jamf

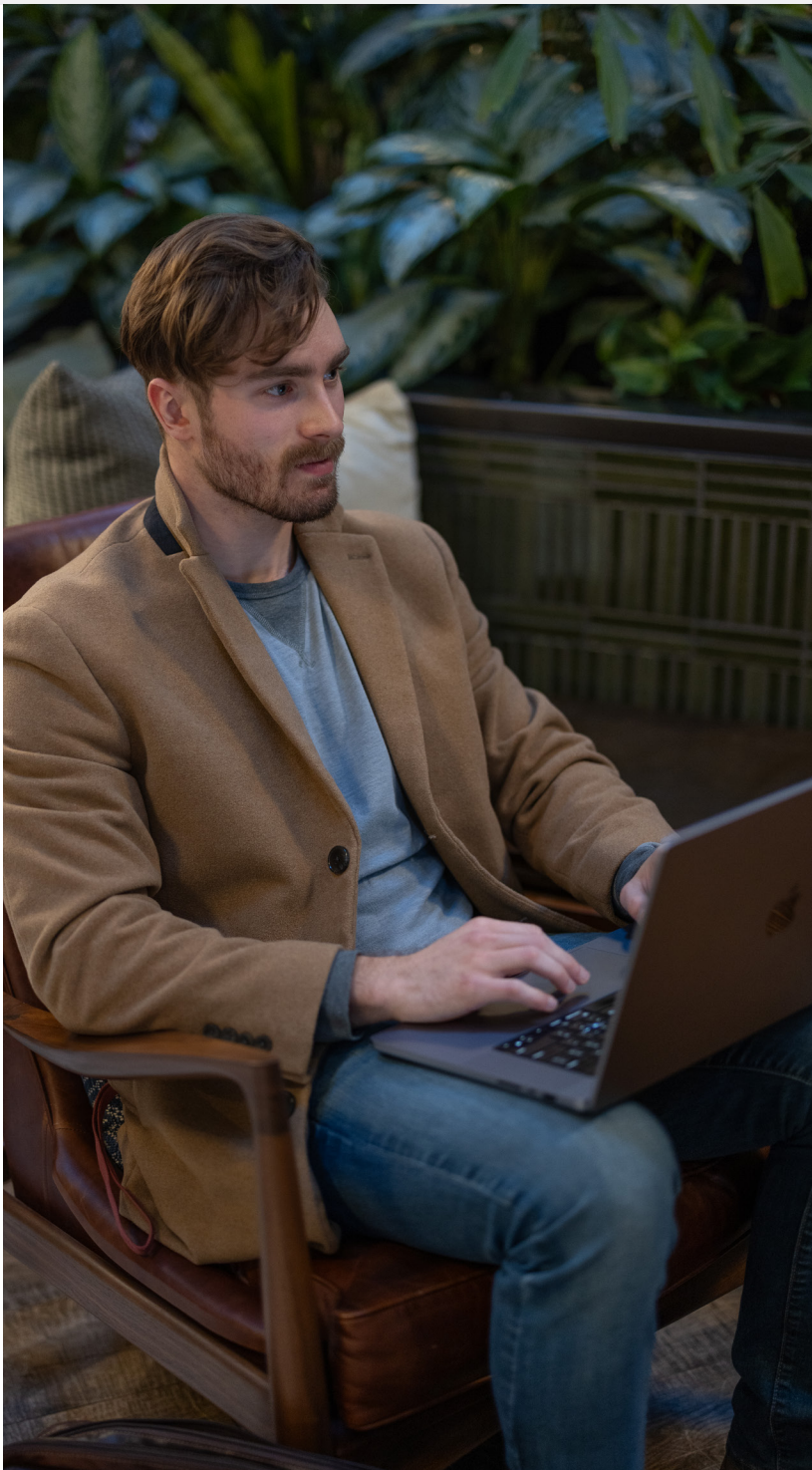
Best Practices:

Acceptable use policies and data management

If you've ever worked for an organization, you've probably had to sign an acceptable use policy (AUP) explaining the terms of your device and internet usage. AUPs are important for an organization's security, regarding both technology use and information.

In this paper, we'll discuss the best practices surrounding AUPs and data management, covering:

- What an AUP is and why it's important
- What goes into an AUP
- How organizations can create and enforce AUPs



What is an acceptable use policy?

At their most basic, AUPs are a set of rules an organization puts forward regarding how their resources, devices and network can be used. They may dictate:

What can be performed on their company devices or networks

How to use (or not use) social media related to the company

How to handle company information and trade secrets

What software, hardware, websites or applications may be accessed or downloaded

If and/or how much an employee can use company devices for personal purposes

Consequences of violating the AUP

And more

Organizations implement AUPs to reduce risky user behavior and their potential for legal liability. By providing expectations to their employees, it's also easier to support users and inform them of the consequences for policy non-compliance. It also creates a consistent experience for users and IT and helps maintain compliance with government regulations. Ultimately, this improves an organization's security posture by limiting unauthorized information transfer or misusage of company resources and networks.

Creating and enforcing AUPs

Evaluate

Before creating an AUP, it's necessary to understand where your organization stands, considering how users are interacting with your network and apps, how this interaction is relevant to their roles and how this helps accomplish your goals. Some questions to ask are:

What applications and data do users have access to and how can they download or access them?

Are users only assigned to the resources they need to perform their job functions (i.e. do they have least-privilege access)?

Where are users accessing the network from; are they using a VPN or Zero Trust Network Access (ZTNA)?

In what ways does a user's behavior or their device configuration put company or customer data or company reputation at risk?

How would a user accidentally or purposefully transmit data to unauthorized parties (e.g. social media, device compromise, email, etc.)?

What regulations must my organization adhere to?

These questions can be a good starting point to understanding what criteria need to be included in your AUP.

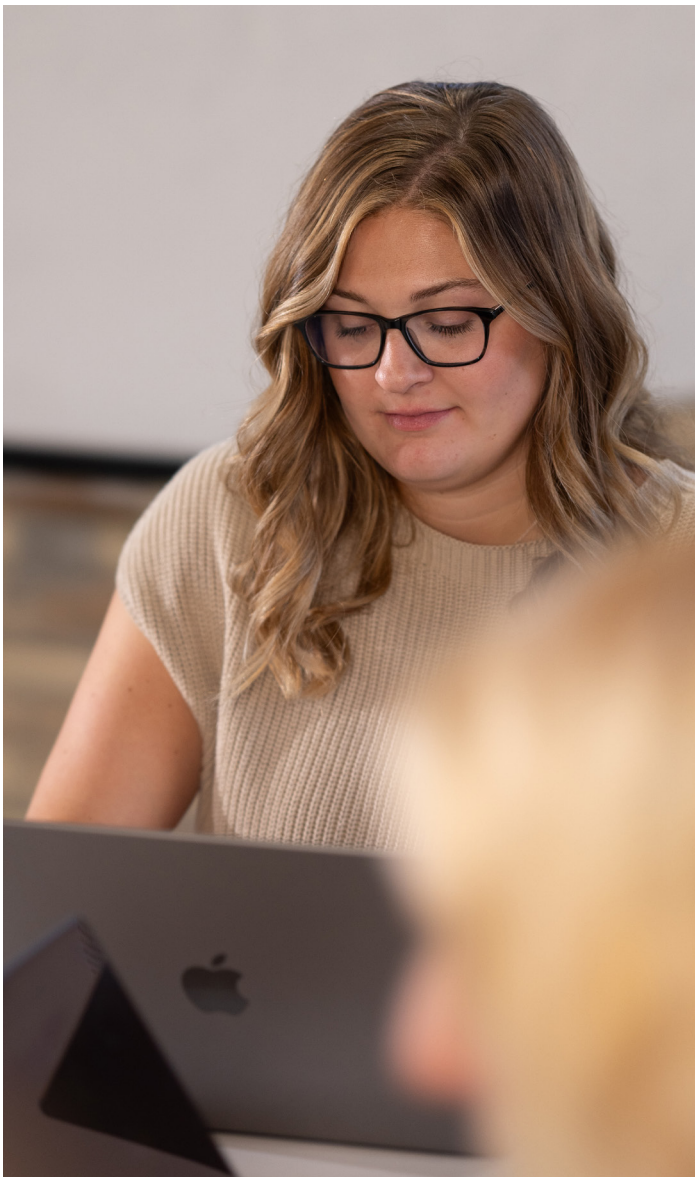
Identify

The next step is to identify what devices and users are subject to your AUP. Corporate-owned devices that are personally enabled (COPE) or devices in a bring-your-own-device (BYOD) program may need to be treated differently than fully corporate-owned devices. It can be difficult to restrict a user's behavior on a COPE or BYOD device that they're also using for personal use — if your security configuration is not set up appropriately, this introduces a lot of risk to your organization's security. It's necessary to consider how your policy can be enforced and how this relates to your security posture; for instance, are all devices with access to company resources required to enroll in mobile device management (MDM)?

Another consideration is how devices can connect to your network. For example, do you have a remote or hybrid workforce where users are connecting via their home or other unsecured networks? How does this inform what they are allowed to do on their devices or what they have access to? You might conclude that:

- Remote users' devices will have additional network protections to compensate for risky network.
- Your network configuration will implement Zero Trust Network Access (ZTNA) to remove access to the network from the network level if a device appears compromised.
- Your network will be segmented to prevent lateral movement in case a compromised device ends up on the network.

In other words, understanding how and where end users work can inform IT configurations — and vice versa. Let's dive into this in the next section.



Align

AUPs are only a part of your defense-in-depth security strategy and should align with security controls. **The Center for Internet Security (CIS)** controls provide guidance for businesses of all sizes — from those with a limited IT team to large enterprises with in-house security professionals.

Here are a handful of countless ways these controls can inform your AUP:

CIS Safeguard 1.1 — Establish and Maintain Detailed Enterprise Asset Inventory
This control recommends keeping a careful and up-to-date list of devices that connect to corporate resources. This can include corporate-owned, COPE and BYOD devices. In your AUP, you may require any devices that access any resources be enrolled in your MDM. This doesn't mean IT needs full supervision of these devices or that user privacy needs to be compromised; only work applications and software should be managed. This can be achieved in devices like the iPhone, which has totally separate work and personal containers that do not transfer data between them.

CIS Safeguard 2.3 — Address Unauthorized Software
This control recommends promptly removing any unauthorized software or carefully documenting any exceptions. In your AUP, you might restrict the download of any unapproved software that is not vetted by IT. You may also decide to offer software in a Self Service portal containing an approved set of software users can download.

CIS Safeguard 3.3 — Configure Data Access Control Lists
This control recommends creating a data access list based on a user's need-to-know — in other words, it recommends least privilege access. In your AUP, you may restrict users from accessing certain applications that are outside of their job function. Better yet, your network should be configured so they don't have access in the first place.

CIS Safeguard 6.3 — Require MFA for Externally-Exposed Applications
This control recommends requiring multi-factor authentication (MFA) for any third-party or corporate applications exposed to any network outside the internal corporate network. In your AUP, you may require users to use MFA — like a password and biometric data, for example — to log into any applicable applications.

CIS Safeguard 9.1 — Ensure Use of Only Fully Supported Browsers and Email Clients
This control recommends using only the most up-to-date and fully supported browsers and clients. This helps ensure these applications have the latest security patches and limits vulnerabilities. In your AUP, you may require devices to have updated software and may push these updates using MDM software.

There are a multitude of other CIS controls that affect your AUP and security posture in areas like accounts and identity, continuous vulnerability management, logging, incident response and beyond.

Repurpose

You don't have to start from scratch — thankfully there is professional guidance from security specialists for AUPs. CIS also offers an **Acceptable Use of Information Technology Resources Policy template** for more explicit guidance for your AUP. It contains sections like:

- Purpose and benefits
- Acceptable use
- Unacceptable use
- Occasional and incidental personal use
- Restrictions on off-site transmission and storage of information
- User responsibility for IT equipment
- Use of social media
- Compliance

And more!

Similarly, the SANS Institute offers a variety of **security policy templates**, including for an AUP. Their template, similar to the CIS one, also offers sections like:

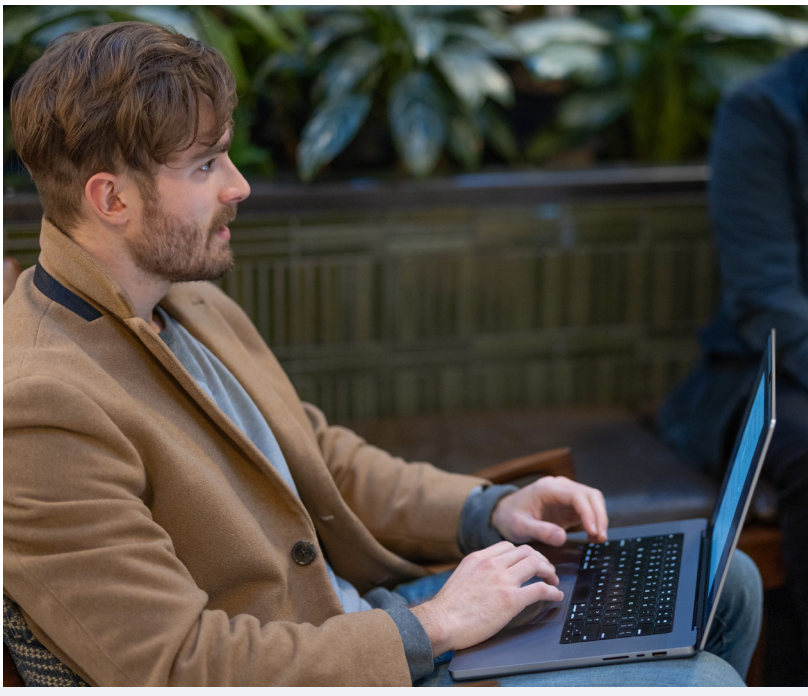
- Security and proprietary information
- Related standards, policies and processes
- Definition and terms

Enforce

It should be clear in your AUP that there are consequences for violations, intentional or not. Users are not only subject to repercussions from your organization, but to applicable laws. Any activity violating these laws, causing damage or harm, or negatively impacting other users should be addressed in your AUP.

Enforcing your AUP can be challenging too. In general, it requires:

- Being clear about what behavior is allowed or disallowed
- A deep understanding of devices and users on your network and their activity
- Network and security configurations that enforce security policies (e.g. ZTNA, Single sign-on (SSO) via identity provider, MDM enrollment, content filtering, endpoint detection software, network monitoring)
- Regularly communicating your AUP to employees
- Having a plan when a user violates the AUP, whether it's major or minor, accidental or purposeful

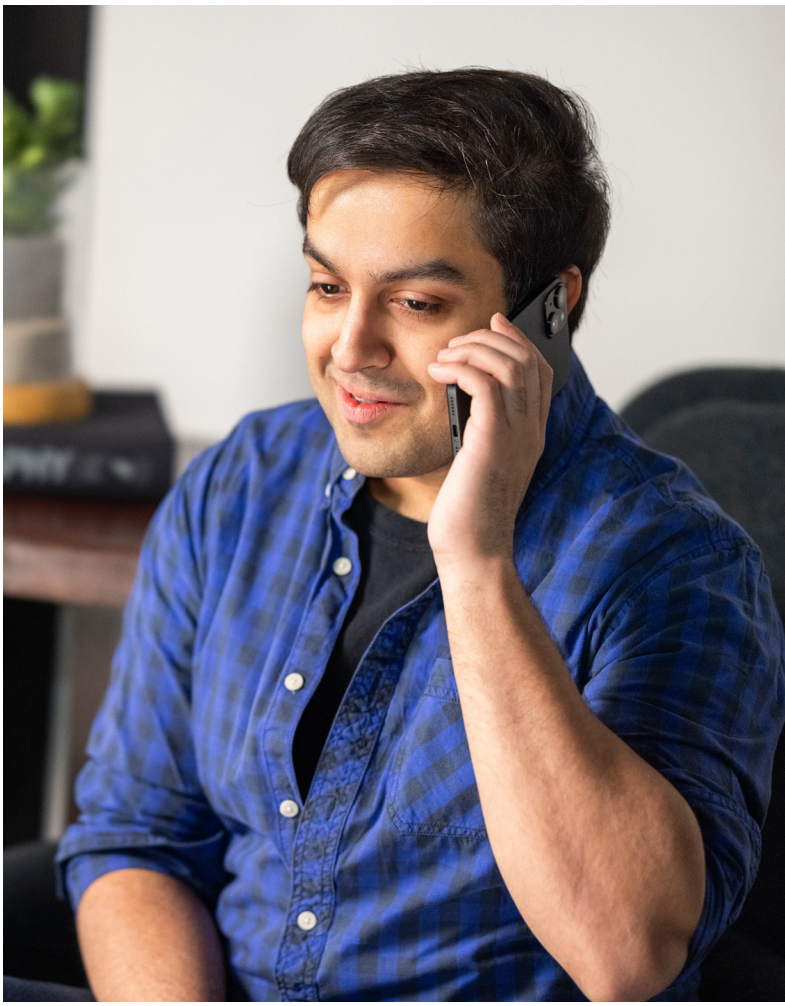


Key takeaways

Your AUP doesn't have to be another annoying form for employees to sign that's forgotten about as soon as they've submitted it. Instead, it provides guidelines and expectations for employee use, keeps them productive, reduces your company's liability and helps improve your organization's security. In other words, they're useful to have in your security toolbox.

Creating an AUP involves:

- **Evaluating** where technology use in your organization stands
- **Identifying** what users and devices are subject to your AUP
- **Aligning** your AUP with recommended security controls, like **CIS Controls**
- **Repurposing** AUPs already created by the security community — like from **CIS** or the **SANS Institute** — and tailoring them for you organization
- **Enforcing** your AUP with a combination of administrative and technical controls



Jamf can help enforce your AUP and keep your data in the right hands.

jamf

www.jamf.com

Request Trial

Or reach out to your favorite reseller to get started.