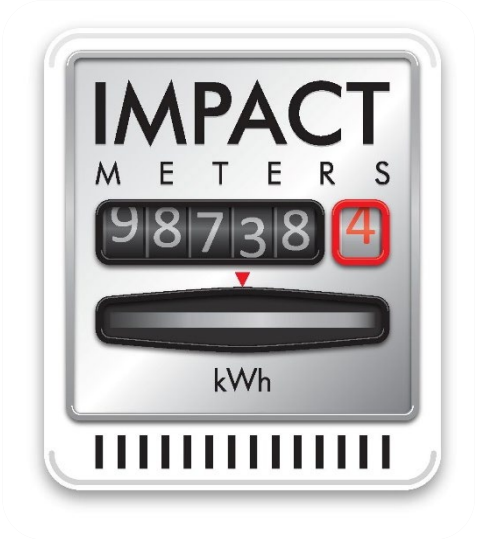
PRIVACY POLICIES AND MANUAL OF IMPACT METER SERVICES



CONTENTS

DEFINITIONS:

The definitions have been taken from the Promotion of Access to Personal Information Act 2 of 2000 as amended (PAIA) and the Protection of Personal Information Act 4 of 2013 (POPIA):

1.1. **"The Company"** means IMPACT METER SERVICES.

1.2. **"Data subject"** means the person to whom personal information relates.

1.3. **"Consent"** means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information.

1.4. **"Information officer"** means the head of a private body as contemplated in section 1 of POPIA.

1.5. **"Personal information"** - means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

1.5.1. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person.

1.5.2. information relating to the education or the medical, financial, criminal or employment history of the person.

1.5.3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other assignment to the person.

1.5.4. the biometric information of the person.

1.5.5. the personal opinions, views, or preferences of the person.

1.5.6. 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.

1.5.7. the personal views opinions, views, or preferences of the person; and

1.5.8. correspondence sent by the person that is implicitly or explicitly or a private or confidential nature or further correspondence that would reveal the contents of the original correspondence.

1.5.9. the views or opinions of another individual about the person; and

1.5.10. 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.

1.6. **"Processing"** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—

1.6.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use.

1.6.2. dissemination by means of transmission, distribution or making available in any other form; or

1.6.3. merging, linking, as well as restriction, degradation, erasure or destruction of information."

1.7. **"record"** means any recorded information—

1.7.1. regardless of form or medium, including any of the following:

1.7.1.1. Writing on any material;

1.7.1.2. 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;

1.7.1.3. label, marking or other writing that identifies or describes anything of which it forms part, or towhich it is attached by any means;

1.7.1.4. book, map, plan, graph or drawing;

1.7.1.5. 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;

1.7.2. in the possession or under the control of a responsible party;

1.7.3. whether or not it was created by a responsible party; and

1.7.4. regardless of when it came into existence.

1.8. **"Responsible party"** means a private body or any other person which, alone or in conjunction

with others, determines the purpose of and means for processing personal information;

1.9. **"requestor",** in relation to –

1.9.1. A public body, means:

1.9.1.1. Any person (other than a public body contemplated in paragraph (a) or (b)(i) of the definition of 'public body', or an official thereof) making a request for access to a record of that public body; or

1.9.1.2. A person acting on behalf of the person referred to in subparagraph (i).

1.9.2. A private body, means:

1.9.2.1. Any person, including, but not limited to, a public body or an official thereof, making a request for access to a record of that private body, or

1.9.2.2. A person acting on behalf of the person contemplated in subparagraph above.

SCOPE AND APPLICATION:

1.10. The purpose of this manual is to ensure that the data subject's right to privacy, respect, confidentiality, and autonomy is respected and attained.

1.11. The manual applies to the collection, storage, access, use and disclosure of the data subject's personal information in accordance with the following legislation and guidelines:

1.11.1. South African Constitution 1996.

1.11.2. Protection of Personal Information, Act No. 4 of 2013.

1.11.3. Basic conditions of employment Act, No. 75 of 1997.

1.11.4. Labour relations Act, No. 66 of 1995.

1.11.5. The unemployment Insurance Contributions Act, No. 4 of 2002.

1.11.6. Income Tax Act, No. 113 of 1993.

1.11.7. Skills Development Act, No. 97 of 1998.

1.11.8. City of Tshwane Metropolitan Municipality Standard Electricity Supply By-Laws.

1.11.9. Electricity Regulation Act, No. 4 of 2006.

INFORMATION OFFICER:

1.12. The details of the information officer for purposes of gathering information, updating information and withdrawal of consent by the data subject is:

Person:	George Farmer
Email address:	complianceofficer@amps.co.za
Contact Number:	012 763 8200

PROCESS LIMITATION

1.13. Only the necessary personal information as held in paragraph 6 hereunder of the data subject will be gathered and will only be used for the purpose for which it is processed as held in paragraph 7 below.

1.14. All information gathered by the Company will be gathered by a duly authorised representative of such Company.

1.15. The following methods will be used to collect the necessary personal information:

- When the data subject contacts the Company through the website;
- When the data subject contacts the Company by e-mail;
- When the data subject contacts the Company through social media.
- When the Company enters into a contract for services with the data subject.
- Where the data subject otherwise engages with the Company.

JUSTIFICATION

1.16. The Company will only process information under one of the following conditions:

- With the consent of the data subject;
- Where the processing is necessary for the performance or conclusion of a contract between the Company and the data subject.
- Such processing is placed on the Company by law;

- The processing protects the legitimate interest of the Company to whom the information is supplied.

INFORMATION CLASSIFICATION:

1.17. The personal information collected by the Company may include the following:

1.18. In respect of employees of the Company:

- Names, surname, marital status, next of kin, race, gender, home language.
- Driver's licenses.
- Identity or Passport Number and copies thereof.
- Banking details.
- Pension fund / Provident fund details.
- Tax details which include PAYE number, UIF contributions, Skills levies etc.
- Curriculum Vitae and accompanying details.
- Record of Employer property issued to employee.
- Training scheduling and record keeping.
- Leave.
- Video footage when recording attendance at premises.
- Video footage inside the office aimed at ensuring the security of the Company's servers.

1.19. In respect of the Company's clients:

1.20. Names, contact details, registration numbers and company registration documents.

1.21. Proof of identification.

1.22. Bank Account details.

1.23. Meter readings and other data relating to the services offered by the Company.

1.24. Telephone recordings when engaging with the Company.

1.25. Video footage inside the office aimed at ensuring the security of the Company's servers.

PURPOSE OF GATHERING:

1.26. The purpose of gathering of the information is to render client's utility services, employment for employees or as required by law.

RETENTION AND DESTRUCTION:

1.27. All personal information will be recorded on the following format:

- Electronically.
- Paper format.

1.28. The personal information will be retained on servers located on the Company's premises and are secured in line with the measures indicated in the Security Safeguards detailed below.

1.29. All personal information of data subjects is stored in line with applicable legislation only that which is necessary for achieving the purpose for which the information was gathered.

1.30. Personal information of active employees will be retained for the duration of the employee's active service and for as long as obliged by law.

1.31. Client records will be kept for 3 years after the termination of services, alternatively after the termination of all engagement with the client.

1.32. We will remove all personal information from our records once the information is no longer necessary to retain and destroy it in such a manner that it is incapable of being reconstructed.

DISCLOSURE:

1.33. Where it is applicable, an authorised person of the Company will, disclose personal information of the data subject to the following categories of persons:

- The Body Corporate(s) where the data subject resides in estates and complexes.
- Operators who process information on behalf of the Company.
- Legal Representatives when enforcing terms and conditions of service agreements, or defending actions or applications instituted against the Company.
- Any authority requiring the information by law.

1.34. The Company ensures that the persons who to whom information is disclosed to is subject to strict agreements to keep information confidential and compliant with the Act.

FURTHER PROCESSING LIMITATION:

1.35. Should the Company intend to use any personal information of the data subject for a purpose other than rendering utility services to the data subject, consent for such use will first be obtained from the data subject.

INFORMATION QUALITY:

1.36. The Company will take reasonable steps, subject to the data subject providing the Company with the correct information, to ensure that the information held is complete, accurate, not misleading and updated where necessary.

1.37. Should a data subject wish to update their information, the requestor is to address such information to the Company who will then affect such an update.

DATA SUBJECT'S RIGHTS:

1.38. The data subject has the right to:

- Request access to his, her or its personal information held by the Company.
- Request the correction, destruction, or deletion of his or her or its personal information where necessary.
- To object, on reasonable grounds relating to his/her or its situation to the processing of personal information by the Company.
- To submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of the employee/employer.
- To institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information.

1.39. A data subject may enquire from the Company whether the Company holds any of his, her or its personal information. Such a request will not be withheld and will not be charged for.

1.40. The Company will however charge a fee to the requestor should the requestor require the full nature and details of the personal information held by the Company.

1.41. The Company holds the right to deny a request to access for information subject to the Promotion of Access to Information Act, No. 2 of 2002 and or any other relevant legislation which will be advised to the requester upon denial.

1.42. **Procedure**:

1.42.1. Should the requestor wish to submit a request to correct, destroy or delete his/her or its personal information held by the Company, the requestor is to complete the form attached hereto as Annexure "A" and submit same to the Information Officer whose details reflect in paragraph 3, who will then respond to the request in the appropriate manner and provide the requestor with the steps to be taken.

1.42.2. Similarly, should the requestor wish to object to the processing of information by the Company, then the requestor is to complete the form marked as Annexure "B" and submit the completed form to the relevant information officer whose details reflect in paragraph 3, who will then respond in the appropriate manner and provide the requestor with the steps taken.

1.42.3. Should the data subject request the Company to destroy or delete his/her/its personal information and the data subject is a party to a provision of services agreement with the Company, the consequences of such request will be that the agreement will be cancelled and the Company will no longer be able to provide such services to the data subject.

1.42.4. Should the data subject wish to access information held by the Company, the requestor is to complete the prescribed form, in accordance with the Company's PAIA Manual available on the website, and submit same to the information officer whose details reflect in paragraph 3, who will then respond in the appropriate manner.

1.42.5. Access to information will be subject to the following Acts:

- Protection of Personal information Act, No 4 of 2013
- Promotion of access to Information Act, No. 2 of 2000

1.42.6. Should the data subject wish to lodge a complaint to the regulator the data subject can contact the Regulator at the following contact details:

Name: Information Regulator South Africa

Address: JD House, 27 Stiemens Street,
Braamfontein,
Johannesburg,
2001

Postal Address: P.O. Box 31533
Braamfontein

Johannesburg

Telephone No: 010 023 5207

Email Address: inforeg@justice.gov.za

RESTRICTION

1.43. The Company will restrict the processing of a data subject's personal information under the following conditions:

- When a data subject contests to the accuracy of the information, the Company will restrict the information for a reasonable time period to enable the data subject to verify the accuracy of the information.
- The personal information is no longer necessary for the Company to achieve the purpose for which it was collected but is required to be retained for purposes of proof.
- Should the information become unlawful, and the data subject requests the restriction thereof as opposed to the destruction thereof.
- The data subject requests to transmit the personal information to another automated processing system.

SECURITY SAFEGUARDS:

1.44. **Physical Security**

The Company houses the servers onsite.

1.45. **Surveillance**

The Company uses internal and external surveillance cameras and perimeter cameras, strategically placed and monitored around the clock to ensure that all servers remain off-limits to anyone without security clearance. High-voltage security fences and a 24/7 security presence helps to deter any opportunistic crimes.

1.46. **Access control**

Clients, employees, and any other third parties have varying levels of authorized access to different areas of our facility, controlled by high-tech biometric scanning system devices and pin-coded keypads.

1.47. **Network Security**

1.47.1. Network-level security consists of a Fortinet firewall that rules the network edge and core.

1.47.2. Firewall rules on the data center network edge and at the core are used to protect the network in several ways:

- Rate-limiting of specific protocols to protect the network infrastructure.
- Blocking of particular protocols and destination IP addresses to safeguard Impact Meter Services' operational systems.
- Restricting access to particular hosts and protocols to defined lists of source addresses.
- Blocking of abusive IP addresses and hosts.

1.48. **Monitoring**

All servers managed by the Company are monitored 24/7 for all critical services and hardware health. The Company's reactive system administrators react to monitoring alerts as they are identified and escalate issues to data centre staff or platform engineers.

PLATFORM SECURITY

1.49. **Servers**

All servers used to provide the Company managed hosting service, both for shared web hosting and dedicated managed servers, are physical servers exclusively provisioned and managed by Impact Meter Services.

1.50. **Security response policy**

The Company is committed to updating all software to the latest stable versions within seven days of their release and 24 hours for critical software updates.

1.51. **Remote access**

Access to managed servers is limited by means of FortiClient firewall software. All managed servers make use of the same incoming firewall rules, and we do not allow any deviation from the standard rulesets

1.52. **Backups**

- All of the Company's Managed Servers are automatically backed up on a regular basis. The backup includes all critical data required for disaster recovery.
- Logs (FTP, web server, and mail logs) are generally kept for a certain period.

1.53. **Software Development**

- Stack: The Company strongly focuses on open-source technologies and mainly uses C# and .net as the Company's backend languages. The Company's frontend stack consists of HTML/HTML5, and various JavaScript frameworks. We use varying database technologies, including MySQL, ESS, and a bespoke CRM.
- Coding Practices: We follow an Agile development methodology and use best practices and industry-standard secure coding guidelines to ensure security is always top of mind.

1.54. **Anti-Virus**

All servers (which are Microsoft-based) run Bitdefender anti-virus, which is updated as new virus definitions are released. Servers are scanned daily.

1.55. **User Passwords**

All client's passwords are stored in a one-way encrypted format. Impact Meter Services is not able to retrieve any passwords. Due to the broad technology implementation across our hosting software and platforms

1.56. **Mail Security**

1.56.1. SSL is used for POP, IMAP, and SMTP protocols for email, resulting in data encryption between our server and clients" mail programs.

1.56.2. The use of strong passwords is enforced when creating or editing mailboxes via the mail admin tool.

1.56.3. The following measures are used to mitigate spam and malware:

- Anti-virus and anti-spam scanning occur on all inbound and outbound emails.
- Common malicious file extensions are blocked for both inbound and outbound emails.
- Our firewall blocks known malicious IP addresses for incoming emails.

1.57. **Payment Data Security**

Banking details used for debit order instructions are secured by various authentication measures and system firewalls.

1.58. **Trust and Safety team**

Our dedicated team of IT consultants monitor the hosting platform for any form of abuse such as compromised websites and mailboxes, network abuse, and phishing attacks and take swift remedial steps. They also contribute towards adapting our systems to current trends in spam to ensure that our spam filtering service is adequate.

SECURITY BREACH:

1.59. Should any personal information of the data subject be accessed by unauthorised persons, the Company will immediately alert the data subject together with the Information Regulator in writing thereof.

1.60. The Company takes full responsibility of any security breaches as a result of a breach occurring from the Company's side and holds all other parties with whom it has contracted with free of liability should the breach occur on the Company's side.

1.61. **Process**

1.62. The data subject and the Information Regulator shall be notified in either of the following ways:

- Post.
- E-mail to the last known e-mail address.
- On the website of the Company, displayed in a prominent manner.
- Published in the news media.
- As may be directed by the Regulator.

1.63. The notification will include the following information:

- The possible consequences of the compromise.
- The measures that the Company intends on taking to address the compromise.
- A recommendation of the measures to be taken by the employee/employer to mitigate possible prejudice caused by the compromise.
- If the identity of the person who compromised the security is known by the Company, then such identity will be disclosed.

ANNEXURE A

REQUEST TO CORRECT, DESTROY OR DELETE PERSONAL INFORMATION

Note:

1. Affidavits or other documentary evidence as applicable in support of the request may be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
3. Complete as is applicable.

Mark the appropriate box with an "x".

Request for:

☐ Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

DETAILS OF REQUESTOR	
Name(s) and surname:	
Identity Number:	
Residential, postal or business address:	
Contact Number(s):	
E-mail address:	
Fax Number:	

DETAILS OF RESPONSIBLE PARTY	
Name and Surname:	
Identity Number:	
Residential, postal or business address:	
Contact Number(s):	
Fax Number:	
E-mail address:	

INFORMATION TO BE CORRECTED/DELETED/DESTROYED/DESTRUCTED

REASONS FOR CORRECTION OR DELETION OF THE DATA SUBJECT'S PERSONAL INFORMATION IN TERMS OF SECTION 24(1)(A) WHICH IS IN THE POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PERSON; AND OR REASONS FOR DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(B) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN (PLEASE PROVIDE DETAILED REASONS FOR THE REQUEST)

_____

Signature

_____

Date of Signature

ANNEXURE B

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION

Note:

1. Affidavits or other documentary evidence as applicable in support of the objection may be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
3. Complete as is applicable.

DETAILS OF REQUESTOR	
Name(s) and surname:	
Identity Number:	
Residential, postal or business address:	
Contact Number(s):	
E-mail address:	
Fax Number:	

DETAILS OF RESPONSIBLE PARTY	
Name and Surname:	
Identity Number:	
Residential, postal or business address:	
Contact Number(s):	
Fax Number:	
E-mail address:	

REASONS FOR OBJECTION IN TERMS OF SECTION11(1)(d) **(Please provide detailed reasons for the objection)**

_____

Signature

_____

Date of Signature

REFERENCES

Genetic Counsellors South Africa. (2013, May). Standards of Practice for Genetic Counsellors. *Standards of Practice for Genetic Counsellors*. HPCSA.

HPCSA. (2016, September). *Uploads: Professional Practice: Conduct.* Retrieved from HPCSA: https://www.hpcsa.co.za/Uploads/Professional_Practice/Conduct%20%26%20Ethics/Booklet%205%20Confidentiality%20Protecting%20and%20Providing%20Information%20September%202016.pdf

Promotion of Acess to Information Act 2 of 2002, South Africa. (n.d.). Promotion of Access to Information Act 2 of 2002.

South Africa, Protection of Personal Information Act. (No. 4 of 2013, No. 4). Protection of Personal Information Act. *Protection of Personal Information Act*.

South African Human Rights Commission. (2014). *Sahrc.* Retrieved from Sahrc/21/files: https://www.gov.za/sites/default/files/gcis_documents/SAHRC-PAIA-guide2014.pdf