TRANSLINE TECHNOLOGIES LIMITED

CIN: U72900DL2001PLC109496

Registered Office: 23A, 3rd Floor, Shivaji Marg, New Delhi 110015

INFORMATION TECHNOLOGY POLICY

[Adopted on 30.09.2024]

1. Purpose

The purpose of this IT Policy is to establish clear guidelines and best practices to ensure that the information technology infrastructure, systems, and data of **Transline Technologies Limited** are used effectively, securely, and ethically. This policy aims to protect the organization's IT resources, ensure compliance with relevant regulations, and promote a safe and productive working environment.

2. Scope

This IT Policy applies to all employees, contractors, consultants, and third-party service providers who use or access the company's IT resources, including but not limited to:

- Computers, laptops, and mobile devices
- Network and communication systems (email, internet, intranet, etc.)
- Software applications, both proprietary and third-party
- Cloud services, storage, and data management systems
- Data and information assets
- IT infrastructure (servers, routers, etc.)

3. IT Resources Usage

- **Authorized Use:** All IT resources should be used for work-related purposes only. Personal use of IT resources is discouraged and should be kept to a minimum.
- **Prohibited Activities:** The following activities are strictly prohibited:
    - Unauthorized access to sensitive data or company systems
    - Downloading, installing, or using unlicensed software
    - Attempting to bypass security protocols (e.g., firewalls, passwords)
    - Use of company systems for illegal activities or any activity that could harm the reputation of the company
    - Using IT resources for personal gain, commercial ventures, or any non-business-related activity

4. Security and Data Protection

- **Data Security:** All employees must take appropriate measures to protect company data from unauthorized access, modification, destruction, or loss. This includes safeguarding sensitive information such as client data, financial records, and intellectual property.
- **Passwords and Authentication:**
    - Employees must use strong, unique passwords for all company systems and change them regularly.
    - Two-factor authentication (2FA) should be enabled on systems that support it, especially for accessing critical systems or data.

- **Encryption:** Sensitive data should be encrypted during transmission and when stored on company devices or servers.
- **Backup:** Regular backups of critical data should be conducted and stored in secure, off-site or cloud locations.

5. Network and Internet Use

- **Internet Access:** Access to the Internet is provided for business purposes. Personal use should be minimal and should not interfere with productivity or network security.
- **Network Security:** All devices connected to the company network must be equipped with approved security software (e.g., antivirus, firewall). Unauthorized devices may not be allowed to connect to the network.
- **VPN Usage:** Remote access to company systems should be done via the company's Virtual Private Network (VPN) to ensure secure communications and data transfers.

6. Software and Hardware

- **Software Installation:** Only authorized personnel may install or upgrade software on company systems. Unauthorized software installations are prohibited to avoid potential security vulnerabilities or software incompatibility.
- **Hardware Maintenance:** Employees must ensure the proper care of company-owned hardware and report any malfunctions or damage immediately to the IT department for maintenance or repair.
- **Bring Your Own Device (BYOD):** If the company allows BYOD, employees must comply with company security protocols for personal devices used for work purposes, including the installation of security software and ensuring devices are password protected.

7. Email and Communication

- **Email Use:** Company-provided email accounts should be used primarily for business purposes. Employees should avoid using company email accounts for personal correspondence or to subscribe to non-business-related mailing lists.
- **Spam and Phishing Protection:** Employees should be cautious when receiving unsolicited emails and avoid clicking on suspicious links or opening attachments from unknown sources. Phishing attacks should be reported immediately to the IT department.
- **Confidentiality:** Sensitive or confidential information should not be sent via email unless encrypted. Employees should ensure that all communications adhere to company confidentiality policies.

8. IT Support and Helpdesk

- **Support Requests:** Employees experiencing IT issues should contact the IT support/helpdesk for assistance. The IT department is responsible for diagnosing and resolving system problems, as well as ensuring that IT resources are functioning properly.
- **Incident Reporting:** Any incidents related to IT security breaches, data loss, system malfunctions, or other critical issues should be immediately reported to the IT department for investigation and resolution.

9. Compliance with Laws and Regulations

- **Legal Compliance:** All employees must comply with applicable local, national, and international laws, including data protection regulations, intellectual property laws, and industry-specific standards.
- **Data Privacy:** Personal data must be processed and protected in accordance with relevant data protection laws (e.g., GDPR, CCPA). Employees are required to ensure that data handling, storage, and sharing practices adhere to these laws.

10. IT Policy Violations

Violations of this IT policy may result in disciplinary action, including suspension, termination of employment, or legal action, depending on the severity of the violation. Examples of violations include, but are not limited to:

- Unauthorized access to systems or data
- Use of unlicensed software or pirated content
- Breach of security protocols (e.g., sharing passwords, disabling security software)
- Sharing or disseminating sensitive information without proper authorization

11. Policy Review and Updates

This IT Policy will be reviewed on an annual basis to ensure that it remains up-to-date with current industry standards, legal requirements, and technological developments. Any changes to the policy will be communicated to employees promptly.

12. Acknowledgment

By accessing the company's IT resources, employees agree to abide by the terms and conditions set forth in this policy. Any questions or clarifications regarding the policy should be directed to the IT department.