# **Sample cyber security policy template**

We have developed this cyber security policy to highlight the security needs that we focus on for our client’s businesses. This template is ready to be edited to your company’s needs and should be considered a starting point for setting up your employment policies.

*Disclaimer: This sample policy/ template is meant to provide general guidelines and should be used as a reference. It may not take into account all relevant local, state or federal laws and is not a legal document. Neither the author or Cloud Cover LLC will be responsible or assume any legal liability that may arise from the use of this policy.*

## **Policy brief & purpose**

*Our company’s cyber security policy outlines our guidelines for preserving the security of our data* *and technology infrastructure.*

*The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may put our company at risk of financial loss and reputational damage that many companies do not recover from.*

*For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. This policy is designed to outline these instructions.*

## **Scope**

This policy applies to all our employees, contractors, volunteers, and anyone who has permanent or temporary access to our systems and hardware including third party partners and vendors.

## **Policy elements**

### **Confidential data**

Confidential data is any information that would be considered secret and valuable. Common examples are:

* Unpublished financial information
* Data of customers/partners/vendors
* Patents, formulas or new technologies, intellectual properties, company created materials
* Customer lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

### **Protect personal and company devices**

When employees use theirdigital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company-issued computer, tablet and cell phone secure. Here are some best practices:

* Keep all devices password protected.
* Choose and upgrade a complete antivirus software.
* Ensure they do not leave their devices exposed or unattended.
* Install security updates of browsers and systems monthly or as soon as updates are available.
* Log into company accounts and systems through secure and private networks only.

We also advise our employees to avoid accessing internal systems and accounts from other people’s devices or lending their own devices to others.

When new hires receive company-issued equipment they will receive instructions for:

* [*Disk encryption setup*]
* [*Password management tool setup*]
* [*Installation of antivirus/ anti-malware software*]

They should follow instructions to protect their devices and refer to our {IT department or 3rd party IT management firm} if they have any questions.

### **Keep emails safe**

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

* Avoid opening attachments and clicking on links when the content is not adequately explained
* Be suspicious of clickbait titles (e.g. offering prizes, advice.)
* Check email and names of people they received a message from to ensure they are legitimate.
* Look for inconsistencies in the language. (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn’t sure that an email they received is safe, they can refer to our {IT department or 3rd party IT management firm} if they have any questions.

### **Manage passwords properly**

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won’t be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

* Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed or found on social media. (e.g. birthdays, children’s names, etc.) You can also use a strong passphrase but you must be certain that the passphrase has more than 14 characters and includes spaces between each word and includes punctuation.
* Remember passwords instead of writing them down. If employees need to record their passwords, they are obliged to use a password manager.
* Exchange credentials only when absolutely necessary. When exchanging them in-person isn’t possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
* Change their passwords every two months.

Remembering a large number of passwords can be daunting. We will purchase the services of a password management tool which generates and stores passwords. Employees are obliged to create a secure password for the tool itself, following the abovementioned advice.

### **Transfer data securely**

Transferring data introduces security risk. Employees must:

* Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our {IT department or 3rd party IT management firm} for help.
* Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
* Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
* Report scams, privacy breaches and hacking attempts

Our {IT department or 3rd party IT management firm} need to know about scams, breaches, and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our {IT department or 3rd party IT management firm} must investigate promptly, resolve the issue, and send a companywide alert when necessary.

Our {IT department or 3rd party IT management firm} are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

### 

### **Additional measures**

To reduce the likelihood of security breaches, we also instruct our employees to:

* Turn off their screens and lock their devices when leaving their desks.
* Report stolen or damaged equipment as soon as possible to [*HR/ IT Department*].
* Change all account passwords at once when a device is stolen.
* Report a perceived threat or possible security weakness in company systems.
* Refrain from downloading suspicious, unauthorized, or illegal software on their company equipment.
* Avoid accessing suspicious websites.

We also expect our employees to comply with oursocial media andinternet usage policy.

Our {IT department or 3rd party IT management firm} will/have:

* Install firewalls, anti malware software and access authentication systems.
* Arrange for security training to all employees.
* Inform employees regularly about new scam emails or viruses and ways to combat them.
* Investigate security breaches thoroughly.
* Follow this policies provisions as other employees do.

Our company will have all physical and digital shields to protect information.

### **Remote employees**

Remote employees must follow this policy’s instructions too. Since they will be accessing our company’s accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage them to seek advice from our {IT department or 3rd party IT management firm}

## **Disciplinary Action**

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

* First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
* Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.  
  We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will faceprogressive discipline, even if their behavior hasn’t resulted in a security breach.

### **Take security seriously**

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind. After all, a breach would not just affect and damage the company, but also every employee, partner, customer and their families would feel the effects.

|  |
| --- |
| *Disclaimer: This policy template is meant to provide general guidelines and should be used as a reference. It may not take into account all relevant local, state or federal laws and is not a legal document. Neither the author nor Workable will assume any legal liability that may arise from the use of this policy.* |