GALVATECH (Pty) Ltd. - PRIVACY POLICY

This policy should be read in conjunction with the POPI Manual and PAIA Manual.

1. Audience - This policy applies to customers/residents who have subscribed to the services we offer, and any or all visitors to our website, if any ("you"). We recognise the importance of protecting your privacy in respect of your Personal Information (as defined in the Protection of Personal Information Act, No 4 of 2013) collected by us when you use our services.

2. Purpose of this policy - We respect your privacy and take the protection of personal information very seriously. The purpose of this policy is to describe the way we collect, store, use and protect information that can be associated with a specific natural or juristic person and can be used to identify that person ("personal information").

Personal information:

2.1 includes:

- Certain information collected on registration for our services (see below); and
- optional information that you voluntarily provide to us (see below).

2.2 excludes:

- information that has been made anonymous so that it does not identify a specific person;
- permanently de-identified information that does not relate or cannot be traced back to you specifically;
- non-personal statistical information collected and compiled by us and information that you have provided voluntarily in an open, public environment or forum including (without limitation) any blog, chat room, community, classifieds or discussion board. Because the information has been disclosed in a public forum, it is no longer confidential and does not constitute personal information subject to protection under this policy.

3. Acceptance of terms. You must accept all the terms of this policy when you register for any of our services. If you do not agree with anything in this policy, then you may not register for and use any of the services. You may not use our services if you are younger than 18 years old or do not have legal capacity to conclude legally binding contracts. By accepting this policy, you are deemed to have read, understood, accepted, and agreed to be bound by all its terms.

4. Changes - We may change the terms of this policy at any time. We will notify you of any changes by placing a notice in a prominent place on the website or by email. If you do not agree with the change you must stop using the services. If you continue to use the services following notification of a change to the terms, the changed terms will apply to you and you will be deemed to have accepted such terms.

5. Collection

5.1 Once you register for our services, you will no longer be anonymous to us as you will provide us with personal information that we require to conduct our services. This personal information will include (if applicable), but not be limited, to:

- Name, surname, identity number, company name, company registration number, VAT number
- Physical address, postal address, email address, telephone number, postal code
- Next of kin information, medical information, including medication list, allergies and the like

5.2 Collection on use. In order to provide the Services to you, you will be asked to provide us with additional information on a voluntary basis such known as “Service information”.

5.3 Optional details. You may also provide additional information on a voluntary basis (“optional information”). This includes any information you provide to us from any promotions, responses to surveys, registration and subscriptions for certain additional services, or otherwise use the optional services we provide.

5.4 Collection from browser. We automatically receive and record Internet usage information on our hosting company’s server logs from your browser, such as your internet protocol address (“IP Address”), browsing habits, click patterns, version of software installed, system type, screen resolutions, colour capabilities, plug-ins, language settings, cookie preferences, search engine keywords, JavaScript enablement, the content and pages that you access on the website, and the dates and times that you visit the website, paths taken, and time spent on sites and pages within the website (“usage information”). Please note that other websites visited before entering our website might place personal information within your URL during a visit to it, and we have no control over such websites. Accordingly, a subsequent website that collects URL information may log some personal information.

5.5 Cookies. When you access our website we may send one or more cookies (small text files containing a string of alphanumeric characters) to your computer to collect certain usage information. We use session cookies (which disappear after you close your browser) and persistent cookies (which remain after you close your browser which can be removed manually) and may be used by your browser on subsequent visits to our website. We use information gathered by cookies to improve the website.

5.6 Web beacons. Our website may contain electronic image requests (called a “single-pixel gif” or “web beacon” request) that allow us to count page views and to access cookies. Any electronic image viewed as part of a web page (including an ad banner) can act as a web beacon. Our web beacons do not collect, gather, monitor or share any of your personal information. We merely use them to compile anonymous information about our website.

5.7 Purpose for collection. We may use any service information and optional information provided by you for such purposes as indicated to you at the time you agree to provide such optional information. We may use your usage information for the purposes described in 5.4 and 5.5 above and to:

- retain your information so that you will not have to provide same again should you chose to use our services again after termination;
- monitor metrics we deem necessary for our business; and
- track your entries, submissions, and status in any promotions or other activities in connection with your usage of the website.

6. Consent to collection - We will obtain your consent to collect personal information:

- In accordance with applicable law; and
- At the time you provide us with any registration information and optional information.

7. Use - We may send administrative messages and email updates to you regarding our Services.

8. Disclosure -

8.1 Sharing:

- We may share your personal information with an affiliate, in which case we will seek to require the affiliates to honour this privacy policy.
- Our service providers under contract who help with parts of our business operations. Our contracts dictate that these service providers only use your information in connection with the services they perform for us and not for their own benefit;
- Credit bureaus to report account information, as permitted by law;
- Banking partners as required by credit card association rules for inclusion on their list of terminated merchants (in the event that you utilise the Services to receive payments and you meet their criteria);

8.2 Regulators. If you contact us regarding your experience with using any of our products, we may disclose your personal information as required of by law or governmental audit.

8.3 Law enforcement. We may disclose personal information if required:

- by a subpoena or court order;
- to comply with any law;
- to protect the safety of any individual or the general public;
- to prevent violation of our terms of service.

8.4 No selling. We will not sell personal information. No personal information will be disclosed to anyone except as provided in this privacy policy.

8.5 Marketing purposes. We may disclose aggregate statistics (information about the customer/resident population in general terms) about the personal information to advertisers or business partners.

8.6 Change of ownership. If we undergo a change in ownership, or a merger with, acquisition by, or sale of assets to, another entity, we may assign our rights to the personal information we process to a successor, purchaser, or separate entity. We will disclose the transfer on the website. If you are concerned about your personal information migrating to a new owner, you may request us to delete your personal information.

8.7 Employees. We will need to disclose personal information to our employees that require the personal information to do their jobs.

9. Security of personal information. We protect your personal information using computer safeguards such as firewalls and data encryption to protect personal information, and we authorize access to personal information only for those employees who require it to fulfil their job responsibilities.

10. Accurate and up to date. We will try to keep the personal information we collect as accurate, complete and up to date as is necessary for the purposes mentioned in clause 5.7. From time to time we will request you to update your personal information. You are able to review or update any personal information that we hold on you by emailing us or phoning us. Please note that in order to better protect you and safeguard your personal information, we do take steps to verify your identity.

11. Retention of personal information. We will only retain your personal information for as long as it is necessary to fulfil the purposes mentioned in clause 5.7, unless:

- retention of the record is required or authorised by law; or

- you have consented to the retention of the record. During the period of retention, we will continue to abide our non-disclosure obligations and will not share or sell your personal information.

12. Transfers of personal information outside South Africa. We may transmit or transfer personal information outside South Africa to a foreign country. Personal information may be stored on servers located outside South Africa in a foreign country whose laws protecting personal information may not be as stringent as the laws in South Africa. You consent to us processing your personal information in a foreign country whose laws regarding processing of personal information may be less stringent.

13. Updating or removing. You may choose to correct or update the personal information you have submitted to us, by contact us either by email or by phone.

14. Enquiries If you have any questions or concerns arising from this privacy policy or the way in which we handle personal information, please contact us.

DATA PROTECTION AND INFORMATION SHARING POLICY STATEMENT AND MANUAL OF

Galvatech (Pty) Ltd.

Corrosion Protection Specialists

POLICY STATEMENT

- This policy forms part of the policy owner's internal business processes and procedures.
- Any reference to the "Company" shall be interpreted to include the "policy owner".
- The Company's governing body, its employees, volunteers, contractors, suppliers and any other persons acting on behalf of the Company are required to familiarise themselves with the policy's requirements and undertake to comply with the stated processes and procedures.
- Risk owners and control owners are responsible for overseeing and maintaining control procedures and activities.

1. INTRODUCTION

This Data Protection and Information Sharing Policy ("Policy) describes the way that **GALVATECH Pty Ltd.**, ("**Galvatech**"), will meet its legal obligations and requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Protection of Personal Information Act, No 4 of 2013 (POPI), as that is the key piece of legislation covering security and confidentiality of personal information. POPI requires **Galvatech** to inform their customers/clients/contractors/visitors as to the manner in which their personal information is used, disclosed and destroyed. **Galvatech** guarantees its commitment to protecting its customers/clients/contractors/visitors 's privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

2. DEFINITIONS

2.1 Personal Information

Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:

- race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person;
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

2.2 Data Subject

This refers to the natural or juristic person to whom personal information relates, such as an individual customers/clients/contractors/visitors or a company that supplies the Company with products or other goods.

2.3 Responsible Party

The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, the Company is the responsible party.

2.4 Operator

An operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For example, a third-party service provider that has contracted with the Company to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

2.5 Information Officer

The Information Officer is responsible for ensuring the Company's compliance with POPIA.

Where no Information Officer is appointed, the head of the Company will be responsible for performing the Information Officer's duties.

Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

2.6 Processing

The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

- the collection, receipt, recording, organising, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- dissemination by means of transmission, distribution or making available in any other form; or
- merging, linking, as well as any restriction, degradation, erasure or destruction of information.

2.7 Record

Means any recorded information, regardless of form or medium, including:

- Writing on any material;
- Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
- Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- Book, map, plan, graph or drawing;
- Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.

2.8 Filing System

Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

2.9 Unique Identifier

Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

2.10 De-Identify

This means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

2.11 Re-Identify

In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

2.12 Consent

Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

2.13 Direct Marketing

Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

- Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
- Requesting the data subject to make a donation of any kind for any reason.

2.14 Biometrics

Means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

3. PURPOSE OF THE POLICY

This purpose of this policy is to protect the Company from the compliance risks associated with the protection of personal information which includes:

- Breaches of confidentiality. For instance, the Company could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
- Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose the Company uses information relating to them.
- Reputational damage. For instance, the Company could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by the Company.

This policy demonstrates the Company's commitment to protecting the privacy rights of data subjects in the following manner:

- Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.
- By cultivating a Company culture that recognises privacy as a valuable human right.
- By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
- By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the Company.
- By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers in order to protect the interests of the Company and data subjects.
- By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

4. SCOPE OF THE POLICY

The Policy applies to all employees, directors, sub-contractors, agents, and appointees. The provisions of the Policy are applicable to both on and off-site processing of personal information.

INFORMATION OFFICER(S)

The Information Officer appointed to Marcel Le Roux.
He/she may be contacted at:

E-mail: marcel@galvatech.co.za

Telephone number: 021 9511211

The Deputy Information Officer appointed to Johanita Gouws
He/she may be contacted at:

E-mail: debtors@galvatech.co.za

Telephone number: 021 9511211

SPECIFIC DUTIES AND RESPONSIBILITIES

4.1 Governing Body

The Company's governing body cannot delegate its accountability and is ultimately answerable for ensuring that the Company meets its legal obligations in terms of POPIA.
The governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The governing body is responsible for ensuring that:

- The Company appoints an Information Officer, and where necessary, a Deputy Information Officer.
- All persons responsible for the processing of personal information on behalf of the Company:
- are appropriately trained and supervised to do so,
- understand that they are contractually obligated to protect the personal information they come into contact with, and
- are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.
- Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.
- The scheduling of a periodic POPI Review in order to accurately assess and review the ways in which the Company collects, holds, uses, shares, discloses, destroys and processes personal information.

4.2 Information Officer

The Company's Information Officer is responsible for:

- Taking steps to ensure the Company's reasonable compliance with the provision of POPIA.
- Keeping the governing body updated about the Company's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.

- Continually analysing privacy regulations and aligning them with the Company's personal information processing procedures. This will include reviewing the Company's information protection procedures and related policies.
- Ensuring that POPI Reviews are scheduled and conducted on a regular basis.
- Ensuring that the Company makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the Company. For instance, maintaining a "contact us" facility on the Company's website.
- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the Company. This will include overseeing the amendment of the Company's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of the Company are fully aware of the risks associated with the processing of personal information and that they remain informed about the Company's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the Company.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by the Company's data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

The Deputy Information Officer will assist the Information Officer in performing his or her duties.

4.3 IT Manager

The Company's IT Manager is responsible for:

- Ensuring that the Company's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
- Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
- Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
- Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
- Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious shacking attempts.
- Ensuring that personal information being transferred electronically is encrypted.
- Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
- Performing regular IT Reviews to ensure that the security of the Company's hardware and software systems are functioning properly.
- Performing regular IT Reviews to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
- Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the Company's behalf. For instance, cloud computing services.

4.4 Marketing & Communication Manager

The Company's Marketing & Communication Manager is responsible for:

- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the Company's website, including those attached to communications such as emails and electronic newsletters.
- Addressing any personal information protection queries from journalists or media outlets such as newspapers.
- Where necessary, working with persons acting on behalf of the Company to ensure that any outsourced marketing initiatives comply with POPIA.

4.5 Employees and other Persons acting on behalf of the Company

Employees and other persons acting on behalf of the Company will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain customers/clients/contractors/visitors, suppliers and other employees.

Employees and other persons acting on behalf of the Company are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of the Company may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the Company or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of the Company must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of the Company will only process personal information where:

- The data subject, or a competent person where the data subject is a child, consents to the processing; or
- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
- The processing complies with an obligation imposed by law on the responsible party; or
- The processing protects a legitimate interest of the data subject; or
- The processing is necessary for pursuing the legitimate interests of the Company or of a third party to whom the information is supplied.

Furthermore, personal information will only be processed where the data subject:

- Clearly understands why and for what purpose his, her or its personal information is being collected; and
- Has granted the Company with explicit written or verbally recorded consent to process his, her or its personal information.

Employees and other persons acting on behalf of the Company will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the Company will keep a voice

recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

- the personal information has been made public, or
- where valid consent has been given to a third party, or
- the information is necessary for effective law enforcement.

Employees and other persons acting on behalf of the Company will under no circumstances:

- Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.
- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from the Company's central database or a dedicated server.
- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.
- Transfer personal information outside of South Africa without the express permission from the Information Officer.

Employees and other persons acting on behalf of the Company are responsible for:

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
- Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of the Company, with the sending or sharing of personal information to or with authorised external persons.
- Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.
- Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.
- Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the customers/clients/ contractors /visitors or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.
- Undergoing POPI Awareness training from time to time.

Where an employee, or a person acting on behalf of the Company, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

5. POLICY STATEMENT

Galvatech collects and uses Personal Information of the individuals and corporate entities with whom it works in order to operate and carry out its business effectively. Galvatech regards the lawful and appropriate processing of all Personal Information as crucial to successful service delivery and essential to maintaining confidence between Galvatech and those individuals and entities who deal it. Galvatech therefore fully endorses and adheres to the principles of the Protection of Personal Information Act ("POPI").

6. GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of the Company will at all times be subject to, and act in accordance with, the following guiding principles:

6.1 Accountability

Failing to comply with POPIA could potentially damage the Company's reputation or expose the Company to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

The Company will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, the Company will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

6.2 Processing Limitation

The Company will ensure that personal information under its control is processed:

- in a fair, lawful and non-excessive manner, and
- only for a specifically defined purpose.

The Company will under no circumstances distribute or share personal information between separate legal entities, associated Company s (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

An example of a "POPI Notice and Consent Form" can be found under Annexure C.

6.3 Purpose Specification

All of the Company's business units and operations must be informed by the principle of transparency.

The Company will process personal information only for specific, explicitly defined and legitimate reasons.

6.4 Further Processing Limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

Therefore, where the Company seeks to process personal information it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, the Company will first obtain additional consent from the data subject.

6.5 Information Quality

The Company will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

The more important it is that the personal information be accurate (for example, the beneficiary details of bank account number is of the utmost importance), the greater the effort the Company will put into ensuring its accuracy.

6.6 Open Communication

The Company will take reasonable steps to notify data subjects that their personal information is being collected including the purpose for which it is being collected and processed.

The Company will ensure that it establishes and maintains a “contact us” facility, for instance via its website or through an electronic helpdesk, for data subjects who want to:

- Enquire whether the Company holds related personal information, or
- Request access to related personal information, or
- Request the Company to update or correct related personal information, or
- Make a complaint concerning the processing of personal information.

6.7 Security Safeguards

The Company will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit card details, the greater the security required.

The Company will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the Company’s IT network.

The Company will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.
All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the Company is responsible.
All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.

The Company's operators and third-party service providers will be required to enter into service level agreements with the Company where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

6.8 Data Subject Participation

A data subject may request the correction or deletion of his, her or its personal information held by the Company.

The Company will ensure that it provides a facility for data subjects who want to request the correction of deletion of their personal information.

Where applicable, the Company will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7. PROCESSING OF PERSONAL INFORMATION

7.1 Purpose of Processing

Galvatech uses the Personal Information under its care in the following ways:

- Conducting credit reference checks and assessments
- Identifying and managing its customers/clients/contractors/visitors
- Identifying customers/clients/contractors/visitors medical and other related health needs
- Administration of agreements
- Providing products and services to customers/clients/contractors/visitors
- Detecting and prevention of fraud, crime, money laundering and other malpractice
- Conducting market or customer satisfaction research
- Marketing and sales
- In connection with legal proceedings
- Staff administration
- Keeping of accounts and records
- Complying with legal and regulatory requirements
- Profiling data subjects for the purposes of direct marketing

7.2 Personal information Collected

Section 9 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."

Galvatech collects and processes customers/clients/ contractors /visitors 's personal information pertaining to the needs of the business. The type of information of information will depend on the needs for which it is collected and will be processed for that purpose only. Whenever possible, Galvatech will inform the customers/clients/contractors/visitors as to the information required and the information deemed optional. Galvatech aims to have agreements in place with all product suppliers, insurers and third-party service providers to ensure a mutual understanding with regard to protection of the customer's personal information. With the customer's consent, Galvatech may also supplement the information provided with the information that it receives from other providers in order to offer a more consistent and personalized experience for its customers/clients/ contractors /visitors s.

7.3 Categories of Data Subjects and their Personal Information

Galvatech may possess records relating to suppliers, shareholders, contractors service providers, staff, customers/clients/ contractors /visitors:

Entity Type	Personal Information Processed
Customers/clients/contractors /visitors: Natural Persons	Names; contact details; physical and postal addresses; date of birth; ID number; tax related information; nationality; gender; confidential correspondence; medical information
Customer – Juristic Persons / Entities	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information
Contracted Service Providers	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information
Employees / Directors	Gender; pregnancy; marital status; colour, race; age; language; education information; financial information; employment history; ID number; physical and postal address; contact details; opinions; criminal record; well-being

7.4 Categories of Recipients for Processing the Personal Information

Galvatech may share the Personal Information with its agents, affiliates, and associated companies who may use this information to send the Data Subject information on products and services. Galvatech may supply the Personal Information to any party to whom Galvatech may have assigned or transferred any of its rights or obligations under any agreement, and/or to service providers who render the following services:

- Capturing and organising of data;
- Storing of data;
- Sending of emails and other correspondence to customers/clients/ contractors /visitors;
- Conducting due diligence checks;
- Administration of the Medical Aid and Pension Schemes.

7.5 Retention of Personal Information Records

Galvatech may retain Personal Information records indefinitely, unless the Data Subject objects thereto. If the Data Subject objects to indefinite retention of its Personal Information Galvatech shall retain the Personal Information records to the extent permitted or required by law.

7.6 General Description of Information Security Measures

Galvatech employs up to date technology to ensure the confidentiality, integrity and availability of the Personal Information under its care. Measures include:

- Firewalls
- Virus protection software and update protocols
- Logical and physical access control;
- Secure setup of hardware and software making up the IT infrastructure;
- Outsourced Service Providers who process Personal Information on behalf of Galvatech are contracted to implement security controls;
- Personal information shall be stored on site and access shall be limited to authorized personal only.
- All electronic files or data shall be backed up on to cloud based services.

8. ACCESS TO PERSONAL INFORMATION

All individuals and entities may request access, amendment, or deletion of their own Personal Information held by Galvatech. Any requests should be directed, on the prescribed form, to the Information Officer.

Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against the Company's PAIA Policy.

The Information Officer will process all requests within a reasonable time.

8.1 RIGHTS OF DATA SUBJECTS

Where appropriate, the Company will ensure that its clients and customers /contractors/visitors are made aware of the rights conferred upon them as data subjects.
The Company will ensure that it gives effect to the following rights of data subjects:

8.1.1 The Right to Access Personal Information

The Company recognises that a data subject has the right to establish whether the Company holds personal information related to him, her or it including the right to request access to that personal information. An example of a "Personal Information Request Form" can be found under Annexure A.

8.1.2 The Right to have Personal Information Corrected or Deleted

The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where the Company is no longer authorised to retain the personal information.

8.1.3 The Right to Object to the Processing of Personal Information

The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information. In such circumstances, the Company will give due consideration to the request and the requirements of POPIA. The Company may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

8.1.4 The Right to Object to Direct Marketing

The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

8.1.5 The Right to Complain to the Information Regulator

The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information. An example of a "POPI Complaint Form" can be found under Annexure B.

8.1.6 The Right to be Informed

The data subject has the right to be notified that his, her or its personal information is being collected by the Company. The data subject also has the right to be notified in any situation where the Company has reasonable grounds to believe that the personal information of the data subject has been accessed or a

8.2 REMEDIES AVAILABLE IF REQUEST FOR ACCESS TO PERSONAL INFORMATION IS REFUSED

8.2.1 Internal Remedies

Galvatech does not have internal appeal procedures. As such, the decision made by the Information Officer pertaining to a request is final, and requestors will have to exercise such external remedies at their disposal if a request is refused, and the requestor is not satisfied with the response provided by the information officer.

8.2.2 External Remedies

A requestor that is dissatisfied with the information officer's refusal to disclose information, may within 30 days of notification of the decision, apply to a court for relief. Likewise, a third party dissatisfied with the information officer's decision to grant a request for information, may within 30 days of notification of the decision, apply to a court for relief. For purposes of the Act, courts that have jurisdiction over these applications are the Constitutional Court, the High Court or another court of similar status.

8.3 GROUNDS FOR REFUSAL

Galvatech may legitimately refuse to grant access to a requested record that falls within a certain category. Grounds on which **Galvatech** may refuse access include:

- Protecting personal information that **Galvatech** holds about a third person (who is a natural person) including a deceased person, from unreasonable disclosure;
- Protecting commercial information that **Galvatech** holds about a third party or **Galvatech** (for example trade secret: financial, commercial, scientific or technical information that may harm the commercial or financial interests of the Company or the third party);
- If disclosure of the record would result in a breach of a duty of confidence owed to a third party in terms of an agreement;
- If disclosure of the record would endanger the life or physical safety of an individual;
- If disclosure of the record would prejudice or impair the security of property or means of transport;
- If disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection scheme;
- If disclosure of the record would prejudice or impair the protection of the safety of the public;
- The record is privileged from production in legal proceedings, unless the legal privilege has been waived;
- Disclosure of the record (containing trade secrets, financial, commercial, scientific, or technical information) would harm the commercial or financial interests of Galvatech;
- Disclosure of the record would put Galvatech at a disadvantage in contractual or other negotiations or prejudice it in commercial competition;
- The record is a computer programme; and
- The record contains information about research being carried out or about to be carried out on behalf of a third party or Galvatech.

8.3.1 Records that cannot be found or do not exist

If **Galvatech** has searched for a record and it is believed that the record does not exist or cannot be found, the requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken to try to locate the record.

8.4 COMPLAINTS PROCEDURE

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. The Company takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:

- POPI complaints must be submitted to the Company in writing. Where so required, the Information Officer will provide the data subject with a "POPI Complaint Form".
- Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day.
- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.
- The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
- The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the Company's data subjects.
- Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer

will consult with the Company's governing body where after the affected data subjects and the Information Regulator will be informed of this breach.

- The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the Company's governing body within 7 working days of receipt of the complaint. In all instances, the Company will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
- The Information Officer's response to the data subject may comprise any of the following:
- A suggested remedy for the complaint,
- A dismissal of the complaint and the reasons as to why it was dismissed,
- An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
- Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.
- The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

9. IMPLEMENTATION GUIDELINES

9.1 TRAINING & DISSEMINATION OF INFORMATION

This Policy has been put in place throughout **Galvatech**, training on the Policy and POPI will take place with all affected employees.

All new employees will be made aware at induction, or through training programmes, of their responsibilities under the terms of this Policy and POPI.

Modifications and updates to data protection and information sharing policies, legislation, or guidelines will be brought to the attention of all staff.

9.2 EMPLOYEE CONTRACTS

Each new employee will sign an Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information, however it is stored. Failure to comply will result in the instigation of a disciplinary procedure.

Each employee currently employed within **Galvatech** will sign an addendum to their Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information, however it is stored. Failure to comply will result in the instigation of a disciplinary procedure.

10. EIGHT PROCESSING CONDITIONS

POPI is implemented by abiding by eight processing conditions. **Galvatech** shall abide by these principles in all its possessing activities.

10.1 ACCOUNTABILITY

Galvatech shall ensure that all processing conditions, as set out in POPI, are complied with when determining the purpose and means of processing Personal Information and during the processing itself. **Galvatech** shall remain liable for compliance with these conditions, even if it has outsourced it processing activities.

10.2 PROCESSING LIMITATION

10.2.1 Lawful grounds

The processing of Personal Information is only lawful if, given the purpose of processing, the information is adequate, relevant and not excessive.

Galvatech may only process Personal Information if one of the following grounds of lawful processing exists:

- The Data Subject consents to the processing;
- Processing is necessary for the conclusion or performance of a contract with the Data Subject;
- Processing complies with a legal responsibility imposed on **Galvatech**;
- Processing protects a legitimate interest of the Data Subject;
- Processing is necessary for pursuance of a legitimate interest of **Galvatech**, or a third party to whom the information is supplied;

Special Personal Information includes:

- Religious, philosophical, or political beliefs;
- Race or ethnic origin;
- Trade union membership;
- Health or sex life;
- Biometric information (including blood type, fingerprints, DNA, retinal scanning, voice recognition, photographs);
- Criminal behaviour;
- Information concerning a child.

Galvatech may only process Special Personal Information under the following circumstances:

- The Data Subject has consented to such processing;
- The Special Personal Information was deliberately made public by the Data Subject;
- Processing is necessary for the establishment of a right or defence in law;
- Processing is for historical, statistical, or research reasons
- If processing of race or ethnic origin is in order to comply with affirmative action laws

All Data Subjects have the right to refuse or withdraw their consent to the processing of their Personal Information, and a Data Subject may object, at any time, to the processing of their Personal Information on any of the above grounds, unless legislation provides for such processing. If the Data subject withdraws consent or objects to processing then **Galvatech** shall forthwith refrain from processing the Personal Information.

10.2.2 Collection directly from the Data Subject

Personal Information must be collected directly from the Data Subject, unless:

- Personal Information is contained in a public record;
- Personal Information has been deliberately made public by the Data Subject;
- Personal Information is collected from another source with the Data Subject's consent;
- Collection of Personal Information from another source would not prejudice the Data Subject;
- Collection of Personal Information from another source is necessary to maintain, comply with or exercise any law or legal right;
- Collection from the Data Subject would prejudice the lawful purpose of collection;
- Collection from the Data Subject is not reasonably practicable.

10.3 PURPOSE SPECIFICATION

Galvatech shall only process Personal Information for the specific purposes as set out and defined above herein. **Galvatech** is permitted to collect only the minimum required personal information for their purpose. In addition, the consent of the data subject is required as it ensures that he/she is aware that personal information is being processed, the purpose as well as the type of information being processed. The need for consent also ensures that personal information is collected directly from the source, further ensuring accuracy.

10.4 FURTHER PROCESSING LIMITATION

New processing activity must be compatible with original purpose of processing. Further processing will be regarded as compatible with the purpose of collection if:

- Data Subject has consented to the further processing;
- Personal Information is contained in a public record;
- Personal Information has been deliberately made public by the Data Subject;
- Further processing is necessary to maintain, comply with or exercise any law or legal right;
- Further processing is necessary to prevent or mitigate a threat to public health or safety, or the life or health of the Data Subject or a third party

10.5 INFORMATION QUALITY

Galvatech shall take reasonable steps to ensure that Personal Information is complete, accurate, not misleading and updated. **Galvatech** shall periodically review Data Subject records to ensure that the Personal Information is still valid and correct.

Employees should as far as reasonably practicable follow the following guidance when collecting Personal Information:

- Personal Information should be dated when received;
- A record should be kept of where the Personal Information was obtained;
- Changed to information records should be dated;
- Irrelevant or unneeded Personal Information should be deleted or destroyed;
- Personal Information should be stored securely, either on a secure electronic database or in a secure physical filing system.

10.6 OPENNESS

Galvatech shall take reasonable steps to ensure that the Data Subject is made aware of:

- What Personal Information is collected, and the source of the information;
- The purpose of collection and processing;
- Where the supply of Personal Information is voluntary or mandatory, and the consequences of a failure to provide such information;
- Whether collection is in terms of any law requiring such collection;
- Whether the Personal Information shall be shared with any third party.

10.7 DATA SUBJECT PARTICIPATION

Data Subject have the right to request access to, amendment, or deletion of their Personal Information.
All such requests must be submitted in writing to the Information Officer. Unless there are grounds for refusal as set out in paragraph 7.2, above, **Galvatech** shall disclose the requested Personal Information:

- On receipt of adequate proof of identity from the Data Subject, or requester;
- Within a reasonable time;
- On receipt of the prescribed fee, if any;
- In a reasonable format

Galvatech shall not disclose any Personal Information to any party unless the identity of the requester has been verified.

10.8 SECURITY SAFEGUARDS

Galvatech shall ensure the integrity and confidentiality of all Personal Information in its possession, by taking reasonable steps to:

- Identify all reasonably foreseeable risks to information security;
- Establish and maintain appropriate safeguards against such risks;

10.8.1 Written records

- Personal Information records should be kept in locked cabinets, or safes;
- When in use Personal Information records should not be left unattended in areas where non-staff members may access them;
- **Galvatech** shall implement and maintain a "Clean Desk Policy" where all employees shall be required to clear their desks of all Personal Information when leaving their desks for any length of time and at the end of the day;
- Personal Information which is no longer required should be disposed of by shredding.

Any loss or theft of, or unauthorised access to, Personal Information must be immediately reported to the Information Officer.

10.8.2 Electronic Records

- All electronically held Personal Information must be saved in a secure database;
- As far as reasonably practicable, no Personal Information should be saved on individual computers, laptops or hand-held devices;
- All computers, laptops and hand-held devices should be access protected with a password, fingerprint or retina scan, with the password being of reasonable complexity and changed frequently;
- **Galvatech** shall implement and maintain a "Clean Screen Policy" where all employees shall be required to lock their computers or laptops when leaving their desks for any length of time and to log off at the end of the day;
- Electronical Personal Information which is no longer required must be deleted from the individual laptop or computer and the relevant database. The employee must ensure that the information has been completely deleted and is not recoverable.

Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to the Information Officer, who shall notify the IT department, who shall take all necessary steps to remotely delete the information, if possible.

11. DIRECT MARKETING

All Direct Marketing communications shall contain **Galvatech's** details, and an address or method for the customer to opt-out of receiving further marketing communication.

11.1.1 Existing Customers/clients/ contractors/visitors

Direct Marketing by electronic means to existing customers/clients/ contractors /visitors is only permitted:

- If the customer's details were obtained in the context of a sale or service; and
- For the purpose of marketing the same or similar products;

The customer must be given the opportunity to opt-out of receiving direct marketing on each occasion of direct marketing.

11.1.2 Consent

Galvatech may send electronic Direct Marketing communication to Data Subjects who have consented to receiving it. **Galvatech** may approach a Data Subject for consent only once.

11.1.3 Record Keeping

Galvatech shall keep record of:

- Date of consent
- Wording of the consent
- Who obtained the consent
- Proof of opportunity to opt-out on each marketing contact
- Record of opt-outs

12. DESTRUCTION OF DOCUMENTS

12.1 Documents may be destroyed after the termination of the retention period specified herein, or as determined by the Company from time to time.

12.2 Each department is responsible for attending to the destruction of its documents and electronic records, which must be done on a regular basis. Files must be checked in order 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.

12.3 The documents must made available for collection by the Shred-It, or other approved document disposal Company.

12.4 Deletion of electronic records must be done in consultation with the IT Department, to ensure that deleted information is incapable of being reconstructed and/or recovered.

13. POPI REVIEW

The Company's Information Officer will schedule periodic POPI Reviews.

13.1 The purpose of a POPI Review is to:

13.1.1 Identify the processes used to collect, record, store, disseminate and destroy personal information.

13.1.2 Determine the flow of personal information throughout the Company. For instance, the Company's various business units, divisions, branches and other associated Companies.

13.1.3 Redefine the purpose for gathering and processing personal information.

13.1.4 Ensure that the processing parameters are still adequately limited.

13.1.5 Ensure that new data subjects are made aware of the processing of their personal information.

13.1.6 Re-establish the rationale for any further processing where information is received via a third party.

13.1.7 Verify the quality and security of personal information.
13.1.8 Monitor the extend of compliance with POPIA and this policy.
13.1.9 Monitor the effectiveness of internal controls established to manage the Company's POPI related compliance risk.

13.2 In performing the POPI Review, Information Officers will liaise with line managers in order to identify areas within in the Company's operation that are most vulnerable or susceptible to the unlawful processing of personal information.

Information Officers will be permitted direct access to and have demonstrable support from line managers and the Company's governing body in performing their duties.

14. STATUTORY RETENTION PERIODS

Legislation	Document Type	Period
Companies Act	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 meeting, 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 directors' meetings, audit committee and directors' committees.	7 Years

	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 5, 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.	Indefinitely

Consumer Protection Act	Full names, physical address, postal address and contact details; ID number and registration number; Contact details of public officer in case of a juristic person; Service rendered; Cost to be recovered from the consumer; Frequency of accounting to the consumer; Amounts, sums, values, charges, fees, remuneration specified in monetary terms; Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions;	3 years

Financial Intelligence Centre Act	Whenever a reportable transaction is concluded with a customer, the institution must keep record of the identity of the customer; If the customer is acting on behalf of another person, the identity of the person on whose behalf the customer is acting and the customer's authority to act on behalf of that other person; If another person is acting on behalf of the customer, the identity of that person and that other person's authority to act on behalf of the customer; 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 the 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; Any document or copy of a document obtained by the accountable institution	5 years

Compensation for Occupational Injuries and Diseases Act	Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees.	4 years
	Section 20(2) documents : -Health and safety committee recommendations 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; -Records of incidents reported at work.	3 years
	Asbestos Regulations, 2001, regulation 16(1): -Records of assessment and air monitoring, and the asbestos inventory; -Medical surveillance records; Hazardous Biological Agents Regulations, 2001, Regulations 9(1) and (2): -Records of risk assessments and air monitoring; -Medical surveillance records. Lead Regulations, 2001, Regulation 10: -Records of assessments and air monitoring; -Medical surveillance records Noise - induced Hearing Loss Regulations, 2003, Regulation 11: -All records of assessment and noise monitoring; -All medical surveillance records, including the baseline audiogram of every employee.	40 years
	Hazardous Chemical Substance Regulations, 1995, Regulation 9: -Records of assessments and air monitoring; -Medical surveillance records	30 years

Basic Conditions of Employment Act	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; -Date of birth of any employee under the age of 18 years.	3 years
Employment Equity Act	Records in respect of the Company's workforce, employment equity plan and other records relevant to compliance with the Act; Section 21 report which is sent to the Director General	3 years
Labour Relations Act	Records to be retained by the employer are the collective agreements and arbitration awards.	3 years
	An employer must retain prescribed details of any strike, lock-out or protest action involving its employees; Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions	Indefinite
Unemployment Insurance Act	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	5 years
Tax Administration Act	Section 29 documents which: -Enable a person to observe the requirements of the Act; -Are specifically required under a Tax Act by the Commissioner by the public notice; -Will enable SARS to be satisfied that the person has observed these requirements	5 years

Income Tax Act	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; Employer Reconciliation return.	5 years
Value Added Tax Act	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 the 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 of supplies; 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.	5 years

Galvatech (Pty) Ltd.

Corrosion Protection Specialists

The Company

MANUAL

in terms of

Section 51 of

The Promotion of Access to Information Act

2/2000

(the "ACT")

INDEX

1. INTRODUCTION

GALVATECH is a Private Company and conducts business as a

The company specialise in the fields of Hot Dip Galvanising (ISO 1461 / SANS 121), Abrasive Grit Blasting (Sand Blasting and Shot Blasting), Powder Coating (Epoxy Coating**),** Industrial Spray Painting (Conventional Wet Spraying), PVC Coating**,** FBE Coating (Fusion Bond Epoxy) and Zinc Metal Spraying**.**

We are authorized to conduct our business in terms of the

- Companies Act 71 of 2008

2.COMPANY CONTACT DETAILS

Duly Authorised Company Official(s):

Directors: Alexis Johan Kearney

Erasmus Jacobus Viviers

Friedrich Emil Krugmann

Managing Director/CEO/MD/Office Manager: Marcel Le Roux

Postal Address: PO Box 2827, Bellville, 7535

Street Address: 53A Sacks Circle, Bellville 7535

Telephone Number: 021 9511211

Fax Number: n/a

Email: marcel@galvatech.co.za

3. THE ACT

3.1 The ACT grants a requester access to records of a private body, if the record is required for the exercise or protection of any rights. If a public body lodges a request, the public body must be acting in the public interest.

3.2 Requests in terms of the ACT shall be made in accordance with the prescribed procedures, at the rates provided. The forms and tariff are dealt with in paragraphs 6 and 7 of the Act.

3.3 Requesters are referred to the Guide in terms of Section 10 which has been compiled by the South African Human Rights Commission, which will contain information for the purposes of exercising Constitutional Rights. The Guide is available from the SAHRC.

The contact details of the Commission are:

Postal Address:	Private Bag 2700, Houghton, 2041
Telephone Number:	+27-11-877 3600
Fax Number:	+27-11-403 0625
Website:	www.sahrc.org.za

4. APPLICABLE LEGISLATION

No	Ref	Act
1	No 61 of 1973	Companies Act
2	No 98 of 1978	Copyright Act
3	No 55 of 1998	Employment Equity Act
4	No 95 of 1967	Income Tax Act
5	No 66 of 1995	Labour Relations Act
6	No 89 of 1991	Value Added Tax Act
7	No 13 of 2006	Older Persons Act
8	No 37 of 2002	Financial Advisory and Intermediary Services Act
9	No 75 of 1997	Basic Conditions of Employment Act
10	No 69 of 1984	Close Corporations Act
11	No 25 of 2002	Electronic Communications and Transactions Act

12	No 2 of 2000	Promotion of Access of Information Act
13	No 30 of 1996	Unemployment Insurance Act

5. Schedule of Records

Records	Subject	Availability
Public Affairs	• Public Product Information • Public Corporate Records • Media Releases	Freely available on web site http://www.galvatech.co.za
Financial	• Financial Statements • Financial and Tax Records (Company & Employees) • Asset Register • Management Accounts	Proprietary (Pty Ltd) - GALVATECH Request in terms of PAIA. Not available.

Marketing	• Market Information
	• Public Customer Information:
	  ○ Product Brochures
	  ○ Owner Manuals
	• Field Records
	• Performance Records
	• Product Sales Records
	• Marketing Strategies
	• Customer Database
	• Dealer Franchise Documents
		Limited Information available on web site. (see above)
		
		Request in terms of PAIA
		Request in terms of PAIA
		Request in terms of PAIA
		Request in terms of PAIA
		Request in terms of PAIA
		Request in terms of PAIA

6. FORM REQUEST

To facilitate the processing of your request, kindly:

6.1 Use the prescribed form, available on the website of the SOUTH AFRICAN HUMAN RIGHTS COMMISSION at www.sahrc.org.za. *(See attached)*

6.2 Address your request to the Marcel Le Roux (CEO/MD).

6.3 Provide sufficient details to enable the Company to identify:

(a) The record(s) requested;

(b) The requester (and if an agent is lodging the request, proof of capacity);

(c) The form of access required;

(d) (i) The postal address or fax number of the requester in the Republic;

(ii) If the requester wishes to be informed of the decision in any manner (in addition to written) the manner and particulars thereof;

(e) The right which the requester is seeking to exercise or protect with an explanation of the reason the record is required to exercise or protect the right.

7. PRESCRIBED FEES

The following applies to requests (other than personal requests):

7.1 A requestor is required to pay the prescribed fees (R50.00) before a request will be processed;

7.2 If the preparation of the record requested requires more than the prescribed hours (six), a deposit shall be paid (of not more than one third of the access fee which would be payable if the request were granted);

7.3 A requestor may lodge an application with a court against the tender/payment of the request fee and/or deposit;

7.4 Records may be withheld until the fees have been paid.

7.5 The fee structure is available on the website of the SOUTH AFRICAN HUMAN RIGHTS COMMISSION at www.sahrc.org.za.

SOUTH AFRICAN HUMAN RIGHTS DISCLAIMER

The South African Human Rights Commission reserves all rights and makes no warranty, either express or implied, with respect to the information and/or promotional material contained herein and is not responsible for any expenses, inconvenience, damage (whether special or consequential) or claims arising out of posting, time and costs incurred and or associated with this information and will not be liable for the latter. Specific exemption from any liability is claimed with regard to the following:

- *The SAHRC does not endorse any third party private service provider and will not bear any costs related to your transaction to compile the manual on your behalf.*
- *Submission to the SAHRC is free and the SAHRC does not charge any fees for advise or administration however all cost to lodge manuals is at the relevant private entities own cost e.g. registered mail etc.*
- *Manuals are subject to review and comment with the possibility of manuals being rejected on the basis of not meeting the minimum requirements and the SAHRC is not liable for the amendment costs if any and resubmission if any of any manuals.*