# How to Use Impact’s Cybersecurity Policy Template

This template is designed to be an easy framework for companies to download, customize with their own information or additional policies, and implement in their organization.

This document offers a variety of best practices that help organizations begin addressing cybersecurity more intentionally.

## Customizing the Template

This template uses placeholders throughout, notated by highlighted brackets (i.e [placeholder]), which should be replaced with company-specific information. After downloading, you can use the find and replace tool in your Word processing program to substitute all instances of [company name] and other [placeholders] with your business’ actual information.

Be sure to review all of the sections in this template thoroughly to ensure that they’re relevant to your organization. For instance, there are some sections that address regulations or situations that may not apply to you. These are notated with **(OPTIONAL)**.

Additionally, some of the requirements outlined in this template are time-based. For example, Impact suggests requiring employees to change their password every 90 days. However, you can adjust that length of time as you see fit.

## Storing and Sharing the Policy

Store this document in a place that’s easy to access for all employees at all times. For this reason, we suggest emailing it to your team and hosting it on your company intranet with a link on the homepage or any other place where staff regularly find company information. Additionally, introducing employees to these practices should be a standard part of onboarding for new hires.

## Expanding and Adding to the Policy

While the information included in these guidelines will help improve your organization’s cybersecurity and should be shared with your staff in places with high visibility, it does not constitute a fully-fledged cybersecurity policy.

To build a comprehensive strategy that goes into depth, offers complete coverage, and keeps your network secure, [consult with an expert](https://www.impactmybiz.com/get-started/?utm_source=gated-content&utm_medium=template-word-doc&utm_campaign=impact-cybersecurity-policy-template) who can help you craft a custom cybersecurity policy suited to your specific security needs.

# Cybersecurity Best Practices

The sections detailed in this document outline some of the best practices you can follow to easily improve [company name’s] cybersecurity.

By following these practices, you will be operating with a security-first mindset, contributing to a culture of cybersecurity.

## Defining Confidential Data

Confidential data is personal and/or highly sensitive. It is often the subject of ransomware, social engineering, and other cyberattacks, and needs to be protected.

Some examples of confidential data include:

* Classified and/or unpublished financial information.
* Personal customer, vendor, or partner information.
* Patents, informational property, formulas, or new technologies.
* Any protected information subject to governance from local regulations or industry standards.

Many of the policies below are designed to protect exactly this kind of confidential data as you use it to perform your job.

## Device Security

All smart devices, such as smartphones, tablets, and other network-enabled devices, need to be secured. This is to maintain the integrity of the network, protect all users, and minimize our cybersecurity risk level.

To secure company smart devices, you should:

* Keep devices password-protected and update passwords regularly.
* **(OPTIONAL)** Sync with [company name’s] multi-factor authentication app, [app name].
* Only access [company name’s] cloud-based platforms from secure internet networks.
* Install device updates regularly and on time.
* Never leave your devices unlocked and unattended.
* Install browser updates regularly and on time.

### Downloading Software to Company Devices

* If software needs to be downloaded it should be accompanied by approval from [the appropriate authority].
* Any software that [the appropriate authority] does permit an employee to download must be done legally and without the violation of any licensing regulations.
* If an employee believes that any damage occurred as a result of downloading software or files, the employee must immediately advise [the appropriate authority].

### Internet Usage

* Use caution when accessing the internet so you don’t jeopardize the interests of the company.
* Before using the internet through the company’s network, employees should first log in using their unique credentials.
* Any personal use of the internet should be on the employee’s own time and should not interfere in any way with the employee’s responsibilities.
* The company reserves the right to monitor each employee’s access to and use of the internet.
* Employees should be prohibited from accessing the internet for any unethical purposes, including pornography, threatening violence, gambling, racism, harassment, or any illegal activity.

## Email Security

Emails are a primary avenue through which scammers conduct cyberattacks. To minimize the risk of a security breach via email, employees should follow these email security practices:

* Look for extensive, obvious misspellings and grammatical errors in the body of the email.
* Double check the sender’s email address and be wary of tricks like replacing “o”s with “0”s.
* Never open attachments from unrecognized senders.
* Be cautious around clickbait titles (like those offering prizes).
* Forward suspicious emails to the IT / cybersecurity team and mark them as potential spam or phishing threats for further investigation.

## Password Management

Strong employee passwords are an important line of defense when it comes to cybersecurity. Your credentials are often the first line of defense between you and a malicious actor. By following these password guidelines, you can significantly reduce cyber risk within the company.

* Passwords should be at least 12 characters in length.
* Passwords should contain at least one number, one special character, one lower case letter, and one upper case letter.
* Passwords should be changed every [90 days].
* Refrain from writing down passwords.
* Do not use the same password across multiple accounts and do not repeat passwords more than once every two years.
* Avoid sharing your password with other employees.
* Under no circumstance should any employee of [company name] ask for another’s login credentials.
* **(OPTIONAL)** Enablethe company’s multi-factor authentication app, [app name].

***(OPTIONAL: Include the below section if your company uses password management software to track and store credentials.)***

[Company name] uses [password management software] to securely store credentials. When using it, follow these guidelines:

* Do not access the password manager from an unsecure network.
* Do not copy, store, or share credentials on the password manager anywhere else.
* Do not access the password manager and then leave your work station unlocked and unattended.
* Employees should only access tools needed to complete the responsibilities of their role.

## How to Secure Data Transfers

The following are some basic guidelines for securing data transfers within your organization:

* Avoid the unnecessary transfer of sensitive or confidential information.
* Verify any recipient, inside or outside the company, of any data being sent or received.
* Whenever possible, use the company network to share or transfer sensitive data. Similarly, do not share any confidential data over unsecured networks.
* Report scams, cyberattacks, and suspicious network activity.
* If you’re uncertain about how to safely and securely transfer sensitive information, consult the IT team.

## **(OPTIONAL)** Local Laws and Industry Regulations

[Many states and industries have specific laws and regulations pertaining to the collection, storage, use, transfer, and safekeeping of sensitive personal information.

For example, if you’re in healthcare, you may need to adhere to HIPAA guidelines. If you’re operating in California, you’ll be required to follow the regulations laid out in the California Consumer Privacy Act (CCPA). This section is designed to be a catch all for any additional rules you may already have in place to stay compliant with those regulations.]

***[Refer to local, state, and industry regulations to fill this section out appropriately. If you’re not sure what you need to do to stay compliant, consider getting in touch with*** [***Impact’s cybersecurity and compliance experts***](https://www.impactmybiz.com/cybersecurity/compliance-services/?utm_source=gated-content&utm_medium=template-word-doc&utm_campaign=impact-cybersecurity-policy-template)***.]***

## Training and Cybersecurity Awareness

The first line of defense against cyberattacks is not a piece of technology; it’s you. Follow these rules around [company name’s] cybersecurity training program to make sure you are informed, aware, and can fully participate in [company name’s] culture of security.

* Take the initial [training software] training program within 90 days of onboarding
* Stay up to date by regularly taking updated modules from [training software] on a [weekly/monthly/yearly] basis
* Always report phishing attempts as some of them will be from [training software/our security team], testing your ability to identify malicious emails

The security team may also assign additional trainings on an as-needed basis. For instance, staff who fall for a faux phishing email may be required to complete an additional cybersecurity awareness training.

Other incidents that may lead to additional cybersecurity trainings can include but are not necessarily limited to:

* Documented failure to follow the guidelines listed in the Password Management section above.
* Using another employee’s credentials.
* Transferring sensitive information over an unsecured network.
* **(OPTIONAL)** Failing to use a VPN when working remotely.

## **(OPTIONAL)** Remote Staff Guidelines

When working remotely, please follow these additional security best practices:

* Don’t access the company network from public or unsecured networks.
* Use a VPN.
* ***(If provided)*** Refrain from using devices other than those provided by the company when working.
* Don’t use public charging stations for company devices.
* Take extra care to never leave devices unlocked and unattended.

***[Consider including these additional tips to take remote cybersecurity practices even further if your company deals heavily with sensitive information.]***

* Lock your home office when not present.
* If working in a public place, use a personal hotspot that can be encrypted.
* Change passwords before and after any travel.
* Be attentive to your surroundings and don’t let strangers see your screen.

## Disciplinary Action

All staff are expected to follow these best practices to the best of their ability to keep [company name] secure, and actions that lead to the company’s harm will not be tolerated.

As such, every breach should be reviewed on an individual basis and corrective measures taken as necessary.

Some disciplinary examples include, but are not limited to:

* Additional awareness training for employees who click on malicious links or emails.
* System privileges revoked if inappropriate internet usage is observed, or if other cybersecurity practices are intentionally violated and/or repeatedly ignored.
* If an account is breached with no involvement of the employee, additional cybersecurity awareness training may still be assigned.

If an employee is found directly and intentionally responsible for the breach, disciplinary action up to and including termination and legal action can be exercised.

## The Big Picture

When it comes to cybersecurity, everyone has a crucial role to play. By taking the guidelines detailed in this policy to heart, you can help protect colleagues, clients, and the organization as a whole.

***[***[***Get in touch with a cybersecurity expert today***](https://www.impactmybiz.com/get-started/?utm_source=gated-content&utm_medium=template-word-doc&utm_campaign=impact-cybersecurity-policy-template) ***who can guide you through everything you need for a modern and comprehensive strategy, including a thorough and personalized policy, that offers you as much protection as possible.]***