Date: 03/28/19

Version 1.0

Cybersecurity Policy Template

# 1. 0 Purpose

To provide our members a template that can be modified to develop a Cybersecurity Policy for their company. The policy should define an overarching strategy that guides the development of all other supporting IT security policies. The policy should identify and be derived from the regulations governing the company’s industry. Additional references and review should include identification of specific data breach notification laws in the states in which the company is registered.

Cybersecurity impacts all IT systems and is designed to mitigate the risks associated with the information on those systems. Mitigating risks includes taking preventative measures to prevent information from being stolen, compromised and/or destroyed through various means (viruses, malicious code, physical theft).

# 2.0 Regulatory Review

The company should undertake a regulatory review of the applicable laws and regulations by which the cybersecurity policy is established. Presented below is a preliminary guide of the regulations to be considered:

* HIPAA - Health Information Portability and Accountability Act
* State Data Breach Notification Laws/Privacy - see our Data Breach Fact Sheet
* 23 NYCRR 500 - Cybersecurity Requirements for Financial Services Companies
* NIST 800-171 - Cybersecurity Requirements for Defense Contractors
* Gramm-Leach-Bliley Act - Consumer Protections for Financial Services
* FTC - Consumer protections (affects consumers affected by data breaches)
* California Consumer Privacy Act - enhances privacy protections for California residents

After the review is conducted, include the list of regulations the company will comply with and under which the cybersecurity policy was based.

**3.0 Board/Senior Leadership Commitment**

## A. Senior leadership commitment and support are critical in ensuring the policy that is developed will be enacted and enforced. Therefore, before, during and upon completion of their cybersecurity policy, the following should occur:

1. Leadership provides the financial support to ensure the policy is completed;

2. Leadership signs the final policy document;

3. Leadership provides the necessary resources to ensure the actions in the plan are implemented;

4. Leadership communicates its support and endorsement to the workforce, customers and stakeholders.

Date: 03/28/19

Version 1.0

Cybersecurity Policy Template

**4.0 Policy Development Management**

Every company’s Cybersecurity Policy will be different, shaped by the business, the sensitivity of the data that is managed and the extent to which IT is deployed throughout. However, as you develop your company’s policy you should consider including the following sections:

* Acceptable Use
* Privacy
* Mobile Device Management
* Retention Policy
* Roles and Responsibilities
* Back up Policy
* Risk Tolerance
* Acceptable Level of Loss
* IT Governance
* Data Inventory/Management
* Password Policy
* Remote Access Policy/VPN
* Incident Response
* Physical Security
* Recovery Plan
* Training

**5.0 Roles and Responsibilities**

A. Employees. All employees are responsible for protecting the company’s critical business operations and data. It is imperative that all employees understand this responsibility as it relates to protecting data and are held accountable for their activities while at work and after work. Having an employee sign an Acceptable Use policy is a first step in communicating expectations for privacy and accountability.

B. Leadership. It is leadership’s responsibility to set the tone for the organization and to demonstrate support for IT security. Without the resources and support from leadership, the organization won’t have the will to make some of the hard decisions around how data is shared, protected and used.

C. IT and IT Security Team. While an organization may decide to outsource this responsibility to a vendor, it is still important to have an internal IT technical lead in the organization identified and assigned. Leadership needs to verify that the IT team they have hired to support their company has IT security skills, many do not. There have been many small businesses that have made the mistake of assuming that the IT company did IT security. Both are critical skills to have employed.

Date: 03/28/19

Version 1.0

D. Data Protection Officer/Privacy Officer. This is an internal position that cannot be outsourced. It is a GDPR requirement to have an internal officer identified and assigned if your company collects data on EU citizens. Other regulations, like HIPAA require a Privacy Officer. The duties are similar.

Identify the key roles and define the responsibilities of these individuals in the policy.

**6.0 IT Governance**

## A. Include a section that references the company’s IT governance plan and how this document compliments the management of IT resources for the company.

**7.0 Data Management**

## A. Include a section that defines how sensitive and protected data will be managed for the company. This section could define such things as:

* Key Business Processes and the Critical Data
* Data Inventory - how it is maintained
* Data Retention Period - Information Schedules
* Approved Storage Locations
* Encryption
* Data Backup/Data Recovery
* Approved Backup Methodology
* Types of Data Managed and the Controls Protecting Access
* Approved Data Disposal/Destruction Methods
* Data Release Approval Methodology

## 8.0 Response, Recovery and Remediation

Include a section that defines and references your Incident Response Plan. Define how your infrastructure is going to be monitored, what the expectations are from a notification perspective, and what your intended response will be. While not all incidents can be planned in advance, management can define certain parameters in which the company will respond to the event. Examples include: 24/7 notification, or only during normal duty hours, number of hours you expect your operations to be impacted, will you be able to operate at full or half capacity? Can operations be shifted to an alternative site? When do you expect to be at full restoration mode, your expected loss threshold, will certain events trigger more aggressive responses, do you have a partner that you can depend upon to direct customers or suppliers to that can provide backup support?

The more detail you can provide of leadership expectations during an event, the less stress your team will have to address during a crisis.

**7.0 Eradication and Recovery**

Cybersecurity Policy Template

Date: 03/28/19

Version 1.0

Cybersecurity Policy Template

**9.0 Learning Organization**

In all likelihood, “it’s not if but when” a cyber event of some sort is going to affect your business. Including a section in your plan about the aftermath of an event, might be a good indication of whether your organization is a learning organization. Will you conduct a lessons learned exercise to learn and improve? Will you use the setback to improve your operations? Rebuild your website? Will you encourage your employees to come forward with ways to improve?

Setting the stage now about how your organization will respond and recover in a positive way might just set the stage for continuous improvement.

**10.0 Training**

Most cybersecurity policies require yearly cybersecurity training - once a year. Including a section in your plan about training your employees more than once a year might be in order. Maybe you might want to include a strategy that you will pay for employees to attain an IT security certificate or lead efforts to become Six Sigma certified. Decide now how you want to include training as a key component to keep your company safe.

# 11.0 Applicability

A. Provide a statement that this policy is applicable to all company employees, all sites and all services that are provided at alternative (backup) sites.

# 12.0 Other Applicable Policies

A. Cross reference all other company policies that have applicability - such as Wi-Fi Policy, IT Governance, BYOD, Social Media, Password etc.