Do You Have These IT Policies?

(If Not, You Should)

**By Rob Landis,
Binary IT Solutions**

IT policies are an important part of your IT security and technology management. So, no matter what size your business is, you should have them. Let's get you started with some of the most important IT policies your company should have in place.

Password Security Policy

A password security policy will lay out for your team how to handle their login passwords. It should include things like:

- How long passwords should be.
- How to construct passwords (e.g., using at least one number and symbol).
- Where and how to store passwords.
- The use of multi-factor authentication (if it's required).
- How often to change passwords.

Acceptable Use Policy (AUP)

The Acceptable Use Policy is an overarching policy. It includes how to properly use technology and data in your organization. This policy will govern things like device security. For example, you may need employees to keep devices updated. If this is the case, you should include that in this policy.

Cloud & App Use Policy

A cloud and app use policy will tell employees what cloud and mobile apps are okay to use for business data. It should restrict the use of unapproved applications. It should also provide a way to suggest apps that would enhance productivity.

Bring Your Own Device (BYOD) Policy

The BYOD policy clarifies the use of employee devices for business. Including the required security of those devices. It may also note the required installation of an endpoint management app. It should also cover compensation for business use of personal devices.

Wi-Fi Use Policy

Your Wi-Fi use policy will explain how employees are to ensure they have safe connections. It may dictate the use of a company VPN. Your policy may also restrict the activities employees can do when on public Wi-Fi. Such as not entering passwords or payment card details into a form.

Social Media Use Policy

With social media use at work so common, it's important to address it. Otherwise, endless scrolling and posting could steal hours of productivity every week. Include details in your social media policy, such as:

- Restricting when employees can access personal social media.
- Restricting what employees can post about the company.
- Noting "safe selfie zones" or facility areas that are not okay for public images.

For more information, call 610.320.2628 or visit www.binaryitsolutions.tech.