BEST PRACTICES:

AUPs

Acceptable Use Policies

As a cybersecurity professional, it's easy to shift focus toward the security controls that actively protect your organizational infrastructure, keeping data secured while mitigating the risk posed by bad actors, threats and numerous attacks. But there are other key elements to your organization's security. Acceptable Use Policies are a prime example.

What is an AUP?

An Acceptable Use Policy (AUP) is a set of rules identified by executives or the management arm of an organization that determines how the devices, software, data, services and resources are to be handled by users of those resources. AUPs explicitly restrict what stakeholders can and should not do.

Why are they important?

AUPs are necessary for several reasons. Most notably, guidelines implemented by organizations from all industries worldwide:

- Set expectations for end-user behavior
- Obtain acknowledgment that users are aware, understand and agree to the rules
- Restrict the use of hardware, software, networks and websites
- Align use policies with information security frameworks for data protection

Many organizations require users of their resources to sign an AUP to reduce the potential for legal liability. **Informing end users and employees of their rights and expectations for using organizational resources makes it easier to support users and communicate the consequences for policy non-compliance.**

Discover:

1. What Acceptable Use Policy means
2. Why they're an essential piece of your security posture
3. How to follow best practices to align an AUP with your existing data management strategy and strengthen your defense-in-depth plan

Best practices for creating and enforcing AUPs

1. **Evaluate.** Assess your organization's starting point. Consider how users should interact with resources, how access relates to their roles and how this fits business needs.

2. **Identify.** You may find your AUP applies to more than organizational devices. It's important to identify devices and users within scope of your policy. Consider if personal devices, like BYOD and user-enrolled devices, should be included. With this determination, IT administrators can implement the proper configuration to permit or deny access to their secure network based on inventory management data segments.

3. **Align.** AUPs should align information security frameworks, like the Center for Information Security (CIS). By aligning the administrative and security controls, AUPs are not a standalone document. They are part of a holistic strategy, which puts you one step closer to defense-in-depth with coverage across multiple layers of security.

4. **Repurpose.** You don't need to start with a blank page. Research and use resources that are available to help you craft an AUP that is customized to your organization's needs. From resources that provide specific verbiage that target unique requirements to broader templates developed by trusted organizations and trusted information security experts, like the SANS Institute's directory of security policy templates or the CIS Acceptable Use of Information Technology Resources Policy template.

5. **Enforce.** Any activities that are deemed harmful, violate local, state, federal or regional laws, negatively impact other users or cause damage – regardless of intention – must be addressed in your AUP. Remember that is is critical to indicate the jurisdiction in which the AUP applies. This may ease the legal burden should an incident that requires legal action arises. By specifically identifying to whom the AUP applies and the region where it is effectively enforceable, organizations that operate in multiple locales can account for the various degrees of legal liability which is geo-dependent.

jamf

www.jamf.com

We're here to help. Dive deeper into data policy and management with our beginner's guide or learn more about securing your workplace with Jamf Trusted Access.