

Acceptable Use Policy

Owner	[Security owner role]
Approved by	[Policy approver role]
Effective date	[Effective date]
Next review	[Next review date]
Version	[Version]

1. Purpose and scope

This policy sets the rules for using [Company name] (the "Company") systems, accounts, devices and data. It supports the SOC 2 common criteria CC1.1, which expects the Company to set standards of conduct, and CC1.5, which expects it to hold personnel accountable for them, here through the acknowledgment each person signs.

This policy applies to all [In-scope personnel], including contractors, to every Company system, account and device, and to any personal device used for Company work.

2. General standards

All personnel must:

- Act with integrity and honesty in all business activities.
- Comply with applicable laws, regulations, and contractual obligations.
- Protect company and customer information from unauthorized disclosure.
- Avoid conflicts of interest and disclose potential conflicts promptly.

3. Accounts and credentials

- Personnel keep credentials private, use a password manager, and enable multi-factor authentication on every account that supports it.
- Personnel do not share accounts, bypass security controls, disable endpoint protection or install unapproved software on Company devices.
- Personnel never approve a sign-in prompt they did not start, and report one at once.

4. Devices

Every Company device is enrolled in [Device management tool], which enforces:

- Full disk encryption: Enabled with keys escrowed.
- Screen lock: Auto-lock after [Screen lock timeout].
- Endpoint protection: [Endpoint protection tool] installed and active.
- Secure configuration: Maintained and monitored.
- Removable media: Use is restricted or prohibited. [Removable media rule]
- Updates: Operating system and browser updates are installed within 14 days of release.
- Loss or theft: A lost or stolen device is reported to the [Security owner role] within 1 hour so it can be locked or wiped.

5. Personal devices and contractors

- A personal phone or computer may reach Company email and chat only if it has a screen lock, a supported operating system and the protections required by [Identity provider].
- Customer data is never stored on a personal device.
- Contractors who use their own equipment meet the device rules in section 4 and confirm it in writing before access is granted.

6. Handling data

- Information is handled according to the Data Classification and Retention Policy, including its rules for storage, sharing and disposal.
- Customer data is never copied to personal devices, personal accounts or unapproved tools, including public AI services.
- Confidential information is not discussed in public places or on open channels where others can overhear or read it.
- Suspected loss, exposure or misuse of information is reported to the [Security owner role] immediately.

7. Personal use, monitoring and prohibited activity

- Limited personal use is permitted when it does not interfere with work, does not break the law and does not put Company data at risk.
- Company systems are never used to harass, to access illegal or sexually explicit material, or to run a personal business.
- The Company monitors its systems for security and compliance purposes to the extent the law allows. Personnel have no expectation of privacy in Company accounts.

8. Reporting

- Suspected security incidents, lost devices and phishing messages are reported to the [Security owner role] within 1 hour.
- Concerns about conduct can be raised through [Ethics reporting channel]. No one is penalized for a report made in good faith.

9. Acknowledgment

Every person in scope signs below before receiving access, and again each year, using [Acknowledgment method].

I have read the [Company name] Acceptable Use Policy, I understand it, and I agree to follow it. I understand that a breach may lead to disciplinary action.

Employee or contractor

Name:

Signature:

Date:

10. Roles and responsibilities

Role	Held by	Responsibility
Policy approver	[Policy approver role]	Approves this policy, each new version, and any risk the Company accepts instead of meeting it.
Policy owner	[Security owner role]	Maintains this policy, makes sure the controls in it operate, keeps the evidence, and reviews it at least once a year.
Device owner	[IT owner role]	Configures and monitors Company devices and keeps the asset inventory current.
All personnel	Everyone in scope	Follow this policy and report a suspected breach of it to the [Security owner role].

11. Evidence and records

The records below show that this policy operates. Each is dated, kept for at least [Evidence retention period], and stored where an auditor can be given it.

Record	What it shows	Where it is kept
Approved policy	This document, signed by the approver, with its version history.	[Documentation system]
Acknowledgment log	Each person signs section 9 at hire and again each year.	[Evidence storage location]
Device management report	Encryption, screen lock and update status for every Company device.	[Device management tool]
Asset inventory	Every Company device and its assigned user.	[Asset inventory]

12. Exceptions and enforcement

A deviation from this policy needs a written exception approved by the [Security owner role] before it begins. Each exception records the rule not met, the business reason, the compensating control and an expiry date no more than 12 months away. Exceptions are reviewed at each annual review.

A breach of this policy is handled under the Company disciplinary process and may lead to action up to and including termination of employment or contract. A breach that exposes customer data is also handled as a security incident.

13. Review and approval

The [Security owner role] reviews this policy at least once a year and after any significant change to the business, the systems in scope or the risks they face. The [Policy approver role] approves each version. Personnel are told of material changes and acknowledge the current version.

Version	Date	Summary of change	Approved by
[Version]	[Effective date]	First version.	[Policy approver role]

Policy approver

Name:

Signature:

Date:

14. Fields to complete

Replace every bracketed field in this document with your own detail, then delete this section.

Field	What to enter
[Company name]	Your legal company name.
[Effective date]	The date the approver signs this version.
[Version]	Start at 1.0 and increase it each time the document changes.
[Security owner role]	The role that runs the security program day to day, for example Chief Technology Officer.
[Policy approver role]	The officer who approves policies and accepted risks, for example Chief Executive Officer.
[Evidence storage location]	The shared folder or system where evidence is kept.
[Documentation system]	Where policies and procedures are published, for example the company wiki.
[In-scope personnel]	Who the policy covers, for example employees and contractors with access to company systems.
[Identity provider]	The single sign-on directory, for example Google Workspace or Okta.

Field	What to enter
[Device management tool]	The tool that enforces settings on company devices.
[Asset inventory]	Where devices and systems are listed.
[Screen lock timeout]	For example 5 minutes.
[Endpoint protection tool]	The anti-malware or endpoint protection on company devices.
[Removable media rule]	Whether USB drives and other removable media may be used, for example not permitted.
[Acknowledgment method]	How people confirm they read the policy, for example an e-signature.
[Ethics reporting channel]	Where concerns can be raised, anonymously where possible.
[Evidence retention period]	How long audit evidence is kept, for example three years.
[IT owner role]	The role that runs company devices and accounts, for example IT lead.
[Next review date]	The date this version must be reviewed by, at most 12 months after the effective date.

Source

Source: free template from www.polaralabs.com/templates/acceptable-use-policy (CC BY 4.0).