

IT, Device and Acceptable Use Policy

Version 1.0 · Effective 21 October 2026

1. Purpose and scope

1.1 This policy explains how interns at TrackMy Tech Private Limited (“TrackMy Tech”, the “Company”, “we”, “us” or “our”) must use Company systems, accounts, devices and data. Its aim is to protect the Company, our clients, and you.

1.2 This policy applies to all interns, whether paid or unpaid, and whether working remotely, on-site or in a hybrid arrangement. It covers any device you use for Company work, whether owned by the Company or by you.

1.3 This policy should be read with the Internship Policy and Terms of Engagement, the Intern Code of Conduct, the Confidentiality and Non-Disclosure Agreement, the Intellectual Property Assignment and the Intern and Candidate Privacy Notice.

2. Definitions

In this policy:

- **“Company Systems”** means all accounts, email, chat, cloud services, code repositories, servers, databases, software, networks and devices provided, managed or paid for by the Company.
- **“Company Account”** means any account created or provided for you by the Company, including your Company email address.
- **“Personal Device”** means any laptop, computer, phone or tablet owned by you that you use for Company work.
- **“Company Data”** means any information you access, receive or create in the course of your internship, including source code, designs, documents, credentials and business information.
- **“Client Data”** means any information belonging to or about a client of the Company, or about the client’s users or customers, including Personal Data.
- **“Personal Data”** has the meaning given in the Digital Personal Data Protection Act, 2023, and means any data about an individual who can be identified by or in relation to that data.
- **“Security Incident”** means any actual or suspected loss, theft, unauthorised access, disclosure, alteration or misuse of Company Systems, Company Data or Client Data, including a lost device, a leaked password or a suspicious login.

- **“Security Contact”** means the Company’s security contact at admin@trackmytech.in.

3. Accounts and passwords

3.1 Use only the Company Accounts issued to you, and only for Company work. Do not share your accounts, and do not use anyone else’s.

3.2 Use a strong, unique password for each Company Account, at least 12 characters long. Do not reuse passwords from personal accounts.

3.3 Store passwords only in a password manager approved by the Company, as notified by the Company in writing. Do not write passwords down, send them in chat or email, or store them in code.

3.4 Turn on two-factor authentication wherever it is available on Company Accounts and on any personal account (such as a personal GitHub account) that is given access to Company Systems.

3.5 Do not try to access any system, file or data that you have not been given permission to access, even if it is technically reachable.

3.6 If you think a password or account has been exposed, change it immediately and report it as a Security Incident under clause 9.

4. Devices

4.1 **Company devices.** If the Company gives you a device, use it mainly for Company work, keep it secure, do not let others use it, and do not remove or disable security software installed on it. Return it when asked or at the end of your internship.

4.2 **Personal Devices.** If you use a Personal Device for Company work, you must:

- (a) keep the operating system, browser and software up to date;
- (b) use a screen lock with a PIN, password or biometric, and lock the screen when you step away;
- (c) enable full-disk encryption where your device supports it;
- (d) run reputable anti-malware protection where appropriate for your operating system;
- (e) avoid installing pirated or untrusted software; and
- (f) keep Company Data in Company Systems rather than on the device, as far as practical.

4.3 Avoid using public or shared computers for Company work. On public Wi-Fi, use only secure (HTTPS) connections and, if provided, the Company VPN.

4.4 If a device used for Company work is lost or stolen, report it immediately as a Security Incident.

5. Code and repositories

5.1 Company source code must be stored only in repositories hosted in the Company’s GitHub organisation.

5.2 Do not copy Company code to personal repositories, public repositories, public gists, code-sharing sites or personal cloud storage.

5.3 Never commit secrets such as passwords, API keys, tokens, private keys or environment files to any repository. If you commit a secret by mistake, do not try to hide it; report it immediately as a Security Incident so the secret can be rotated.

5.4 Follow the team's branching, code review and deployment process. Do not push directly to protected branches or deploy to production unless you have been authorised to do so.

5.5 Do not add third-party code, libraries or assets to Company projects unless their licence allows it and your Supervisor has approved it.

5.6 Ownership of code and other work you create is governed by the Intellectual Property Assignment.

6. Client data and personal data

6.1 Access Client Data and Personal Data only when it is needed for a task you have been assigned, and only to the extent needed.

6.2 Do not copy, download, export, screenshot, print or forward Client Data or Personal Data unless your Supervisor has approved it for a specific task.

6.3 Use test or anonymised data for development and testing wherever possible. Do not use real production data on your Personal Device unless you have been specifically authorised.

6.4 Do not share Client Data with anyone outside the Company, or with Colleagues who do not need it.

6.5 Delete working copies of Client Data when the task is complete, as directed by your Supervisor.

6.6 Your confidentiality obligations are set out in the Confidentiality and Non-Disclosure Agreement. How the Company handles your own personal data is explained in the Intern and Candidate Privacy Notice.

7. AI tools

7.1 You may use AI tools (such as code assistants and chat assistants) for Company work only if they are approved by the Company, as notified by the Company in writing, and only in the ways described in this clause.

7.2 You must not enter into any AI tool that is not approved for the purpose:

- (a) Client Data or Personal Data;
- (b) passwords, keys, tokens or other secrets;
- (c) confidential Company information, including unreleased product plans; or
- (d) Company source code, unless the tool and the account type have been approved for code.

7.3 You are responsible for any output you use. Review AI-generated code and content carefully for accuracy, security problems and licence issues before you submit it, and do not present it as checked if you have not checked it.

7.4 Tell your Supervisor when a significant part of a deliverable was produced with an AI tool, if they ask or if the client has restrictions on AI use.

7.5 Some clients may prohibit or restrict AI tools on their projects. Client rules take priority over this clause.

8. Acceptable use

8.1 You must not use Company Systems or your Company work to:

- (a) access, store or share illegal, obscene, hateful or harassing material;
- (b) infringe anyone's copyright, trademark or other rights;
- (c) send spam or unsolicited bulk messages;
- (d) attempt to bypass security controls, scan networks, or test for vulnerabilities, unless that is an authorised part of your task;
- (e) install or run malware, cryptocurrency miners, or unlicensed software; or
- (f) run a personal business.

8.2 Limited, reasonable personal use of a Company device or account (for example checking personal email on a break) is acceptable if it does not interfere with work or breach this policy.

9. Reporting security incidents

9.1 Report any Security Incident to the Security Contact and your Supervisor immediately, and in any case within 1 hour of noticing it. Report even if you are not sure, and even if you caused it.

9.2 Include what happened, when, which systems or data may be affected, and what you have already done.

9.3 Do not try to investigate further, delete evidence, or contact affected clients yourself unless the Security Contact asks you to.

9.4 Honest and prompt reporting of a mistake will be treated very differently from hiding it. Failing to report, or concealing, a Security Incident is a serious breach of this policy.

10. Monitoring notice

10.1 To protect security, meet legal and client obligations, and manage work, the Company may monitor and log the use of Company Systems. This may include:

- (a) login and access logs for Company Accounts and Company Systems;
- (b) activity in code repositories, task trackers and cloud services;

(c) email and chat sent through Company Accounts, where needed for a security investigation, a legal requirement or a conduct matter; and

(d) device management on Company devices.

10.2 The Company does not monitor your Personal Device or personal accounts, except for the Company-managed apps, accounts or profiles you use for work, and only to the extent described above.

10.3 You should not expect privacy in Company Accounts or Company Systems. Monitoring is carried out in a proportionate way, accessed only by authorised people, and handled as described in the Intern and Candidate Privacy Notice.

11. Return of access and data at exit

11.1 When your internship ends for any reason, or when asked, you must:

- (a) return all Company devices, access cards and other Company property;
- (b) hand over your work, including code, documents and credentials you were given, to your Supervisor;
- (c) make sure all your code is committed to the Company repository;
- (d) permanently delete all Company Data and Client Data from your Personal Devices and personal accounts within 2 working days, and confirm this in writing; and
- (e) not access any Company System after your last working day.

11.2 The Company will remove your access to Company Systems on or before your last working day.

11.3 Issue of the completion certificate is subject to completion of these exit steps, as set out in the Internship Policy and Terms of Engagement.

12. Breach of this policy

A breach of this policy may lead to action under the disciplinary process in the Intern Code of Conduct, including removal of access and termination of the internship. Some breaches may also be offences under the Information Technology Act, 2000 or other laws.

13. Changes and contact

13.1 The Company may update this policy from time to time. Current interns will be told of material changes by email.

13.2 Questions about this policy can be sent to admin@trackmytech.in.

Acknowledgement

By accepting your offer online, you confirm that you have read, understood and agree to this IT, Device and Acceptable Use Policy, including the monitoring notice in clause 10.