Information Security Policy

This statement sets out telent`s strategic commitment to information Security management covering all aspects of our business activities.

It is the policy of telent to ensure that the Confidentiality, Integrity and Availability of both telent, and customer owned, information is maintained in order to ensure continued quality of service and the meeting of our statutory, regulatory, legal and contractual obligations.

Commitment

telent is committed to:

- Treating information security as a business critical issue;
- Creating a security positive culture;
- Ensuring that legislative and contractual obligations are met;
- Assuring and maintaining the confidentiality, integrity and availability of information by ensuring that information and information processing Assets are protected against unauthorised access and change;
- Developing, implementing and maintaining and continually improving an Information Security Management Systems (ISMS) in accordance with the requirements contained within ISO/IEC 27001:2013;
- Identifying and implementing controls that are proportionate to levels of risk;
- Producing, maintaining, and testing business continuity plans to ensure the availability of information and information systems;
- Protecting intellectual property rights;
- Achieving individual accountability for compliance with this policy, supporting related policies and supporting procedures and;
- Communicating this policy to all employees, contractors, customers and all other relevant parties.

Implementation

The Chief Executive Officer (CEO), with support from the telent Senior Management Team, has overall responsibility to ensure that this policy is effectively implemented and delivered throughout the telent business.

To support this policy, detailed procedures are published separately and updated in response to changes in both legislation and working practices.

Information is treated as an integral part of line management activities and is pursued in the same manner and with the same vigour as other managerial objectives.

The management team implements and manages Information Security within their respective area and ensures line management accountability for effective performance.

As an integral part of Information Security Management system, an Objectives framework is in place to measure the effectiveness of the system.

All Managers are responsible for implementing and communicating this policy, supporting policies and procedures within their area of responsibility.

All staff (i.e. permanent staff, contractors and temporary staff) will adhere to this policy and supporting policies and procedures.

The CEO is the ultimate Risk Owner and through the management review process, delegates the daily management of that risk to the Head of Security and Business Continuity.

Review

As a minimum, this policy and our performance in meeting its requirements is monitored and reviewed annually by the telent Senior Management Team.

Mark Plato
Chief Executive Officer