Infogressive

Cybersecurity **Solved.**

9 easy steps to BETTER CYBERSECURITY

Must-have security policies & procedures to implement now

TABLE OF CONTENTS

9 EASY STEPS TO BETTER CYBERSECURITY

So you already know how to protect your security online, but now you're wondering, *How does this apply to my business as a whole?*

Protecting the information systems in your business is not only a larger task, but a more complicated one. It requires deliberate and consistent efforts from every member of your team. Regulations must be established to protect your physical and technical security investments, safeguard the information contained in your systems, reduce business and legal risks, and protect the reputation of your company.

In this guide, you'll find 9 easy security policies and procedures to implement in your business to improve your cybersecurity posture.

ACCEPTABLE USE GUIDELINES

Whether your employees are issued a work desktop, laptop, tablet, or phone, it is important to have policies and procedures in place to regulate them.

1. Personal Use

Just as personal phone calls might be prohibited on company time, personal business should be prohibited on company devices in order to ensure your security. Advise employees to avoid using company devices to check personal email accounts, conduct personal financial business, or any other personal use of company property. Employees should also avoid conducting business from an offsite or unsecured network, but we will go deeper into that policy in the next section.

The reason for these policies is simple: unauthorized and unsafe use of company devices can open doors and invite attackers into your network. The end-user is the #1 target for attackers, so it is important that users eliminate as many of the "easy" opportunities that hackers may take. This includes using unsecured wifi networks, logging into personal accounts on unsafe websites, or accessing accounts secured by weak passwords.

2. Sharing of Property

It's important to also have policies in place that prohibit the sharing or loaning of company technology, devices, and accounts. Specifically, make it clear that devices must not be loaned or shared with any person outside of the company. This policy may seem intuitive, but ensure that it is written, followed, and enforced. An unauthorized person using your company technology or devices can put your network and your information at risk.

DIGITAL SECURITY POLICIES

Just as you have physical security procedures, you should also have standards in place that direct employees to properly secure their devices. At the most basic level, this means requiring passwords and other security features like lock screens to be employed on company devices and accounts.

3. Password Policies

First, implement a password changing policy. This can be enforced on a monthly, quarterly, bi-annual, or even annual basis. The frequency is up to your company, but keep in mind that the more frequently important passwords are changed, the more secure your accounts will be. This policy does not have to be enforced manually, either. Many accounts, like Office 365 and Microsoft Active Directory Services, have features built in that allow you to implement password expirations.

Next, require employee account passwords to be strong and secure. Here are a few characteristics of strong passwords:

- Contain both uppercase and lowercase characters
- Punctuation and symbols
- Minimum of 10 characters long
- Not based on personal information, like family names or important dates
- No use of common, easy-to-guess words or phrases

The combination of two or more of these requirements will lead to the strongest passwords. The more complicated the password is, the harder it will be to crack. Don't settle for employee accounts secured by passwords like "Password123."

Finally, prohibit the sharing, reuse, and duplication of business password or account information. Employees should not use the same passwords between company and non-company accounts, and they should also avoid using the same password across multiple company accounts. Advise employees to never write passwords or account information down, except for inside a secure password management application, if your company uses one. Also encourage employees to avoid the "remember password" feature on websites and in their browser.

4. Wireless Networks

Not only should your office network be secured by a strong password, but you should also advise employees to only use their company devices on password-secured wireless networks. That's right, that means no more McDonald's or coffee shop wifi for the company laptops. Unless you're setting up a VPN (Virtual Private Network) for employees to access outside of the office, it's best that everyone steers clear of unsecured, public wifi networks. These unsecured networks are like feeding grounds for hackers—putting your users and your devices at risk. Don't let your information become an easy target.

5. Device Policies

Company devices should be secured by a password-protected screensaver at minimum. This is one easy step to avoid a non-employee from physically accessing the information on a stolen or discovered device. The automatic lock feature should also be set for 10 minutes or less in order to secure devices left unattended. To strengthen this policy, you can also utilize device encryption software, which will be discussed further in the Hardware & Software section.

COMMUNICATION POLICIES

As covered in the first section, use of company accounts and devices for personal business should be prohibited for security reasons. For the same reasons, email communication activities and other forms of digital communication should be restricted to business-only activities as well.

6. Email Use

The email security features you deploy may do their part in keeping spam and phishing emails out of your users' inboxes, but the users must do their part as well. Ensure that the creation, sending, and forwarding of any type of unsolicited chain mail or advertisements is not conducted on company devices using business email accounts. This will minimize the risk to other users and to your network as a whole. Email is the most commonly-used method of attack for hackers, so it's important that your users are not spreading or inviting malicious activity into your email system.

HARDWARE & SOFTWARE

Employees can do their part in protecting the security of your company, but their efforts cannot stand alone. Here are three key security solutions that will take your defenses to the next level:

7. Encryption

As mentioned in the Digital Security Policies section, device encryption software can supplement and strengthen any device policies you have in place. An encryption software will lock down your information and require a key or password to access it. This encryption can be file-based or whole-disk encryption. If you're looking to protect the contents on portable devices like laptops, the disk encryption option is best for you. It works by locking down all of the contents on the hard drive of the device and placing them behind the encryption key. In the event of a lost or stolen device, a person could not access the contents of the hard drive, even if they removed it from the device. This option is an easy, low-maintenance solution that will not cause added stress to your devices or your users—all it requires is an extra password when the device is powered on.

8. Anti-virus Software

All those anti-virus programs are all the same, right? Not exactly. While having just about any anti-virus in place is a good first step, you want to look for a solution that will be effective against both known and unknown threats. Many traditional AV programs rely on signatures of known malware and cannot protect you against new or "zero-day" threats. For the best protection, look for a program that does not rely on signatures or reputation lookups. With the right anti-virus solution in place, you won't have to worry when the next ransomware attack makes the news.

But you don't need anti-virus software for Mac devices… right? Wrong again. While Macs are more difficult to infect and exploit, they are not unhackable. You'll need to deploy your anti-virus software on all of your devices, no matter what operating system they use.

9. Firewall

You may already have a firewall in place at your organization, and that's a great step. This section will cover information for those who may not already have a firewall and for those that are looking to improve their current setup.

First, a firewall is a device that filters the traffic that flows through your network. The device connects directly to the source of your internet service and acts as an extra layer of digital protection on the outskirts of your network. The most common metaphor is that it's the moat around your castle—if you think of your network as a castle where your valuable items are kept, you want an extra obstacle to keep attackers out of your kingdom.

If you already have a firewall, the next step is to ensure that it is properly configured and doing its job effectively. These are not just set-it-and-forget-it devices. They need to be configured, monitored, and patched in order to provide the most protection to your network.

Not sure you have the manpower and expertise to keep up with your firewall? Try looking into a managed security service provider who can help maintain and manage your device.

WHEN IT COMES DOWN TO IT...

If you've made it this far, you're probably thinking, "Wow, security is a lot of work."

...and you would be right.

> *Security is hard... because it's supposed to be.*

But it's worth it in the end. With only a few extra steps, you can protect your employees, your customers, your information, and your business's identity from being breached.

WANT TO LEARN MORE ABOUT IMPLEMENTING THESE POLICIES IN YOUR COMPANY?

We're a ***Managed Security Services Provider,*** *and we're here to help. Contact us about any of your cybersecurity needs.*

CONTACT US