Network Security and Data Centre Management Policy

Document ID: A12

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

Version: 1.6

Date: 22 Mar 2021

Document details	
Name of the document	**A12 Network Security & Data Centre Management Policy**
Document reference	Tanla/ISMS/Policy/A12
First 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
0.1	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

The security of networks shall be so managed as to ensure the protection of information in networks and the protection of supporting information processing facilities against external and internal threats and failures. The operations and administration of equipment and information assets at all Tanla's information processing facilities such as data centers and secure IT installations, shall be managed to ensure secure operations.

2. Objective

Tanla is significantly dependent on its computer networks and core Information processing and communications facilities to carry on its day to day business. With inherent risks surrounding the networking and Internet technology, it is critical that the networks are designed, implemented and operated so as to deploy appropriate security technology and practices to thereby protect the information assets of Tanla and its customers. These factors apply equally to local and wide area networks and to data and voice communication.

This policy lays down requirements to ensure secure network operation and management such that the information assets of Tanla and its customers are protected from risks arising from undesirable network traffic and unauthorized external access to information transmitted on its networks. Networks should be managed so as to ensure continued availability of network services critical to Tanla's business.

The security relating to data centre operations at Hyderabad should be managed so as to ensure that critical information assets of Tanla and its customers are protected against risks arising from errors and negligence, technical failures, unauthorized access and alteration etc.

3. Scope

The scope and applicability of this policy is detailed in the **Information Security Policy** and specifically applies to all data centers, networks, data inter-networking devices and equipment which are owned and managed by Tanla across its various locations, including internal and external wireless and mobile networks that are owned by and/or support the business of Tanla.

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, ISMS Officer and the IT Team at Tanla.

5. Requirements

5.1 Network security

5.1.1 Network controls

1. Tanla's network architecture including perimeter, links, inter-networking / data communication devices and equipment should be designed & implemented on the principles of defense-in-depth supporting layered security so as to protect the confidentiality, integrity and availability of information, and related systems. Firewalls and security mechanisms at critical network gateways shall conceal the internal network and shall be implemented with fault tolerance. All devices on the network like servers, desktops, laptops, routers, firewall etc. shall be suitably hardened as per defined procedures to reduce the vulnerability of these assets as described in **Network Security Procedure**, **Technical Build Procedure and Desktop, Laptop Build Procedure.**
2. Responsibilities and procedures for the management of networking equipment should be established. Operational responsibility for networks should be separated from computer operations where appropriate.
3. Controls shall be implemented to safeguard the confidentiality and integrity of data passing over public networks and to protect connected systems and applications.
4. Procedures shall be put in place for logging and monitoring and detection of actions that may affect information security.

5. All network traffic shall be routed through a firewall, prior to being allowed access to the network. Network firewalls and inter-networking devices performing firewall services must be configured to support a least-privilege approach to security, allowing only specific systems, services and protocols to communicate through the network perimeter.
6. Any change to the Tanla network architecture, data center, inclusion of new devices etc. shall implemented only after due risk assessment.
7. Systems on the Tanla network shall be authenticated.
8. Systems connection to the network should be restricted.

5.1.2 Security on network services

1. Security mechanisms, service level and management requirements of all network services should be identified and included in the network service agreements, whether these activities are provided in-house or outsourced.
2. The network service provider's ability to manage agreed upon services in a secure manner should be determined and regularly monitored and right to audit should be agreed to where required.

5.1.3 Network capacity management

1. The capacity utilization of all key networks shall be continuously monitored to be within threshold limits so as to insure against any risks

of disruption due to non-availability or latency in networks as mentioned in **Capacity Management and Planning Procedure**.

2. Single point of network failure should be minimized by providing for adequate redundancy for network links and components that are considered critical to the functioning of Tanla's business and alternate modes of network administration shall be provided.

5.1.4 Network security administration

1. Networks shall be physically segregated based on the sensitivity of the information asset wherever required.
2. For sensitive environments, consideration should be made to treat all wireless access as external connections and to segregate this access from internal network until the access has been passed through a gateway.

5.1.5 Technical vulnerability management

1. Information about the technical vulnerabilities of information systems being used should be obtained, the organizations exposure to such vulnerabilities must be evaluated and appropriate measures shall be taken to address the associated risk.
   a) Tanla shall define the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking etc.

b) Information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them should be identified for software and other technology.

c) For any potential technical vulnerability that has been identified; Tanla shall identify the associated risk and the action to be taken: such action could involve patching of vulnerable systems.

d) Patches should be tested and evaluated before they are installed to ensure their effectiveness and to avoid any side effects.

2. Procedure for installation of software by the user should be established and implemented.
   - Rules to be designated for installation of software.
   - Types of software to be installed and permitted.
3. Penetration testing/Vulnerability Analysis (VA) shall be performed periodically for timely identification of technical vulnerabilities of information systems and networks and appropriate measure shall be taken to address the associated risks.

5.2 Data center management

1. All servers and sensitive inter-networking and communication devices and equipment shall be physically located in secure and specifically designated data center(s)/ communication closets and access to such facilities shall be strictly enforced as per the **Physical and Environmental Controls Policy**.

2. Every change to the data center equipment, facilities and utilities shall be strictly governed by the **IT Helpdesk, Incident and Change Management Policy** and **Procedures.**
3. Access to data centers and sensitive locations such as communication closets etc. shall be secured using access control mechanisms and shall be subject to video surveillance. Every entry, of visitors and external/third parties to the data centers shall be logged and reviewed periodically.
4. All servers shall have access logging enabled and all logs shall be reviewed regularly.
5. All data center operations shall be governed by the **Server Room Operations Procedure**.

6. Roles & responsibilities

Roles	Responsibilities
ISMS Forum	♦ Approval of policy & overall governance.
ISMS Officer	♦ Ensure effective implementation of policy requirements and continuously monitor. ♦ Reporting to the ISMS forum on policy performance and other reporting obligations.
IT Team	♦ Formulate, review &modify policy. ♦ Implement policy and related procedures.
ISMS Auditor	♦ Audit implementation of the policy requirements. ♦ Report on gaps and weaknesses, provide recommendations and ensure closure thereof.

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 subjected to interrogation and investigation.

8. Associated documents

a) Information Security Policy
b) Capacity Management and Planning Procedure
c) IT Help Desk, Incident and Change Management Policy
d) Physical and Environmental Controls Policy
e) Network Security Procedures
f) Desktop, Laptop Build Procedure
g) Technical Build Procedure
h) Server Room Operations Procedure
i) Code of Conduct and Disciplinary process