FIRST TECHNOLOGY INVESTMENTS (PTY) LTD AND ITS AFFILIATES

INTERNAL DATA PRIVACY AND SECURITY POLICY

In accordance with

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

Group Legal Department
Internal Data Privacy and Security Policy - Revision 5
Effective Date: June 2021

This document (including but not limited to any manuals, policies, procedures, forms, and other documents) ("Policy") applies to all Affiliates of First Technology Investments (Pty) Ltd ("Company"). Reference to Company in this Policy means each Affiliate as applicable.

"Affiliate(s)" means, in relation to First Technology Investments (Pty) Ltd, a subsidiary of this entity, or any division or operating branch of each subsidiary of this entity and all of its subsidiaries. Including but not limited to:

- BUI Medical and Technology Suppliers (Pty) Ltd
- BUI Security Services (Pty) Ltd
- CHM Vuwani Computer Solutions (Pty) Ltd
- CHM Vuwani Computer Solutions (KZN) (Pty) Ltd
- CHM Vuwani Computer Solutions (Eastern Cape) (Pty) Ltd
- Comptronics (Pty) Ltd
- First Horizon Technology (Pty) Ltd
- First Technology National (Pty) Ltd
- First Technology Western Cape (Pty) Ltd
- First Technology KwaZulu Natal (Pty) Ltd
- First Technology (Central) (Pty) Ltd
- First Technology (Pty) Ltd
- First Technology Digital (Pty) Ltd
- First Technology MPS (Pty) Ltd
- First Technology (Audio) (Pty) Ltd
- First Technology IT Suppliers (Pty) Ltd
- First Technology Security (Pty) Ltd
- First Retail (Pty) Ltd
- FirstNet Technology Services (Pty) Ltd
- EVAR Technology (Pty) Ltd
- Galdon Data Computer Services (Pty) Ltd
- Galdon Data Services (Pty) Ltd
- Marketplace Solutions (Pty) Ltd
- Phoenix Distribution (Pty) Ltd
- Pylot (Pty) Ltd
- The CRM Team (Pty) Ltd
- Techsonic (Pty) Ltd

This list is subject to amendment at the sole discretion of the First Technology Investments (Pty) Ltd and will include all Affiliates whether listed or not.

Contents

1. PURPOSE

1.1. This Policy defines the internal requirements necessary to ensure compliance with all laws and regulations applicable to the Company's collection, use, storage, and transmission of personal data and private information throughout its business.

1.2. The Company is committed to complying with the applicable data privacy and security requirements in the Republic of South Africa, and in particular the Protection of Personal Information Act 4 of 2013 ("POPI"). The Company has adopted an internal data privacy and security Policy which creates a common core of values, supplemented with alternative or additional policies or implementation procedures.

1.3. It is recorded that the Employee (as defined in clause 2.4), by virtue of his/her/its association with the Company, has and will continue to gather certain information about individuals, including but not limited to personal data and private information, as well as Personal Information of Data Subjects which the Company has a relationship with or who the Employee may come in contact with, during the course of his/her employment and/or association with the Company.

1.4. This Policy describes how Personal Information must be collected, processed, used, stored, and transmitted by the Employee to meet the Company's data protection standards. These standards have been adopted by the Company to build trust with its Data Subjects and to ensure its compliance with certain laws and regulations. This Policy forms an integral part of the Company's business.

1.5. This Policy ensures that the Company:

1.5.1. follows good practice guidelines;

1.5.2. complies with general accepted privacy principles and data protection legislation;

1.5.3. is open to Data Subjects about how it stores and processes their Personal Information;

1.5.4. takes reasonable measures to protect itself from the risk of a possible breach.

1.6. Additionally this Policy seeks to ensure that Company :

1.6.1. Complies with international legal standards and best practice for the receipt, importing, processing, handling and storing of Personal Information, whether received from its clients and suppliers, or as held in respect of its own Employees;

1.6.2. Protects itself, as far as reasonably possible, from the risks of a data breach;

1.6.3. Ensures that each Employee understands what is expected of the Employee when he/she processes, handles, stores or transfers Personal Information.

2. SCOPE OF POLICY

2.1. This Policy applies to the Company and to all Employees, as defined in this Policy. Personal Information shall only be processed fairly and lawfully in accordance with this Policy and POPI.

2.2. "Data Subjects" means any natural person or juristic entity, including, but not limited to:

2.2.1. Customers;

2.2.2. Potential Customers;

2.2.3. Suppliers;

2.2.4. Vendors

2.2.5. Business Contacts;

2.2.6. Business Partners;

2.3. "Personal Information" means all private and personal information as well as personal identifiable information, including but not limited to:

2.3.1. Names and surnames of Data Subjects;

2.3.2. Date of birth of Data Subjects;

2.3.3. Legal name and registration number;

2.3.4. Physical and/or postal addresses of Data Subjects;

2.3.5. Email addresses of Data Subjects;

2.3.6. Telephone numbers or other contact numbers of Data Subjects.

2.4. "Employee" means any person or entity who receives Personal Information from the Company and/or processes Personal Information on behalf of the Company and includes, but is not limited to:

2.4.1. Employees of the Company;

2.4.2. Independent contractors of the Company;

2.4.3. Subcontractors of the Company;

2.5. "Operator" means any person or entity who processes Personal Information for or on behalf of the Company in terms of a contract or mandate, but who is not under the authority or control of the Company.

3. COMPANY'S COMMITMENT TO THE EIGHT CONDITIONS OF LAWFUL PROCESSING UNDER POPI

APPLICATION

It is important that each and every Employee plays its part in ensuring that any unauthorised disclosure or access to Personal Information is prevented to the greatest extent possible, as any compliance failure could result in both financial and reputational damage to the Company. In the execution of their duties to the Company, Employees must always process Personal Information lawfully and in particular comply with the 8 conditions for lawful processing as set out in POPI and below.

3.1. **CONDITION 1 - ACCOUNTABILITY**

When collecting Personal Information, determining the purpose and means of processing Personal Information, and during the processing itself, each Employee is personally responsible for ensuring that they comply with the terms of this Policy and POPI. Employees will also be responsible for ensuring that when transferring Personal Information to a third party Operator, that they taken all necessary steps as outlined in this Policy prior to transferring Personal Information to a third party Operator. **in particular Employees must ensure that the third party Operator has signed an Operator Agreement with the Company, a copy of which can be obtained from the Employee's Line Manager or on request to the Group Legal Department**.

3.2. **CONDITION 2 - PROCESSING LIMITATION**

3.2.1. Lawful grounds

The processing of Personal Information is only lawful if the purpose for which it is processed is adequate, relevant and not excessive. **Employees may only process Personal Information if one of the following grounds of lawful processing exists**:

3.2.1.1. **The Data Subject consents to the processing;**

3.2.1.2. **Processing is necessary for the conclusion or performance of a contract with the Data Subject;**

3.2.1.3. Processing complies with a legal responsibility imposed on Company;

3.2.1.4. Processing protects a legitimate interest of the Data Subject;

3.2.1.5. Collection of Personal Information must be directly from the Data Subject unless it is contained in a public record;

3.2.1.6. Personal Information collection must be proportionate to purpose;

3.2.1.7. Processing is necessary for pursuance of a legitimate interest of Company, or a third party to whom the information is supplied;

3.2.2. 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. Employees must in general not collect or process Special Personal Information and where this is required it may only be done with the prior consent of their Line Manager and under the following circumstances:

3.2.2.1. The Data Subject has consented to such processing;

3.2.2.2. The Special Personal Information was deliberately made public by the Data Subject;

3.2.2.3. Processing is necessary for the establishment of a right or defence in law;

3.2.2.4. Processing is for historical, statistical, or research reasons;

3.2.2.5. If processing of race or ethnic origin is in order to comply with any applicable laws

3.2.3. 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 Personal Information. If the Data Subject withdraws consent or objects to processing, then the Employee must immediately refrain from processing the Personal Information.

3.2.4. Collection directly from the Data Subject

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

3.2.4.1. Personal Information is contained in a public record;

3.2.4.2. Personal Information has been deliberately made public by the Data Subject;

3.2.4.3. **Personal Information is collected from another source with the Data Subject's consent**;

3.2.4.4. Collection of Personal Information from another source would not prejudice the Data Subject;

3.2.4.5. Collection of Personal Information from another source is necessary to maintain, comply with or exercise any law or legal right;

3.2.4.6. Collection from the Data Subject would prejudice the lawful purpose of collection;

3.2.4.7. **Collection from the Data Subject is not reasonably practicable**.

3.3. CONDITION 3 - PURPOSE SPECIFICATION

Employees must only process Personal Information for the specific purpose for which it was given or in accordance with the Lawful Grounds stated above, and must not be retained for longer than is reasonably or legally required. This condition ensures that processing is carried out in the least intrusive manner considering the possible security risks.

3.4. CONDITION 4 - FURTHER PROCESSING

Any new processing activity must be compatible with original purpose of processing, failing which the Employee must obtain additional consent form the Data Subject for such processing. Further processing will be regarded as compatible with the purpose of collection if:

3.4.1 Data Subject has consented to the further processing;

3.4.2 Personal Information is contained in a public record;

3.4.3 Personal Information has been deliberately made public by the Data Subject;

3.4.4 Further processing is necessary to maintain, comply with or exercise any law or legal right;

3.4.5 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.

3.5. CONDITION 5 - INFORMATION QUALITY

3.5.1. Employees must take reasonable steps to ensure that all Personal Information it collects and/or processes is complete, accurate, not misleading and updated where necessary

3.5.2. Employees must periodically review Data Subject records to ensure that the Personal Information is still valid and correct.

3.5.3. **Employees should, as far as reasonably practicable, adhere to the following guidelines when collecting Personal Information**:

3.5.3.1. Personal Information should be dated when received;

3.5.3.2. A record should be kept of where the Personal Information was obtained;

3.5.3.3. Changes to information records should be dated;

3.5.3.4. Irrelevant or unneeded Personal Information should be permanently deleted or destroyed;

3.5.3.5. Personal Information should be stored securely, either on a secure electronic database or in a secure physical filing system.

3.6. CONDITION 6 - OPENNESS

3.6.1. The Company expects each Employee to take reasonable steps to ensure that the Data Subject is made aware of the following:

3.6.1.1. What Personal Information is being collected, and (where applicable) the source of the information;

3.6.1.2. The purpose of collection and processing;

3.6.1.3. Whether the supply of Personal Information is voluntary or mandatory, and the consequences of a failure to provide such information;

3.6.1.4. Whether the collection is required in terms of any law;

3.6.1.5. Whether the Personal Information shall be shared with any third party.

3.7. CONDITION 7 - DATA SUBJECT PARTICIPATION

3.7.1. The Data Subject is entitled to:

3.7.1.1. An explanation of the Personal Information currently held and the necessity and extent of such processing;

3.7.1.2. Request deletion or correction of the Personal Information.

3.7.2. All such requests must be submitted in writing to the Company and Employees must immediately discuss such requests with their Line Manager who will escalate the request where necessary. Employees must not disclose any Personal Information to any party unless the identity of the requester has been verified

3.8. CONDITION 8 - SECURITY SAFEGUARDS

3.8.1. Integrity and confidentiality

Employees shall treat all Personal Information as strictly confidential and shall follow all policies and procedures set out by the Company to ensure the integrity and confidentiality of all Personal Information in its possession.

3.8.2. Electronic Records

3.8.2.1. All electronically held Personal Information must be saved in a secure database;

3.8.2.2. As far as reasonably practicable, no Personal Information should be saved on the Employees computers, laptops or hand-held devices, or any removable media;

3.8.2.2.1. Where this is required it should only be for the shortest time strictly necessary, whereafter it should be transferred to the secure database and deleted from the Employees device.

3.8.2.3. All computers, laptops and hand-held devices should be access protected with a password, fingerprint or retina scan, with the password being of an acceptable complexity and changed frequently;

3.8.2.4. 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;

3.8.2.5. Electronic Personal Information which is no longer required must be permanently deleted from the individual laptop or computer and the relevant database.

3.8.2.6. Where Personal Information is stored on removable media such as a CD/DVD/USB devices, these must at all times be locked away securely when not in immediate use;

3.8.2.7. All servers containing Personal Information are located in secure protected locations away from general office space;

3.8.2.8. Personal Information will be backed up frequently in accordance with the Company's backup protocols and procedures. Such backups will be tested regularly under the direction of the IT Manager;

3.8.2.9. Personal Information will never be saved directly to laptops or other mobile or removable devices such as tablets or smart phones or sticks or data sticks;

3.8.2.10. All servers and computers containing Personal Information will be protected by approved security software, and one or more firewalls under the direction of the Company's IT Manager.

3.8.3. Written Records

3.8.3.1. Personal Information records should be kept in locked cabinets, or safes ideally in a secure place where an unauthorised person cannot access or see it);

3.8.3.2. When Personal Information records are in use, they should not be left unattended in areas where other employees or third parties may be able to access them. In particular Employees should ensure that paper and print outs are not left in places where unauthorised persons can see them, e.g. on/in the printer;

3.8.3.3. All Employees shall be required to clear their desks of all Personal Information when leaving their desks unattended for any length of time and at the end of the day;

3.8.3.4. Personal Information which is no longer required should be disposed of by means of physical shredding.

3.8.4. 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.

4. MANAGEMENT: KEY INDIVIDUALS AND DEPARTMENTS

4.1. In order to ensure and facilitate the effectiveness of the Company's efforts to secure and manage the Personal Information which it collects, the Company's Executive Management Team will coordinate the Company's data privacy and protection obligations, in conjunction with the Company's Internal IT Department and Company's Management Teams.

4.2. The designations and roles stated in Annexure "A" have been identified as being the individuals with key responsibilities in respect of the Company's data privacy and protection obligations. Should the Employee have any questions or uncertainties regarding data privacy or this Policy, the Employee shall approach the person that has been assigned as the Employee's Line Manager, or alternatively they may approach the Group Legal Department directly.

5. EMPLOYEE CONSENT

5.1. The Employee acknowledges that the Company has, and will continue to, collect and process the Employee's own Personal Information in accordance with POPI, this Policy and the Employee's employment agreement with the Company. The Employee expressly acknowledges and consents to the Company collecting, processing and transferring his/her Personal Information for general human resource purposes and/or as may be necessary for the effective operation of the Company's business, which will include, but not be limited to, providing the Employees Personal Information to current or prospective customers, including it as part of any tender submissions, or for general compliance purposes. The Employee further agrees to provide such additional Personal Information as may be reasonably required by the Company for the above purposes.

6. NOTICE, CHOICE AND CONSENT

6.1. Except as is strictly necessary for the Company to fulfil its contractual obligations to the Data Subject, Employees must not collect or process Personal Information of Data Subjects without the voluntary and express consent of the Data Subjects.

6.1.1. **When first engaging with a new Data Subject (e.g. a new customer) Employees must ensure that the Data Subject signs an express written consent in favour of the Company, a copy of the required consent can be obtained from the Employee's Line Manager or the Group Legal Department**

6.2. The Company's External Data Privacy and Security Policy sets out how the Company will process, secure, and transfer the Personal Information of new and existing Data Subjects.

6.3. The Employee shall provide all Data Subjects with adequate notice of the Company's External Data Privacy and Security Policy prior to the Employee processing any Personal Information of the relevant Data Subject. A copy of the Company's External Data Privacy and Security Policy may be obtained by the Employee on request to his/her Line Manager

7. COLLECTION AND USE OF PERSONAL INFORMATION

7.1. The Employee shall ensure, when collecting Personal Information, that he/she only collects such Personal Information as is reasonably necessary and required in order for the Company to fulfil its obligations towards, or enforce its rights against, the Data Subjects.

7.2. The Employee shall only obtain Personal Information that is relevant and adequate in relation to the purpose for which it is collected and shall only use the Personal Information that has been obtained for the purpose for which it is collected. The Employee shall not collect Personal Information that is outdated, excessive or irrelevant in relation to the purpose for which it is collected.

7.3. When the Employee collects Personal Information from Data Subjects, he/she shall ensure that he/she is prepared to discuss the applicable data collection, handling, use, and retention practices and policies of the Company with the Data Subjects.

8. RETENTION, SECURITY AND DISPOSAL OF PERSONAL INFORMATION

8.1. The following guidelines describe a high level overview on how and where Personal Information should be safely stored by the Employee. Further questions about storing data safely can be directed to the Company's Internal IT Department or the Company's Information Officer. Detailed requirements on IT security policies and procedures are set out in the Company's IT Security Policy.

8.2. The Employee shall ensure that Personal Information stored on paper:

8.2.1. is kept and stored in a secure place where unauthorised Employees and/or third parties cannot see the Personal Information or have access to such data;

8.2.2. is kept and stored in a locked drawer or filing cabinet to ensure that unauthorised Employees and/or third parties do not have access to such Personal Information;

8.2.3. is not left where unauthorised Employees and/or third parties can see the Personal Information;

8.2.4. is shredded and disposed of securely when no longer required by the Employee or the Company for business purposes.

8.2.5. Personal Information that is usually stored electronically, but has been printed out or written down, shall be deemed to be Personal Information stored on paper.

8.3. The Company's Internal IT Department and/or the Employee, where applicable, shall ensure that Personal Information stored electronically:

8.3.1. is protected from any unauthorised access, accidental deletion and malicious hacking attempts from unauthorised Employees and/or third parties;

8.3.2. is protected by strong passwords that are changed regularly, and shall not share passwords with unauthorised Employees and/or third parties;

8.3.3. is locked away securely when not in use if the Personal Information is stored on any removable storage devices or removable media;

8.3.4. is stored on designated drives and servers to which unauthorised Employees and/or third parties cannot access;

8.3.5. shall only upload Personal Information to a cloud computing server approved by the Company, where applicable;

8.3.6. is backed up frequently in accordance with backup protocols. Such backups will be tested regularly in line with the company's standard backup procedures and protocols under the direction of the IT Manager;

8.3.7. is not saved directly to any personal mobile devices, including tablets, smart phones and laptops;

8.3.8. is stored on the Company's computer or laptops that is protected by a security software and firewall approved by the Company, where applicable;

8.3.9. is disposed of securely when no longer required by the Employee or the Company for business purposes (through the Company's Internal IT Department, where applicable).

8.4. The Employee shall keep all Personal Information secure at all times by taking sensible precautions and following the guidelines of this Policy.

9. ACCESS TO PERSONAL INFORMATION AND THE TRANSMISSION THEREOF TO THIRD PARTIES, SUB-CONTRACTORS AND BUSINESS PARTNERS

9.1. Personal Information should only be accessed by Employees who need the Personal Information to fulfil their obligations with regards to First Technology and must be processed on a "need to know" basis. The Employee may not share Personal Information informally and may not disclose Personal Information to any unauthorised Employees and/or third parties.

9.2. When access to Personal Information is required by the Employee for business purposes, the Employee can request the Personal Information from the Employee's Line Manager, where applicable, or from a person nominated in Annexure A.

9.3. When a subcontractor, business partner or any other third party ("third party") requests access to Personal Information for business purposes, the third party's request must be referred to one of the Company's Line Managers or a person nominated in Annexure A.

9.4. The relevant Line Manager and/or Employee of the Company must ensure that a prior to the Company providing the third party with Personal Information that the third party Operator has signed an with the Company, a copy of which can be obtained from the Employee's Line Manager or the Group Legal Department

9.5. Personal Information shall only be transmitted to third parties for reasons consistent with the purpose for which it was originally collected. Before transmitting Personal Information to third parties, the Employee shall ensure that:

9.5.1. a written Operator Agreement is in place between the Company and the third party requesting access to the Personal Information;

9.5.2. the third party actually requires the information requested to perform its services;

9.5.3. Personal Information transmitted to third parties is protected against unauthorized access by use of encryption.

9.6. In certain circumstances, South African legislation will allow for Personal Information to be disclosed to law enforcement or other agencies without the consent of the Data Subject. In such circumstances, the Company may be obliged to disclose the requested Personal Information, and the Information Officer and Group Legal Department will first ensure that the request is legitimate. Only the Information Officer will be authorised to furnish the requested data to the enquiring party.

10. DATA SUBJECT'S REQUESTS TO ACCESS

10.1. All Data Subjects whose Personal Information is being held by the Company or the Employee are entitled to:

10.1.1. Enquire what Personal Information the Company holds regarding that Data Subject;

10.1.2. Enquire as to how that Data Subject can obtain access to such Personal Information;

10.1.3. Be informed on how to keep the Personal Information up to date;

10.1.4. Be informed on how the Company is meeting its data protection obligations.

10.2. The Data Subjects right to access information shall be subject to, and be handled in accordance with, the Company's PAIA Manual, a copy of which will be made available to the Employee on request and which is available on the Company's website.

10.3. The Group Legal Department will attend to all requests for access, in consultation with the Company's Information Officer. Any request for access by Data Subjects or any other related requests can be submitted in writing to the Company's Group Legal Department at legal@firsttech.co.za.

11. QUALITY AND ACCURACY OF DATA

11.1. The Employee shall take reasonable steps to ensure that Personal Information is kept accurate and updated on regular basis and as far as possible require that the Data Subject agrees to advise the Company if any updates or amendments are required.

11.2. The Employee must ensure that Personal Information is held or kept in as few places as possible and shall not create unnecessary additional sets thereof.

11.3. The Employee must update Personal Information records when he/she discovers inaccuracies in Personal Information. For example, updating outdated contact details of Data Subjects.

12. GENERAL RESPONSIBILITIES OF THE EMPLOYEE

12.1. The Employee acknowledges and accepts that he/she has a responsibility to ensure that Personal Information is collected, stored and handled appropriately in accordance with this Policy.

12.2. General guidelines for the Employee:

12.2.1. The Company will provide training to the Employee from time to time to assist the Employee in understanding his/her responsibilities when handling Personal Information. The Employee undertakes to participate in and complete the training offered by the Company at least once every 12 (twelve) months and whenever the Company requests the Employee to complete such training.

12.2.2. The Employee shall regularly review Personal Information in his/her possession and ensure that same is up to date. If the Employee or the Company no longer require the Personal Information for business purposes, then the Employee shall dispose of the Personal Information in accordance with this Policy and where necessary in consultation with his/her Line Manager.

12.2.3. The Employee can at all times approach his/her appointed Line Manager or any other Department nominated in annexure "A" should the Employee require clarity or guidance on any aspects regarding this Policy.

13. DISCIPLINARY CODE AND CONSEQUENCES

13.1. This Policy governs every Employee of Company, both during his/her services to Company, and to the extent applicable, after termination of services.

13.2. To the extent that this Policy sets out workplace rules governing the Employee in the course of his/her work and services to the Company, it shall form part of the Company's Disciplinary Code and Procedure and is hereby also incorporated into it. A breach of any rule in relation to the protection Personal Information set out in this Policy may subject the Employee to disciplinary action.

13.3. The imposition of any disciplinary sanction or dismissal shall not preclude the Company from instituting civil proceedings against an Employee who acted in breach of this Policy where such breach has resulted in liability, loss, reputational damage and/or other damages to the company in the course of pursuing its commercial operations.

13.4. It shall be incumbent upon every Employee to familiarise him/herself with the content of this Policy, and to remain up to date as to any changes to it issued in written form as part hereof by the Company.

Annexure "A"

Position	**Department / Individual**
Group Policy Coordinator	Group Legal Department
Responsible for IT Security	Company's IT Manager
Information Officer	Company's Managing Director or General Manager, or such other person as appointed by the CEO.
Deputy Information Officer(s)	As appointed by the Information Officer