ENLITEN ELECTRIC (PTY) LTD:
DATA BREACH POLICY

TABLE OF CONTENTS

1. INTRODUCTION AND PURPOSE OF THIS POLICY 2
2. DEFINITIONS 2
3. RESPONSIBILITY 3
4. SECURITY AND DATA-RELATED POLICIES 5
5. DATA BREACH PROCEDURE 5
6. WHEN TO REPORT A DATA BREACH 6
7. REPORTING A DATA BREACH 7
8. MANAGING AND RECORDING THE BREACH 7
9. NOTIFYING THE INFORMATION OFFICER 8
10. NOTIFYING DATA SUBJECTS 8
11. ASSESSMENT OF THE BREACH 10
12. PREVENTING FUTURE BREACHES 11
13. REPORTING DATA PROTECTION CONCERNS 12
14. MONITORING 12

1. INTRODUCTION AND PURPOSE OF THIS POLICY

1.1. The *Protection of Personal Information Act* 4 of 2013 ("**POPIA**" / "**the Act**") aims to protect the rights of Data Subjects about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure, processing or destruction of personal data.

1.2. POPIA places an obligation on staff to report actual or suspected data breaches and ourprocedure for dealing with breaches is set out below.

1.3. All members of staff are requiredto familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

1.4. All employees will be provided with a copy of this policy and will be required to notify Enliten of any data breach without undue delay after becoming aware of the data breach.

1.5. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action being taken against employees in terms of the Disciplinary Code of Enliten, which disciplinary action may include dismissal.

2. DEFINITIONS

2.1. **Personal Data** means any information relating to a Data Subject where the said subject can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data, but excludes anonymous data, or data of which the identity of a Data Subject has been permanently removed. Personal data may be factual (for examples a name, email address, location or date of birth) or an opinion

about that person's actions or behaviour. Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the Data Subjector criteria relating to that Data Subject.

2.2. **SAPS** means the South African Police Service.

2.3. **Sensitive Data** means Personal Data concerning the racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions of a Data Subject.

2.4. **Personal Data Breach** means a breach of security leading to the accidental and / or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data stored or otherwise processed.

2.5. **Data Subject** means the person to whom the personal data relates.

2.6. **Deputy Information Officer** means the individual employee to who the responsibilities of the IO is delegated in terms of the Act.

2.7. **Information Officer** means the person appointed by Enliten as contemplated in Section 1 and 7 of the Act.

2.8. **The Regulator** means the Information Regulator established in terms of Section 39 of the Act.

3. RESPONSIBILITY

3.1. The Managing Director of Enliten, shall be responsible for breach notifications within Enliten and shall delegate certain responsibilities to the Information Officer ("**IO**") in accordance with the Act.

3.2. In the absence of the IO, data breaches shall be reported to the Head of Information Technology.

3.3. The above individuals shall be responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

3.4. The IO will be responsible for overseeing this policy and developing data-related policies and guidelines.

3.5. Staff should address questions about the operation and / or enforcement of this policy or POPIA to the IO and / or the DIO.

3.6. The Details of the IO / DIO are:

Information Officer:	Joalane Tladi
Address:	58 Frere Street Kensington B, Ransburg, 2194 P.O. Box 4179 Dainfern, 2055
Email:	joalane@enliten.co.za
Telephone:	011 326 3013
Deputy Information Officer (if applicable)	Angela Holtshausen
Address:	58 Frere Street Kensington B, Ransburg, 2194 P.O. Box 4179 Dainfern, 2055
Email:	angela.holtshausen@enliten.co.za
Telephone:	011 326 3013

4. SECURITY AND DATA-RELATED POLICIES

4.1. Staff should refer to the following policies that are related to this data protection policy:

4.1.1. **Privacy Policy:** which sets out the obligations of Enliten under POPIA regarding the processing of personal data.

4.1.2. **ICT Policy:** which sets out how staff are to use company desktops, laptops, and other information communication technology within Enliten.

5. DATA BREACH PROCEDURE

5.1. A personal data breach is a breach of security leading to the accidental and / or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

5.2. A data breach may include the following:

5.2.1. Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);

5.2.2. Inappropriate access controls allowing unauthorised use;

5.2.3. Equipment failure;

5.2.4. Human error (for example sending an email or SMS to the wrong recipient);

5.2.5. Unforeseen circumstances such as a fire or flood;

5.2.6. Hacking, phishing, and other “blagging” attacks where information is obtained by deceiving whoever holds it.

6. WHEN TO REPORT A DATA BREACH

6.1. The IO must be informed of a data breach (“**the breach**”) where such a breach is likely to result in a risk tothe rights and freedoms of Data Subjects.

6.2. The breach needs to be more than the loss of personal data and must result in significant detrimental effects if it remains unresolved and is not addressed.

6.3. A breach which may have a significant effect includes: -

6.3.1.1. Potential or actual discrimination;

6.3.1.2. Potential or actual financial loss;

6.3.1.3. Potential or actual loss of confidentiality;

6.3.1.4. Risk to physical safety or reputation;

6.3.1.5. Exposure to identity theft (for example through the release of non-public identifiers, such as passport numbers);

6.3.1.6. The exposure of the private aspect of a person’s life becoming known by others.

6.4. If the breach is likely to result in a high risk to the rights and freedoms of Data Subjects,then the affected Data Subjects must also be notified directly of the breach.

7. REPORTING A DATA BREACH

7.1. If a personal data breach is suspect, and such breach meets the criteria set out above in paragraph 6, employees should: -

7.1.1. Complete a data breach report form (which can be obtained from the IO); and

7.1.2. Email the completed form to the IO.

7.2. Where appropriate, employees are expected to liaise with their line manager about completion of the data report form. Breach reporting is encouraged throughout Enliten and employees are expected to seek advice if they are unsure whether a breach should be reportedand/or could result in a risk to the rights and freedom of Data Subjects.

7.3. Upon receipt of the data breach report form, the IO shall be required to acknowledge receipt thereof within 24 hours and shall takeappropriate steps to deal with the report in collaboration with the Head of IT.

7.4. Once a breach has been reported in accordance with this Policy, employees should not take any further action in this regard. In particular employees may not notify Data Subjects or regulators of any suspected and / or actual breaches and / or investigate the breach further.

8. MANAGING AND RECORDING THE BREACH

8.1. The IO shall immediately take all reasonable steps to establish whether a personal data breach has in fact occurred.

8.2. If a personal data breach has occurred, the following steps shall be taken:

8.2.1. Where possible, contain the data breach;

8.2.2. As far as possible, recover, rectify or delete the data which has been lost, damaged and / or disclosed;

8.2.3. Assess and record the breach in the data breach register of Enliten;

8.2.4. Notify the Information Officer of the breach;

8.2.5. Notify Data Subjects affected by the breach;

8.2.6. Notify other appropriate parties to the breach; and

8.2.7. Take all reasonable steps to prevent future breaches.

9. NOTIFYING THE INFORMATION OFFICER

9.1. If a breach is reported to the IO, he / she will notify the CEO within 48 hours of becoming aware of the breach.

9.2. If the IO is unsure of whether to report a breach, he / she will be to report it in accordance with the guidelines set out in this Policy.

9.3. Where the notification is not made within 48 hours of becoming aware of the breach, written reasons must be furnished to the IO in order to explain why the breach was not reported in accordance with the terms of this Policy.

10. NOTIFYING DATA SUBJECTS

10.1. Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the IO and / or DIO will notify the affected Data Subjects without undue delay including the likely consequences of the data breach and the measures Enliten has implemented, alternatively

intends to implement to address the breach.

10.2. The notification referred to in paragraph 10.1 above must provide sufficient information to allow the Data Subjects to take protective measures against the potential consequences of the breach, including-

10.2.1. Description of the possible consequences of the breach;

10.2.2. A description of the measures that Enliten intends to take or has taken to address the security compromise;

10.2.3. A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the breach; and

10.2.4. If known to the Enliten, the identity of the unauthorised person who may have accessed or acquired the personal information.

10.3. When determining whether it is necessary to notify Data Subjects directly of the breach, the IO will seek guidance from the head of IT, and any other relevant authorities (such as the legal counsel of Enliten and / or the SAPS).

10.4. The notification to a data subject referred to in subsection must be in writing and communicated to the Data Subjects in at least one of the following ways:

10.4.1. Mailed to the data subject's last known physical or postal address; and / or

10.4.2. Sent by e-mail to the data subject's last known e-mail address.

10.5. If the direct notification of the Data Subjects would involve

disproportionate effort (for example, by not having contact details of the said Data Subjects), then Enliten must consider alternative means to make those Data Subjects affected aware of the breach and the consequences thereof (for example by making a statement on the website of Enliten and / or making a media statement).

10.6. Enliten may only delay notification of the Data Subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

10.7. In the event that the IO and / or the DIO is unsure on whether and / or how to report on the breach, guidance should be sought from the Regulator.

11. ASSESSMENT OF THE BREACH

11.1. Once initial reporting procedures set out above have been carried out, Enliten will carry out all necessary investigations into the breach.

11.2. Enliten will identify how the breach occurred and take immediate steps to stop or minimise further loss and / or breach, destruction, or unauthorised disclosure of personal data. Enliten will further identify ways to recover correct or delete data (for example notifying insurers and / or the SAPS if the breach involves stolen hardware and / or data).

11.3. Once the breach has been contained, Enliten will conduct associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: -

11.3.1. What type of data is involved and how sensitive it is;

11.3.2. The volume of data affected;

11.3.3. Who is affected by the breach (i.e. the categories and number of peopleinvolved);

11.3.4. The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;

11.3.5. Are there any protections in place to secure the data (for example, encryption,password protection, pseudonymisation);

11.3.6. What has happened to the data;

11.3.7. What could the data tell a third party about the data subject;

11.3.8. What are the likely consequences of the personal data breach on Enliten; and

11.3.9. Any other wider consequences which may be applicable.

12. PREVENTING FUTURE BREACHES

12.1. Once the data breach has been dealt with, Enliten will review its security processeswith the aim of preventing further breaches. In order to do this, we will: -

12.1.1. Establish what security measures were in place when the breach occurred;

12.1.2. Assess whether technical or organisational measures can be implemented toprevent the breach happening again;

12.1.3. Consider whether there is adequate staff awareness of security issues and look tofill any gaps through training or tailored advice;

12.1.4. Consider whether it is necessary to conduct a privacy or data protection impactassessment;

12.1.5. Consider whether further audits or data protection steps need to be taken;

12.1.6. To update the data breach register; and

12.1.7. To debrief management following the investigation.

13. REPORTING DATA PROTECTION CONCERNS

13.1. Enliten strives to prevent the breach of data. As concerns regarding data security may arise at any time, employees are encouraged to report any concerns (even if they do not meet the criteria of a data breach) to the DIO as early detection of risks will protect Enliten from data breaches and ensure that data security processes remain current and effective.

14. MONITORING

14.1. Enliten will continuously monitor the effectiveness of this Policy and internal procedures and review and update the Policy as required from time to time.

14.2. Monitoring and review of this Policy will include but not be limited to the review and analysis of the practicability and functioning of the policies and procedures in reducing the risks posed to Enliten.