Small Business Cybersecurity Self Assessment

Why Cybersecurity is important...

Small businesses represent an opportunity for hackers and cyber criminals. Here are a few reasons why:

- Small businesses are a soft target – No/Limited Cybersecurity
- You have desirable data:
  - Credit Card Info
  - HIPAA data
  - PII – Personal Identity Info
  - Young Adult / Children's PII
- Small businesses may have access to larger companies' and government systems
- You have a legal obligation to protect the data and access you maintain

Cybersecurity Maturity Model Certification (CMMC)

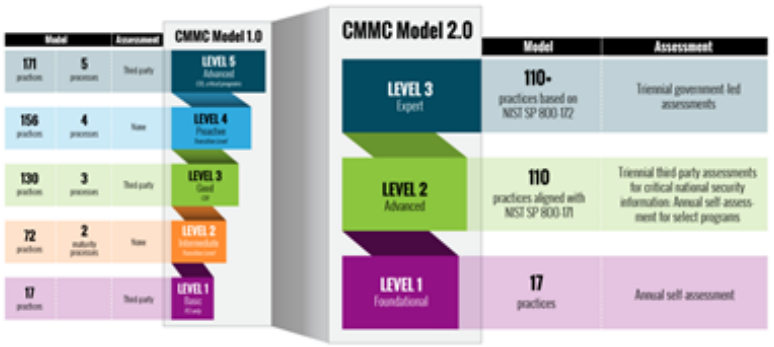
CMMC Model version 2.0, specifically the 17 requirements provided by CMMC and adopted by the Department of Defense for Level 1 maturity. CMMC Level 1 requirements match 2020 "17 Critical FAR controls"

Guidelines & Assessment Foundation

NIST Framework

- Identify—What assets are at risk?
- Protect—What systems are threatened?
- Detect—Would you know if you were breached?
- Respond—How would you respond to an incident?
- Recover—Can you return to "normal" after a breach?

CMMC 1.0 to 2.0 Transition



SC SBDC Resources

- South Carolina Cyber Breach Law
- Small Business Cybersecurity Self-Assessment
- Small Business Cybersecurity Guide & Workbook

SCSBDC.com/cyber || 803.777.4907

CONSULTING * EDUCATION * RESOURCES

Cyber Security Self Assessment

Physical Security - Hardware/ Software/ Personnel	Y / N	Notes
Are hardware and software being used less than 5 years old?		
Are there any devices used by both employees and clients?		
Do multiple employees use common equipment?		
Is hardware/software maintained internally?		
What malware, virus, intrusion detection is in place?		
Is there a breach/data loss recovery plan in place?		
Are cloud data storage services being used?		
What equipment is connected to the internet (IoT)?		
Are networking and computer equipment physically secured?		
Is encryption being used where applicable?		
Are hard copy files locked?		
Is there a secure method for data / paper disposal?		
Is there a cybersecurity plan/policy in place?		
Is there an inventory of all equipment?		
Has a list of acceptable software been established?		
Are classes or cybersecurity news updates performed regularly?		
Does the company randomly test employees regarding cyber threats?		
Are firewalls in place (hardware/software)?		
Does the company know who to report an incident to and the procedure to do so?		
Does the company have a copy of applicable breach/incident reporting laws?		
Mobile Devices / BYOD	**Y / N**	**Notes**
Who owns the mobile devices used within the company?		
Do you allow personal device use by employees (BYOD)?		
What mobile carriers are used and are security measures in place?		
Is there an inventory of devices and software installed on each?		
Does each device have access controls in place?		
Can the company remotely lock / wipe a lost device?		
Are devices set to auto connect to bluetooth and wifi networks?		
Are company owned devices encrypted?		
Is malware/virus protection loaded on each device and up to date?		
Is a virtual private network (VPN) being used for remote access?		
Login / Password	**Y / N**	**Notes**
Is there a strict password creation and update policy in place?		
Can employees reset passwords / lock out owners?		
How many users have admin level access to their devices?		
Are passwords set up with specific, focused permissions?		
Have you audited/searched facilities for passwords being left out?		
Does someone monitor login activity?		
Website / Social Media	**Y / N**	**Notes**
Who has access and authorization to distribute web/social media content?		
Are all host, URL and social media accounts owned and maintained internally?		
Do all employees have web access and is it monitored?		
Does the company manage social media internally?		
Has anyone been assigned to monitor web traffic for company information?		
Is web security in place for vendors, suppliers and international transactions?		
Data Storage / Backup	**Y / N**	**Notes**
Is there a backup plan identifying what data and frequency of backups?		
Are backups stored in a separate location?		
Does the company use cloud based back up services?		
Has the company performed a test restoration of data lately?		
Is there a regular accounting of data and where it is stored?		
Does anyone monitor who is accessing/storing data remotely?		
Are regulatory guidelines being followed (HIPPA, DoD, PCI)?		

Name of person responsible for Cybersecurity:

Current Data Inventory (PII, CC, HIPPA, HR, Financials, IP)

Data Type	Location of Data

Equipment/ Device Inventory: (Attach additional sheets if needed)

Equipment Type	Owner	Location	ID Number

Operating Systems (Window, Apple OS, Linux, Other)

Type	Version	Date No Longer Supported

Approved Software

Title	Purpose	Owner	Version

User Identities (Attach additional sheets if needed)

UID	Name	Access Level	Remote Access	Multi-User	Multi-Factor
			Y/N	Y/N	Y/N
			Y/N	Y/N	Y/N
			Y/N	Y/N	Y/N
			Y/N	Y/N	Y/N

Passphrase Management

Complexity	Upper and Lower case letter, at least one
Length	Minimum of 12 characters
Change Frequency	Change at a minimum of 180 days
Reuse	No reuse of the past 6 passphrases
Lockout	15 minute lockout after 3 unsuccessful

Data Encryption Checklist

Type	In Place	Needed

Virtual Private Network (VPN) Software in use:

Endpoint Protection Checks and Scanning

Type	Name
Antivirus	
Vulnerability Scan	
Anomaly Detection	
Intrusion Detection	
Active Response	
Alerting/ Notification	
Historical Analysis and Stats	
Reporting	
Other	

Firewall

Type	Brand	Software Version

Backup Procedures

Full System			
Frequency:		Stored at:	
User Files Only			
Frequency:		Stored at:	
File Change Only			
Frequency:		Stored at:	

Incident Response Team

Type	Company	Contact	Phone	Email

Authorities

Type	Company	Contact	Phone	Email
Local Police				
Forensics				
Other				

Cybersecurity Insurance

Type	Company	Contact	Phone	Email

Questions?
SCSBDC.com/Cyber
803.777.4907

Important Information

Small Business Cybersecurity Tips

Guidelines for "Non-Techy" Entrepreneurs

Common Do's and Don't of Cybersecurity

- DO Maintain physical control of cyber assets
- DO Stay updated on threats
- DO Remove unused apps/software
- DO Enable password protection
- DO Turn off Bluetooth
- DO Use encryption
- DO Understand device app permissions
- DO Watch auto-installs
- DO Configure your browser correctly

- Do NOT use public USB ports
- Do NOT use public wi-fi (without VPN)
- Do NOT scan random QR codes
- Do NOT download apps from unknown sources
- Do NOT set laptop to auto-connect to networks

For more information:

SC Title 39 Trade and Commerce – Section 39-1-90
https://www.scstatehouse.gov/code/title39.php

CMMC Requirements
https://www.cmmcab.org/

NIST Protection Framework
https://www.nist.gov/cyberframework

To Report a Breach:

Notify local law enforcement, the local office of the FBI or the U.S. Secret Service.

For incidents involving mail theft, contact the U.S. Postal Inspection Service.

SOUTH CAROLINA SBDC

AMERICA'S SBDC

POWERED BY SBA

SC SBDC Contact Information:

Phone: 803.777.4907

Web: SCSBDC.com/cyber

Office: 1014 Greene St., Columbia, SC 29208

Funded in part through a Cooperative Agreement with the Small Business Administration.

CONSULTING * EDUCATION * RESOURCES