# Company Computer Use Policy

A plain-language policy for company laptops, desktops, software, local admin rights, updates, files, and everyday computer use.

## Purpose

This policy explains how employees may use company computers and business systems. The goal is to keep devices reliable, protect company data, and reduce avoidable security risk.

## Scope

This policy applies to company-owned desktops, laptops, shared workstations, virtual desktops, servers, and any personal computer approved for company work.

## Acceptable use

Company computers are provided for business purposes. Reasonable limited personal use may be allowed if it does not interfere with work, create security risk, violate law, consume excessive resources, or conflict with company policy.

Employees must use company computers responsibly and protect customer, employee, and business information.

## Prohibited use

Employees must not use company computers to:

- Download illegal, pirated, or unauthorized software
- Access malicious, illegal, or inappropriate content
- Disable antivirus, endpoint protection, firewall, logging, or security tools
- Bypass company access controls
- Share accounts or passwords
- Store company files in unapproved personal cloud services
- Connect unknown USB drives or storage devices without approval
- Install remote access tools without approval
- Mine cryptocurrency or run unrelated high-resource workloads
- Use the device for outside business unless approved

## Software installation

Software should be installed only when there is a business need and the software is approved or trusted. Employees should not install random utilities, browser extensions, remote access agents, cracked software, or tools that request broad access to company data.

When possible, software should come from vendor websites, managed app stores, or company deployment tools.

## Updates and patching

Employees must allow operating system, browser, application, firmware, and security updates to install. Devices should be restarted when required to complete updates.

Employees should not postpone updates indefinitely. If an update breaks a business application, report it promptly so the issue can be handled through support.

## Local administrator rights

Local administrator rights should be limited. Employees should not have permanent administrator access unless their role requires it and the risk has been accepted.

Temporary elevation may be provided for approved work. Administrator access should not be used for daily browsing, email, or routine office work.

## Files and storage

Company files should be stored in approved locations such as company file shares, approved cloud storage, or business applications. Files should not be stored only on a local desktop or personal drive if the company needs backup, audit, or shared access.

Sensitive files should not be copied to personal email, personal cloud drives, personal USB drives, or unmanaged devices.

## Email, web browsing, and downloads

Employees should treat links, attachments, downloads, and login prompts with caution. Suspicious messages should be reported instead of forwarded broadly or opened repeatedly.

If a website asks for company credentials unexpectedly, stop and verify the site before logging in.

## Remote access

Remote access to company computers or systems must use approved tools. Employees must not install consumer remote access software to bypass support, work from home, or allow vendors into the environment without approval.

## Monitoring and privacy

The company may monitor company devices, accounts, network activity, security alerts, and system logs to protect business operations, investigate incidents, support users, and meet compliance obligations.

Employees should not expect personal privacy when using company-owned systems or company accounts.

## Lost, stolen, or damaged computers

Employees must report lost, stolen, damaged, or compromised computers promptly. The company may revoke sessions, reset passwords, wipe data, disable accounts, or take other steps to protect the environment.

## Return of equipment

Company computers and accessories must be returned when employment ends or when requested. Company data must not be copied, retained, deleted, or transferred unless authorized.

## Implementation checklist

- Maintain an inventory of company computers
- Require endpoint protection
- Require automatic updates
- Limit local administrator rights
- Standardize approved software
- Back up important files
- Document remote access tools
- Remove company access from returned or replaced devices

## Disclaimer

This starter policy is general information, not legal advice. Adapt it to your business, contracts, regulatory obligations, and state law.