Risk Management Policy

Document ID: A02

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

Version: 1.6

Date: 22 Mar, 2021

Document details	
Name of the document	**A02 Risk Management Policy**
Document reference	Tanla/ISMS/Policy/A02
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
1.0	07/03/2018	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

Purpose, scope and users

The purpose of this document is to give a detailed overview of the processes and documents used during assessment and treatment of information risks to Tanla.

Risk assessment shall be applied to the entire information security management system ('ISMS').

This document is intended for management of Tanla, ISMS Officer, owner(s) information assets and everyone involved in planning, implementing, monitoring and improving the ISMS.

1. Policy

All critical interested parties (stakeholders) as regards management of risks to information assets at Tanla, shall be clearly identified. External and internal issues concerning stakeholder's needs and expectations shall be appropriately documented. As issues could be seen as a potential opportunity or a risk and the same shall be categorized. This Risk Management Policy and the related procedure defines the methodology that is suited to Tanla's ISMS and the associated identified business information security, legal and regulatory requirements. Risks that exceed the acceptable risk rating score approved by the ISMS Forum shall be appropriately treated. Information risk analysis shall be performed regularly and as well as before every major change having potential impact on Tanla's information resources.

2. Objective

Risk management holds the key to ensuring right level of security and trust as regards protection of Tanla's information resources. As a founding step risk assessment through risk analysis and risk evaluation ensures timely identification of all risks to Tanla's information resources.

The objective of the policy is to ensure:

- Determination of interested parties and the nature and criticality of their dependencies on Tanla's information resources.
- Identifying the potential risks to information asset(s), the likelihood of occurring, considering the state of controls and the potential impact if they would occur.
- Ensuring that such risks identified and not acceptable are treated in a timely manner.

3. Scope

This policy is applicable to Tanla's information resources as stated in Tanla's **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

1. All key interested parties shall be clearly identified.

2. External and internal issues impacting stakeholder needs and expectations shall be documented. An issue can be seen as a potential opportunity and/or a risk, the same shall be categorized. Risks and opportunities shall be mapped to existing issues.

3. Asset categories including information and client provided assets shall be classified in a manner that takes into consideration their value, criticality, sensitivity, requirements from a legal perspective based on Confidentiality, Integrity & Availability attributes.

4. For each potential risk identified, the concerned asset type at stake shall be assessed. Likelihood and impact analysis shall be performed to assess the business impact, identify risk rating, score and record in the risk register.

5. Risks with score exceeding the acceptable risk threshold shall require treatment, unless otherwise such risk is formally accepted with reasons and approved by the management.

6. A risk treatment plan for all risks requiring treatment shall be identified and documented. Such plan shall be assigned to a risk owner(s)

7. The process of risk management is the collective responsibility of various internal stakeholders. This shall be achieved through participation from the business, related support functions, information technology etc., through Risk Workshops and based on the principles of control self-assessment directed and driven by the ISMS Forum.

8. Risk identified for treatment may be treated in one or more of the following treatment options:
    a. Designing and putting in place appropriate controls
    b. Transferring the associated business risk
    c. Avoiding the risk
    d. Knowingly and objectively accepting the risk.

9. The appropriate treatment for each risk shall be determined in consultation with the concerned risk owners. The risks identified, risk rating and the treatment identified shall be signed off by respective risk owners (generally business process owners), ISMS Forum and ISMS Officer.

10. The RTP (Risk Treatment Plan) shall be presented and reviewed by the ISMS Forum. The ISMS Forum shall also provide the necessary resources and priorities to execute the Risk Treatment Plan.

11. Implementation of Risk Treatment plans shall be pro-actively monitored and completed in a timely manner. Review of Risk Register and RTP shall be performed as part of internal monitoring and audit reviews.

12. The residual risk, after implementation of necessary controls shall be reviewed to ensure that it is within the acceptable limits. Where the residual risk is found to be unacceptable, additional controls must be introduced. The residual risk shall be reviewed and approved by the ISMS Forum.

13. Documented standards/procedures for information risk analysis shall be developed and implemented and must consider the following:
    a. Business Information resources that are key to Tanla
    b. Deployment of /changes to major new technologies
    c. Changes in regulations or contractual stipulations

d. Request to permit access from new external locations or by external parties

14. Decision makers including top management, information resource owners and IT management shall be aware of the need to apply information risk analysis to critical environments throughout the enterprise.

15. Management of risks to information resources shall be applied in a consistent manner across Tanla, with a centralized risk repository maintained by the ISMS Officer.

6. Roles & responsibilities

Roles	Responsibilities
ISMS Forum	♦ Approve policy. ♦ Review and approve Risk Register and changes thereto from time to time. ♦ Provide sponsorship. ♦ Direct and monitor implementation of policy. ♦ Provide overall governance.
ISMS Officer	♦ Formulate, review & modify policy as required. ♦ Maintain the risk register.

	♦ Ensure effective implementation of policy requirements and continuously monitor for improvements. ♦ Report to the ISMS Forum on policy performance and other reporting obligations.
Department Heads	♦ Participate in risk workshops, identify issues pertaining to interested parties, evaluate risk, agree on risk treatment plans and implement & supervise the action items. ♦ Assess and approve risks from their functional/process perspective and implement policy requirements. ♦ Proactively monitor policy implementation and comply with reporting obligations.
ISMS Auditor	♦ Audit implementation of the policy requirements. ♦ Continually challenge the implementation to ensure effective policy implementation. ♦ Report on gaps and weaknesses, provide recommendations and ensure closure thereof.

7. Compliance

Violations to the 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 subjected to interrogation and investigation.

8. Associated documents

a) Information Security Policy
b) ISMS Scope Document
c) Risk Management Procedure
d) Code of Conduct & Disciplinary process