by POPIA in terms of section 14(5).

In certain instances, practices may consider taking the easy route out and hire a reputable company to destroy the hard copy or electronic data for them. Practices should exercise caution on this approach as in such instances where it is the organisation's responsibility to ensure that such a company is compliant with POPIA when such data is destroyed and deleted, as in instances of a data beach, both the company providing the service and the organisation could be held liable in terms of POPIA.

Considering POPIA, the onus is on practices to ensure that personal information is sufficiently destroyed and deleted.

Any actions undertaken by practices to destroy or delete personal information will be under scrutiny should such processes not at a minimum ensure that the personal information is destroyed or deleted in a manner that prevents its reconstruction in an intelligible form.

So therefore, disposing of personal information by recycling or deleting a file electronically may not in the face of POPIA be enough as some remanence of that personal information may be retained. It is therefore incumbent upon practices to take control of the way personal information is disposed of and to ensure that appropriate mechanisms within the practice established to address potential risks.

- All information of a confidential or sensitive nature on paper or electronic media must be destroyed when it is no longer needed. This ensures compliance with POPI and the duty of confidentiality that Trade Link (Pty) Ltd owes to its employees, customers, and members.
- Shredding machines and confidential waste disposal units are made available throughout the building and where the company uses service providers, regular collection takes place to ensure that confidential data is disposed of properly.
- Personal or sensitive paper-based information should not be discarded in a trashcan. Such documents must first be processed in a specific way by shredding method. Documents that do not contain confidential information can be destroyed in the usual way.

- Under certain circumstances, data subjects have the right to request that their personal data be deleted. Data subjects have the right to delete personal data only and to prevent processing if any of the following conditions apply:
  - Where the personal data is no longer needed for the purpose for which it was originally collected.
  - When the individual withdraws consent.
  - When there is no relevant legitimate interest in the continued processing.
  - The personal data has been processed illegally; or
  - Extermination is required by law.

The following table serves as a guide to facilitate the decision-making of retention periods for the types of information. The data subject is the original source of, and the subject of the information, and thus also owns it.

DATA SUBJECT	TYPE OF INFORMATION	RETENTION PERIOD
Company Information	Agendas of Board meetings	Indefinite period
Clients or Service Provider data	All information from customers, business contacts and suppliers	At least (5) years and maximum (7) years after termination of service as set out in applicable law
Financial Data	Financial information related to and owned by the company	As set out in applicable law
Electronic Documents	Email	Not all emails need to be retained depending on the topic
Employee Data	PDF documents	Must be based on the contents of the file.
Job Seekers Data	Personnel records (attendance records, application forms, job or status change records, evaluations, termination documents, test results, training, qualification records)	At least (5) years and a maximum of (7) years after termination of service contract.
	Service contracts – Individually, CV, cover letter, qualifications, work history, references	A maximum of 6 months, after which the job seeker must give permission again

By law, all information stored under this policy must be non-encrypted. Encryption and decryption keys must be kept secure for as long as the information is retained.

4. Roles and Responsibilities

4.1. Employees Must:

4.1.1. Ensure that all information held by The Company is destroyed in accordance with this policy.

4.1.2. Incorrect or unnecessary data retention devices (HARD DISK, FLASH, CD, etc.) must be passed to the IT Department for safe destruction.

4.1.3. Make regular backups of all sensitive information.

4.2. Heads of departments and information asset owners

4.2.1. Have overall responsibility for the management of records and data generated by their department's activities, namely, to ensure that records created, received and controlled within the scope of their department, and the systems (electronic or otherwise) and procedures that they are adopted to manage in a manner that meets the objectives of this policy.

Where an information officer has been appointed, he must be involved in any data retention processes and records or all archives and the destruction of certain information.

4.3. IT Department

4.3.1. The IT department is responsible for archiving, destroying information and sanitizing hardware and software. Any hardware that can store sensitive information must be destroyed by the IT department.

4.3.2. Only the IT department may authorise the disposal of any IT equipment and must personally accept and authorize such assets of the department. In all cases, the IT department must confirm the successful deletion and destruction of each asset.

4.4. Prohibited Activities

4.4.1. Employees May Not:

4.4.1.1. Get rid of The Company patents and business-related information by throwing it in the trash.

4.4.1.2. Get rid of The Company's patents, client, and business-related information anywhere other than the company’s business premises.

4.4.1.3. Use a memory device (FLASH) containing The Company’s patents and business-related information.

4.4.1.4. Open and / or reuse a flash disk, hard drive, or CD-ROM for personal reasons, initially containing The Company’s patents and business-related information; and

4.4.1.5. Donate or sell any mobile, portable, wireless device capable of retaining sensitive information issued to The Company by any other person.

4.4.2. Employees Must

4.4.2.1. At all times destroy The Company's patents and business information in accordance with this policy

4.4.2.2. Delete any paper-based information related to The Company and its patents and/or clients in accordance with this policy.

4.4.2.3. Transmit any hard drive to the IT Department in accordance with this policy.

4.4.2.4. Use CLOUD REVIEW (like OneDrive accounts)

4.4.2.5. Use FILE-DROP technologies such as OneDrive accounts are included in this policy. OneDrive accounts are provided to The Company's employees. This platform (like Dropbox or Google Drive) can be an easy solution for employees in terms of backup and secure file transfer. Your OneDrive Account and therefore all information stored on it is the property of The Company and is still subject to this policy.

4.4.2.6. Backup - For a user's email, calendar and other items, a retention policy is applied at the level of the mailbox. For public files, the retention policy is applied at the file level.

4.4.2.7. File Transfer - Cloud technology can provide an effortless way to transfer information to other parties. If you decide to process sensitive information in this way, it must be encrypted, and must be properly maintained as explained in this policy.

Heads of departments and information asset owners - Have overall responsibility for the management of records and data generated by their department's activities, namely, to ensure that records created, received and controlled within the scope of their department, and the systems (electronic or otherwise) and procedures that they are adopted to manage in a manner that meets the objectives of this policy.
Where an information officer has been appointed, he must be involved in any data retention processes and records or all archives and the destruction of certain information.

5. Policy Compliance

5.1. Compliance Measurement

The Information Security team will verify compliance to this policy through various methods, including but not limited to, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.