Access Control policy

Document ID: A04

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

Version: 1.6

Date: 22 Mar,2021

s

Document details	
Name of the document	**A04 Access Control policy**
Document reference	Tanla/ISMS/Policy/A04
First 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 doneby	Approved by / Date
1.0	07/03/2018	Initial Version	ISMS Officer	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

Contents

1. Policy

Access to Tanla's information assets and information processing facilities shall be provided based on business and security requirements. Controlling access to Tanla's information assets based on business requirements, shall be identified, appropriately designed and implemented to prevent any unauthorized access to Tanla's information assets.

2. Objective

The objective of this policy is to ensure that access to Tanla information assets and information processing facilities are controlled on the basis of business and security requirements. This policy states that only authorized individuals can access applications and associated information and ensures individual accountability is achieved.

3. Scope

The scope of this policy shall be as detailed in the **Information Security Policy** and this policy shall be applicable to all Tanla's employees, contractors and third party users.

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's critical business information assets may be accessed by internal and external users, which need to be protected. The Access Control Policy provides for putting in place the access controls to its information assets so as to protect their confidentiality, integrity and availability of its data and information.

6. Business requirements for access control

As part of its operations, Tanla handles various kinds of information that include sensitive information relating to its clients, their customers and other stakeholders, methods, techniques, internal operational information, the unauthorized disclosure/access of which may adversely impact the business interests of Tanla and its stakeholders. Tanla shall establish, document and review the **Access Control Policy** based on business and security requirements for access.

This policy document shall take into account:

a) the security requirements of individual business applications;
b) the applicability of relevant legislation and/or contractual obligations;
c) standard user access profiles for common job roles to ensure consistency of user access rights;
d) wherever application systems do not provide support for role based access controls, appropriate compensating controls and procedures shall be defined to achieve the said purpose;

e) need for segregation of duties in the access management functions;

f) requirements for periodical review of the access controls;

g) removal of access rights wherever it is not required

h) user access rights are provided only on a "need to know" and "need to do" basis and restricted according to individual roles applying the principle of "least privileges"

7. User Access Management

To ensure authorized user access and to prevent unauthorized access to information assets/resources, Tanla shall:

a) Put in place formal procedures and appropriate technologies to control registration and de-registration of users, the allocation and revocation of access rights to information assets and services. These procedures shall address the creation, modification and deletion or disabling of user accounts.

b) Implement a formal user access provisioning process to assign and revoke access rights for all types of users to systems and services as documented in the **User Access Management Procedure.**

c) Restrict and control the allocation and use of privilege accounts that shall be subject to specific authorization for each such addition/deletion or modification of rights to such accounts. The allocation of privileges shall be controlled through a formal authorization process and allocated to users on a need basis and revoked forthwith thereafter.

d) Ensure that the access controls implemented provide accountability of user actions with respect to information assets/resources. Where it is required for more than one person to share an access mechanism, appropriate mechanisms shall be built to identify users to actions.

e) Put in place a formal management process to control the allocation of passwords, that to the extent feasible, be automated. All users shall be required to comply with the requirements as specified in the **Password Procedures and Standards.**

f) Put in place a formal process for reviewing user access rights and privileges at defined intervals. All privilege access should be reviewed at more frequent intervals and any changes to the privilege accounts shall be logged for periodic review.

g) To prevent unauthorized user access, and compromise or theft of information and information processing facilities, Tanla shall:

   a. Implement appropriate identification and authentication technologies including where required multi-factor authentication to secure sensitive resources
   b. ensure that users are aware of their responsibilities for maintaining effective access controls and practice good security practices;
   c. require users to be responsible for selection and use and management of their secret authentication methods;
   d. strictly prohibits its members from sharing or disclosing their secret authentication information such as passwords, PINs etc., to any other individual or insecure maintenance;

h) Ensure revocation or adjustment of user access to information and information processing facilities depending on the termination of services, contract and agreement or upon role change.

8. System and Application Access Control

To prevent unauthorized access to both internal and external networked services, systems and applications, Tanla shall:

a) Ensure that users are provided access to those services that they have been specifically authorized to use.

b) Put in place secure log-on procedures to control access to the operating system.

c) Put in place appropriate authentication methods to control access by remote users. To ensure that only authorized users gain access, Tanla shall individually identify, verify, record and approve all external connections. External access shall be provided only after subjecting users to strong authentication, and remote access shall be controlled by routing traffic through firewalls and VPNs, limiting the methods of connection and removing all external connections when no longer required. The procedure for implementation of the same shall be documented in the **Network Security Procedure.**

d) Provide users with unique identifier (user ID) for use by the identified individual and shall have strong authentication mechanisms to verify and authenticate the identity and credentials of the user.

e) Restrict and limit the use of system utilities, which can override the system and application controls, to a minimum number of trusted authorized users and

maintain a trail of their use, as detailed in the Server Build and Desktop, laptop build procedure.

f) Ensure to put in adequate measures to restrict access to application and program source code.

9. Roles & Responsibilities

Roles	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 and continuously monitor. ♦ Report to the ISMS forum on policy performance and other reporting obligations.
IT Team	♦ Formulate, review & modify policy ♦ Monitor and manage access and compliance with policy and procedures ♦ Implement the policy
Department heads	♦ Monitor policy compliance at departmental level ♦ Ensure compliance with the policy through effective implementation

Users	♦ Comply with policy and procedures
ISMS Auditor	♦ Audit implementation and compliance of the policy requirements ♦ Report on gaps and weaknesses, provide recommendations and ensure closure thereof

10. 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.

11. Associated Documents

a) Information Security Policy
b) User Access Management Procedure
c) Password Procedure and Standards
d) Network Security Procedure
e) Server Build Procedure

f) Desktop, Laptop build procedure

g) Code of Conduct & Disciplinary Process