

Information Exchange and Electronic Messaging Policy

Document ID: A07

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

Version: 1.6

Date: 22 Mar 2021

Tanla/ISMS/Policies/A07	Version No.	1.6	Internal
-------------------------	-------------	-----	----------

The information contained in this document is confidential and is intended only for the persons to whom it is delivered by Tanla. Any reproduction, disclosure or distribution of this document, in whole or in part, is strictly prohibited.

Document details	
Name of the document	A07 Information Exchange and Electronic Messaging Policy
Document reference	Tanla/ISMS/Policy/A07
Releasedate	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	Initial Version	ISMSOfficer	ISMSForum
1.1	15-07-2019	Reviewed the document and there are no changes	ISMS Officer	ISMSForum
1.2	22-03-2019	Reviewed the document and there are no changes	ISMS Officer	ISMSForum
1.3	23-09-2019	Reviewed the document and there are no changes	ISMS Officer	ISMSForum
1.4	25-03-2020	Reviewed the document and there are no changes	ISMS Officer	ISMSForum
1.5	23-09-2020	Reviewed the document and there are no changes	ISMS Officer	ISMSForum
1.6	22-03-2021	Reviewed the document and there are no changes	ISMS Officer	ISMSForum

Tanla/ISMS/Policies/A07	Version No.	1.6	Internal
-------------------------	-------------	-----	----------



Contents

- 1. Policy 4
- 2. Objective 4
- 3. Scope 4
- 4. Approval 5
- 5. Requirements 5
- 6. Roles & responsibilities..... 6
- 7. Compliance 7
- 8. Associated documents 8

1. Policy

Exchange of information and software within Tanla and/or with any external parties shall be based on agreements/conventions that approve exchange of such information appropriate to the contractual relationship between the exchanging parties. Such exchange shall be secured to protect their confidentiality and integrity using appropriate controls and shall be in compliance with relevant regulatory requirements and stipulations.

2. Objective

This policy outlines the requirements for ensuring security of information and software exchanged both within Tanla and with any external parties and to prevent their misuse. The security of storage and media for exchanging information, electronic mail, and other messaging services are critical to the business of Tanla.

3. Scope

This policy is applicable to Tanla's information exchange capabilities including, but not limited to electronic mail, application interface, fax, FTP, SMS, chat messages, social media, posting information on any electronic media, inter and intra device data/file synchronization mechanisms, internet web site updates etc. The policy shall be complied with by all users of Tanla information resources including its contractors and

third party users who directly/indirectly access Tanla's information processing facilities, as detailed in the Tanla 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, ISMS Officer and the IT Team at Tanla.

5. Requirements

- a. Tanla shall establish appropriate policies, procedures and standards for the secure implementation, operation, use and disposal of information exchanged through all types of communication facilities.
- b. Establish appropriate exchange agreements including disclaimers for exchange of information and software between the organization and external parties, where necessary. Critical and sensitive communications received/sent by the organization shall be identified and appropriate measures put in place for their retention and disposal.
- c. Protect media used for exchange, containing/carrying information against unauthorized access, misuse or corruption during transportation, beyond the boundaries of Tanla.

- d. Where sensitive business information or other information assets of Tanla or its customers and partners is exchanged with external parties, prior agreements shall be established for exchange of information and software. Such agreements shall also ensure compliance with the relevant and identified applicable laws and regulations governing such exchange of information.
- e. Tanla shall establish appropriate controls for protection of information, data and instruction sets over media and storage used for such exchanges.
- f. As regards publicly available information such as marketing, publicity information posted on websites/social media channels, Tanla shall ensure appropriate integrity controls for unauthorized modification and denial of service.
- g. Such requirements shall be defined in the **Information and Media Handling Procedure**.

6. Roles & responsibilities

Roles	Responsibilities
ISMS Forum	<ul style="list-style-type: none"> ◆ Approval of policy & overall governance.
ISMS Officer	<ul style="list-style-type: none"> ◆ Coordinate and manage Implementation of the policy. ◆ Monitoring of key parameters. ◆ Ensure effective implementation of policy requirements and

	<p>continuously monitor.</p> <ul style="list-style-type: none"> ◆ Report to the ISMS forum on policy performance and other reporting obligations.
IT Team	<ul style="list-style-type: none"> ◆ Formulate review & modify policy. ◆ Implement the policy.
Departments Heads	<ul style="list-style-type: none"> ◆ Monitor policy compliance at departmental level. ◆ Ensure compliance with the policy through effective implementation.
Users	<ul style="list-style-type: none"> ◆ Comply with policies and procedures.
ISMS Auditor	<ul style="list-style-type: none"> ◆ Audit implementation and compliance 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 & 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) Information and Media Handling Policy and Procedure
- c) Code of Conduct & Disciplinary Process