Information Security Policy

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

Purpose and Scope

This policy sets out Telents strategic commitment to information Security management and covers all aspects of business activities. By delivering appropriate security arrangements Telent can meet customer requirements and provide protection from current threats.

It applies to everyone who uses Telent's IT facilities, whether employees, contractors, visitors or other users, and regardless of where you work within the business.

Responsibilities

Senior Managers will ensure activities within their areas of responsibility are conducted in a manner that results in conformance with this policy, supporting related policies and supporting procedures.

All Managers will be 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.

Enforcement

By logging onto a Telent laptop or another device, the Telent network, or use any Telent IT service, you are confirming that you understand and accept this Policy.

Review

This document is subject to review at least annually or in response to operational changes.

Stephan Badesha

Group Chief Security Officer

Valid until End May 2022 – Issue 3 **Telent Technology Services Ltd. No 703317**

Information Security Statement

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

telent
talent with technology

Our Aim and Commitment

Telent is a provider of technology, network services and innovation on many of the UK and Ireland's largest and mission-critical operational systems: from Public Safety and Defence to Transport and Service Providers. Our aim is to provide high-quality, dependable and ever advancing solutions and services as the trusted partner of choice to our customers in the UK and Ireland.

Telent is committed to providing high quality services that consistently meet our customers' expectations and promoting a security culture that encourages continual improvement in business performance and promotes organisational learning.

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

Telent is committed to maintaining an Information Security Management System that, as a minimum, satisfies the requirements of BS EN ISO27001:2013, contract specific schemes, relevant legal and regulatory requirements, and the requirements of Cyber Essentials Plus. We understand the needs and expectations of our interested parties and where practicable and agreed, incorporate those requirements and needs into our service delivery to ensure we meet or exceed them.

We will monitor and act where required by reviewing performance against agreed objectives and targets and using effective methods of Control and Assurance. This policy supports Telent`s security objectives of:

- Delivering appropriate security arrangements to meet customer requirements and provide protection from current threats;
- Ensure Telent staff understand their security responsibilities by maintaining and developing the knowledge and competency of our people.

Governance

At Telent, we have a framework of governance which provides overview of our security performance.
Roles and responsibilities for security management are clearly defined and assurance is in place to assess performance within the business.
Tools and processes are in place to monitor the security of information, controls and actions needed to ensure best performance and support the ongoing development and improvement of our information security management system in line with social and technological advances.

Implementation

The Telent Senior Management Team has overall responsibility to ensure that this policy is effectively communicated, implemented and delivered across the business and our supply chain. This is cascaded to Telent Business Units by:

- Deploying and integrating the Information Security Policy into Business Unit activities.
- Identifying activities that have the potential for negative impact on quality and managing mitigation through appropriate controls and actions.
- Supporting Telent's corporate objectives and targets by implementing and monitoring successful security management plans and programmes.
- Training, developing and instructing colleagues on the importance of their roles and responsibilities and ensuring they fully understand the relevant processes and procedures for the delivery of those roles.

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