Business Continuity and Disaster Recovery Policy

The Security Business Continuity and Disaster Recovery Policy sets the guidelines and procedures for ensuring the continued availability of critical systems, data, and services in the face of disruptions, disasters, or other incidents.

It applies to all Telent employees.

The Business Continuity and Disaster Recovery Policy sets the guidelines and procedures for ensuring the continued availability of critical systems, data, and services in the event of disaster. This is expected from all employees and contractors.

The establishment of a Business Continuity and Disaster Recovery (BCDR) policy is necessary in today's business landscape. This policy serves as a framework, outlining protocols, and procedures to ensure the uninterrupted operation of critical business functions. By defining a comprehensive BCDR policy for data backup, system recovery, and continuity planning telent can improve operational resilience. It protects critical assets including data repositories, IT infrastructure, and key business assets. Reducing the impact of events such as natural disasters, cyber incidents, or operational outages. The goal is to minimise downtime, maintain service delivery and maintain customer and stakeholder trust by recovering essential operations in a timely manner.

The BCDR policy addresses the need to preserve business continuity by safeguarding assets integral to day-to-day operations. Beyond preservation of data and systems, it recognises the broader impact of disruptions on Telent's reputation, customer relationships and overall market competitiveness. By proactively preparing for unforeseen events, the BCDR policy reinforces Telent's commitment to resilience, customer service and the delivery of products or services, reflecting a proactive approach to risk management.

Business Continuity and Disaster Recovery policy forms a key part of the Telent Information Security Management System (ISMS) and our ongoing ISO27001 (2022) certification. It applies to everyone who uses Telent's IT facilities, whether employees and contractors and regardless of where you work within the business.

Responsibilities

Managing Directors and departmental managers are expected to, and are directly responsible for, ensuring that this Policy is effectively implemented and delivered throughout our organisation and where applicable whilst liaising with Telent's Corporate Security team: Security@Telent.com

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

Enforcement

While employed with Telent, you are confirming that you understand and accept this Policy as well all current applicable policies (Exception Management Policy, Incident Management Policy, Patch Management Policy, Security Backup Policy, Risk Management Policy)

Non-compliance will be escalated to senior leadership. Telent has a formal disciplinary process for employees who violate organisational security policies and procedures. In serious cases, Telent may take legal action and/or involve the police or security authorities.

The following ISO 27001 2022 controls are directly linked to this policy.

5.30	ICT Readiness for Business Continuity
5.37	Documented operating procedures
8.29	Security testing in development and acceptance
8.31	Separation of development, test and production environments
8.32	Change management

Review

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

Dave Moore

Chief Information Security Officer

Next Review March 2027 – Version 2.2

Telent Technology Services Ltd. No 70331

Business Continuity and Disaster Recovery Policy

The Security Business Continuity and Disaster Recovery Policy sets the guidelines and procedures for ensuring the continued availability of critical systems, data, and services in the face of disruptions, disasters, or other incidents.

It applies to all Telent employees.

Maintaining the Confidentiality, Integrity, and Availability of both Telent and customer owned information processed by Telent is critical to ensure continued quality of service delivery and the meeting of our regulatory, legal, and contractual obligations.

All staff are required to play an active role in the protection of company assets and treat information security appropriately in order that this purpose can be achieved.

Commitment

In support of this Policy, the Senior Leadership Team are committed to:

- Treating information security management as a business-critical issue.
- Treating business continuity management as a business-critical issue.
- Creating a security positive culture.
- Identifying and implementing security controls to protect Telent assets that are proportionate to levels of risk; and
- Achieving individual accountability for compliance with the policy, related policies and supporting procedures.

Policy

The Telent Senior Leadership Team has overall responsibility to ensure that this policy is effectively implemented and delivered.

A comprehensive risk assessment **must** be conducted to identify potential threats and vulnerabilities that could impact the availability of critical systems and data. This includes natural disasters, cyber-attacks, geopolitical risks, and other potential disruptions.

All staff must be conversant with the Crisis Management and Business Continuity strategy.

There **must** be a Business Continuity risk assessment process.

Risk tolerance levels **must** be defined and prioritise risks based on the potential impact to critical operations.

There **must** be a process to review and manage risks.

The risk assessment **must** inform the development of risk mitigation strategies within the Business Continuity and Disaster Recovery Plan.

Telent **must** conduct a regular Business Impact Assessment (BIA) to identify and prioritize critical business functions, systems, and data. Recovery time objectives and recovery point objectives **must** be established for each critical function.

There **must** be a process to define priority business functions and apply to resilience and architecture / network/ platform development and design process.

BIA and business function criticality **must** be regularly reviewed.

The BIA **must** inform the development and maintenance of the Business Continuity and Disaster Recovery Plan.

Telent **must** develop and maintain a business continuity plan (BCP) and a disaster recovery plan (DRP) that outlines procedures for responding to disruptions and recovering IT systems and physical infrastructure. (5.37)

The disaster recovery plan (DRP) **must** include, as a minimum:

- Emergency response procedures.
- Communication and notification procedures.
    - Including out of band communications
- Roles and responsibilities of key personnel.
    - Resilience, location, logistics
- Data backup and recovery procedures.
- Offsite storage arrangements.
- Alternative processing facilities.
- Testing and exercising schedules.

- Reviewed Annually

Telent **must** establish a crisis management team with define roles and responsibilities to manage and coordinate responses during an incident. These roles and responsibilities **must** be regularly reviewed.

Telent **must** develop communication plans to ensure appropriate internal and external stakeholders are informed during and after an incident.

There **must** be a process for the communication of any incident to the relevant stakeholders.

All employees and relevant stakeholders **must** receive training on the Business Continuity and Disaster Recovery Plan.

Awareness campaigns **must** be conducted periodically to reinforce the importance of preparedness and response.

There **must** be a process to review the effectiveness of any training package.

Regular testing and exercising of the Business Continuity and Disaster Recovery Plan **must** be conducted to ensure its effectiveness.

There **must** be a process for BCDR testing.

Lessons learned from tests and exercises **must** be used to update and improve the plans.

Telent **must** ensure detailed documentation of BCDR plans, risk assessments and incident responses are maintained.

Telent **must** establish a reporting mechanism for employees and contractors to report potential risks or incidents promptly.

Considerations

Telent **must** ensure that the BCDR plans are reviewed and updated in line with new legislation, changes to industry standards, and updates in best practice.