Information Security Policy

It is Cornerstone's policy that the information it manages, in both electronic and hard copy, is appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information. Cornerstone is committed to satisfying applicable requirements (legal and other) relating to information security.

This Information Security Policy provides direction and support for information security across the organisation and is applicable to any enviroment that contains Cornerstone data.

Cornerstone will meet its information security commitments by:

- Determining and maintaining the appropriate levels of security through regular risk assessments, exercises and reviews to identify the probability and impact of security failures;
- Formulating the appropriate information security measures indicated by the risk assessments and maintaining a record of these measures detailing the control environment;
- Ensuring that the information security policy is communicated and understood throughout the organisation;
- Establishing the behaviours and values that frame our goals for ensuring the protection against the consequences of breaches of confidentiality, failures of integrity, or interruptions to the availability of information;
- Requiring our contractors and other relevant parties to demonstrate a strong commitment to information security;
- Providing the necessary training to our employees and others, including temporary employees to ensure their competence with respect to information security matters, including information classification;
- Ensuring that measurable information security objectives are established and reviewed.

In addition to this, we will:

- Provide sufficient physical and financial resources and technical expertise;
- Maintain systems to track our contractors and suppliers performance with respect to information security, ensuring that they share our information security standards and values;
- Ensure that employees and contractors are made aware of the importance of meeting information security statutory and regulatory requirements.

We are committed to the continual development of our people and the continual improvement of our Information Security Management system operating in accordance with ISO 27001:2013 Standard. We will review this policy regularly for continuing suitability, and communicate it to all persons affected by our activities, and interested parties. This policy is available to relevant interested external parties, as appropriate.

Pat Coxen
CEO

Date: 13-May-2024