Bloomfire

Acceptable Use Policy for Company-Issued Devices

Policy Owner	Information Security & IT Governance
Effective Date	January 1, 2026
Last Reviewed	April 2026
Next Review Date	October 2026
Applies To	All employees, contractors, and vendors with company-issued hardware
Related Documents	Data Classification Policy | Remote Work Policy | BYOD Policy

1. Purpose

This policy defines the acceptable and prohibited uses of all hardware and software assets issued by the organization to its employees, contractors, and authorized third parties. The intent of this policy is to protect organizational data, maintain system integrity, and ensure compliance with applicable laws and regulations.

2. Scope

This policy applies to all individuals who receive a company-issued device, including but not limited to laptops, desktop computers, mobile phones, tablets, and peripheral equipment. It covers all use of these devices, whether on-premises or remote, during or outside of normal business hours.

3. Permitted Uses

Company-issued devices may be used for the following purposes:

- Performing job-related duties and responsibilities
- Accessing company systems, applications, and data as authorized by your role
- Communicating with colleagues, clients, vendors, and partners in a professional manner
- Limited personal use that does not interfere with work performance, consume significant bandwidth, or create legal or security risks for the organization

Bloomfire

Acceptable Use Policy for Company-Issued Devices

4. Prohibited Uses

The following activities are strictly prohibited on company-issued devices:

- Accessing, downloading, or distributing illegal, obscene, or discriminatory content
- Installing unauthorized software, applications, browser extensions, or plug-ins not approved through the IT self-service portal
- Disabling or circumventing endpoint security tools, antivirus software, or device management agents
- Using the device for personal business activities, freelance work, or activities that compete with the organization
- Connecting to unsecured or untrusted public Wi-Fi networks without an active VPN connection
- Transferring company data to personal cloud storage services (e.g., personal Google Drive, Dropbox, iCloud)
- Mining cryptocurrency or running non-work-related compute-intensive processes

Warning: Use of company-issued devices for cryptocurrency mining is strictly prohibited and constitutes grounds for immediate disciplinary action, up to and including termination of employment.

5. Data Handling Requirements

All employees are responsible for handling company data in accordance with the Data Classification Policy. On company devices specifically:

- Confidential and Restricted data must never be stored locally on unencrypted drives. Use approved cloud storage (OneDrive or SharePoint) for all sensitive files.
- Devices must be locked when unattended (Windows Key + L or automatic lock after 5 minutes of inactivity — this is enforced via MDM policy).
- Employees must not connect unauthorized external storage devices (USB drives, external hard drives) without prior IT approval.

6. Monitoring and Privacy

Employees should be aware that company-issued devices are subject to monitoring in accordance with applicable laws. The organization reserves the right to inspect, monitor, and review device activity, including internet usage, installed applications, and stored files, for purposes of ensuring policy compliance, security incident investigation, and legal obligations. Employees have no expectation of privacy on company-owned devices.

Bloomfire

Acceptable Use Policy for Company-Issued Devices

7. Reporting Lost or Stolen Devices

A lost or stolen device must be reported immediately — within one hour of discovery — by contacting the IT Security team. Prompt reporting is critical to allow the team to remotely lock or wipe the device before unauthorized access can occur.

- IT Security: itsecurity@company.com | #security-incidents on Slack | ext. 5911 (24/7)

8. Consequences of Violation

Violations of this policy may result in:

- Temporary or permanent revocation of device access
- Formal disciplinary action in accordance with the Employee Code of Conduct
- Termination of employment or contract
- Legal action where violations involve criminal activity or significant data loss

Note This policy is reviewed semi-annually. Employees will be notified of material changes via email and are expected to review and acknowledge the updated policy within 10 business days of notification.

9. Policy Acknowledgment

All employees and contractors are required to acknowledge this policy upon device issuance and upon each annual review. Acknowledgments are recorded in the HR Information System (HRIS). Contact HR Operations if you have not received a policy acknowledgment request.

10. Related Policies and Resources

- Data Classification Policy
- Remote Work and Hybrid Work Policy
- BYOD (Bring Your Own Device) Policy
- Incident Response Plan
- IT Self-Service Portal: it.yourcompany.com