VERTO
SKILL TO TRANSFORM

Information Security Policy

Statement of policy
VERTO is committed to protecting its information assets. VERTO recognises that it has a responsibility to safeguard information from unauthorised or accidental modification, loss or dissemination.

This policy is applicable to information being created, processed, transmitted and/or stored by:

- VERTO information technology system resources
- Information Technology systems utilised by VERTO partners on behalf of VERTO or by VERTO in providing a service to a third party.

VERTO is dedicated to creating and maintaining an environment where particular emphasis is concentrated on ensuring:

- The confidentiality of all information (protecting sensitive information from unauthorised disclosure)
- The integrity of VERTO information systems (safeguarding the accuracy and completeness of information, systems and software)
- Accountability, non-repudiation of events (all activities occurring within the information systems environment can be confirmed, accounted for and assigned to an individual)
- Availability of system resources (ensuring information and vital services are available to users of the system when required)
- All requirements of information security legislation are fulfilled
- All information security risks and incidents are managed appropriately.

Security practices must be undertaken at all times in order to protect VERTO's software, hardware and information resources.

Scope of policy
All VERTO employees, contractors, consultants, and third-party users who have access to VERTO information must comply with this policy.

Implementation of policy
Information security management is used to manage the level of risk to the business and its customer information assets, according to VERTO's established risk criteria. These risks include unauthorised access, breach of confidentiality, loss of integrity and lack of availability.

Context

1. Information that is fit for purpose, secure, available, and accessible, and complies with applicable laws and regulations.
2. The implementation of an Information Security Policy, Information Security Framework and an Information Security Management System (ISMS), along with effective governance, enables VERTO to identify, manage and achieve its information security objectives.
3. This Policy supports the Department of Education, Skills and Employments directive that all agencies appropriately protect information by establishing an Information Security Management System (ISMS). The ISMS meets the following Standards for Information Security:
    - ISO/IEC 27001 ISMS Requirements.

    An ISMS is a framework and methodology used to manage information security risks.
4. This policy is guided by relevant legislation, agreements and policies.
5. This policy is approved and endorsed by the CEO.

Responsibilities and delegations

Information Technology (IT) Manager

- The IT Manager is responsible for establishing appropriate monitoring and auditing measures to ensure these accountabilities are managed effectively. The IT Manager is responsible for the management and maintenance of the Information Security Management System.
- The IT Manager is responsible for the management and maintenance of the infrastructure on which the department's data resides. The IT Manager must ensure that VERTO's data is managed securely in line with the Information Security Framework.

Chief Financial Officer

- The Chief Financial Officer (CFO) is responsible for establishing governance and management accountabilities for the Information Security Management System and related activities; and is responsible for defining and implementing an information security plan for the protection of VERTO's information and systems.

Management

- All managers are responsible for ensuring that this policy, associated standards and procedures and ISMS objectives are effectively communicated and implemented throughout all corporate programs and service areas.

Employees (including contractors)
All employees are responsible for

- Familiarisation with the Information Security Policy and the relevant standards and procedures.
- Exercising duty of care to protect information assets.
- Reporting suspected breaches, in accordance with Reporting a Cyber Incident Procedure.

Ultimate responsibility for information security rests with the VERTO CEO, however, responsibility for the management of information security within the system is delegated to the CFO.

Monitoring and review
The Chief Financial Officer monitors the implementation of this policy and reviews its contents for relevance and accuracy at least every two years.

Contact
Privacy Officer
1300 4 VERTO