CONTROLLED DOCUMENT

Acceptable Use Policy

Sample Company LLC

Prepared as a structured operating document for internal use, review, and controlled distribution.

Review this document after major operational, regulatory, or technology changes.

Version 1.0

DOCUMENT CONTROL

RECOMMENDED

PREPARED FOR Sample Company LLC	**DOCUMENT OWNER** Chief Information Security Officer
CLASSIFICATION Confidential	**DISTRIBUTION** Executive Leadership, Full-time employees, Part-time employees, Contractors and consultants, Temporary workers
GENERATED June 12, 2026	**NEXT REVIEW DATE** 2027-06-12
STATUS Internal Review Draft	**DOCUMENT VERSION** 1.0
TEMPLATE VERSION 1.0.0	**TARGET CONTROL LEVEL** Recommended
FRAMEWORKS Core baseline only	

Table of Contents

INFO: IMPORTANT NOTICE — READ BEFORE USE

This document was generated as a structured starting template from the information provided. It does not constitute legal, regulatory, or professional compliance advice, and it does not by itself establish or prove compliance with any framework or regulation. Specific obligations vary by jurisdiction, industry, and circumstance. Before adopting or relying on it, have this document reviewed by qualified legal counsel and the appropriate internal owners, and adapt it to your organization's actual environment.

Policy Framework

Executive Summary

This Acceptable Use Policy establishes Sample Company LLC's rules for the use of company-owned technology systems, networks, devices, and data. It applies to: Full-time employees, Part-time employees, Contractors and consultants, Temporary workers, Third-party vendors with system access.

Policy posture: limited personal use is permitted, personal devices are permitted under documented BYOD requirements, monitoring activities are disclosed with each activity's purpose, and a tiered enforcement framework escalates from verbal warning through termination.

Policy owner: Chief Information Security Officer · re-acknowledgment both annually and when updated · effective 2026-04-02.

All individuals covered by this policy must read, understand, and acknowledge its contents. Violations may result in disciplinary action up to and including termination of employment or contract, and may be reported to law enforcement where applicable.

Acceptable Use Rules

Authorized Use of Company Systems

These rules apply to all company-owned or company-managed systems — desktop computers, laptops, mobile devices, email accounts, collaboration tools, and any other technology provided or funded by the organization — and to personal devices used for work under the BYOD provisions in this policy.

Personal Use of Company Systems

Limited personal use of company systems is permitted during breaks and non-working hours, provided it does not interfere with job responsibilities, consume excessive network bandwidth, or expose the organization to security risks.

Email Usage

Company email is for business use. Do not forward company email to personal accounts. Use approved secure sharing for sensitive data.

- Do not open suspicious attachments or click links from unknown senders
- Report suspected phishing emails to IT immediately — do not forward or reply
- Do not use company email to send confidential data without appropriate encryption
- Do not use personal email accounts to conduct company business or share company files
- Treat company email as a business record — it may be reviewed during audits or legal proceedings

Internet and Web Browsing

Occasional personal browsing is permitted during breaks. Prohibited: illegal content, unauthorized downloads, and personal cloud storage for company data.

Accessing illegal content, sites associated with malware distribution, or content that would constitute harassment or discrimination is prohibited regardless of personal use permissions. The organization monitors web activity on company systems and networks — see the Monitoring and Enforcement section for details.

Remote Work and Connectivity

Employees working remotely or accessing company systems from outside the office must follow these requirements to protect company data and systems from unauthorized access.

A virtual private network (VPN) connection is required for all remote access to company systems, regardless of the network being used. Employees must connect to the VPN before accessing any internal applications, file shares, or administrative tools.

Public Wi-Fi Policy

The use of public Wi-Fi networks (coffee shops, airports, hotels, co-working spaces) is prohibited for work purposes. Employees must use a mobile hotspot or cellular connection when working outside the office or home.

Home Network Security Requirements

Employees working from home must ensure their home network meets the following security requirements:

- Wi-Fi must be password-protected (no open networks)
- Router firmware should be kept up to date
- Default router passwords must be changed

These requirements reflect a minimum baseline for protecting company data in home environments. Employees who are uncertain whether their home network meets these standards should contact IT for guidance.

Physical Workspace Requirements

Employees handling sensitive or confidential data while working remotely must do so in a private workspace where screens cannot be viewed by others and phone conversations cannot be overheard.

Even in low-risk environments, employees should be mindful that screen content, phone calls, and printed materials may be visible or audible to others in shared spaces. Good judgment about physical privacy is an extension of the organization's security culture.

Device and BYOD Policy

These rules define how company devices must be maintained and what the organization's position is on personal devices used for work. Compliance is enforced through IT management tooling and is a condition of continued access to company systems.

Company-Owned Devices

Company devices require full-disk encryption, automatic screen lock after five minutes, and IT-approved software only.

Personal Devices (BYOD)

Personal devices (BYOD) are permitted for work use, provided they meet the security requirements listed below. All personal devices used for work must be registered with IT and comply with organizational security standards.

BYOD Security Requirements

SECURITY REQUIREMENT	STATUS
Device encryption required	Required
Screen lock or PIN required	Required
Mobile device management software required	Required
Remote wipe capability required	Required
Approved antivirus or endpoint protection required	Required
Company data must stay in managed apps	Required

By using a personal device for work, employees consent to the organization's right to remotely wipe company data from the device in the event of loss, theft, or separation from employment. The organization will make reasonable efforts to wipe only company data and not personal content, but cannot guarantee separation in all circumstances.

Removable Media and USB Devices

USB storage devices and removable media are blocked on all company systems. USB ports are disabled for storage devices through endpoint management. This control prevents data exfiltration and reduces the risk of malware introduced through removable media.

Lost or Stolen Devices

A lost or stolen device is a potential data breach. The sooner IT is notified, the sooner the device can be remotely locked or wiped and credentials can be revoked.

Report lost or stolen devices to IT within one hour. IT will initiate remote wipe and credential resets.

Failure to report a lost or stolen device promptly may result in disciplinary action and increases the risk of unauthorized access to company data. Employees must not wait to see if the device turns up before reporting — assume the worst and report immediately.

Software and Cloud Services

This section defines how new software and cloud services are approved, the list of approved tools, and the rules for emerging technologies including generative AI. Unapproved software on company devices can void insurance coverage, fail compliance audits, and bypass IT review.

Software Installation and Requests

Software request process: Submit software requests through the IT helpdesk. IT reviews security and licensing within 48 business hours.

Approved Collaboration and Cloud Storage Tools

Approved: Microsoft Teams, Outlook, OneDrive, and SharePoint. Personal cloud storage is not permitted for company data.

Using unapproved cloud services (personal Google Drive, Dropbox, WeTransfer, etc.) for company data is prohibited. If you need a tool that is not on the approved list, submit a request through the software approval process described above.

Generative AI Tools

Only company-approved AI tools may be used for work purposes. Employees must not use unauthorized AI services, even for seemingly harmless tasks, as data entered into these tools may be used for model training. Contact IT for the current list of approved AI tools.

AI tools process and, in many cases, store or use for model training anything that is entered into them. A single careless prompt containing a client name, an internal document, or proprietary source code can result in a data breach that the organization may never learn about. Treating AI tools with the same scrutiny as any other third-party data processor is the appropriate security posture.

SaaS and Cloud Service Signups

Employees may not create accounts on new SaaS or cloud services using their work email address without prior approval from IT. This includes free trials, freemium tools, and services that require only an email address to sign up. Unauthorized signups create unmanaged accounts that may expose company data.

Security & Compliance

Data Handling Responsibilities

The following rules apply to all personnel covered by this policy. They are minimum required behaviors that protect the data the organization holds — including credential hygiene, physical-security practices, and approved channels for sharing information.

Credential and Password Management

Protecting login credentials is one of the most important things you can do to prevent unauthorized access. Compromised credentials are involved in the majority of data breaches — most of which begin not with a sophisticated technical attack, but with a stolen or guessed password. The following credential handling rules are mandatory:

- Never share passwords with anyone
- Use a password manager for all work accounts
- Use unique passwords for each account
- Never write passwords on paper or sticky notes
- Report any suspected credential compromise immediately

Multi-factor authentication (MFA) must be enabled on all accounts that support it, including email, VPN, cloud services, and any system containing sensitive data. MFA is the single most effective control for preventing unauthorized account access, and its absence is a material finding in most cyber insurance underwriting assessments.

Clean Desk Policy

The organization enforces a clean desk policy. All sensitive documents, removable media, and confidential materials must be secured in locked storage when not actively in use. At the end of each workday, desks must be cleared of all sensitive materials. Whiteboards containing sensitive information must be erased. This applies to both office and remote workspaces.

Physical Security Expectations

Physical security of devices and workspaces is essential to protecting company information. A device left unattended, an unlocked door, or a visitor allowed beyond a reception area can result in the same data exposure as a sophisticated cyberattack — with less chance of detection. All personnel must follow these practices:

- Lock screens when stepping away (even briefly)
- Do not leave devices unattended in public
- Shred sensitive printed documents
- Secure devices in locked areas when not in use
- Do not discuss sensitive information in public places
- Do not print sensitive documents unless necessary

Data Sharing and Transfer

Sharing company or customer data carries inherent risk. Data sent to the wrong recipient, transferred through an unencrypted channel, or stored in an unapproved location creates exposure that may not be discovered until a breach has already occurred. The following rules govern how data may be shared:

Share company data only through approved Microsoft 365 channels. Do not use personal email or consumer file-sharing services.

When in doubt about whether data can be shared or how to share it securely, contact IT before proceeding. It is always better to delay a transfer than to create an uncontrolled exposure.

Prohibited Activities

The following activities are strictly prohibited on all company-owned systems, on personal devices used for work, and in any activity conducted using company accounts or credentials — regardless of work hours or location. This list is not exhaustive: any activity that compromises security, violates law, or conflicts with the organization's interests is prohibited whether or not it is explicitly listed.

Explicitly Prohibited Activities

- Installing unauthorized software
- Disabling or circumventing security controls
- Sharing login credentials with others
- Storing company data in unapproved cloud services
- Sending company data to personal email accounts

Additional Restrictions

Employees may not connect personal USB storage to company computers.

Employees who are uncertain whether an activity is permitted should contact IT or their manager before proceeding. Ignorance of this policy is not a defense against violations. Employees who discover that a colleague may be violating this policy are encouraged to report it through the organization's reporting channel — all reports will be treated confidentially.

Social Media and Public Communications

These guidelines apply to both official company social media accounts and personal accounts when the employee identifies themselves as working for the organization or when the content relates to company business, clients, or operations.

Social Media Use

Social media use — both on company accounts and personal accounts that reference the organization — carries risk. Seemingly harmless posts can reveal details about internal systems, office security, or business operations. The following guidelines apply to all personnel:

Do not post photos of internal systems, credentials, or customer information. Do not speak for the company without approval.

- Never post photographs of internal systems, server rooms, or security infrastructure
- Do not share company-issued badges, access cards, or security tokens on social media
- Do not disclose customer names, project details, or financial information without authorization
- Do not post content that could be interpreted as an official statement of the organization without approval
- Report any suspected social engineering attempts through social media to IT immediately

When in doubt about whether a post could reveal sensitive information, the safest choice is not to post. Employees who are uncertain whether specific content is appropriate should consult their manager or the communications team before publishing.

Public Statements and Media Inquiries

Only designated spokespersons from the communications or public relations team are authorized to make public statements about the organization, its security practices, or its technology systems. All media inquiries must be directed to the communications team.

This includes statements made in interviews, press releases, conference presentations, industry publications, blog posts, podcasts, and any other public forum — whether or not the employee is explicitly representing the organization at the time. Unauthorized public statements about the organization's security posture, incident history, or technology infrastructure are of particular concern and will be treated as a serious policy violation.

Enforcement & Acknowledgment

Monitoring and Enforcement

The organization monitors use of its technology systems to protect against security threats, ensure compliance with this policy, and maintain the integrity of its information assets. By using company systems, all personnel consent to the monitoring described in this section.

Monitoring Activities

The organization performs the following monitoring activities on company-owned systems and networks:

Organizational Monitoring Activities

MONITORING TYPE	PURPOSE
Email monitoring	Phishing detection, data loss prevention
Web browsing monitoring	Malware prevention, policy compliance
Endpoint or device monitoring	Endpoint protection, threat detection
Login and authentication logging	Unauthorized access detection, compliance

Monitoring data is accessible only to authorized IT and security personnel. Monitoring is conducted to protect the organization and its employees — not to track individual productivity. Data from monitoring systems is retained in accordance with the organization's data retention policy and may be used as evidence in investigations, disciplinary proceedings, or legal matters.

Reporting Your Own Security Mistakes

Report suspected incidents to IT immediately. Honest mistakes reported quickly are handled as learning opportunities.

Employees who promptly report their own honest mistakes will not face punitive action for the mistake itself. The organization values a culture where security concerns are raised early. Concealing a security incident is itself a policy violation and will be treated accordingly.

Policy Enforcement

Violations of this Acceptable Use Policy are addressed through the following enforcement framework, which ensures consistent, proportionate consequences and gives employees clear notice of what to expect:

Enforcement Actions by Violation Severity

VIOLATION LEVEL	ACTION
First violation	Verbal warning and mandatory security awareness refresher training
Second violation	Written warning placed in personnel file with review period
Third violation	Suspension of system access pending management review
Severe violation (data theft, sabotage, illegal activity)	Immediate suspension of all access pending investigation; may result in termination and legal action

Violations may result in retraining, written warnings, or access suspension depending on severity.

In cases where a policy violation also constitutes a criminal offense, the organization reserves the right to refer the matter to law enforcement. The organization will cooperate fully with any legal investigation related to misuse of its

technology systems.

Policy Acknowledgment and Review

All individuals covered by this policy must formally acknowledge that they have read, understood, and agree to comply with its terms. Acknowledgment is a condition of access to company systems and provides the documented, auditable record required for cyber insurance, SOC 2 audits, and regulatory compliance.

Acknowledgment Method

Acknowledgment is collected through the organization's HR or compliance management system via electronic signature. This provides a timestamped, auditable record of each individual's acknowledgment.

Re-Acknowledgment Schedule

All personnel must re-acknowledge this policy annually and whenever it is materially updated, whichever comes first.

Record Retention

Acknowledgment records are retained for the duration of the individual's employment or contract, plus three years following separation.

Acknowledgment records may be requested by auditors, insurers, or legal counsel during an investigation or compliance review. Records must be stored in a manner that ensures their integrity and accessibility for the full retention period. HR is responsible for maintaining acknowledgment records in accordance with this requirement.

Policy Review and Maintenance

An AUP that is never reviewed becomes inaccurate as the organization's technology, workforce, and threat environment evolve. This policy should be reviewed at a minimum annually, and whenever significant organizational changes occur — such as the adoption of new technology platforms, a change in remote work practices, a security incident involving policy violations, or changes in applicable regulatory requirements.

- Annual review by the policy owner and IT/security team
- Review triggered by material changes in the organization's technology environment
- Review following any security incident where an AUP violation was a contributing factor
- Review when applicable regulations or compliance frameworks are updated

The policy owner is responsible for ensuring the policy is reviewed on schedule, updated as needed, and re-distributed with acknowledgment collected whenever material changes are made.

Acknowledgment Requirements Summary

PARAMETER	VALUE
Acknowledgment Method	Electronic signature via HR or compliance system
Re-Acknowledgment Frequency	Both annually and when updated
Record Retention Period	Duration of employment plus 3 years

Appendix: Revision History

VERSION	DATE	DESCRIPTION
1.0	2026-06-12	Initial document generation

Appendix: Glossary of Terms

TERM	DEFINITION
Acceptable Use	The defined boundaries for how employees and contractors may use an organization's technology systems, networks, devices, and data, including what is permitted, what is restricted, and what is prohibited.
Audit Log	A tamper-resistant, time-stamped record of significant system and user actions, retained as evidence for security investigations, compliance reviews, and accountability.
Bring Your Own Device (BYOD)	A policy permitting employees to use personal devices (phones, tablets, laptops) for work, typically subject to security requirements such as encryption, screen lock, and the ability to remotely wipe company data.
Credential Management	The practices and tools used to create, store, rotate, and protect login credentials — including password managers, unique passwords per account, and prompt revocation of compromised credentials.
Data Classification	The practice of categorizing information by sensitivity (for example public, internal, confidential, or restricted) so that appropriate handling, access, and protection controls can be applied to each category.
Encryption	The process of encoding data so that only authorized parties holding the key can read it. Used to protect data at rest (for example full-disk encryption) and in transit (for example TLS) against unauthorized access.
Endpoint Protection	Security software deployed on devices (laptops, desktops, servers, mobile) to detect, prevent, and respond to malware and other threats. Often used interchangeably with endpoint detection and response (EDR) or antivirus.
Information System	The combination of hardware, software, networks, data, and people that an organization uses to collect, process, store, and distribute information.
Least Privilege	The principle that each user, account, or process should have only the minimum access rights needed to perform its function, limiting the damage from compromised accounts or insider misuse.
Mobile Device Management (MDM)	A platform that lets an organization enforce security policies on managed devices — such as requiring encryption and screen lock, pushing configuration, and remotely wiping company data on loss, theft, or separation.
Monitoring	The ongoing collection and review of activity on systems and networks — such as endpoint, file-access, and authentication logging — to detect threats, support investigations, and verify policy compliance.
Multi-Factor Authentication (MFA)	Authentication method requiring two or more verification factors (something you know, have, or are) to gain access to a resource.

TERM	DEFINITION
Remote Access	Connecting to an organization's systems and data from outside its premises, typically over the internet. Common controls include VPNs, multi-factor authentication, and device posture checks.
Shadow IT	Hardware, software, or cloud services used for work without the knowledge or approval of the IT or security function, creating unmanaged data exposure and compliance gaps.
Software as a Service (SaaS)	Software delivered over the internet and accessed through a browser or app rather than installed locally. Because company data often lives in the SaaS provider's environment, each new service is a third-party data-processing relationship.
Virtual Private Network (VPN)	An encrypted network tunnel that extends a private network across a public network, enabling remote users to securely access organizational resources as if they were directly connected to the internal network.

Appendix: Identified Gaps and Improvement Opportunities

The questionnaire responses are complete: no missing-prose or empty required sections were found. Contact and identifier fields are intentionally left for local completion and are marked where they appear. Control implementation gaps and partial safeguards, if any, are listed in the maturity summary and remediation roadmap sections. The following governance and operational items should be completed before this document is considered approved for operational use:

- Obtain approval signatures from all designated signatories before the document is approved for operational use.
- Complete any local-fill placeholders in the exported copy only — do not re-enter named contacts or company identifiers into the hosted workspace.
- Confirm legal and regulatory applicability with counsel for any obligations referenced in this document.
- Schedule the first annual review date and assign the review owner.

These items represent standard governance follow-up for a newly generated document and do not indicate deficiencies in the document content itself.

Appendix: Internal Review and Local Completion Checklist

This document was generated from questionnaire responses and requires internal validation before it is approved for operational use. The following checklist should be completed by the designated review team.

- Complete any local-fill placeholders in the exported copy only: do not re-enter named contacts or company identifiers into the hosted workspace.
- Confirm legal and regulatory applicability: engage legal counsel to verify notification timelines, jurisdictional obligations, and contractual requirements referenced in this document.
- Obtain approval signatures from all designated signatories before the document is approved for operational use.
- Schedule the first annual review date and assign the review owner.

Local completion items for the final distribution copy:

- Replace role placeholders with the approved local titles or personnel for the final distribution copy.
- Add direct contact details such as shared mailboxes, emergency phone paths, vendor support numbers, and named coordinators only in the local copy.
- Insert company-specific legal names, locations, domains, internal system identifiers, and account references only after export.

Once all checklist items are complete, update the document status from "Internal Review Draft" to "Approved" and re-export.