



Primeplant (Pty)

Reg No: 2006 / 021699 / 07

Vat No: 4300146893

P O Box 14738
Bredell
1623

e-mail: barbara@primeplant.co.za

Tel: 011 396 1575
Fax: 011 396 1653

POLICY STATEMENT & MANUAL OF:

PROTECTION OF PERSONAL INFORMATION & THE RETENTION OF DOCUMENTS

FOR

PRIMEPLANT (PTY) LTD

all its subsidiaries

(hereinafter referred to as "Primeplant")

(Registration Number: 2006/021699/07)

A: PROTECTION OF PERSONAL INFORMATION IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

1. PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

PRIMEPLANT POPI POLICY 2021

1. INTRODUCTION

Primeplant is a Company functioning within the construction space that is obligated to comply with the Protection of Personal Information Act 4 of 2013.

POPI requires Primeplant to inform their clients as to the manner in which their personal information is used, disclosed, and destroyed.

Primeplant guarantees its commitment to protecting its client's privacy and ensuring that their personal information is used appropriately, transparently, securely, and in accordance with applicable laws.

The Policy sets out the manner in which Primeplant deals with their client's personal information as well as stipulates the purpose for which said information is used. The Policy is made available on Primeplant's website www.primeplant.co.za and by request from Primeplant's head office.

2. DEFINITIONS:

- 2.1 **Clients** includes, but are not limited to, shareholders, debtors, creditors as well as the affected personnel and/or departments related to a service division of the Company;
- 2.2 **Confidential information** refers to all information or data disclosed to or obtained by the Company by any means whatsoever and shall include, but not be limited to:
- Financial information and records; and
 - All other information including information relating to the structure, operations, processes, intentions, product information, know-how, trade secrets, market opportunities, customers, and business affairs but excluding the exceptions listed in Clause 3 hereunder.
- 2.3 **Constitution** – Constitution of the Republic of South Africa Act 108 of 1996.
- 2.4 **Data** refers to electronic representations of information in any form.
- 2.5 **Documents** include books, records, security or accounts, and any information that has been stored or recorded electronically and or physically.
- 2.6 **Electronic communication** refers to communication by means of data messages.
- 2.7 **Electronic signature** refers to data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature.
- 2.8 **Electronic transactions** include e-mails send and received.

3. ACCOUNTABILITY

- 3.1 Francois van den Heever and Jaqueline Swanepoel will be tasked with the responsibility of compliance in the Company.
- 3.2 Primeplant has a POPI policy and procedure in place and ensures that there is a culture in line with the protection of personal information in the company.

4. PERSONAL INFORMATION COLLECTED

Section 10 of POPI states that "*Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.*"

Primeplant collects and processes client's personal information pertaining to the client's needs. The type of information will depend on the need for which it is collected and will be processed for that purpose only. Whenever possible, Primeplant will inform the client as to the information required and the information deemed optional. Examples of personal information Primeplant collects include, but are not limited to:

- The client's identity number, name, surname, address, postal code, marital status, and number of dependants;

- Description of the client's residence, business, assets, financial information, banking details, etc; and
- Any other information required by Primeplant and/or suppliers in order to provide clients with the best possible service.

Primeplant aims to have agreements in place with all product suppliers, insurers, and third-party service providers to ensure a mutual understanding concerning the protection of the client's personal information. Primeplant's suppliers will be subject to the same regulations as applicable to Primeplant.

With the client's consent, Primeplant may also supplement the information provided with information Primeplant receives from other providers to offer a more consistent and personalized experience in the client's interaction with Primeplant.

For the purpose of this Policy, clients include potential and existing clients.

5. PROCESSING LIMITATION

- 5.1** Personal information will be obtained directly from the client;
- 5.2** Consent from the client is essential before gathering or processing any personal information and clients will undersign that they consent accordingly;
- 5.3** If the personal information has been gathered from a third party, it is a requirement that the third party will undersign that the client has consented to information being shared.
- 5.4** Only information that is required for the specific purpose for which it is gathered will be stored. In the event that the company collects more information than required for the intended purpose for future use, the company shall obtain the necessary consent from the client (this will be regarded as "Further processing" in the Act).
- 5.5** Should the company wish to re-use existing personal information for any other purpose other than what the information was gathered for, permission will be requested from the client again.
- 5.6** Upon the gather of personal information from the client, the client will be advised what the purpose for the information gathered will be and the time period that the information will be held for.
- 5.7** To ensure that the personal information is reliable and accurate at all times, the company will request the information directly from the client. If it is not possible for the client to produce their own information or if the information is captured from one format to another for example from a paper to an IT system, the information will be revised by a senior authorized person for the accuracy thereof.
- 5.8** Personal information will be gathered directly (in person) if possible, telephonically (in order to provide confirmation of e-mail / electronic method) or e-mail.
- 5.9** The client will be informed of how the data will be used at the time of gathering the information. (The company's POPI Policy will be provided for the client for undersigning wherein they acknowledge the purpose for which their information is being gathered.)
- 5.10** Proof of consent will be by way of a signature by the client.
- 5.11** When gathering information, the client will be given details of the responsible person in the company including contact details.
- 5.12** At the time the personal information is gathered, the client shall be advised of his / her rights to complain to the Information Regulator if misuse is suspected. The Information Regulator's information and contact details will be provided to the client.
- 5.13** The client will be advised of his / her rights to access his / her information and to object to the processing of said information upon undersigning of an agreement.

6. THE USAGE OF PERSONAL INFORMATION

The client's personal information will only be used for the purpose for which it was collected and as agreed.

The information is collected for the purpose of loading the company (cash sales, COD's, or 30 Day Accounts) onto the company's accounting software. This information is also required to ensure the company complies with SARS (legislative) requirements.

The client shall have the right to know what information the company has and for what purpose it was gathered and the client shall sign that they acknowledge same.

Personal information will only be gathered for specific, explicit, and lawful purposes.

This may include:

- Providing products or services to clients and carrying out the transactions requested;
- For underwriting purposes;
- Confirming, verifying, and updating client details;
- For the detection and prevention of fraud, crime, money laundering, or other malpractices;
- For audit and record-keeping purposes;
- In connection with legal proceedings;
- Providing Primeplant's services to clients, to render the services requested, and to maintain and constantly improve the relationship;
- Providing communication in respect of Primeplant and regulatory matters that may affect clients; and
- In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

According to Section 11 of POPI, personal information may only be processed if certain conditions, listed below, are met along with supporting information for the Primeplant Company processing of personal information:

- The client's consents to the processing: - consent is obtained from clients during the introductory, appointment and needs analysis stage of the relationship;
- Processing complies with an obligation imposed by law on Primeplant; and
- Processing is necessary for pursuing the legitimate interest of Primeplant or a third party to whom information is supplied – in order to provide Primeplant's clients with products and or services both Primeplant and any of our products suppliers require certain personal information from the clients in order to make an expert decision on the unique and specific product and or service required.

7. DISCLOSURE OF PERSONAL INFORMATION

The Primeplant Company may disclose a client's personal information to any of the Primeplant Company's companies or subsidiaries, joint venture companies, and or approved product – or third-party service providers whose services or products clients elect to use. The Primeplant Company has agreements in place to ensure that compliance with confidentiality and privacy conditions are met.

The Primeplant Company may also share client personal information with, and obtain information about clients from third parties for the reasons already discussed above. The Third Party will undersign that the client has consented to such information being shared. Primeplant may also disclose a client's information where it has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary in order to protect Primeplant's rights.

8. SAFEGUARDING CLIENT INFORMATION

It is a requirement of POPI to adequately protect personal information, Primeplant will continuously review its security controls and processes to ensure that personal information is secure.

The following procedures are in place in order to protect personal information:

- 8.1** The **PRIMEPLANT COMPANY INFORMATION OFFICER** is Conraadt Van Den Heever whose details are available below and who is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPI. He is assisted by Jaqueline Swanepoel who will function as the Company's Deputy Information Officer;
- 8.2** **THIS POLICY** has been put in place throughout Primeplant and training on this policy and the POPI Act has already taken place and will be conducted on a regular basis;
- 8.3** Each new employee will be required to sign an **EMPLOYMENT CONTRACT** containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI;
- 8.4** Every employee currently employed within Primeplant will be required to sign an addendum to their **EMPLOYMENT CONTRACTS** containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI;

- 8.5 Primeplant's archived client information is stored on-site which is also governed by POPI, access is limited to these areas to authorized personnel only;
- 8.6 Primeplant's product suppliers, insurers, and other third-party service providers will be required to sign a **SERVICE LEVEL AGREEMENT** guaranteeing their commitment to the Protection of Personal Information; this however is an ongoing process that will be evaluated as needed;
- 8.7 All electronic files or data are **BACKED UP** by the Company's IT Division which is also responsible for system security that protects third-party access and physical threats. The Company's IT Division is responsible for Electronic Information Security;
CONSENT to process client information is obtained from clients (or a person who has been given authorization from the client to provide the client's personal information)
- 8.8 The internal procedure the company has in place to identify any foreseeable risks to personal information:
Only authorized personnel will have access to personal information therefore a limitation on authorized access.
- 8.9 The external procedure the company has in place to identify any foreseeable risks to personal information:
Antivirus software (Avast & Malwarebytes) is installed on the company's server and computers as well as Microsoft Firewall are installed, which will notify the company of a data breach / unauthorized access.
- 8.10 Only authorized personnel have access to personal information which is password protected. The hard copy information is locked away and only authorized personnel will be granted access.
- 8.11 Limited personnel have access to personal information. Electronic information is password protected. The company's server has a firewall and antivirus software (Malwarebytes / Avast).
- 8.12 All employees who require personal information in an effort to perform their duties accordingly will be permitted access.
- 8.13 The necessary processes are implemented by the company. Hard copies are locked away with only authorized personnel being granted access and electronic copies are being protected by passwords.
- 8.14 If a data breach does occur, the client and the third party will immediately be notified of such breach.
- 8.15 Hard copy information will be continuously checked for the proper functioning of processes and if required be improved in order to secure confidentiality.
- 8.16 Electronic data will be kept secure by continuously updating the software of the firewall and the antivirus.
- 8.17 Company policy is that if there is a data breach, the Information Regulator and client will be notified of such a breach via e-mail and telephonically immediately.

9. **ACCESS & CORRECTION OF PERSONAL INFORMATION**

Clients have the right to access the personal information Primeplant holds about them. Clients also have the right to ask Primeplant to update, correct, or delete their personal information on reasonable grounds. Once a client objects to the processing of their personal information, Primeplant may no longer process said information. Primeplant will take all reasonable steps to confirm its client's identity before providing details of their personal information or making changes to their personal information.

When advising the client of the information the company hold and for what purpose the company holds it, the client will be provided with details of how to update their information or withdraw consent. It is advisable to develop procedures for automatically checking the accuracy of the information regularly, by sending a validation request to the client. The aforementioned includes giving the client the option to request at any time (via e-mail and/or via telephone) to update their information and to notify the client at reasonable periods of their right to update their information.

Clients may request their information from our company in writing via e-mail whether the company is in possession of their personal information. This request shall not be declined and may not be charged for. The full nature and details of the information being held shall also be provided on request but a charge may be levied for this information.

The client has the right to correct the personal information that the company is in possession of. The client also has the right to withdraw consent at any time. As

mentioned above, the client may at any time either via e-mail or telephonically correspond with the company to request the correction of their personal information.

9.1 The details of Primeplant's Information Officer and Head Office are as follows:

INFORMATION OFFICER DETAILS

NAME: FRANCOIS VAN DEN HEEVER

TELEPHONE NUMBER: 011 396 1575

FAX NUMBER: n/a

E-MAIL ADDRESS: faf@Primeplant.co.za

DEPUTY INFORMATION OFFICER DETAILS

NAME: JAQUELENE SWANEPOEL

TELEPHONE NUMBER: 011 396 1575

FAX NUMBER: n/a

E-MAIL ADDRESS: accounts@primeplant.co.za

HEAD OFFICE DETAILS

TELEPHONE NUMBER: 011 396 1575

FAX NUMBER: n/a

POSTAL ADDRESS: P.O Box 14738, Bredell, 1623

PHYSICAL ADDRESS: 434 Killarney street, Bredell, 1623

E-MAIL ADDRESS: accounts@primeplant.co.za

WEBSITE: www.primeplant.co.za

10. **AMENDMENTS TO THIS POLICY**

Amendments to, or a review of this Policy, will take place on an *ad hoc* basis or at least once a year. Clients are advised to access Primeplant's website periodically to keep abreast of any changes. Where material changes take place, clients will be notified directly or changes will be stipulated on Primeplant's website.

11. **AVAILABILITY OF THE MANUAL**

This manual is made available at the Head Office and on the Website.

12. **THE PRESCRIBED FORMS AND FEES**

The prescribed forms and fees are available on the website of the Department of Justice and Constitutional Development at www.doj.gov.za under the regulations section.

B: POLICY ON THE COMPANY'S INTERNAL RETENTION & CONFIDENTIALITY OF DOCUMENTS, INFORMATION & ELECTRONIC TRANSACTIONS

1. **PURPOSE**

1.1 To exercise effective control over the retention of documents and electronic transactions:

- As prescribed by the legislation; and
- As dictated by business practice.

1.2 Documents need to be retained to prove the existence of facts and to exercise rights the Company may have. Documents are also necessary for defending legal action, for establishing what was said or done in relation to the business of the Company, and to minimize the Company's reputational risks.

1.3 To ensure that the Company's interests are protected and that the Company's and client's rights to privacy and confidentiality are not breached.

1.4 Queries may be referred to the Company Secretary.

2. **SCOPE & DEFINITIONS**

2.1 All documents and electronic transactions generated within and/or received by the Company.

3. ACCESS TO DOCUMENTS

3.1 All Company and client information must be dealt with in the strictest confidence and may only be disclosed, without fear of redress, in the following circumstances (also see clause 3.2 below):

- Where disclosure is under compulsion of law;
- Where there is a duty to the public to disclose;
- Where the interests of the Company require disclosure; and
- Where disclosure is made with the express or implied consent of the client.

3.2 Disclosure to 3rd parties:

A responsible party must, in terms of a written contract between the responsible party and operator, ensure that the operator establishes and maintains the required security measures. The operator must advise immediately if there is the possibility that personal data has been accessed or acquired by any unauthorized person.

All employees have a duty of confidentiality in relation to the Company and clients. In addition to the provisions of clause 3.1 above, the following are also applicable:

- Information on clients:
Our client's right to confidentiality is protected in the Constitution. Information may be given to a 3rd party if the client has consented in writing to that person receiving the information.

3.3 Requests for the company information:

- In terms hereof, requests must be made in writing on the prescribed form to the Company Secretary, who is also the Information Officer. The requesting party has to state the reason for wanting the information.
- Confidential company and/or business information may not be disclosed to third parties as this could constitute industrial espionage. The affairs of the Company must be kept strictly confidential at all times.

3.4 The Company views any contravention of this policy very seriously and employees who are guilty of contravening the policy will be subject to disciplinary procedures, which may lead to the dismissal of any guilty party.

3.5 The client shall be advised via e-mail or in writing immediately if it is suspected that their personal information has been accessed by unauthorized persons. Sufficient information shall be provided to allow the client to put measures in place to safeguard themselves against potential consequences of the security compromise.

4. STORAGE OF COMPANY DOCUMENTS

4.1 HARD COPIES & ELECTRONIC DATA

Documents are stored in an archived different location.

Hard copy information will be continuously checked for the proper functioning of processes and if required to be improved to secure confidentiality. If required even stricter processes will be implemented.

Electronic data will be kept secure by continuously updating the software of the firewall and antivirus on the company's server. If necessary enhanced software will be installed.

4.2 COMPANIES ACT NUMBER 71 OF 2008

With regards to the Companies Act, Number 71 of 2008 and the Companies Amendment Act Number 3 of 2011, hard copies of the documents mentioned below must be retained for 7 (SEVEN) years:

- Any documents, accounts, books, writing, records, or other information that a company is required to keep in terms of the Act;
- Notice and minutes of all shareholders meetings, including resolutions, adopted and documents made available to holders of securities;
- Copies of reports presented at the annual general meeting of the Company;
- Copies of annual financial statements required by the Act;
- Copies of accounting records as required by the Act;

- Record of directors and past directors, after the director, has retired from the Company;
- Written communication to holders of securities; and
- Minutes and resolutions of director's meetings, audit committee, and director's committees.

Copies of the documents mentioned below must be retained indefinitely:

- Registration certificate;
- Memorandum of Incorporation and alterations and amendments;
- Rules;
- Securities register and uncertified securities register;
- Register of company secretary and auditors; and
- Regulated companies (companies to which Chapter 4, Part B, C, and Takeover Regulations apply) – Register of disclosure of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued.

4.3 CONSUMER PROTECTION ACT NUMBER 68 OF 2008

The Consumer Protection Act seeks to promote a fair, accessible, and sustainable marketplace and therefore requires a retention period of 3 (THREE) years for information provided to a consumer by an intermediary such as:

- Full names, physical address, postal address, and contact details;
- ID number and registration number;
- Contact details of the public officer in case of a juristic person;
- Service rendered;
- Intermediary fee;
- Cost to be recovered from the consumer;
- Frequency of accounting to the consumer;
- Amounts, sums, values, charges, fees, remuneration specified in monetary terms;
- Disclosure in writing of a conflict of interest by the intermediary in relevance to goods or service to be provided;
- Record of advice furnished to the consumer reflecting the basis on which the advice was given;
- Written instruction sent by the intermediary to the consumer.
- Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions; and
- Documents Section 45 and Regulation 31 of Auctions.

4.4 BASIC CONDITIONS OF EMPLOYMENT ACT NUMBER 75 OF 1997

The Basic Conditions of Employment Act requires a retention period of 3 (THREE) years for the documents mentioned below:

Section 29(4):

Written particulars of an employee after termination of employment.

Section 31:

- Employee's name and occupation;
- Time worked by each employee;
- Remuneration paid to each employee; and
- Date of birth of any employee under the age of 18 (EIGHTEEN) years.

4.5 EMPLOYMENT EQUITY ACT NUMBER 55 OF 1998

Section 26 and the General Administrative Regulations, 2009, Regulation 3(2) requires a retention period of 3 (YEARS) for the documents mentioned below:

- Records in respect of the company's workforce, employment equity plan, and other records relevant to compliance with the Act.

Section 21 and Regulations 4(10) and (11) require a retention period of 3 (THREE) years for the report which is sent to the Director-General as indicated in the Act.

4.6 UNEMPLOYMENT INSURANCE ACT NUMBER 63 OF 2002

The Unemployment Insurance Act applies to all employees and employers except:

- Workers working less than 24 (TWENTY FOUR) hours per month;
- Learners;
- Public servants;
- Foreigners working on a contract basis;
- Workers who get a monthly State (old age) pension; and
- Workers who only earn a commission.

Section 56(2)(c) requires a retention period of 5 (FIVE) years from the date of submission for the documents mentioned below:

- Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration, and address where the employee is employed.

4.7 TAX ADMINISTRATION ACT NUMBER 28 OF 2011

Section 29 of the Tax Administration Act states that records of documents must be retained to:

- Enable a person to observe the requirements of the Act;
- Are specifically required under a Tax Act by the Commissioner by the public notice; and
- This will enable SARS to be satisfied that the person has observed these requirements.

Section 29(3)(a) requires a retention period of 5 (FIVE) years from the date of submission for taxpayers that have submitted a return and an indefinite retention period until the return is submitted then a 5 (FIVE) year period applies for taxpayers who were meant to submit a return, but have not.

Section 29(3)(b) requires a retention period of 5 (FIVE) years from the end of the relevant tax period for taxpayers who were not required to submit a return but had capital gains/losses or engaged in any other activity that is subject to tax or would be subject to tax but for the application of a threshold or exemption.

Section 32(a) and (b) require a retention period of 5 (FIVE) years but records must be retained until the audit is concluded or the assessment or decision becomes final, for documents indicating that a person has been notified or is aware that the records are subject to an audit or investigation and the person who has lodged an objection or appeal against an assessment or decision under the TAA.

4.8 INCOME TAX ACT NUMBER 58 OF 1962

Schedule 4, paragraph 14(1)(a) – (d) of the Income Tax Act requires a retention period of 5 (FIVE) years from the date of submission for documents pertaining to each employee that the employer shall keep:

- Amount of remuneration paid or due by him to the employee;
- The amount of employees tax deducted or withheld from the remuneration paid or due;
- The income tax reference number of that employee;
- Any further prescribed information; and
- Employer Reconciliation return.

Schedule 6, paragraph 14(a) – (d) requires a retention period of 5 (FIVE) years from the date of submission or 5 (FIVE) years from the end of the relevant tax year, depending on the type of transaction for documents pertaining to:

- Amounts received by that registered micro business during a year of assessment;
- Dividends declared by that registered micro business during a year of assessment;
- Each asset as at the end of a year of assessment with cost price or more than R10 000 (TEN THOUSAND RAND); and
- Each liability as at the end of a year of assessment that exceeds R10 000 (TEN THOUSAND RAND).

4.9 VALUE ADDED TAX ACT NUMBER 89 OF 1991

Section 15(9), 16(2), and 55(1)(a) of the Value Added Tax Act and Interpretation Note 31, 30 March requires a retention period of 5 (FIVE) years from the date of submission of the return for the documents mentioned below:

- Where a vendor's basis of accounting is changed the vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period;
- Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act, and proof that VAT charge has been paid to SARS;
- Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists, and paid cheques;
- Documentary proof substantiating the zero-rating supplies; and
- Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.

4.10 ELECTRONIC STORAGE

4.10.1 The internal procedure requires that electronic storage of information, important documents, and information must be referred to and discussed with IT who will arrange for the indexing, storage, and retrieval thereof. This will be done in conjunction with the departments concerned.

4.10.2 Scanned documents:

If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 (ONE) year after the date of scanning, with the exception of documents pertaining to personnel. Any document containing information on the written particulars of an employee including remuneration and date of birth of an employee under the age of 18 (EIGHTEEN) years must be retained for a period of 3 (THREE) years after termination of employment.

4.10.3 Section 51 of the Electronic Communications Act Number 25 of 2005 requires that 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 and a record of any third party to whom the information was disclosed must be retained for a period of 1 (ONE) year or for as long as the information is used. It is also required that all personal information that has become obsolete must be destroyed.

5. DESTRUCTION OF DOCUMENTS

5.1 The company will account for what information are in our possession and for what purpose it was gathered and a date on which the information must be destroyed.

5.2 Documents may be destroyed after the termination of the retention period. Registration will request departments to attend to the destruction of their documents and these requests shall be attended to as soon as possible.

5.3 Each department is responsible for attending to the destruction of its documents which must be done regularly. Files must be checked to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by the Company pending such return.

5.4 After completion of the process in 5.2 above, the General Manager of the department shall in writing authorize the removal and destruction of the documents in the authorization document. These records will be retained by Registration.

5.5 The documents are then made available for collection by the removers of the Company's documents, who also ensure that the documents are shredded before disposal. This also helps to ensure the confidentiality of information.

5.6 Documents may also be stored off-site, in storage facilities approved by the Company.

5.7 Information held in hard copy will be shredded and information held on the company's electronic database will be permanently deleted.