THREAT INSIGHT

ActZero

Why Businesses Need An Acceptable Use Policy

Reducing risk from the inside out

Does your business have an acceptable use policy (AUP) regarding use of your organization's network, devices, and the Internet? Is the policy actively enforced, or is it a document that's only seen upon the point-of-hire? There are many reasons why your company needs an AUP, and why the document needs to play a bigger role in corporate governance.

Why have an Acceptable Use Policy?

Having a cybersecurity plan is more critical than ever. With the number and intensity of cyber attacks increasing, it is paramount that all companies — regardless of size — understand current cyber threats and what to do to prevent and combat them.

A crucial component of this cybersecurity plan, is an acceptable use policy. The acceptable use policy serves many key functions:

- It protects your business from any legal actions, while clearly communicating to employees your expectations regarding their behavior
- It provides a roadmap for your users to understand their responsibilities as they relate to your protected infrastructure, access, and information
- It serves as a living document that helps with understanding the latest threats and what to do to prevent them from impacting your organization
- It's the best first step to keeping your company and customer information safe
- It may limit or even safe harbour your liability around illegal file sharing, by discouraging, training against and monitoring for the practice

The key to successful AUP adoption

It is far better to lay out acceptable usage and get employees on board early than to having to spend cycles correcting behaviour and problems if something goes wrong. In a worst-case scenario, a staff member could introduce ransomware into the corporate environment simply by visiting a site that would have been blacklisted if you had an AUP in place, or sharing passwords in a public space. To be successful, your policies should be:

- Executed thoroughly and reviewed regularly. Security should never be a set it and forget it exercise
- Readily available to your employees
- Written in simple, everyday language; scrap the legalese
- Clear and concise; leave no room for interpretation
- Easily linked to documents if Isolated into separate policy statements, standards, and processes
- A corporate KPI; scoring the entire organization for compliance

Successfully implementing the AUP means overcoming traditional 'Set it and and Forget it' methods.

What should your AUP Include?

The basics of an acceptable use policy should include guidelines on your company's information assets (including but not limited to computer systems; software applications including cloud and 3rd party; storage media; communications systems; and, accounts providing email and Internet access), including policies on how to handle corporate and customer data. Typically, AUP policies include:

- **Purpose**: The business reason for the policy
- **Security Training Policy**: How employees and other users will be trained on the policy, as well as the general expectations on how to conduct themselves when using available resources
- **Data Classification and User Access Rights**: Data Classification helps users identify acceptable methods of use, storage, and transmission of files
- **Account/Credential management**: Policies around account access, passwords, and vendor access
- **Device, Network and Cloud use**: Detailed policies regarding use of corporate infrastructure and IT environments
- **Email and Social Media policies**: Parameters for which employees and 3rd party contractors can use email and social media for informational sharing
    - e.g. for company Internet. It may focus on banning specific sites (i.e. social media) or on prohibiting behaviors
- **Physical Access**: Rules and regulations regarding to access to and use of company offices and physical buildings
- **Enforcement**: Outlines how your business will monitor for AUP infractions
- **Infraction Handling**: Clearly identified penalties for infractions

Level-up your AUP now

Need a place to begin your policy journey? Our AUP template delves deeply into the aspects behind Acceptable Usage, including both IT-team and employee-facing guidelines for:

- Use of technology across multiple attack vectors (email, cloud, endpoint software),
- Network access, both on-prem and remotely,
- Monitoring by leveraging logs across your infrastructure
- Responding to an incident, and
- reporting a breach

Our template allows you to fill in the details specific to your organization, and provides a great starting point for thinking about your policies such that you can comply with regulatory frameworks. While it is not legal advice, this guiding document can help point your security program, and your ability to demonstrate progress within it, in the right direction.