SMALL BUSINESS CYBERSECURITY

POLICY WORKBOOK

AMERICA'S SBDC WASHINGTON

Helping Washington Businesses
Grow & Succeed

Insert Your

Company Logo

Here

Cybersecurity Policy Manual

<Insert Company Name>

Updated: <Date>

TABLE OF CONTENTS

FIRST STEPS

Cyber Security Contacts

Person(s) responsible for cybersecurity at the firm:

Additional Consultants	Name	Contact Information
Managed Service Provider		
Insurance		
Financial		
SBDC Advisor		
Legal Contact		
Digital Forensics Contact (in the event of a breach)		

Inventory of Data

Our company maintains the following types of sensitive information:

-
-
-
-
-
-

Our company uses the following classification labels:

(Use 3-4 simple classifications. Ex: public information, internal access only information, and confidential information.)

-
-
-
-

Our company permits access to drives, folders, and files on an as-needed basis. For example, only our accounting and HR 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

Inventory of Devices

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

Hardware Inventory		Today's Date:	
Desktops	Laptops	Smartphones	Tablets

Inventory of Software

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)

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	☐ Automatically ☐ Manually Before Each Scan
We Run Scans	☐ Hourly ☐ Daily ☐ Weekly ☐ As Necessary
Scans are Initiated	☐ Automatically ☐ Manually

Anti-malware Application

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

Anti-malware Information:	Date:
We use the following antimalware product: _____	
We update anti-malware:	☐ 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 _____	

STANDARD: Physical Protection (PE)

Limit physical access

Clarification:

Only authorized employees should have access to the physical areas where your data information systems are located. Control and manage physical access to buildings, vehicles, or other properties using protection mechanisms such as keys, key cards, badges, gates, fences, guards, etc. to prevent unauthorized access to digital or other media related information or equipment. [Data media would include information that could identify an individual or payment method.]

Do not allow visitors, even those people you know well, to walk around your facility without an escort. Make sure that all non-employees wear special visitor badges and are escorted by an employee at all times while on your property.

Maintain and retain a record of who is accessing both your facility (e.g., office, plant, factory, secure rooms) and your equipment. You can do this in writing by having employees and visitors sign in and sign out as they enter and leave your physical space, and by keeping a record of who is coming and going from the facility or to secure areas within your facility.

Controlling physical access devices like locks, keys, badging, key cards, etc. is just as important as monitoring and limiting who is able to physically access certain equipment. Keys, badges, and key cards are only strong protection if you know who has them and what access they allow.

Practice - PE.1

Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

Practice - PE.2

Escort visitors and monitor visitor activity*;* maintain audit logs of physical access; and control and manage physical access devices.

Practice - PE.1

Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

POLICY: Physical Protection (PE.1)

Define the company goals and motivations for securing the physical environment.

_____
_____
_____
_____
_____
_____

Procedures: Physical Protection (PE.1)

How will the business limit physical access to organizational information systems, equipment, and the respective operating environments? Where will sensitive equipment and documents be stored? How will these areas be secured? Which individuals or company roles will be authorized to access these areas? Does the business use monitoring systems (security cameras, security guards, alarm systems, etc.)?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Practice - PE.2

Escort visitors and monitor visitor activity*;* maintain audit logs of physical access; and control and manage physical access devices.

POLICY: Physical Protection (PE.2)

Define the company goals and motivations for monitoring visitor activity, maintaining logs of physical access, and controlling and managing physical access devices.

_____
_____
_____
_____
_____
_____

Procedures: Physical Protection (PE.2)

How will the business greet visitors? Are there areas of the business where visitors are allowed to enter without escorting? How are these areas separated from secure areas? How will visitors be required to sign in (upon entry and exit), wear a badge, and be escorted through secure areas? What is the company process for logging entry and exit from secured areas? Are records digital or paper? How long will records be kept? What physical access devices does the business use? How will the business record who has access to specific devices? How will the business ensure physical access devices are returned upon employee departure or when access is no longer needed? What would happen if a physical access device is lost?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

STANDARD: Media Protection (MP)

Sanitize media

Clarification:

Ensure all system media has been either wiped of all *data* before reuse or has been destroyed before being disposed. The word “media” can refer to any type of information media, such as paper, thumb drives, mobile phones, etc.

Wiping means to overwrite the existing data using third party software designed to perform this task.

Practice - MP.1

Sanitize or destroy information system media containing Federal Contract Information [and other information protected by confidentiality rules and regulations] before disposal or release for reuse.

Practice - MP.1

Sanitize or destroy information system media containing Federal Contract Information [and other information protected by confidentiality rules and regulations] before disposal or release for reuse.

POLICY: Media Protection (MP.1)

Define the company goals and motivations for sanitizing or destroying media before disposal or release.

_____
_____
_____
_____
_____
_____

Procedures: Media Protection (MP.1)

What types of sensitive information does the business store or handle? What media (hard drives, thumb drives, CDs, paper files, etc.) contain sensitive information? How will the media be sanitized or destroyed to ensure information cannot be recovered?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

STANDARD: Identification and Authentication (IA)

Ensure that users, software processes and devices are identified before giving them access to your information system.

Clarification:

Authentication helps you to know who is accessing/using your system. Make sure to assign individual, unique identifiers, like usernames, to all employees/users who access company systems. Confirm the identities of users, processes, or devices before allowing them access to the company's information system-usually done through passwords.

Create and maintain a list of all Network devices.

Create and maintain a list of all users.

Grant access only to authenticated entities.

Practice - IA.1

Identify information system users and processes acting on behalf of users, or devices.

Practice - IA.2

Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Practice - IA.1

Identify information system users and processes acting on behalf of users, or devices.

POLICY: Identification and Authentication (IA.1)

Define the company goals and motivations for identifying system users and having unique usernames.

_____
_____
_____
_____
_____
_____

Procedures: Identification and Authentication (IA.1)

When and how will accounts be created as part of the onboarding process? What user naming convention will the business use to ensure that usernames are not repeated? Will the business use user groups to assign permissions? When and how will user accounts be suspended or deleted?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Practice - IA.2

Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

POLICY: Identification and Authentication (IA.2)

Define the company goals and motivations for authenticating users and having strong passwords.

_____
_____
_____
_____
_____
_____

Procedures: Identification and Authentication (IA.2)

What are the company password requirements for length and complexity? How often are users required to change passwords? What password management practices does the business require (ex: do not write passwords down, do not share them, do not use the same password for multiple accounts.)? Does the business use multifactor authentication (highly recommended) or biometric authentication?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

STANDARD: Access Control (AC)

Establish system access requirements.

Clarification:

Control who can use company computers and who can log on to the company network. Limit access to services and devices, such as third-party software, printers, scanners, data storage devices, that can be accessed by company computers and users. Set up your system so that unauthorized users and devices cannot access the company network or devices.

Practice - AC.1

Limit information system access to authorized users and processes acting on behalf of authorized users, or devices (including other entities information systems or entities accessing your information system).

Control internal system access.

Clarification:

Limit users/employees to only the information systems, roles, or applications they are permitted to use and that are needed for their jobs.

Practice - AC.2

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

Limit data access to authorized users and processes.

Clarification:

Control and manage connections between your company network and outside networks, such as the public internet or a network that does not belong to your company. Be aware of applications that can be run by outside systems. Control and limit personal devices like laptops, tablets, and phones from accessing the company networks and information. You can also choose to limit how and when your network is connected to outside systems and/or decide that only certain employees can connect to outside systems from network resources.

Practice - AC.3

Verify and control/limit connections to and use of external information systems.

Practice - AC.4

Control information posted or processed on publicly accessible information systems.

Additional information:

Do not allow sensitive information, including Federal Contract Information (FCI), which may include Controlled Unclassified Information (CUI), to become public. It is important to know which users/employees are allowed to publish information on publicly accessible systems, like your company website. Limit and control information that is posted on your company's website(s) that can be accessed by the public.

Sensitive information includes:

- Items listed in the Data Protection Act of 2021
- Personally Identifiable Information (PII)
- Payment Card Information (PCI)
- Health Insurance Portability and Accountability Act of 1986 (HIPAA)
- Intellectual Property (IP)
- Your business information that if exposed could cause harm to your ability to do business, harm to your vendors, clients, employees, yourself, your family:
    - Payroll
    - Accounts Receivable/Payable
    - HR files
    - Vendor List
    - Client List
    - Pricing/Profit structure information
    - Other business information that you deem to be sensitive.

FCI is part of contracting with the Federal Government.

CUI is more than just information that is obtained as part of a Federal Government Contract. CUI includes your business information that if exposed or access to it was lost would affect your ability to do business.

Retained Data can be classified into 3 or 4 simple internal classifications, examples below.

Version 1 - Categorized as:	Version 2 - Categorized as:
4. Controlled Unclassified (Highly Sensitive)	3. Confidential Information
3. Restricted access	2. Internal access only information
2. Controlled	1. Public information
1. Public	

Practice - AC.1

Limit information system access to authorized users and processes acting on behalf of authorized users, or devices (including other entities information systems or entities accessing your information system).

POLICY: Access Control (AC.1)

Define the company goals and motivations for limiting information system access.

_____
_____
_____
_____
_____
_____

Procedures: Access Control (AC.1)

How will the business limit system access to only authorized users, devices, and processes acting on behalf of authorized users and devices?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Practice - AC.2

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

POLICY: Access Control (AC.2)

Define the company goals and motivations for limiting the transactions and functions users are allowed to execute.

_____
_____
_____
_____
_____
_____

Procedures: Access Control (AC.2)

For each category of information, which job functions need access? What types of functions (read only, edit, delete) does each job function need to execute?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Practice - AC.3

Verify and control/limit connections to and use of external information systems.

POLICY: Access Control (AC.3)

Define the company goals and motivations for limiting connections to and use of external information systems.

_____
_____
_____
_____
_____
_____

Procedures: Access Control (AC.3)

Which employees will be allowed to connect to outside systems from company computers? Which systems are those employees allowed to access? For example, are employees allowed to access Facebook? Are personal devices allowed on the company network? If so, what security standards will be enforced on those devices?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Practice - AC.4

Control information posted or processed on publicly accessible information systems.

POLICY: Access Control (AC.4)

Define the company goals and motivations for controlling publicly accessible information.

_____
_____
_____
_____
_____
_____

Procedures: Access Control (AC.4)

What information will be publicly accessible? Who in the company is allowed to post information to websites, social media, and other publicly accessible platforms? How will materials be reviewed before posting? What is the process for removing improper posted information? When and how will posting permission be removed upon employee separation?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

STANDARD: System and Communication (SC)

Control communications at system boundaries

Clarification:

Just as your office, home, or facility has fences and locks for protection from the outside, and uses badges and keys, codes, or other personnel access systems to keep non-employees out, your company's IT Network or system has boundaries that must be protected. Many companies use a web proxy and a firewall.

If your business wishes to have a public facing network, i.e. a website, social media, or public Wi-Fi, ensure that your internal network is separated and protected from the publicly accessible systems. Do not place the internal systems on the same network as the publicly accessible system(s). All business functions should be conducted on a password protected Wi-Fi, never on a public network.

Practice - SC.1

Monitor, control, and protect company communications (i.e., information transmitted or received by organization information systems) at the external boundaries and key internal boundaries of the information systems.

Practice - SC.2

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Practice - SC.1

Monitor, control, and protect company communications (i.e., information transmitted or received by organization information systems) at the external boundaries and key internal boundaries of the information systems.

POLICY: System and Communication (SC.1)

Define the company goals and motivations for controlling the flow of information and communications into and out of the organization information systems.

_____
_____
_____
_____
_____
_____

Procedures: System and Communication (SC.1)

How does the company network connect to the internet? Does the internet connection device monitor and restrict network traffic? Is the device's firewall enabled? (Tip: contact your internet service provider to discuss the security features they can provide.) What is the company policy for enabling and monitoring firewalls on company devices? How will the company utilize encryption?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Practice - SC.2

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

POLICY: System and Communication (SC.2)

Define the company goals and motivations for

_____
_____
_____
_____
_____
_____

Procedures: System and Communication (SC.2)

How will publicly accessible systems (email, websites, etc.) be logically separated from completely private systems? What internal systems need additional protection and should be separated from the rest of the network? How will these systems be separated? Will the business have public or guest Wi-Fi? How will the public Wi-Fi network be separated from the private Wi-Fi network used for business functions?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

STANDARD: System and Information Integrity (SI)

Identify and manage information system flaws & identify malicious content

Clarification:

All software has potential flaws. Create a process to review relevant third party software or service vendor newsletters for updates about recently released fixes (patches/updates). After identifying updates, execute the patch management process updating the vulnerable devices as soon as possible.

Protect devices from malware by enabling anti-malware scans on a regular schedule. Malware can come from emails, over the web, or from infected external devices or portable media devices. It is important to protect information, at both external and internal boundaries, from malware to maintain confidentiality, integrity, and accessibility of the organization's data storage and network devices.

System boundaries may include firewalls, electronic mail servers, web servers, proxy servers, remote- access servers, workstations, notebook computers, and mobile devices.

Update all devices and applications on a regulated schedule to protect against emerging threats. Update anti-malware software within 24 hours of receiving the update notification.

End point protection and Anti-malware software can scan devices to make sure that no viruses entered the information systems and isolate/quarantine suspect code if found. It is important to conduct these scans periodically to make sure that no virus has entered the system through downloaded files and to maintain protection of previously saved files. Conduct threat scans as and after new files are downloaded or saved.

Practice - SI.1

Identify, report, and correct information and information system flaws in a timely manner.

Practice - SI.2

Provide protection from malicious code at appropriate locations within organizational information systems.

Practice - SI.3

Update malicious code protection mechanisms when new releases are available.

Practice - SI.4

Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Practice - SI.1

Identify, report, and correct information and information system flaws in a timely manner.

POLICY: System and Information Integrity (SI.1)

Define the company goals and motivations for implementing device and software updates in a timely manner.

_____
_____
_____
_____
_____
_____

Procedures: System and Information Integrity (SI.1)

What is the company policy for reviewing support from device and software vendors? What is the schedule for implementing device and software updates and patches? Who does the schedule apply to?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Practice - SI.2

Provide protection from malicious code at appropriate locations within organizational information systems.

POLICY: System and Information Integrity (SI.2)

Define the company goals and motivations for providing protection from malicious code on organizational information systems.

_____
_____
_____
_____
_____
_____

Procedures: System and Information Integrity (SI.2)

Which devices are required to have antimalware software? How will employees be trained to avoid malware from phishing scams, suspicious emails, and infected websites? What is the process for employees to report suspected malware?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Practice - SI.3

Update malicious code protection mechanisms when new releases are available.

POLICY: System and Information Integrity (SI.3)

Define the company goals and motivations for updating malicious code protection.

_____
_____
_____
_____
_____
_____

Procedures: System and Information Integrity (SI.3)

What is the company policy for reviewing support from antimalware software vendors? What is the schedule for implementing antimalware software updates and patches? Who does the schedule apply to?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Practice - SI.4

Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

POLICY: System and Information Integrity (SI.4)

Define the company goals and motivations for performing periodic scans of information systems and real-time scans of files from external sources.

_____
_____
_____
_____
_____
_____

Procedures: System and Information Integrity (SI.4)

What is the schedule for performing periodic scan of information systems? Which devices should have automatic scans enabled? How often should automatic scans be run? Describe how files from external sources, such as emails, should be scanned when they are downloaded, opened, or executed.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Additional Resources

- CMMC Assessment Guide Level 1, Version 2.13 (September 2024)
  - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL1v2.pdf
- CISA Cyber Guidance for Small Businesses
  - https://www.cisa.gov/cyber-guidance-small-businesses
- FTC Cybersecurity for Small Businesses, Cybersecurity Basics
  - https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf
- SBA Strengthen Your Cybersecurity
  - https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity
- SBA Cybersecurity In-Person and Virtual Events
  - https://www.sba.gov/events?keyword=cybersecurity

The content of this workbook was compiled by Washington SBDC staff from multiple sources including, but not limited to, National Institute of Standards and Technology, Department of Homeland Security, America's SBDC Cybersecurity Program, Department of Defense, and U.S. Small Business Administration.

For questions or more information, please contact:

wsbdc.org | Washington@wsbdc.org | 833-4WA-SBDC

POWERED BY SBA U.S. Small Business Administration

AMERICA'S SBDC WASHINGTON

WASHINGTON STATE UNIVERSITY

The Washington SBDC network, hosted statewide by Washington State University, is an accredited member of America's SBDC. Funded in part through a cooperative agreement with the U.S. Small Business Administration, institutions of higher education, economic development organizations and other public and private partners.