ICT POLICY

At Trackita Pty Ltd, we rely on efficient and secure use of technology resources to maintain smooth business operations. This policy clarifies how employees should use and protect the Company's IT systems and data. Although these guidelines are not part of your employment contract, compliance is mandatory.

---

1. Purpose

- **Safe & Effective Use**: Ensure the Company's hardware, software, and networks remain secure and available for business needs.
- **Professional Conduct**: Set standards for proper, respectful use of digital resources and online communication.

---

2. Scope: What Are ICT Resources?

ICT (Information and Communications Technology) resources include, but are not limited to:

- Laptops, desktops, and mobile devices
- Printers and scanners
- Email systems and cloud platforms (e.g., SharePoint, OneDrive)
- Software, licenses, and applications
- Network access, internet, and data storage solutions

---

3. Non-Contractual Nature

- This policy is not part of your employment contract.
- Trackita reserves the right to modify or replace the policy as needed.

---

4. Acceptable Use Guidelines

4.1 Professional Use

- **Work-Related Activities**: ICT resources should primarily support your job responsibilities.
- **Minimal Personal Use**: Occasional personal tasks (e.g., checking personal email) are permissible, provided they do not interfere with work duties or pose security risks.

4.2 Software Requests

- **Approval Process**: If you require additional software or applications, email emailaddressemail addressemailaddress for authorization. Unauthorized downloads or installations are prohibited.

4.3 Internet Usage

- **Safe Browsing**: Avoid visiting harmful or inappropriate websites.
- **Data Consumption**: If you receive alerts about high data usage, notify your manager or IT immediately.

---

5. File Storage & Management

- **Cloud Platforms**: Use SharePoint or OneDrive for file storage so your work is easily accessible and backed up.
- **Data Ownership**: All work-related documents and data belong to the Company and may not be shared externally without management approval.

---

6. Security Measures

6.1 Antivirus

- **Mandatory**: Keep antivirus software active and updated on all Company devices.

6.2 USB Drives

- **Scan First**: Always scan USB drives for malware before using them on Company systems.
- **Office USBs**: Delete files from shared office USB drives once you no longer need them.

6.3 Passwords

- **Confidential**: Never share your passwords with anyone.
- **Regular Changes**: Update passwords periodically.
- **Device Protection**: Ensure all devices (laptops, smartphones) have secure passwords or PINs.

6.4 Email Safety

- **Phishing Alerts**: Report suspicious or spam emails and do not reply to them.
- **Printing & Disposal**: Retrieve printed documents promptly and dispose of sensitive paperwork in secure bins.

---

7. Accountability & Reporting

- **Care of Equipment**: Exercise due diligence when using Company-provided devices.
- **Incident Reporting**: Immediately report lost or damaged equipment, security incidents, or suspicious system behavior.

---

8. Other Relevant Policies

You are expected to be familiar with and adhere to the following:

- **Code of Conduct**
- **Privacy Policy**
- **Social Media Rules**
- **Workplace Surveillance**
- **Communication Policies**

The client you are working for will have polices that will supersede what we put here.

---

9. Consequences of Non-Compliance

Violations of this ICT Policy may result in disciplinary action, up to and including termination of employment.