Information Security Policy Statement

Cetix will secure confidential information and Information Technology (IT) services in a manner which complies not only with current legislation, but is appropriate for the protection from unauthorised use, disclosure, or destruction. The implementation of appropriate controls and monitoring will ensure the continuity of business operations and limit damage in the event of a security incident.

This policy applies to all confidential Cetix information such as electronic data stored on computers, (or physical storage media such as solid state, magnetic or optical media), transmissions across networks, fax, paper media or verbal.

This policy is applicable to users of such information including employees, temporary employees, and contractors on Cetix premises. All employees are directly responsible for implementing and complying with this policy. Sub-contractors shall be made aware of confidentiality obligations by means of the standard contract terms at purchase. Information passed to sub-contractors is on a "need to know" basis.

The goal of the policy is to ensure:

Confidentiality – information is accessible only to those authorised for access.

Availability – authorised users can have access to information when required.

Integrity – information is accurate and complete including processing methods.

Cetix will strive to:

- Appropriately protect all client data and not to communicate such data or information to any third party without prior authorisation.
- Assure confidentiality and the integrity of the information will be maintained.
- Suitably protect premises by physical and environmental controls, and where appropriate restrict access to authorised employees only.
- Prohibit unauthorised access to confidential information.
- Ensure all regulatory, legislative, and contractual requirements are met.
- Provide employees with training in information security awareness and define individual responsibilities.
- Ensure all managers are directly responsible for implementing the policy within their business areas, and for adherence by their employees.
- Ensure all employees adhere to the Information Security Policy.

All breaches actual or suspect must be reported to the CEO who will ensure they are investigated. Breaches of this policy may lead to gross misconduct and will be subject to the disciplinary actions as communicated in the Employees Handbook.

Signed:  *Dated:* 03/01/2024

Paul Deehan
CEO, Cetix LTD

Last Reviewed Jan 2024