CSERT POPI Policy

Community Security Emergency Response Team

WWW.CSERT.ORG.ZA
Non-Profit Organisation Registration Number: 240-877

1. INTRODUCTION

CSERT (Community Security Emergency Response Team), a non-profit organisation with registration number 240-877, is committed to compliance with, and adheres to, the Protection of Personal Information Act, Act No. 4 of 2013 (POPIA).

The POPI Act requires CSERT to:

- Sufficiently inform all CSERT subscribed community residents or CSERT members/volunteers (data subjects), on the purpose for which the organisation will process their personal information;
- Protect CSERT information assets from threats, whether internal or external, deliberate or accidental, to ensure business continuation, minimise business damage and maximise business opportunities.

This policy establishes measures and standards for the protection and lawful processing of personal information within our organisation and provides principles regarding the right of individuals to privacy and to reasonable safeguarding of their personal information.

The CSERT Management Committee (CSERT ManCo) is responsible for:

- Conducting a preliminary assessment;
- The development, implementation, and monitoring of this policy;
- Ensuring that this policy is supported by appropriate documentation;
- Ensuring that documentation is relevant and kept up to date;
- Ensuring this policy and subsequent updates are communicated to relevant CSERT members and volunteers, where applicable.

All members, volunteers and individuals directly associated with CSERT activities and business are responsible for adhering to this policy and for reporting any security breaches or incidents to the CSERT Management Committee (CSERT ManCo).

Any service provider that provides information technology services, including data storage facilities, to our organisation is to adhere to the requirements of the POPI Act, to ensure adequate protection of personal information held by them on our behalf.

2. Policy Principles

2.1.1. Principle 1: Accountability

CSERT must take reasonable steps to ensure that the personal information obtained from CSERT members/volunteers and community residents is stored safely and securely. This includes any personal information that may be obtained for the purpose of identifying and registering residents on social media platforms.

2.1.2. Principle 2: Processing Limitation

CSERT may be required to collect personal information directly from CSERT members/volunteers and community residents. Once in CSERT possession, CSERT will only process or release personal information in the case of an emergency or with their consent, except where CSERT is required to do so by law. In the latter case CSERT will always inform the data subjects.

2.1.3. Principle 3: Specific Purpose

CSERT collects personal information from CSERT members/volunteers and community residents to enable CSERT to:

- Provide support services such as police, security and medical to community residents in the case of an emergency;
- Vet and endorse community residents, for security reasons, to be included in the CSERT social media platforms;
- Conduct normal CSERT activities and business for CSERT members/volunteers.

2.1.4. Principle 4: Limitation on Further Processing

Personal information may not be processed further in a way that is incompatible with the purpose for which the information was collected initially.

2.1.5. Principle 5: Information Quality

CSERT is responsible for ensuring that members/volunteers and community residents' information is complete, up to date and accurate before we use it. This means that it may be necessary to request members/volunteers and community residents, from time to time, to update their information and confirm that it is still relevant. If CSERT are unable to reach members/volunteers and community residents for this purpose, their information will be deleted from CSERT records.

2.1.6. Principle 6: Transparency/Openness

Where personal information is collected from a source other than directly from members/volunteers and community residents and according to legal requirements, CSERT is responsible for ensuring that the members/volunteers and community residents are aware:

- That their information is being collected;
- Who is collecting their information;
- Of the specific reason that other sources are collecting their information.

2.1.7. Principle 7: Security Safeguards

CSERT will ensure technical and organisational measures to secure the integrity of personal information, and guard against the risk of loss, damage, or destruction thereof. Personal information will also be protected against any unauthorised or unlawful access or processing. CSERT are committed to ensuring that information is only used for legitimate purposes with members/volunteers or community residents' consent and only by authorised CSERT members/volunteers.

2.1.8. Principle 8: Participation of Individuals

CSERT members/volunteers and community residents are entitled to know particulars of their personal information held by CSERT, as well as the identity of any authorised employees of CSERT members/volunteers that had access thereto. They are also entitled to correct any information held by CSERT.

3. Operational Considerations

3.1.1. Monitoring

The CSERT Management Committee is responsible for administering and overseeing the implementation of this policy. All CSERT members/volunteers are to be trained, according to their functions, in the regulatory requirements, policies and guidelines that govern the protection of personal information. CSERT will conduct periodic reviews and audits, where appropriate, to ensure compliance with this policy and guidelines.

3.1.2. Operating Controls

CSERT will establish appropriate standard operating procedures that are consistent with this policy and regulatory requirements, if required. This will include:

- Allocation of information security responsibilities;
- Incident reporting and management;
- User ID addition or removal;
- Information security training and education;
- Data backup.

3.1.3. Policy Compliance

Any breach of this policy may result in disciplinary action and possible termination of membership of CSERT members/volunteers.

As members/volunteers and community residents, and by submitting information to CSERT, data subjects hereby confirm that they have read and understood the CSERT POPI Policy and that:

1. Data subjects have no objection to CSERT retaining personal information in CSERT databases according to this POPI policy;
2. Information provided by data subjects to CSERT is true, correct and up to date.

If members/volunteers and community residents have any additional questions CSERT's collection and storage of personal information, please contact CSERT on email via manco@csert.org.za.