VeriSure Audit
Information Security Policy

1. Introduction

VeriSure Audit is committed to information security, which is the practice of maintaining the confidentiality, integrity, and availability of information assets and systems including its clients' records.

This Information Security Policy sets the baseline security principles governed under VeriSure Audit' Information Security Management Framework (ISMF) with the objective of its people, information and assets, in line with its risk appetite.

The purpose of the ISMF is to proactively identify, manage, mitigate and monitor security threats and risks to IT systems and assets.

1.1. Who does this Policy apply to?

This Policy applies to:

- all employees, contractors and temporary staff of VeriSure Audit and its related bodies; and
- suppliers of goods or services to the VeriSure Audit.

2. General Principles

VeriSure Audit strives to protect its information assets and systems through its commitment to the following objectives:

- Ensuring employees and contractors exercise due diligence in respect of information security within each business undertaking.
- Ensuring an effective risk management process is in place that is consistent with the nature of work activities and level of associated information security risk.
- Ensuring managers are responsible and accountable for their employees' commitment to information security.
- Ensuring measurable objectives and targets for information security are in place;
- Complying with relevant information security regulations, standards, and other requirements placed upon the organisation.

- Providing information, instructions and training to employees and contractors on matters relating to information security.
- Ensuring all employees and contractors are informed of, understand and fulfil their information security responsibilities.
- Measuring, monitoring and reporting the objectives, targets and effectiveness of information security.
- Continually improving our processes for information security management, to create and maintain a culture that values information security.

3. What are the consequences of breach of this Policy?

3.1. Consequences for employment or engagement

The relationship of employment is characterised by obligations of honesty and fidelity owed by the employee to their employer. Engagement in inadequate information security practices is incompatible with this obligation of trustworthiness. Similarly, VeriSure Audit holds its contractors to a high standard and seeks to do business with people and entities it can trust.

Any staff member or contractor who does not comply with this policy may be subject to disciplinary action, up to and including termination of their employment or engagement. Any decision to take disciplinary action against a staff member is at the discretion of the CEO.

3.2. Criminal and other legal consequences

In addition to being a breach of a staff member's obligations to VeriSure Audit, breach of information security and privacy may amount to criminal behaviour. Staff members or contractors who have taken part a breach of information security and privacy can expect the matter to be reported to the Police or other appropriate regulatory authority. Where a breach of information security or privacy results in loss or damage to VeriSure Audit, staff members and contractors who have participated in such activity may also be the subject of legal action by VeriSure Audit to recover compensation.

3.3. Reputational impact

A breach of information security and privacy are each a betrayal of trust. The damage potentially inflicted on the VeriSure Audit may greatly exceed the material value of the information security breach or privacy. VeriSure Audit may seek to recover its losses fully caused by such reputational impact the law allows.

This Policy may be updated or revised from time to time. Updated or revised versions of this Policy will be made available on VeriSure Audit's internet site. It is each staff member or contractor's responsibility to access the internet to ensure he or she has is familiar with the most recent version of this Policy.

Approved Date: November 2024
Deon Rossouw Chief Executive Officer

Version Information Version Date Comment

Version	Date	Comment
1.0	November 2024	Original