Information Security Policy

Document ID: A01

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

Version: 1.6

Date: 22 Mar 2021

Document details	
Name of the document	**A01 Information Security Policy**
Document reference	Tanla/ISMS/Policy/A01
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	Approvedby/ Date
1.0	14/03/2018	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	22-03-3021	Reviewed the document and there are no changes	ISMS Officer	ISMS Forum

Contents

1. Policy Statement

Tanla Solutions is a global telecom solutions provider serving as a trusted and transparent technology partner for its customers. Tanla focuses on services that include messaging & voice. With critical dependence on IT for customer delivery as well as its internal operations, Tanla recognizes Information as a strategic business asset of significant value to the company and its customers that needs to be diligently protected. The management and all employees of Tanla are committed to an effective Information security management system in accordance with its strategic business objectives.

To achieve the above, Tanla shall:

- establish and implement policies, processes and organization structures (Information security management system) to protect the information assets of Tanla and its customers from threats, both external as well as internal.
- continually improve the Information security management system through the establishment and regular monitoring of measurable security objectives.
- commit to comply with business, legal, regulatory and contractual security obligations, as may be applicable from time to time.
- develop, implement, test and maintain a business continuity plan as appropriate to the nature of its business
- create mechanisms to identify and review the risk and impact of incidents to protected information assets
- communicate all pertinent security policies to customers, employees and other interested parties as applicable.

This policy applies to all employees of Tanla and other users of Tanla's information processing facilities. The Managing Director and the senior management shall ensure

that this policy is implemented, communicated, monitored and maintained at all levels of the organization and regularly reviewed for compliance and continual improvement.

2. Objective

Tanla will continually review the internal and external factors that influence its ability to deliver its business objectives. Stakeholder's needs and expectations for information security would be evaluated to determine the scope for the Information Security Management System. Tanla shall identify and prioritize stakeholder's needs and address information security risks directly impacting their expectations. Tanla shall plan actions to address such risks and identify opportunities to achieve continual improvement. The primary objectives of establishing Tanla's Information Security Management System are:

- To maintain risk to enterprise information at an acceptable level and protect information against unauthorized disclosure, unauthorized or inadvertent modifications, and possible intrusions.
- To ensure that services and systems are continuously available to internal and external stakeholders and ensure compliance with all applicable legal, statutory, regulatory and contractual provisions.
- To establish responsibility and accountability for information security in the organization.
- To encourage management and staff to maintain an appropriate level of awareness, knowledge and skills so as to minimize information security incident

3. Scope

This document is the capstone policy and is designed to cover the protection of any information that is created, processed, stored or transmitted in digital form during the normal course of Tanla's business and management of security thereof.

The scope of this policy includes:

The Information Security Management System covers all information, data and supporting IT and other assets pertaining to its service line operations including messaging, voice, including support functions like human resources, administration and IT operations. This is in accordance with the Statement of Applicability (SOA) version 1.0, dated 14/03/2018.

Services:

- Messaging services
- Voice services

Supported by:

- Business applications, supporting IT infrastructure, resources, services and facilities critically supporting the above-mentioned business operations.
- All users of the information assets of Tanla including, but not limited to employees, vendors, customers, business partners, and contractors.
- Data and information relating to the business of Tanla including but not limited to
  - Delivery to customers.
  - Intermediate work products relating to the above.
  - Internal to Tanla such as business workflow information/data
  - Personnel or human resources data.
  - System support and technical data.
  - And processed or stored in any form like data, text, images, sound, voice, codes, computer programs, software, and databases.

Locations covered:

Tanla Solutions Limited
CIN: L72200AP1995PlC021262
Tanla Technology Centre
Madhapur, Hyderabad
India - 500081

3.1 Scope exclusions

The following locations and category of information asset is not in the purview of ISMS.

- Functions not mentioned above.
- Branches/Offices not included in the scope above.
- Information processing facilities of its customers used to deliver services where the management control of the facility does not rest with Tanla.

4. Information Security Principles

Tanla as a global Telecom solutions provider provides key services to its customers using its unique combination of people, technology and processes. Tanla's clientele include mobile operators and is the preferred service provider for fortune 500 companies globally. As trusted partners, with over 100 customers in 32 countries Tanla seeks to enable enterprises and telcos to integrate complex communications into their applications & create and enhance value for their stakeholders. The dynamic business environment that Tanla operates in, continually introduces challenges in the protection of information assets. Maintaining the confidentiality, integrity of their businesses, applications, data, and processes is vital to the growth and success of Tanla.

Some of the business/ technical factors inherent in the environment are:

- Critical dependence on information systems including business and supporting applications associated IT components and network resources for service delivery.
- Increasing use of external networks and the Internet for providing services.
- Regulatory and compliance requirements.
- Growing vulnerability of computers and communications networks to security threats such as computer viruses, computer hacking, interception and denial of service attacks.
- Rapid changes in technology in use and the emergence of new technologies.

Risks to Tanla's Enterprise Information Resources

The following are some of the risks that could arise in the absence of an effective information security management system:

- compromise of confidentiality, integrity and availability of information essential to achieve business objectives;
- non-compliance with legal, contractual and regulatory requirements which bears potential consequences of lawsuits, fines, penalties etc.;
- dilution of customer confidence and damage to the brand and reputation of the company;
- inability to maintain competitive edge, profitability and brand value

As challenging as it may be, it is essential to safeguard information and information assets from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities.

Tanla's Information Security Philosophy

In consideration of the various factors outlined in the preceding paragraphs, Tanla's initiatives towards Information Security shall be guided by the following philosophy:

Tanla shall manage the protection of its information assets by establishing a risk based framework using reasonable, appropriate, practical and effective processes and technologies and people integrated into an effective Information Security Management System (ISMS) so as to enable Tanla to meet its contractual, applicable legal and regulatory requirements and its strategic objectives through the continual protection and management of its information assets.

The approach to development and management of such system shall be guided by global best practices, primarily the Code of Practice for Information Security Management laid down in the ISO/IEC 27001:2013. Such information security practices shall be reviewed continually to keep it aligned with the business requirements, changing technology landscape and the regulatory and compliance framework.

5. Management Commitment

The senior management of Tanla is committed to information security and governance and therefore undertakes to provide oversight, direction, support including necessary resources thereof. The intent and rigor of management commitment is also reflected in Tanla's organization of security that consists of various exclusive functions and roles charged with security responsibilities besides integrating information security roles and responsibilities in the Tanla organization structure.

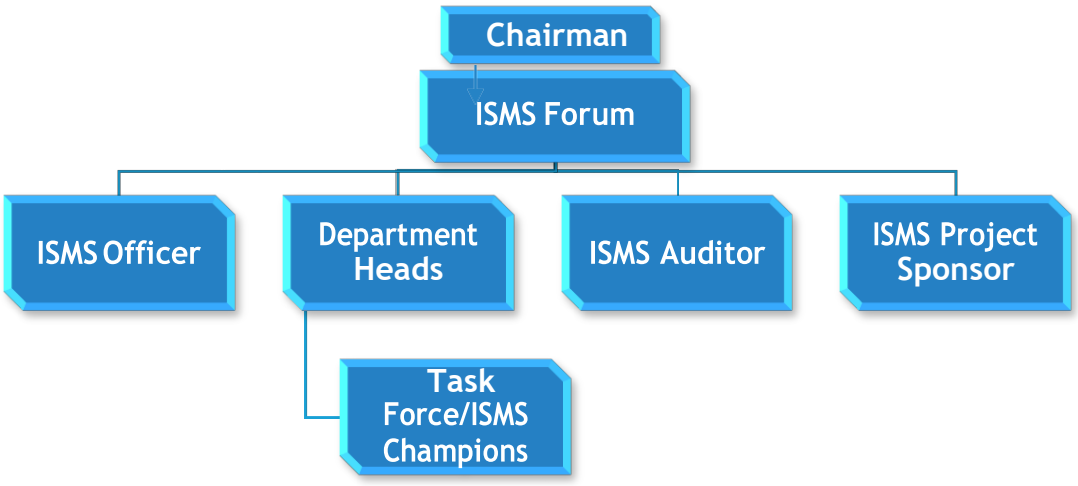
6. Information Security Organization

Recognizing the importance of information and the need for information security, Tanla's security organization structure has been conceived to ensure smooth integration of security responsibilities into its organization structure, while providing for

appropriate functions and roles to specifically focus on achievement of the security objectives.

Tanla is committed to ensuring that its information and the supporting information systems are protected from active threats. While a management framework exists to initiate and control the implementation of information security and information security policies within the organization, a multidisciplinary approach to information security is encouraged and each user of its information resources must ensure that their actions positively contribute to the promotion of information security.

The direction and overall governance oversight is entrusted to the ISMS Forum, who report to the Chairman and Managing Director. The ISMS Officer and the ISMS Task force are entrusted with the responsibilities of operationalizing and monitoring the security initiatives and policies and the department heads are responsible for ensuring security is implemented, effectively managed and monitored in their respective areas, supported and coordinated by the ISMS Champions. The internal audit of the ISMS would be performed by a team independent of the ISMS officer, either internal / external to Tanla. The ISMS organization structure for Tanla is defined based on the below structure. The responsibilities of each function are also described.



Role	Responsibilities
ISMS Forum - Chairman	♦ Ultimate sponsorship and responsibility for information security across the organization. ♦ Provide direction and endorse security strategy and objectives.
ISMS Forum	♦ Approve information security program, policies and processes aligned with business of Tanla and encourage continued improvement. ♦ Provide direction, support and oversight for information security initiatives. ♦ Ensure appropriate level of resource availability to the program. ♦ Support information security policy formulation, enforcement, and maintenance. ♦ Monitor and review the implementation of this IS Policy in ensuring an effective ISMS and provide oversight.
ISMS Officer	♦ Co-ordinate with business process owners and other stakeholders to operationalize, monitor, maintain and continuously improve the ISMS. ♦ Develop & maintain policies, procedures and standards. ♦ Monitor and report on compliance with ISMS.
ISMS Task Force	♦ Ensure timely identification of security technical and process dependencies and ensure timely implementation.
Department Representatives (Business Owners)	♦ Conduct periodic Information security trainings within departments. ♦ Continually ensure security requirements relating to department functions are identified, escalated for approval, implemented and monitored. ♦ Drive the adoption of ISMS within the respective

	teams of departments.
ISMS Champions	♦ Facilitate implementation of and adherence to information security policies and procedures. ♦ Continually support and educate department members on information security. ♦ Contribute towards improvement of information security.
ISMS Project Sponsor	♦ Supports and co-ordinates the ISMS investment requirements with the board and management ♦ Assists and helps in resolution of major issues. ♦ Conducts Forum meetings.
ISMS Auditor	♦ Audit the implementation of this policy. ♦ Challenge the design and operating effectiveness of security controls to ensure effective and efficient ISMS.

7. Approach to Information Security Management System

Tanla shall implement plans to support and achieve its information security objectives. Steps taken to achieve such objectives shall be documented. Tanla shall ensure to control planned changes, reduce the opportunity of unplanned changes and identify and control risks arising out of outsourced processes.

Tanla's ISMS is designed on the principle of building Information Security Management System while facilitating and supporting continual improvements.

The management review and internal audit procedure and the continual improvement Procedure specify the activities and the responsibilities for complying with these requirements.

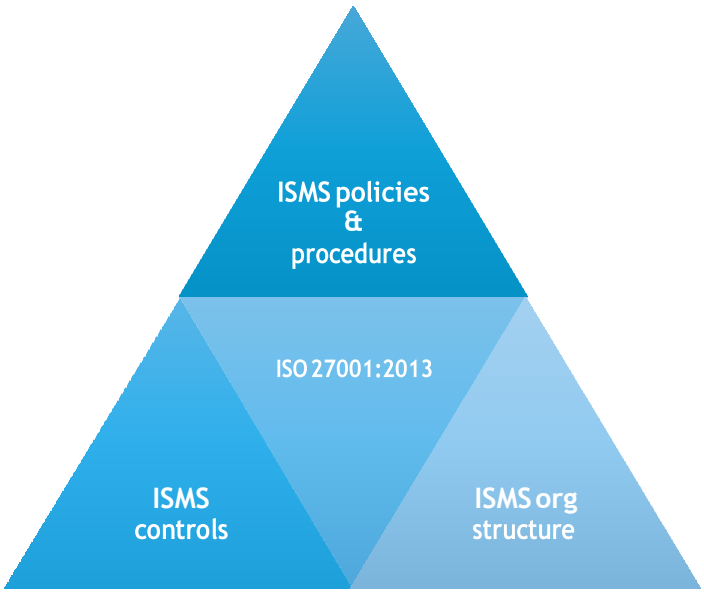
Integral to the ISMS, is the identification of applicable stakeholders and their expectations from Tanla. Tanla shall identify issues being faced and prioritize

stakeholder's needs and address information security risks directly impacting their expectations. Tanla shall plan actions to address such risks and identify opportunities for continual improvement. Risk assessments shall be performed on a periodic basis to ensure timely identification and evaluation of all emerging risks in the external and internal environment. In respect of risks that are found not within the acceptable risk appetite, suitable risk treatment plans shall be identified and effectively implemented in a timely manner. Reviews shall be performed to ensure that the controls implemented have been effective in reducing the risk to an acceptable level.

The end goal of protection is to minimize the number, duration and intensity of events that may affect Tanla's stakeholders and to minimize the damage incurred during any incident. The **Risk Management Policy and Procedure** outlines the methodology in greater detail.

8. Information Security Policies

Information Security Policy along with the supplementary domain-specific security policies are intended to provide a common basis for consistent, prudent protection and preservation of the confidentiality, integrity and availability of information assets. By putting in place and maintenance of the information security framework, the management of Tanla has established the direction towards, demonstrated support for, and commitment to, information security consistently across the organization.



The Information Security framework at Tanla consists of the Tanla **Information Security Policy**, which is the capstone policy and supported by supplementary policies and procedures in each of key information security domains, the security organization and management review, governance and audit mechanisms. The ISMS policies and standards are drawn in line with meeting the control objective and controls as prescribed by the ISO: IEC 27001:2013 Standard and the risk assessment. The ISMS policies and procedure ensure that the business operations of Tanla are secured and the impact of business interruptions, if any from internal and external events is minimized. The policies and procedures will be supported by required resources and technologies to achieve the desired objectives.

Tanla information security policies will undergo a standardized process of development, review and approval by persons with organizational responsibility for these functions so that the direction and support of management for information security is clearly established. The **Document Control Procedure** outlines the specifics for creation, maintenance and archival of documents.

Tanla shall set information security objectives for functions identified in the scope stated in this policy. Such objectives are derived from periodic risks assessments and compliance requirements, communicated to relevant stakeholders, measurable, and updated on a yearly basis. Tanla's IS objectives shall be documented and detail the action to be taken, responsibility for the action, the resources required and how the results shall be evaluated. Each ISMS procedure shall specify details to achieve Tanla's information system objectives that ultimately contribute to the high level objectives as stated in the **Annexure** given below.

Tanla shall monitor and measure the effectiveness of the Information Security Management System from time to time by conducting **Internal Audits** as stated in the **Management Review and Internal Audit procedure.** Such audits shall determine the conformity of Tanla's requirements for its ISMS.

Tanla's management shall review and provide feedback on the continual improvement and suitability of the ISMS, as detailed in the **Management Review and Internal Audit procedure.**

Tanla shall identify, fix and take action to prevent recurrence of nonconformities, documenting the actions. Nonconformities, when identified shall be dealt with as detailed in the **Continual Improvement Procedure**.

9. Maintenance & review of Information Security policies

The Tanla Information Security policy and supplementary domain specific policies shall be reviewed once a year and updated, as necessary, to be consistent with business needs, to factor for changes in the information security environment, emerging threats, and new technologies. Such policies should also be reviewed if significant changes occur

in the environment to ensure its continuing suitability, effectiveness and adequacy. The management review process ensures that reviews take place in response to any changes arising out of the latest risk assessment, significant security incidents, new vulnerabilities, and changes to organizational or technical infrastructure. The implementation of this policy should also be reviewed independently by the ISMS Internal Audit, to assess the status of compliance, and effectiveness of the policy.

10. Resources, competence, communication & awareness

Tanla shall provide adequate resources for the establishment, implementation, sustenance and continual improvement of the Information Security Management System.

Tanla shall ensure that persons identified to perform key information security activities shall be competent. Tanla shall provide training to improve the competence of personnel carrying out activities that affect the performance of information security requirements. Efforts taken to ensure the suitability of competence shall be documented and retained by Tanla.

All employees of Tanla and, where relevant, contractors and third party vendors shall be provided appropriate security awareness, training and regular updates in information security as relevant for their job function, to keep them aligned with organization security needs as detailed in the **Human Resource Policy**.

Tanla's internal and external stakeholders shall be communicated on the relevant aspects of ISMS at predetermined intervals. Information communicated shall include compliance obligations, security incidents, and interdepartmental communication. The frequency, concerned stakeholder, matter and mode of communication are detailed in the **ISMS Roles & Responsibilities, Competence and Communication** sheet.

11. Key policy requirements

11.1 Information Security roles and responsibilities

Tanla shall identify information security responsibilities which would be assigned to specific roles. The information security organization has been described earlier in Section 6. The project charter identifies the individuals assigned to these roles.

11.2 Segregation of duties

Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. Application access rights should be documented and mapped to all users based on the activities / duties performed by the users. System access to systems and functionalities should be provided on a need to have basis. The access rights provided to the users should be reviewed and monitored by the application owner on a periodic basis to assess any unwanted access rights and revoke the same. These shall be further elaborated in the **Access Control Policy**. Where segregation of duties is not possible, adequate compensating controls shall be implemented.

11.3 Contact with authorities

Tanla shall maintain appropriate contacts with relevant authorities for timely reporting and seeking support for managing information security incidents. To ensure business continuity and requirements for support for contingency planning process, Tanla would identify and maintain contacts with authorities such as the law enforcement, fire department, telecommunication providers, water suppliers etc. The ISMS officer /facilities manager are designated to initiate such contact whenever the need arises.

11.4 Contact with special interest groups

Tanla shall establish and maintain contacts with special interest groups or special security forums and professional associations to stay up to date and keep abreast with the relevant security requirements. This is essential to understand the emerging security threat scenarios and contemporary information security practices and to incorporate appropriate and timely improvements in Tanla's ISMS. This is also necessary to help Tanla to gain access to specialist information security advice and share and exchange information about new technologies, products, threats or vulnerabilities. The head IT and the ISMS officer shall initiate and maintain such contacts.

11.5 Information security in project management

Tanla shall ensure to specify and implement information security requirements when managing projects. Projects could be implementation of a new information system for managing the core business process, setting up of a new facility, introduction of new IT components. Tanla shall identify the information security objectives as relevant to new project, perform a risk assessment and take appropriate actions to manage such information security risks, ensure that information security is integrated in all the phases of the project.

11.6 Mobile device policy

The risks inherent in the use of **Mobile Computing devices** shall be managed based on the **Mobile Device Management Procedure** that identifies the risks and appropriate security measures that should be adopted to protect against the risks of mobile computing and communication facilities. Controls should be devised to

ensure that information security is not compromised while using mobile computing resources.

11.7 Human resource security

Security is only as strong as its weakest link and it has been observed that people are the weakest link. It is therefore imperative that the **Human Resource Information Security policy** be designed to ensure achievement of security objectives through the users – employees, non- employees who access Tanla's information processing facilities. Roles and responsibilities associated with security activities are identified, defined, documented and are appropriately assigned to designated Tanla members. Screening and awareness training for Tanla employees, third party users, contractors shall be done by Tanla. Terms and Conditions of employment contract shall be agreed to by Tanla employees & third party users, contractors. Security breaches committed shall be handled thru a formal disciplinary process. Termination responsibilities such as revoking access rights or removal of assets shall be defined clearly in the HR policy. Adequate Human Resource Information security controls encompassing the above shall be established, that seamlessly integrate with Tanla's human resource process and is detailed in the **Human Resource Information Security Policy.**

11.8 Asset management

1. Responsibility for assets

To achieve and maintain appropriate protection and safeguarding of the information assets, Tanla shall clearly identify and take inventory of its information assets. Owners for each asset or group of assets shall be identified and each asset shall be classified based on the importance of **Confidentiality**, **Integrity** and **Availability** of such information assets for performing the business operations. The

Risk Management Policy and related procedure provide stipulations for identifying, classifying and inventorying assets. Access to and use of the information resource shall be established in **the Access Control Policy** and **Acceptable Use Policy.** Return of assets upon role change and employee termination shall be covered in the **HR Policy and Procedure**.

2. Information classification

To ensure that the information receives the appropriate level of protection, it should be classified as per the norms defined in the **Document Control Procedure** or the **Risk Management Procedure** such classification should be guided by its value, legal requirements, sensitivity, and criticality. It should be the responsibility of the asset owner to define the classification of an asset, periodically review it, and ensure it is kept up to date and at the appropriate level. An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme. Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label (in the output). The labeling should reflect the classification according to the norms. Items for consideration include printed reports, screen displays, recorded media (e.g. tapes, disks, DVD/CD's), electronic messages, and file transfers. For each classification level, handling procedures including the secure processing, storage, transmission, declassification, and destruction should be defined. This should also include the procedures for chain of custody and logging of any security relevant event. Classification guidelines are given in the **Document Control Procedure and the Risk Management Procedure,** while the procedures for handling information according to its classification are detailed in the **Media Handling and Backup Policy and Procedure.**

3. Media handling

Tanla shall put in place appropriate **Media Handling and Back up Policy** and Procedures to protect documents, computer media, input/output data and system

documentation from unauthorized disclosure, modification, removal or destruction. Formal procedures shall be developed for the management of removable media, and for safe and secure disposal of assets when no longer required. Procedures shall also be established for the handling and storage of information to prevent unauthorized disclosure or misuse. System documentation shall be protected from unauthorized access.

11.9 Access control

---

1. Business requirements for access control

Controls shall be established to ensure that access to information, information processing facilities and business processes are based on business and security requirements. Access to Tanla's information resources shall be controlled based on the **Access Control Policy and procedures** thereof. Access control rules should take account of policies for information dissemination and authorization.

2. Network access control

Controls shall be designed and implemented to prevent unauthorized access to internal and external networked services as established in the **Network Security and Data Centre Management Policy** users shall be provided access to the services only upon specific authorization. The network access rights of users shall be maintained and updated as required by the **Access Control Policy**.

External or remote connections by users shall be secured using appropriate authentication methods. The selection of an appropriate authentication method shall be determined by a risk assessment.

To minimize the risk of unauthorized access to existing information systems that use Tanla network groups of information services, users and information systems shall be segregated on networks. The criteria for segregation of networks into

domains shall be in accordance with the requirements specified in the **Access Control Policy** based on access requirements.

Physical and logical access to diagnostic and configuration ports shall be controlled. Routing controls shall be implemented to ensure that computer connections and information do not breach the access control policy of the business applications.

3. User access management

To ensure authorized user access and to prevent unauthorized access to information systems, access rights to information systems shall be authorized, allocated and maintained in accordance with the **Access Control Policy**. Formal user registration and de-registration procedures shall be put in place to control the allocation of user rights to information systems and services. The procedure shall also address the authorization and control requirements for the allocation, use and the management of privilege accounts, passwords and the review of user access rights on a periodic basis.

4. User responsibilities

Users shall be informed of their responsibilities on the use of Tanla's information processing facilities through periodic training and other means. **Acceptable Use Policy** shall be defined stipulating these requirements including requirements for password use, protecting unattended user equipment and implementing clear desk and clear screen practices.

5. System and application access control

To prevent unauthorized access to information held in application systems, Tanla shall put in place appropriate controls to restrict the access to and within application systems. Restrictions to access information and application system

functions by users shall be based on individual business application requirements and in accordance with the requirements specified in the **Access Control Policy**.

Technical controls and secure log-on procedures shall be designed to minimize the opportunity for unauthorized access. Suitable authentication techniques shall be chosen for user identification and authentication. Security requirements will be factored through all stages in the systems life cycle as defined in the **Systems Development and Maintenance Policy**. Further, utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled. The source code of production systems will be secured through appropriate access control policies as per the requirements defined in the **Access Control Policy**.

11.10 Cryptography

Tanla shall implement appropriate cryptographic controls to protect the confidentiality, integrity, authentication of information which shall be detailed in the **Cryptographic Controls Procedure.** Protection and lifetime of cryptographic keys shall be clearly stated in the **Cryptographic Controls Procedure.**

11.11 Physical and environmental security

Tanla shall implement appropriate controls to minimize the risk of unauthorized physical access, damage or interference to Tanla's premises and information. Adequate security perimeters, entry controls, design of secure work areas, delivery areas shall be detailed in the **Physical & Environmental Controls Policy and Procedure**. All critical information processing facilities, utilities, and equipment shall be defined and controlled. Controls shall be implemented to minimize access to restricted areas, reduce risk of potential physical threat to information processing facilities. The access to Tanla premises and facility and its surrounding

environment shall be established in the **Physical & Environmental Controls Policy and Procedure**. Movement, maintenance, re-use and removal of equipment shall be clearly stated in the **Physical & Environmental Controls Policy and Procedure.**

11.12 Operations security

Tanla shall implement appropriate controls that ensure the correct and secure operations at the information processing facilities:

1. Operational procedures and responsibilities documented operating procedures

Tanla shall put in place documented operating procedures with defined roles and responsibilities for all system activities associated with information processing, communication facilities, which shall be made available to users on a need to know basis.

2. Change management

Tanla shall put in place a change management process to ensure that all changes to the information processing facilities, including equipment, supporting facilities and utilities, networks, application software, systems software and security devices are managed and controlled. Change management process shall be governed by the **IT Help Desk, Incident and Change Management Policy**. Tanla shall establish formal procedures for implementation, monitoring and recording of the changes to baselines.

3. Capacity management

Capacity management controls as defined in **Capacity Monitoring and Planning Procedure** shall be put in place to ensure Tanla's resources are monitored, tuned and projections are made to ensure system performance, to minimize the risk of systems failure and capacity related issues.

4. Separation of development, testing and operational environments

The systems development, test and production environments shall be identified and separated to reduce the risk of unauthorized access or changes to application on production environment and business data. Developers/support team will have restricted access to the production environment. The **Access Control Policy** and related procedure shall govern the security requirements in this regard.

5. Protection from malware

Tanla shall take adequate precautions and design appropriate controls to prevent and detect the introduction of malicious code and unauthorized mobile code, to protect the integrity of the software and information. Appropriate awareness programs and procedures shall be implemented. Corrective or recovery controls shall also be designed.

Anti-malware and security practices shall be in accordance with the **Malware Protection Policy**.

6. Backup

Back-up copies of information and software shall be taken and tested regularly to ensure availability of key data and information during an emergency. Appropriate recovery procedures shall be developed to ensure that critical information can be recovered in the event of damage to information resources.

Backup requirements shall be governed as per the **Media Handling and Backup Policy**. The policy shall specify that critical information residing on Tanla network shall be periodically backed up. The backup of data shall be tested for restoration on a regular basis or as a part of the DR drill plan on a periodic basis to ensure the effectiveness and integrity of backup.

Where confidential information is stored, the backups shall be protected suitably. The retention period for essential business information, and requirements for archive copies to be permanently retained shall be determined.

7. Logging and monitoring

Tanla shall devise and implement adequate monitoring controls to record events and generate evidence as detailed in the **Monitoring Policy**. The level of logging and monitoring required shall be determined by any relevant or applicable legal requirements to ensure that the monitoring activities comply with the requirements. Procedures for monitoring shall be established and results of such monitoring shall be reviewed periodically. User activity shall be logged and such audit logs shall be retained for a predefined period of time. Logs shall be protected from modification and or destruction. Privileged user activity shall be logged and reviewed. Faults shall also be logged and analyzed for corrective action to be taken. Clocks of all systems and devices shall be synchronized with an accurate time source.

8. Control of operational software

Tanla shall implement adequate controls on the installation of software on operational systems as documented in the **Desktop/laptop build procedure**, **Systems Development and Maintenance Policy and procedure.**

9. Technical vulnerability management

Tanla shall carry out periodic reviews to identify technical vulnerabilities in information systems, analyze risks and take appropriate measures to address identified risks. Tanla shall also implement rules to control the installation of software as detailed in the **Patch Management procedure**. Appropriate restrictions will be placed to prevent users from installing software as defined in the **Desktop/Laptop Build Procedure**.

10. Information systems audit considerations

Tanla shall devise appropriate controls to maximize the effectiveness of and to minimize the interference from/to the information system audit process. The

Management Review and Internal audit procedure shall detail the necessary controls to be implemented.

11.13 Communications security

1. Network security management

Tanla shall implement controls that ensure that adequate protection and safeguards of information in its network and the protection of the supporting utilities as defined in the **Network Security & Data Centre Management Policy.**

In this regard, the controls implemented should ensure that networks are adequately managed to protect against threats and to maintain security for the systems and applications using the network, including information in transit. Management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

2. Information transfer

Exchange of information and software within Tanla or with customers, regulators or any external party shall be secured in accordance with the regulatory requirements and stipulations. A formal exchange shall be developed that would govern the exchange of information and software. Where information is exchanged outside the premises of Tanla, using a removable media, adequate controls shall be exercised. The exchange of information shall be in accordance with the **Information Exchange and Electronic Messaging Policy.**

Internet and electronic messaging including email and instant messaging and interconnection of business information systems shall also be governed by the above.

Requirements for confidentiality or non-disclosure of information shall be identified, reviewed and documented in the contracts with third parties.

11.14 System acquisition, development and maintenance

The design and implementation of the information system supporting the business process is crucial for security. Such security requirements shall be identified and agreed prior to development and or implementation of the information systems. The security in acquisition, development and maintenance of information systems shall be governed by the **Systems Development and Maintenance Policy and procedures** thereof. Such policy and procedures shall include, among others criteria and stipulations as regards security requirement of information systems, security in development and support processes, Changes to operational systems shall be governed by the **IT Helpdesk, Incident and Change Management Policy and procedure.**

Information about the technical vulnerabilities of information systems being used shall be obtained on a timely basis and Tanla's exposure to such vulnerabilities shall be evaluated and appropriate measures and controls shall be implemented to address the associated risks. These requirements will be defined in the **Network Security and Data Centre Management Policy** and procedures.

11.15 Supplier relationships

Appropriate requirements for controlling risks with supplier's access to Tanla's risks shall be agreed with each supplier and documented. Such information security requirements shall be addressed suitably in agreements with suppliers. Tanla shall list down procedures for supplier relationships in the **Vendor Relationship Policy and procedure policy/procedure**.

11.16 Information security incident management

It shall be ensured that information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. Individuals, including external parties observing or suspecting any information security breach shall be required to report such events. The **IT Helpdesk Incident and Change Management Policy** shall govern the manner of incident security reporting and management consistently and effectively. Mechanisms shall be in place for learning from such security related events and the collection of evidence thereto.

11.17 Information security aspects of business continuity management

1. Information security aspects of business continuity management

Tanla shall implement controls to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. A business continuity management process shall be implemented in Tanla to ensure that impact of disasters are minimized and reduce and recover from loss of information assets and security failures to an acceptable level through a combination of preventive and recovery controls. In this regard:

a) Tanla shall develop and maintain **Business Continuity Management Policy** applicable throughout the organization and shall include procedures for disaster recovery. The policy and procedure documents shall address the relevant information security requirements.

b) Business impact analysis shall be performed to identify, quantify and prioritize risks, including critical resources, impacts of disruptions, allowable outage times and recovery priorities.

c) Disaster recovery plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes. The recovery procedures should take into account the business objectives and the critical business processes that require immediate restoration. The plans shall clearly describe the roles and responsibilities of individuals and teams required for implementation of the business continuity procedures. The plans shall be tested periodically to ensure that critical business functions are recovered according to the plan. The business continuity plans shall be tested regularly to ensure they are up to date and effective.

2. Redundancies

a) Tanla shall take appropriate steps to ensure continued availability of critical resources required for business operations.

11.18 Compliance

Tanla shall devise appropriate controls to ensure that it complies with the rules, laws, and statutory requirements in order to avoid breaches of such regulatory and contractual obligations.

a) All relevant statutory, regulatory, and contractual requirements and Tanla's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.

b) Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products. Such requirements shall be governed by the Legal and **Contractual Compliance Policy.**

c) All important records and critical data or information shall be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

d) Appropriate controls shall be defined to protect data and ensure privacy of personal information as required in relevant legislation, regulations and in applicable contractual clauses.

e) Management shall authorize the use of IT facility for business purposes and controls shall be applied to prevent the misuse of such facilities. Any use of the information processing facilities for non-business purposes without management approval or for any unauthorized purposes shall be regarded as improper use of the facilities.

f) Management shall ensure that the use of cryptographic controls is in compliance with applicable laws and regulations.

g) To ensure compliance of systems with information security policies and procedures, managers should ensure that security procedures are carried out within their areas of responsibility. This will be addressed in the **Human Resource Security Policy**. Besides the technical compliance of information systems shall be regularly checked as detailed in the **Network Security and Data Centre Management Policy** and the **Systems Development and Maintenance Policy**.

h) To maximize the effectiveness of and to minimize the interference from/to the information system audit process, the **Management Review and Internal Audit Procedure** shall detail the necessary controls to be implemented.

12. Exception

The information security policy is applicable to all areas as defined in the scope. An exception can be claimed through the policy exception process in situations that cannot be addressed because of procedural, technical or policy limitations defined under this section.

Exceptions shall be documented in the **Exception Handling Form** embedded and presented to the ISMS Forum for approval. Management of risks arising out of the exception proposed shall be justified in the form.

13. Conformance

It is the responsibility of the intended audience viz. is the board, management, staff members of Tanla, contract personnel and authorized partners, to comply with the requirements of information security policy and related documents.

Failure to comply with or willful breach of information security policies shall be viewed seriously and may result in one or more of resulting steps being taken in line with the **Code of Conduct and Disciplinary process**, that may constitute, but not limited to, one of more the following:

- disciplinary measures as per the disciplinary process including complete or partial loss of employment consideration and benefits, termination of employment or service agreement(s);
- proceedings under civil and/or criminal law and/or recovery of damages;
- all necessary legitimate actions that is essential to protecting the interests of Tanla and its stakeholders including legal action, financial damages and penalties

14. Glossary

Particulars	Description
Capstone	Provides the leading guidance for the set of operational policies which provide detailed requirements related to specific security subjects such as Password policy, Antivirus policy etc.
Control	A mechanism or procedure implemented to mitigate a risk.

Control objective	A statement of intent with respect to control over securing an organization's resources.
Risk assessment	The process of identifying security risks and determining their Potential impact.
Policy	An information security policy consists of high level statements relating to the protection of information across the business and should be produced by senior management.
Standard	Standards consist of specific low level mandatory controls that help enforce and support the information security policy.
Procedure	Procedures consist of step by step instructions to assist users in implementing the various policies, standards and guidelines.
Guideline	Guidelines consist of recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place.
Availability	The property of being accessible and usable upon demand by an authorized entity.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, etc.
Information security	Preservation of confidentiality, integrity and availability of information, in addition other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.
Information security management	Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

system	
Integrity	The property of safeguarding the accuracy and completeness of assets.
Residual risk	The risk remaining after risk treatment.
Risk evaluation	The process of estimating the estimating risk with the given risk criteria to determine the significance of risk.
Asset	Anything that has value to the organization.
Information security event	An identified occurrence of a system, service or network state indicating a possible breach of information. security policy or failure of safeguards, or a previously unknown situation that may be security relevant
Information security incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Risk management	Coordinated activities to direct and control an organization with regard to risk.
Risk analysis	Systematic use of information to identify sources and to estimate the risk.

Appendix A

The list of ISMS policies is given below:

S.No	Policy	Policy Name
1	Information Security	**A01** Information Security Policy
2	Risk Management	**A02** ISMS Risk Management Policy
3	Human Resource	**A03** Human Resource security Policy
4	Access Control	**A04** Access Control Policy
5	Malware Protection	**A05** Malware Protection Policy
6	Backup and Media Handling	**A06** Media Handling and Back up Policy
7	Information and Electronic Messaging	**A07** Information Exchange and Electronic Messaging Policy
8	Monitoring	**A08** Monitoring Policy
9	Acceptable Use	**A09** Acceptable Usage Policy
10	Physical and Environmental Security	**A10** Physical and Environmental Controls Policy
11	IT Helpdesk Incident and change Management	**A11** IT Helpdesk, Incident and change Management Policy
12	Network Management	**A12** Network Security & Data Centre Management
13	Business Continuity	**A13** Business Continuity & Disaster Recovery Management Policy
14	Regulatory, Legal and Compliance	**A14** Legal, Regulatory and Contractual Policy

15	Systems Acquisition and Development	**A15** Systems Development and Maintenance Policy
16	Vendor Management	**A16** Vendor Management Policy
17	Privacy	**A17** Privacy Policy