Written Information Security Program

_____

Updated: _____

Person Responsible For Cybersecurity At Firm:

Additional Resources (Consultants):

DATA CLASSIFICATION

Our Company maintains the following types of sensitive information:

-
-
-
-
-
-

HARDWARE INVENTORIES

Our company maintains hardware inventories and updates them on an as-needed basis. Below are a list of the current hardware in use at _____.

Hardware Inventory		**Today's Date:**	
Desktops	Laptops	Smartphones	Tablets

Operating Systems

In order to maintain secure systems, our company only uses operating systems that are actively supported by the manufacturer. We periodically review our operating systems in use to ensure that any operating systems that are being retired are removed from use or upgraded.

Software & Cloud Inventory

Our company uses the following software and cloud services in day-to-day business. It is our policy to only use supported and patched software. We maintain the following inventory of Software and Services that is updated on an as-needed basis.

Software and Cloud Inventory		**Today's Date:**
Local Software (You installed the software on your computer)	Hosted Software (You go to a website to access the software)	Cloud Storage (You go to a website or have an installed program to save files to – like Dropbox)

Usernames

Our company requires each user to have their own username and distinct password to access company resources and systems. In the event that common logins are required we will change the password whenever an employee leaves the company or changes roles and no longer needs access.

Passwords

Our company requires complex passwords that are changed regularly. We require our passwords to meet the following standards:

- A minimum of 3 of the following 4 types of characters:
  - Upper-Case Letters
  - Lower-Case Letters
  - Numbers
  - Symbols
- A minimum length of 8 characters
- Changed every 180 days
- No Reuse on the last 6 passwords
- 10 Minute Lockouts after 8 unsuccessful attempts.

Mobile Devices must be secured by a four digit pin at a minimum.

Lockouts

Our systems are configured to manually lock after _____ minutes. In addition, users are required to lock their screens whenever they are leaving the immediate vicinity of their computers.

Encryption

Our company uses encryption in the following locations:

ENCRYPTION CHECKLIST	**Date:**
Our Company Encrypts The Following: ☐ Database ☐ Server Hard Drives ☐ Laptops ☐ Mobile Devices ☐ Email in Transit ☐ Other _____	

Segregation of Data

_____ permits access to drives, folders, and files on an as-needed basis. For example, only our accounting team has access to payroll information. Specifically, we restrict the following types of data to the user groups listed below

DATA SEGREGATION LIST:	**Today's Date:**
Type Of Data	Who Should Have Access

Home Access

Our company allows access to our files and servers to employees who are working remotely on their own systems. We require that individuals who are accessing our systems are doing so in a secure manner and provide training as necessary. In addition, we require that any systems connecting to our company's resources are patched and have proper password controls in place.

Firewalls

Our company recognizes the necessity of firewalls to securing our information. We use the following:

☐Large Businesses: Large businesses that can afford separate firewalls to protect their entire network structure at the edge of the network (IE – where your internet connection from the outside world joins your internal network) should have firewalls. Any firewalls that are in place should still be supported and patched with the most recent firmware.

☐Small Businesses: Small businesses that may not have an internal network can take advantage of the internal firewalls that are present on windows and apple computers. All workstations and laptops should have these firewalls enabled at all times.

Patching

Our company automatically downloads and installs Operating System patches. In addition, we regularly update applications as updates are released.

Training

We provide regular training to our employees and staff on developing cybersecurity items. As required, we also provide remedial training for employees and users if necessary, such as if a user falls victim to a phishing scam.

Antivirus Application

Our company uses antivirus software in order to protect our network from various threats. We have listed the particulars below:

Antivirus Information:	**Date:**
We Use the Following Antivirus Product: _____	
We update Antivirus Definitions ☐ Automatically	☐ Manually Before Each Scan
We Run Scans ☐ Hourly ☐ Daily ☐ Weekly ☐ As Necessary	
Scans are Initiated ☐ Automatically ☐ Manually	

Antimalware Application

Our company uses antimalware software in order to protect our network from various threats. We have listed the particulars below:

Antimalware Information:	**Date:**
We Use the Following Antimalware Product: _____	
We update Antimalware Definitions ☐ Automatically	☐ Manually Before Each Scan
We Run Scans ☐ Hourly ☐ Daily ☐ Weekly ☐ As Necessary	
Scans are Initiated ☐ Automatically ☐ Manually	

Backups

Our company backs up critical information on a regular basis in order to reconstruct our data in the event of drive failure, disaster, or hacking event. We have listed the particulars below:

Backup Schema:	**Date:**
We Back up the following Information: _____	
We Back Up Data on the Following Timeline: ☐ Daily ☐ Weekly ☐ Monthly ☐Other _____	

Digital Forensics

In the event our firm discovers breach and requires support to determine its extent and severity we will contact the following:

Digital Forensics Contact:	**Telephone:**

Legal Support

In the event our firm discovers breach and requires legal support we will contact the following:

Digital Forensics Contact:	**Telephone:**

Incident Reporting

In the event our firm discovers a cybersecurity incident we will use the following form to help us determine the nature and severity of the event.

Date of Incident:

Explanation of Incident:

How Discovered?:

How Remediated?:

Data Affected:

Steps Taken To Close Vulnerability: