2026

COMPANY POLICY DOCUMENT

ISO 9001:2015 Certified
Certified by TÜV SÜD South Asia Pvt Ltd
Cert. No. 99 100 25410

Pratham®
PRATHAM TRANSOLUTIONS (I) PVT LTD
Western Gateway. Global Trust.

D1007-1008, West Gate, Near YMCA Club, Makarba,
Ahmedabad, Gujarat - 380051

+91 9512027754

hr@theptpl.com
info@theptpl.com

PRATHAM TRANSOLUTIONS (I) PVT LTD
Western Gateway. Global Trust.

ISO 9001:2015 Certified
Certified by TÜV SÜD South Asia Pvt Ltd
Cert. No. 99 100 25410

Policy Name – IT Policy

Index :

Policy Name – **IT Policy**

Purpose of Policy

The purpose of this policy is to ensure the secure, efficient, and responsible use of the company's IT resources. It is designed to protect company data, maintain system integrity, and prevent misuse of technology. This policy also supports compliance with applicable Indian laws related to data protection and cybersecurity.

Scope of the Policy

This policy applies to all employees and any individuals who use company IT resources. It covers all devices, systems, networks, servers, and data used within office premises as well as remote working environments.

IT Asset Procurement & Approval

All IT equipment such as computers, laptops, and related devices must be purchased only through authorized vendors approved by the company. The requirement for such equipment must be identified by the reporting manager based on business needs. Final approval for procurement will be provided by the Directors to ensure proper control over cost and standardization.

Acceptable Use of IT Resources

Company IT resources including computers, internet, and email must be used primarily for official work. Limited personal use may be permitted only if it does not impact productivity or system security. Employees must not use company systems for illegal activities, personal business, or accessing inappropriate or harmful content.

Wi-Fi and Network Usage

Employees are required to use only the company's secured Wi-Fi network within office premises. Personal Wi-Fi connections are not permitted. Wi-Fi credentials must not be shared without authorization. In case of network downtime exceeding one hour, employees may use mobile hotspot only after obtaining approval from their reporting manager. All network usage may be monitored for security purposes.

Information & Data Protection

All company data is confidential and must be handled with strict care. Employees are not allowed to share company data with any external party without proper authorization. Data must be stored only on company-approved systems such as servers or secured platforms. Unauthorized storage on personal devices is strictly prohibited. Any breach of data confidentiality may result in serious disciplinary action, including termination.

Password & Access Management

Employees must maintain strong and secure passwords for all systems. Passwords should not be shared with anyone, including colleagues. The company follows a mandatory password change policy every six months. Access to systems and data will be provided based on job roles and will be revoked immediately upon role change or exit.

Cybersecurity & Anti-Virus

All systems must have updated antivirus software installed and maintained at all times. Regular updates, security patches, and system scans must be ensured by the IT team. Employees should avoid installing unauthorized software and must be cautious while opening emails, links, or attachments from unknown sources to prevent cyber threats.

Policy Name – **IT Policy**

Hardware Maintenance

The IT team is responsible for ensuring that all hardware is properly maintained and serviced regularly. Employees must handle company equipment responsibly. In case of any hardware issue or failure, the IT team must first ensure data protection before proceeding with repair. If the issue cannot be resolved, the hardware must be replaced.

Data Backup & Server Usage

All employees must store their work on the company server or approved systems. Storing official data on personal laptops, mobile devices, or external drives is not allowed. Regular data backups must be maintained to prevent loss of critical business information.

Remote Work & Device Usage

Employees working remotely must follow the same IT security standards as in the office. Access to company systems should be done through secure methods as defined by the IT team. Use of personal devices for company work should be limited and must comply with security guidelines.

Email & Communication Usage

Official email must be used in a professional and responsible manner. Employees should not send confidential information without authorization. Suspicious emails, phishing attempts, or unknown attachments must be reported immediately to the IT team.

Incident Reporting

Any IT-related issue such as system failure, data breach, hacking attempt, or suspicious activity must be reported immediately to the IT team or reporting manager. Timely reporting helps in minimizing risks and preventing further damage.

Monitoring & Privacy

The company reserves the right to monitor usage of IT systems, including internet activity and emails, to ensure compliance and security. Such monitoring will be conducted responsibly and only for official purposes.

Hardware Scrap & Disposal

When hardware reaches the end of its lifecycle or becomes unusable, it must be handed over to the IT team. Before disposal, all data must be permanently erased. The equipment will then be disposed of through authorized scrap vendors.

Non-Compliance & Disciplinary Action

Any violation of this policy will be treated seriously. Depending on the severity of the violation, disciplinary action may include warning, suspension, or termination of employment.

Policy Name – IT Policy

Conclusion

This IT Policy is established to ensure that all technology resources within the organization are used in a secure, responsible, and efficient manner.

Every employee plays a crucial role in safeguarding company information and preventing misuse of IT systems. Adherence to this policy not only supports smooth business operations but also helps the organization stay compliant with applicable Indian laws.

All employees are expected to understand and follow this policy at all times. Responsible use of IT resources will contribute to overall productivity, data security, and the long-term success of the organization.

Approval & Acknowledgement

This Policy is approved and issued under the authority of the Director, Pratham Transolutions India Pvt. Ltd.

Date	Description of Change	Approved By
01.10.2025	**Initial Issue**	**Tushar Gorasiya (Director)**

Tushar Gorasiya
Founder & Director