
INFORMATION SECURITY AND DATA PRIVACY POLICY

1. Objective:

To provide a framework and guidelines to manage and mitigate Information security risks, to establish guideline and procedures to safeguard our organization, individual's data and system. To safeguard information assets from unauthorized access, to protect individual's personal information.

2. Scope

This policy applies to every employee, suppliers, vendors, partners and or individuals with access to Company's IT systems, information and/or hardware of M/s TTK Prestige Limited.

The Information security policy is published to all people who are employees of the organization, suppliers, customers and anyone who has temporary / permanent access to our systems.

3. Company Policy:

a. Protection to IT Systems, Software, Hardware of the company:

- i. Protect company's IT Systems, Software, Hardware using strong credentials
- ii. Ensure upgrade of anti-virus software from time to time
- iii. Ensure timely patching for Endpoints and Servers
- iv. Carry out physical inventory of all IT assets once in a year
- v. Maintain asset register, add, change, delete the assets wherever applicable with respect to the applicable processes
- vi. Allow only company assets to connect to company network
- vii. Ensure company network access given to external people with due verification / Approval and limited access to the extent of permitting internet.
- viii. Enable Multi factor authentication wherever necessary

b. Protection to Internal, vendor and customer data:

- i. Protect the organisation data using least access privilege principle
- ii. Data access through user log in credentials and password authentications
- iii. Regular Data back up with specific schedules
- iv. Upgrade patches to all applications and endpoints
- v. Scan the network with appropriate tool, identify anomalies and act
- vi. Categorize the risks, mitigate timely through remedial actions
- vii. Maintain agreements and SLA with Software application partners for regular upgrade of the SaaS software.
- viii. Enable MFA authentication wherever necessary.

c. Policy on data privacy

- i. Establish roles and responsibilities. Extend only the required access to perform the activities as per the least access privilege principles.
-

-
- ii. Segregate the duties in three categories like Create, Change and display
 - iii. Establish data retention and safe disposal using archiving tools wherever required, appropriately.

4. Audit of Information Security and Data Privacy Policy

The security audit of TTK Prestige Information Security and Data Privacy Policy shall be conducted periodically by an organization approved Person.

5. Communication

A current version of the policy shall be made available to all required staff using IT assets via email or portal.

6. Review

IT Head will review this policy on an annual basis or following a significant incident or organisational / technical change.
