Malware Protection Policy

Document ID: A05

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

Version: 1.6

Date:22 Mar 2021

Document details	
Name of the document	**A05 Malware protection Policy**
Document reference	Tanla/ISMS/Policy/A05
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	07/03/18	Initial 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 Systems shall take adequate precautions and accordingly design and establish appropriate technologies and controls to primarily prevent, if not, then detect, and at the earliest correct the risks arising from actions of any kind of malicious code to protect the integrity, availability and confidentiality of Tanla's information assets.

2. Objective

The objective of this policy is to establish the requirements for preventive and detective controls to protect against viruses, other malicious code and network threats, and provide guidance on identification and control over various kinds of malicious threats such as virus/worm infections, root kits, ransomware, spyware, adware, phishing and other such attacks and ensure capability to respond to such attacks within critical timescales.

3. Scope

The scope and applicability of the policy is as detailed in the Tanla Information Security Policy. This policy shall specifically apply to all Tanla information processing systems and supporting systems such as network devices, security devices and telecommunication equipment.

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

Tanla shall:

a) Prohibit the use of unauthorized software in the organization. The procedure of monitoring and tracking unauthorized software shall be detailed in the **License Monitoring Procedure**.

b) Prohibit the use of insecure hardware and components such as pen drives, wireless synchronization with insecure devices etc.

c) Implement controls to prevent or detect the use of unauthorized software.

d) Implement controls that prevent or detect suspicious/malicious websites.

e) Usage of networks, applications and devices relating to Tanla business shall be governed by **"Acceptable use Policy".**

f) Deploy appropriate industry standard licensed anti-virus, anti-malware, network threat management technology solutions to protect the integrity of Tanla's information assets and associated IT infrastructure including perimeter network devices, internal network devices, servers, network terminals, desktops, laptops, data-enabled mobile equipment from actions of malicious code and network

threats. Such technologies should be capable of centralized deployment, control and monitoring, and shall be capable of detection, prevention and recovery from any incidents due to malware attacks/network threats.

g) Train users for identifying and appropriately responding to such risks and vulnerabilities that lead to compromise, compliance with practices and procedures for protecting against such risks, and escalating incidents thereof as detailed in the "**Human Resource Procedure"**.

h) For providing protection against malware, establish documented "**Malware Protection Procedures**", which shall specify the methods for configuring malware protection software, update mechanisms and frequency thereof and the process for dealing with the same.

i) Deploy appropriate security technology for intrusion detection/Prevention and develop documented standards and procedures for monitoring threats which shall specify the methods of identifying unauthorized activity, analysis of suspected intrusions and appropriate responses to different types of intrusions and attacks.

j) Establish mechanisms and procedures to regulate the use of external media, portable/mobile data devices and unauthorized internet/network resources by users. This shall be detailed in the **Information and Media handling Procedure**.

k) As part of the **"IT Helpdesk, Incident and Change Management Policy** and **Procedure"**, documented emergency procedures shall be developed for reporting serious attacks and to appropriately deal with malware attacks and incidents. The procedures shall outline the actions required to be taken in the event of a serious attack.

l) Implementing procedure to recover from malware attacks shall be addressed in the **IT Helpdesk, Incident and Change Management Procedure**.

m) Ensure network vulnerability assessments are performed at regular intervals to identify, report and correct vulnerabilities in the Tanla IT infrastructure.

n) Ensure that all the systems attached to Tanla network shall have their security patches up to date as and when released by the respective vendors of the applications, software or systems and shall be maintained regularly as required by the "**Patch Management Procedures**". The patch management process shall address the methods of obtaining the patches, validating patches, deploying patches and dealing with patch failure.

o) Tanla shall ensure timely removal/upgrading of insecure unsupported software and systems that present with potential for attacks and cyber threats.

p) Ensure that all the information processing and storage devices are regularly scanned for malicious code and ensure that the scan result are reviewed for any infection and shall be handled as per **"IT Helpdesk ,Incident and Change Management Procedure"**

q) Contact with special interest groups and security bulletins shall be maintained to ensure that the latest information regarding information security threats are collected and addressed.

r) Isolating environment where catastrophic impact may result.

6. Roles & Responsibilities

Role	Responsibilities
ISMS Forum	♦ Approval of policy & overall governance
ISMS Officer	♦ Coordinate and manage Implementation of the policy. Monitoring of key parameters. ♦ Ensure effective implementation of policy requirements, controls and continuously monitor. ♦ Report to the ISMS forum on policy performance and other reporting obligations.
IT Team	♦ Implement the policy ♦ Formulate, review & modify policy ♦ Monitor and manage access and compliance with policy and procedures. ♦ Implementation of technology and related process controls. ♦ Monitor threats on a continuing and proactive basis ♦ Ensure timely and appropriate response.
ISMS Auditors	♦ Audit implementation and compliance of the policy requirements. ♦ Report on gaps and weaknesses, provide recommendations and ensure closure thereof.

7. Compliance

Violations of the provisions of the policy:

- Shall be subject to Tanla's Code of Conduct & 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) IT Help Desk, Incident and Change Management Policy

c) Malware Protection Procedure

d) Patch Management Procedure

e) IT Helpdesk ,Incident and Change management Procedure

f) Code of Conduct & Disciplinary process

g) Human Resource Procedure

h) License Monitoring Procedure

i) Acceptable Use Policy