P-CO-13 PRIVACY/DATA PROTECTION POLICY

Land Equity International

1. PURPOSE

The purpose of this policy is to provide for the responsible collection and handling of data.

2. RESPONSIBILITY

All LEI employees, consultants and representatives of the company.

3. DEFINITION

"Personally Identifiable Information" means any data that could potentially identify a specific individual or any information that could be used to distinguish one person from another and can be used for de-anonymising anonymous data.

4. POLICY

LEI is dedicated to safeguarding the privacy and protection of Personally Identifiable Information and sensitive data throughout our business from unwarranted invasions that could result in misuse, embarrassment, inconvenience or unfairness to any with which the Company has a relationship.

Due to the nature of its work LEI may be provided with or require access to data belonging to the client or other stakeholders. Representatives must not access Personally Identifiable Information they do not need to complete their job and must not disclose such data to unauthorised parties.

LEI employees and consultants will take all practical steps to ensure the security, integrity and reliability of this data. LEI will do this by:

1. Ensuring that confidential information, data and personal information is kept in the strictest confidence, and not stored, copied or shared except as necessary for the fulfilment of the contract.
2. Maintaining the highest standards of security and virus protection on all devices and networks.
3. Having a real time back up of its company data through a cloud-based server with appropriate security protocols.
4. Encrypting all company/project files on individual laptops.
5. Agreeing to be audited in respect of our security systems and compliance with the client's requirements.
6. Ensuring that disposal of information is carried out in a secure way so that data cannot be recovered by unauthorised third parties.
7. Ensuring all relevant personnel are suitably trained in the area of data security.

INCIDENT REPORTING

All employees, consultants or representatives of the company are required to report immediately, to a superior, Team Leader, LEI Managing Director or through the LEI Whistleblower Platform, any data breach, loss or wrongful disclosure/release of data or suspected breach/loss/disclosure or a request or complaint under any data protection legislation.

The platform asks for the kind of misconduct being reported, details of the persons involved, when the misconduct took place and a detailed description of the incident. All reports lodged through the platform will be reviewed and actioned by the Chair of the LEI Board, as an independent body external to LEI.

LEI will report the incident or request to the client / contact as promptly as possible (and in any event within 2 working days). Any report must include details of what data was involved (or suspected), how the data was compromised, and what mitigating steps are being taken to prevent future loss (or details of the request or complaint).

Failure to protect Personally Identifiable Information and sensitive data may result in disciplinary action or termination of employment of the responsible employee or contractor.

P-CO-13 PRIVACY/DATA PROTECTION POLICY

SIGN OFF:

MANAGING DIRECTOR: 

Date: 03-04-25