[Company Name] - Security Policy

Prepared by: The Penn Group, LLC

This is a sample security policy, intended to be used as a template. It is important that companies review their own corporate structure, identify, and prioritize corporate requirements and risks, and customize this policy template to meet the business needs of the company.

Table of Contents

Change History

Version	Date of Change	Author(s)	Description of Change
1.0			

Purpose

The purpose of this cybersecurity policy is to prevent the loss, unauthorized access, disclosure, destruction, and alteration of *[Company Name]* information produced by, entrusted to, or under the control of *[Company Name]*. This policy identifies and documents the rules, responsibilities, and procedures for all individuals accessing and using *[Company Name]* information, infrastructure, assets and resources to continuously provide for the confidentiality, integrity and availability of company information systems. This cybersecurity policy is built on standards, guidelines, and specific procedures that have been determined appropriate to ensure the best affordable protection and practices are in place to securely support the growing customer and organizational needs of *[Company Name]* information systems. A violation of this policy may result in disciplinary action.

Cybersecurity components.

The fundamental components of cybersecurity, often referred to as the cybersecurity triad, are:

- **Confidentiality.** Provides protection of assets from unauthorized entities. The company's information and information entrusted to the company (i.e., personal, financial, vendor, partner, etc.) should only be accessible to personnel, or systems, that have been given expressed and documented permission.
- **Integrity.** Provides assurance that the information is trusted and not manipulated. The assurance that the data and assets are uncorrupted, complete, and any modification of assets is handled in a specified and authorized manner.
- **Availability**. Provides assurance that the infrastructure, services, and systems will be accessible and available to authorized users when needed. This is tied to business continuity, redundancy, and resilience. Availability may be affected by cyberattacks, misuse, or environmental risks, such as hurricanes, floods, or earthquakes.

Information Security Objectives.

[Company Name] is committed to ensuring the protection of all aspects related to information and data assets of the organization. This includes ensuring that regulatory compliance, contractual, and operational requirements are satisfied. The following is a list of cybersecurity goals for *[Company Name]:*

- Maintain compliance with all current and applicable federal, state, and local laws and regulations.
- Establish and apply security controls to provide protection *[Company Name]*against information systems and data against threats, such as cyber attack, theft, or loss.
- Ensure all employees, from the top down, are educated …..
- Privacy and personal data …
- Resiliency, continuity, and availability of information systems and infrastructure tied to business functions and prioritized assets. …
- Guidance and methods from ISO, NIST, etc.
- Ensure vendor and external service providers are compliant with *[Company Name]* cybersecurity policy and requirements. …

Internet and computer acceptable use policy.

This policy applies to all [company name] employees provided authorized access to *[Company Name]* computing and communications resources.

[Company Name] recognizes that having access to the internet and e-mail from the workplace is necessary to perform the activities of employment. Unauthorized access and inappropriate use of systems

can place the company, the employees, shareholders, customers, and partners are risk. This policy documents the guidelines for acceptable us of [company name] computers, network, and communications systems, to mitigate the risk.

Employees are trusted to use company-provided technology responsibly and in an appropriate manner in accordance with job requirements. Internet access and email use is provided as a privilege for work-related activities. Minimal personal use is acceptable, with discretion.

Company employees shall not use *[Company Name]* provided internet, email, or any company-furnished communications devices to transmit, receive, retrieve, or store data or content that may be viewed or interpreted as defamatory, pornographic, harassing, or discriminatory.

All employees are responsible, and are held accountable for, transmitted, stored, or downloaded content of text, images, audio, video associated with the company's internet and email infrastructure.

It must be understood, by all employees, that there should be no expectation of privacy, when using company information systems or communications networks.

In order to ensure protection of the company's corporate interests, *[Company Name]* reserves the right to monitor, access, record, copy, filter, retrieve, search, modify, and/or delete any document or message, that has been composed, sent, received, or stored on company information systems and log files related to usage. At every login, users will be made aware of the fact that the company monitors the systems that they use.

All outgoing e-mail communications will identify the company and, therefore, shall reflect company ethics, values and will reflect appropriate language, content, and conduct.

Prohibited activities.

Prohibited activities include, but are not limited to:

- Abusive, offensive, profane, or disparaging remarks or language.
- Illegal activities, such as piracy, extortion, cracking, hacking, and unauthorized access to computers or hosts on the company network or the internet.
- The intentional downloading, installing, or running of malicious code, software, or program (e.g., virus, worm, bot, trojan horse, etc.) intended to cause damage to or place excessive load on the network, subnet, host or computer system.
- Sharing of passwords, usernames, or forms of login credentials.
- Downloading of unauthorized applications, program files, software, or online services from the internet without prior approval from the IT support department.
- Sender obfuscation or hiding. It is prohibited to send an email or other electronic communication with the intent to hide the identity or association of the sender.
- The use of a computer or user account that the user/employee is not authorized to use. Obtaining a password or other login credentials for a computer account to access the system.
- Attempts to circumvent data protection, event logging, or auditing activities.
- Disruption of services and activities impacting infrastructure availability. This includes sending or receiving large files and spamming activities. This also includes any activity that interferes with normal operation of network, hosts, computers, peripherals, or terminals.
- Copyright infringement. Copyrighted materials attributed to non-[company name] persons or entities shall not be transmitted by employees via the company internet connected infrastructure without the copyright holder's permission.

- Solicitation for political, religious, or commercial endeavors, or organizations without prior and proper authorization.

Confidentiality

The protection and understanding of confidential information is of the utmost importance at *[Company Name]*. For the purposes of this policy, Confidential information is information that is disclosed to an individual employee or becomes known to that employee in the course of the employee's employment at *[Company Name]*, and not generally known outside of the company, or is protected by law. Confidential may include proprietary information, trade secrets, private or personal information. Employees will, in the course of their duties, receive and handle confidential information regarding our company, other employees, our clients, partners, and vendors. We are committed to ensuring that this information remains protected. This is important to the company because it is a legal obligation and it allows us to maintain a competitive advantage, which constitutes an important cornerstone of our business.

Each employee shall have the following responsibilities regarding *[Company Name]* Confidential Information:

- During employment and after the termination of employment, an employee will hold all confidential information in trust and confidence, and will only use, access, store, or disclose confidential information, directly or indirectly, as appropriate in the performance of the employee's duties for *[Company Name]*.
- All employees and authorized users of *[Company Name]* must comply with all applicable state and federal laws and *[Company Name]* policies relating to access, use, and disclosure of confidential information, including but not limited to the Family Educational Rights and Privacy Act (FERPA); Health Insurance Portability and Accountability Act (HIPAA); and Payment Card Industry (PCI) standards and related policies.
- All employees and authorized users, prior to being granted access to internal *[Company Name]* will sign a non-disclosure agreement (NDA).
- Employees will not remove materials or property containing confidential information from company physical or logical spaces unless it is absolutely necessary in the performance of the person's job duties. Removal of confidential information materials will be handled appropriately.
- Lock or secure confidential information at all times.
- When no longer needed, documents containing confidential information shall be properly destroyed.
- For questions relating to appropriate use or disclosure of confidential information, consult with the immediate supervisor or other appropriate management personnel.

Data Protection

[Company Name] is committed to protecting the proprietary data of the company, personal data and to ensuring compliance with applicable data protection and privacy laws. Data Protection describes the methods and policies in place to secure data against unauthorized access, compromise, or loss.

The *[Company Name]* policy on data protection is to ensure that the company will follow best practices and comply with data protection laws of the state, federal, and international laws that apply. *[Company Name]* follows best practices to protect against the risk of unauthorized access resulting in a data breach and protects the interest of company stakeholders and the rights of employees, partners, and consumers.

General Data Protection Guidelines.

Every employee shares a responsibility for ensuring data is collected, stored, and handled properly, and in accordance with this policy.

- Data collection shall be limited to that which is consistent with the context of the specific transaction or the consumer's relationship as required or specifically authorized by law.
- If data must be transferred electronically, it will be encrypted before prior to the transfer. The IT department can be contacted for encryption methods and details on how to send data to authorized external contacts.
- Electronically stored data shall be protected from unauthorized access using robust identity and access management techniques, such as strong passwords, multi-factor authentication, and group policy.

Personal Data and Privacy Protection.

For the purposes of conducting business functions, it is often required to collect, store, process, transmit, and use certain information about individuals. This may include customers, suppliers, business contacts, employees, and other personnel, for which the company has a relationship or may need to contact.

Personal information has no real value to the company unless it can be used for legitimate business purposes. It is when this data is accessed, transmitted, or used that it is at the most risk of theft, exploitation, or loss.

Training is provided to all employees to ensure responsibilities for handling personal data is clear and understood all company personnel.

[Company Name] adheres to the following data protection guidelines:

- Only the personnel who are required, due to the nature of their position, shall access personal data.
- Access to personal data is controlled through strict administrative and technical access control.
- Data shall not be shared informally or to unauthorized personnel.
- Data shall be reviewed and updated on a regular schedule. If data is determined to be out of date, no longer relevant, or needed, it will be deleted or destroyed appropriately.
- Express consent shall be obtained prior to the collection of personal data and clear notice will be provided to consumers of the collection of personal data use and sharing practices.
- When personal data is being used, *[Company Name]* employees shall ensure computer screens computers are always locked when left unattended.
- Personal data should not be saved on desktops or local drives.
- Details on how personal data is stored, used, and processed shall be provided upon request.

End Point Usage.

Text

Auditing and Logging.

Text

Business Continuity, Disaster Recovery and Resilience.

Tied directly to availability, business continuity and resilience, the ability of the company to recover quickly after any type of disruption, corruption, compromise, or loss is a key element to data protection.

Data shall be backed up frequently. Backups will be tested on a regular basis in accordance with the company's backup policy and procedures.

Awareness and Training

It is important that company employees understand and are briefed on the policy for use of company computers. Users will receive initial cybersecurity awareness training at the time of hire and subsequent annual refresher training to ensure they are kept aware of their responsibilities and any new threats.

Maintenance and Review

Text

Terms and Definitions

Text

Data Breach. The unauthorized access, acquisition, or disclosure of computerized or electronic data that compromises the security, confidentiality, or integrity of personal information.

Conclusion.

Text