CYBER SECURITY POLICY

While using the Internet, e-mail, and other electronic mediums is necessary for remote work, employees of [Company Name] are advised to use digital systems responsibly. Irresponsible use of digital platforms puts [Company Name] and our clients at risk. This policy outlines the guidelines for the acceptable use of [Company Name]'s technology systems.

Questions regarding the appropriate use of [Company Name]'s electronic communications equipment or systems, including e-mail and the Internet, should be directed to your supervisor or the information technology (IT) department.

Confidentiality and Monitoring

All technology provided by [Company Name], including computers, company programs, company work records, and other information stored electronically, is the property of [Company Name]. As such, [Company Name] reserves the right to monitor and access e-mail and other electronic communications, files, and all other content, including Internet use, transmitted by or stored in its technology systems.

Employees must be aware that internal and external e-mail, voice mail, text messages, and other electronic communications are considered business records and may be subject to discovery in the event of litigation.

Appropriate Use

[Company Name] employees are expected to use technology responsibly and productively, and solely for job-related activities.

Employees may not use [Company Name]'s e-mail or other electronic mediums to send, retrieve or store any communications or other electronic media of a discriminatory or hostile nature.

Employees are prohibited from downloading software, or other program files, from the Internet without prior approval from the IT department. All software should be passed through virus-protection programs prior to use. Failure to detect viruses, or other malware, could result in unauthorized entry into company systems and cause damage to [Company Name]'s infrastructure.

Best Security Practices

In order to accomplish the previously outlined expectations, the following best practices should also be respected to ensure maximum cybersecurity:

Employees must use strong and unique passwords for all accounts, and passwords must be changed on a [time basis]. Using computer-generated passwords is a good practice that allows for unique passwords. Passwords should not be shared with anyone, nor should passwords be saved in multiple locations.

Employees must only access company data and systems that are required for their job duties. Access to sensitive and confidential data is restricted unless the information is needed to perform specific job duties.

All company data and information must be protected against unauthorized access, modification, or disclosure. Utilizing a secured wireless internet connection and refraining from using a public internet connection is a way to avoid unauthorized access to company data.

Incident Response Protocol

In the event of a suspected security incident or a breach, employees must report the incident to the information technology (IT) department immediately. Employees must also answer any questions the IT department may have regarding a suspected security breach.

I have read and fully understand this policy.

____

(Signature)

____

(Print Name)

____

(Date)

These template policies were provided by Nonprofit Resources and are **available for download at nonprofitresources.us/policies.**

For more info, contact us at info@nonprofitresources.us