ABC SOLUTIONS INC.

Company Laptop Policy Template

Document ID	POL-IT-2026-04	**Effective Date**	October 20, 2023
Prepared By	Human Resources	**Approved By**	Management / IT Security
Version	2.1	**Review Cycle**	Annual

1. Purpose & Scope

This policy outlines the guidelines and security requirements for the acceptable use of company-issued laptops, hardware, and mobile computing assets. The objective is to protect the intellectual property, digital infrastructure, and sensitive client information handled by employees of **ABC Solutions Inc.**

This policy applies to all full-time employees, contractors, temporary workers, and third-party vendors who are allocated a company laptop or access company infrastructure remotely.

2. Laptop Ownership & Issuance

- **Company Property:** All issued laptops, peripherals, and software remain the exclusive property of ABC Solutions Inc.
- **Deployment & Tracking:** IT Asset Management will log the device serial number, MAC address, and specifications against the employee profile prior to provisioning.
- **Formal Sign-off:** Employees must sign an Asset Acknowledgement Form immediately upon receipt confirming the working condition and model specification of the asset.

3. Proper Use & Security Protocols

Employees are expected to use the laptop primarily for business-related operations. The following conditions must be met at all times:

- **Password Complexity:** Laptops must utilize enterprise-level multi-factor authentication (MFA) and strong passwords that adhere to the corporate credential policy.
- **Software Installation:** Only software approved and distributed by the IT department may be installed. The installation of unauthorized, unlicensed, or personal applications is strictly prohibited.
- **Network Security:** When operating outside the corporate network, employees must route all internet traffic through the official Corporate Virtual Private Network (VPN). Unsecured public Wi-Fi networks must be avoided unless a secondary encrypted bridge is verified.
- **Physical Security:** Devices must never be left unattended in public places, open vehicles, or unmonitored office spaces. Lock screens must be engaged automatically after a maximum of 5 minutes of inactivity.

> **Critical Security Warning:** Under no circumstances should employees bypass security controls, firewalls, anti-virus agents, or data loss prevention (DLP) frameworks deployed on the machine.

4. Data Protection & Confidentiality

- **Local Storage:** Critical and confidential business files should be stored directly on authorized cloud drives (e.g., SharePoint, Google Drive Enterprise) rather than local drives to prevent permanent data loss in the case of local hardware failure.
- **Encryption:** Full Disk Encryption (FDE) must remain active. Any attempt to modify system partition security will flag an automated alert to the SOC (Security Operations Center).
- **Incident Reporting:** Any potential data breaches, malware infections, phishing vulnerabilities, or suspicious system behaviors must be reported directly to the IT Security Desk within two (2) hours.

5. Maintenance & Technical Support

Routine updates, operating system patches, and security definitions are automated by the IT Support department. Employees must not delay or indefinitely postpone system restarts required to complete critical patches.

Physical modifications, hardware updates, or repairs by external unauthorized service providers are strictly prohibited. All physical asset maintenance must be organized natively through the IT service desk ticketing system.

6. Lost, Stolen, or Damaged Assets

In the event that an asset is lost, stolen, or physically damaged beyond standard wear-and-tear:

1. Report the event immediately to the IT Security Desk and Human Resources.
2. For stolen devices, file a report with local law enforcement within 24 hours and supply the official incident report to the company administration.
3. The IT Department will trigger a remote wipe protocol to protect local caches and access tokens.

7. Laptop Return Policy

Upon resignation, termination, or formal request by management, the employee must return the laptop and all related accessories (chargers, docking stations, adaptors) in good operating condition within two business days. Failure to return corporate assets may result in legal action or financial withholding where permitted by local labor regulations.

8. Policy Acceptance & Sign-off

By signing below, I acknowledge that I have read, fully understand, and agree to abide by the terms and conditions outlined in the ABC Solutions Inc. Company Laptop Policy.

Employee Signature

Date

Printed Employee Name

Asset Serial Number (IT Use Only)