Information Security Policy

1.0 Introduction

Triveni Turbine Limited (TTL) is committed to orderly and efficient service delivery through the strict adherence to the policies and practices. TTL has established& organized risk-based information security governance framework to ensure constant monitoring, reviewing, exception reporting and taking actions thereon for improving effectiveness of information security management system.

The Information Security Policy (ISP) of TTL is applicable to all information assets of the Company and our stakeholders. The Information Security Policy is applicable to all employees and third parties of TTL. The Head of IT shall be responsible for maintaining and updating of the Information Security Policy.

2.0 Objectives

It is the policy of TTL that its information assets be protected from all types of threat, whether internal or external, deliberate or accidental, such that:

- personal information of all stakeholders is protected,
- confidentiality of information is maintained,
- integrity of information can be relied upon,
- information is available when required,
- access to information assets is granted only for justified business needs,
- reputation of Triveni Turbine is protected and
- all statutory, regulatory and contractual obligations are met

3.0 Controls

Operations security controls deployed to ensure these objectives, inter alia, are:

- access controls for users to their IT assets and network assets of Triveni Turbine
- controls on 3rd party service delivery management
- separation of development, test and operational facilities to achieve segregation of the roles involved
- monitoring and projection of processing and storage capacity requirements
- risk-based back-up, restore and disaster recovery strategy

TRIVENI TURBINE LIMITED
12-A, Peenya Industrial Area, Bangalore 560 058, India. Tel: +91-80-2216 4000 Fax: +91-80-2216 4100 Website: www.triveniturbines.com
Regd. Off: A-44, Hosiery Complex, Phase-II Extn., NOIDA 201 305, Uttar Pradesh
CIN: L29110UP1995PLC041834

- security controls on in-house data centres
- control on exchange of information and software between TTL and other stakeholders
- controls and solutions to safeguard confidentiality and integrity of data passing over public networks and to protect the connected systems
- controls against computer virus and malicious code
- controls against malicious software and appropriate user awareness procedures
- risks to current information security landscape shall be identified and recorded in Enterprise Risk Management (ERM) Register for further treatment of the risk
- the Information Security Policy shall be the basis for compliance audits and security risk analysis
- any exception to the controls outlined are evaluated and approved by CEO, after consultation with Head – Digitalization
- Data input controls on the application systems to validate and ensure that data is correct and appropriate.
- Checks to be applied to the inputs of business transactions, standing data (names and addresses, credit limits, customer reference numbers) and parameter tables (sales prices, currency conversion rates, tax rates)
- To ensure that IT Projects and support activities are conducted in a secure manner, Access to system files should be controlled. Maintaining system integrity should be the responsibility of the user function or development group to whom the application system or software belong.
- The use of operational databases containing personal information is forbidden.
- The software used on the system of Triveni, is the legal property of the company. They must be accompanied with appropriate licenses.

4.0 Information Security & Incident Management

In order to minimize damage from security incidents and malfunctions, security incidents are reported to the direct management and to the Head – IT at the earliest. Also all users are are advised against any attempt to prove a suspected weakness. Users are also required not to attempt removing any suspected software, unless authorized to do so. The impacted asset shall be isolated completely from the network and the appropriate action taken immediately.

5.0 Compliance

Compliance with legal requirements is ensured by avoiding any breaches of civil law, statutory, regulatory or contractual obligations and of any security requirements. The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements. Advice on specific legal requirements is sought from the organization's legal advisers, or suitably qualified legal practitioners.

All applications, software are used with an up-to-date license. It is forbidden to use unlicensed software on the Information system of the Triveni. Compliance with data protection and privacy legislations of respective country of operation are followed.

Compliance with security policies and technical compliance is ensured and regularly reviewed. Information systems should be audited for compliance with security implementation standards.

Managers of Triveni Turbine ensure that all security procedures within their area of responsibility are carried out correctly. Information systems are regularly checked for compliance with security implementation standards (e.g. Windows with security patch). Any technical compliance check is carried out by, or under the supervision of, competent and authorized persons (e.g. Specialized Control Company or IS consultants).

***