Business Continuity & Disaster Recovery Management Policy

Document ID: A13

Author(s): Chiranjeevi Chekka, *Associate director | IT & networks*

Version: 1.6

Date: 22 Mar 2021

Document details	
Name of the document	**A13 Business Continuity & Disaster recovery Management Policy**
Document reference	Tanla/ISMS/Policy/A13
Release date	22-03-2021
Owned by	Chair, ISMS Forum
Implemented by	Chiranjeevi Chekka, ISMS Officer
Governed by	ISMS Forum

Revision history

Version No.	Date	Details of Change	Changes done by	Approved by / Date
1.0	07/03/2018	Draft Version	ISMS Officer	ISMS Forum
1.1	15-07-2019	Reviewed the document and there are no changes	ISMS Officer	ISMS Forum
1.2	22-03-2019	Reviewed the document and there are no changes	ISMS Officer	ISMS Forum
1.3	23-09-2019	Reviewed the document and there are no changes	ISMS Officer	ISMS Forum
1.4	25-03-2020	Reviewed the document and there are no changes	ISMS Officer	ISMS Forum
1.5	23-09-2020	Reviewed the document and there are no changes	ISMS Officer	ISMS Forum
1.6	22-03-2021	Reviewed the document and there are no changes	ISMS Officer	ISMS Forum

Contents

1. Policy

Tanla's business continuity policy and plans shall establish a framework to counteract interruptions to its business operations and activities and protect its critical business processes from the effects of major failures of information system or disasters and thereby ensure their timely resumption. Tanla shall ensure continuity of critical operations and other activities of the scoped areas in case of a disaster affecting or disruption to Tanla's business services.

It is the intent of the management to establish a **Business Continuity Framework** which clearly defines the accountability, structure, roles and responsibilities. For critical processes, a **Disaster recovery plan** shall be put in place and their appropriateness and effectiveness reviewed over time. Appropriate levels of resilience and capacity planning shall also be provided for.

2. Objective

Tanla is committed to its employees and other stakeholders and thus human life will be its number one priority in the event of a disaster. To keep its business edge, Tanla must be in a position to continue critical operations even in case of a disruption or disaster, whether the interruption relates to large or small incidents. Effective business continuity management is not only minimizing the likelihood of an event occurring but also having the ability to recover and restore disrupted business processes and facilities.

3. Scope

This policy is applicable to scoped businesses carried out in the specified locations and employees of Tanla, contractors and third party users in employment or in contract with Tanla as detailed in the Information Security Policy.

4. Approval

This policy bears the approval of the ISMS forum and the implementation, maintenance and operation of the policy shall be the responsibility of the respective department heads/owners of information assets and the IT team of Tanla.

5. Requirements

1. Tanla shall develop and maintain a managed process for business continuity that addresses the information security requirements needed for its continuity of operations and resumption of critical business services.

2. A formal risk assessment shall be conducted to determine the probability and impact of the events that can cause interruptions to business processes and facilities and their consequences for information security in terms of its impact on business operations of Tanla. This shall be documented in the **Business Impact Analysis.**

3. Tanla shall develop and maintain **Business Continuity and Disaster Recovery Plans** to maintain and restore operations and ensure availability of information at the required level and in the required timescales following an interruption to or failure of critical business processes.

4. A single framework of business continuity and recovery plans shall be maintained in the Tanla Head office (Hyderabad) to ensure that all plans are consistent, and also to identify priorities for testing and maintenance.

5. Business continuity and disaster recovery plans shall be tested by Tanla at least annually to ensure that critical functions can be recovered according to the plan, and also to ensure that information processing can resume within critical timescales making sure that all components of the scoped function as expected.

6. The plan shall be maintained and re-assessed by regular reviews and updates to ensure their continuing effectiveness, at least annually.

7. Tanla shall establish strategy and its continued implementation for training of staff members to effectively handle their roles required of them as part of emergency procedures, responding to disasters and recovering therefrom. In the event of any major operational or system changes as well as the contingency strategy, the requisite changes shall be forthwith made to the training strategy.

6. Roles & responsibilities

Roles	Responsibilities
ISMS Forum	♦ Approval of policy & overall governance.
ISMS Officer	♦ Review implementation of the policy. ♦ Development of plans. ♦ Co-ordinate development, implementation, testing and operation of the strategy & plans ♦ Monitoring of key performance parameters.
IT Team	♦ Formulate, review & modify policy.
Department Heads	♦ Participate in the plan preparation, implementation and operation.
ISMS Auditor	♦ Audit compliance to the plan to determine suitability of design and operating effectiveness.

7. Compliance

Violations to provisions of this policy:

- Shall be subject to Tanla's Code of Conduct and Disciplinary process and can invite disciplinary action including dismissal of the user or termination of contract and can extend to legal action.
- Any person alleged with the act of violation and related acts can be subject to interrogation and investigation

8. Associated documents

a) Information Security Policy

b) Business Impact Analysis

c) Business Continuity Plan & Disaster Recovery Plans

d) Code of Conduct and Disciplinary Process