TATA STEEL

TATA

Information Security Sustenance Policy

- TSL has instituted a comprehensive set of Information Security Policies and Procedure to protect the confidentiality, integrity and availability of its information assets.
- In order to ensure that policy deployment and implementation stays consistent with planned outcomes, TSL shall establish a sustenance, audit and a compliance mechanism to ensure continual improvement of ISMS takes place.
- In order to achieve the said objectives, Points of Audit, Evidences and Metrics shall be defined in every policy document to cover all the domains of ISMS. These shall be reviewed to ensure that they stay relevant and consistent with business requirement and contribute towards the compliance so desired.
- The policy covers the following areas
  - Audit
  - Sustenance
  - Compliance

Audit

- The Internal Audit Team under the Corporate Audit function shall be responsible for conducting audits as per the published schedule every year in coordination with the CISO.
- External audits shall be conducted if the organization seeks to be certified and wishes to bring an independent review.
- The audit approach could be by way of a desktop review and or process review.
- All new facilities of TSL which manage information shall also be audited post them getting commissioned.
- Those involved in implementation shall not be allowed to conduct the audit.
- Independence of an auditor shall be ensured in any audit activity.

Sustenance

- Sustenance shall be done at a business level by the BISO and functionaries below.
- Sustenance activities shall involve all the activities as mandated by the metrics which have been developed, participation in information security initiatives, audits and activities as an outcome of the corrective and preventive action plans.

Compliance

- Compliance at the corporate level shall be ensured by the CISO as per the outcome of the audit, ensuring implementation effectiveness through the controls deployed and submissions towards regulatory requirements if any.
- Compliance at a business level shall be the responsibility of the BISO through the Positive Assurance Report mechanism.
- Use or creation of Intellectual Property within TSL shall be in accordance to the regulatory and legislative norms.
- Appropriate mechanisms shall be developed for protecting privacy of employees within TSL.
- Use of approved and licensed tools shall be necessary for the purpose of conducting audits, monitoring of implementation and sustenance activities and ensuring compliance in accordance within the regulatory landscape.
- Dashboards, reports and corrective and preventive action plans shall be deployed as means of communication to the Apex Committee and to the rest of the employees on a need to know basis.
- The CISO shall be responsible for defining the periodicity of audit, monitoring and review of metrices to ensure their relevance and adequacy; and submission of Compliance Reports to the Apex Committee.
- Any exception to this policy shall be managed by a formal process.

Date : November 1, 2017

T V Narendran
CEO & Managing Director