SOUTH CAROLINA SBDC

Small Business Cybersecurity Guide & Training Workbook

AMERICA'S SBDC

POWERED BY SBA U.S. Small Business Administration

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

Welcome to the South Carolina SBDC Cybersecurity Assistance Program

One of the largest threats currently facing small businesses is cybersecurity. Small to medium size businesses are particularly at risk because they are viewed by hackers as easier targets due to their general lack of awareness and resources. Furthermore, federal, state and industry regulators have decided that the threats posed by malicious actors in cyberspace must be addressed. Small businesses can no longer afford to remain unaware of the threats or remain complacent with inadequate technology. They have to take action to enhance their systems, processes and staffing in order to remain viable in today's online economy. You are not alone, however. The South Carolina Small Business Development Center network (SC SBDC) is here to help.

For over 40 years, the SC SBDC has been helping small businesses start, grow and succeed. We keep our finger on the pulse of today's rapid economic and technological changes; and we continually adapt our advising approaches and educational programs to meet the unique, evolving needs of South Carolina's small business community.

Supported by a grant from the U.S. Small Business Administration through the CARES Act, the SC SBDC has responded to the need to equip small businesses with the knowledge and tools needed to craft a solid cybersecurity program. This guidebook and other accompanying materials are designed to provide ongoing face-to-face and web-based training to help any small business in need of cyber guidance. Personal and confidential assistance is available from our team of experienced business consultants.

The information in this guidebook is a starting point for your planning and should be updated regularly. As the cybersecurity landscape continues to change rapidly, so must your business strategy and operations. So, don't wait for a cyber-attack to get started.

A final note: Security does not have to mean reduced productivity and increased operational costs. In fact, it can mean quite the opposite. Having a strong security system and policies in place can allow your employees to be far more productive, increasing efficiency and saving on IT costs.

Work with the SC SBDC experts to plan ahead and become Data Assured today. Visit our website at www.scsbdc.com to sign up for consulting services, find an expert near you and access all of our cybersecurity materials. Our consulting services are offered at no fee.

Ask Us. We Can Help.

SOUTH CAROLINA SBDC

AMERICA'S SBDC

CONSULTING * EDUCATION * RESOURCES

How to Use the SC SBDC Cybersecurity Program

While the materials offered by the SC SBDC are valuable to all levels of an organization to help minimize exposure to potential cybersecurity threats, we realize time is limited. Use the chart below to determine your best course of action when implementing our programs.

	Intended Audience/Skill Level		
	General Understanding	Application Non-Technical	Technical Understanding
Topics/Tools	(C-Suite, Owner)	(Employee, Vendor)	(IT Workers)
Cybersecurity Best Practices	X	X	X
SC Breach Law Requirements	X	X	X
NIST Framework		X	X
CMMC Level 1 Controls		X	X
SC SBDC Cybersecurity Assistance Program-book	X	X	X
SC SBDC Cybersecurity Self Assessment			X
SC SBDC Cybersecurity Awareness Training	X	X	X

SC SBDC Cybersecurity Assistance Available in All 46 Counties

Earl Gregorich,
Greenville Area Manager
P 864.326.5504
egrego5@clemson.edu

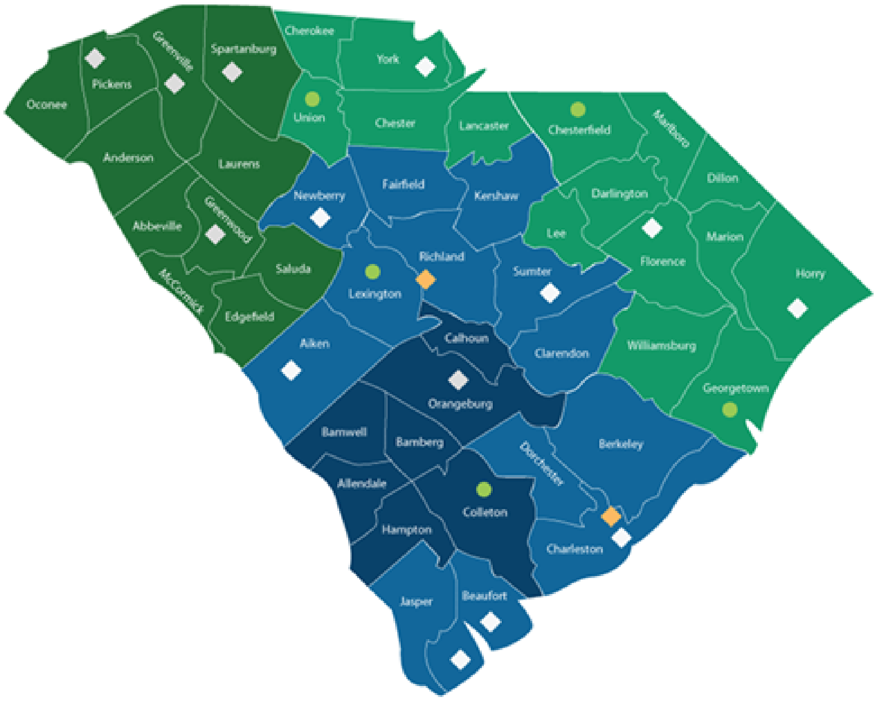
Brent Hoover,
Business Consultant
P 803.641.3468
brentho@usca.edu

John Blomberg
Rock Hill Area Manager
P 704.564.9954
blombergj@winthrop.edu

Beth Smith,
Business Consultant
smithem6@mailbox.sc.edu

Scott Bellows,
Procurement Consultant
P 803.777.7877
shbellows@sc.edu

Sherry Pittinger,
Procurement Specialist
P 864.326.5504
Spittin@clemson.edu



SC SBDC Cybersecurity Assistance Program

Guideline Foundation Basis

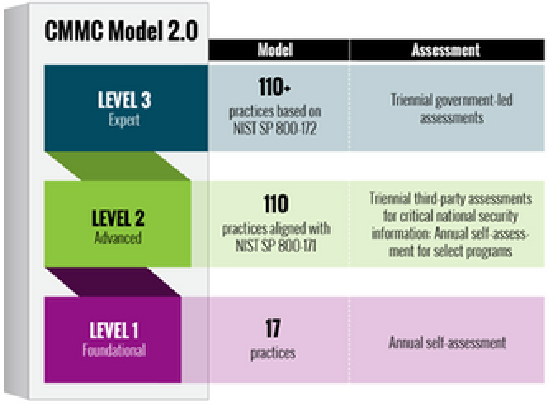
The basis for the guidelines presented in this document are formed from the National Institute of Standards and Technology (NIST) Cybersecurity Framework, a widely accepted benchmark for cybersecurity planning and the Cybersecurity Maturity Model Certification (CMMC) documentation used by the Department of Defense to assess vendor readiness within the small business community. The SC Cyber Breach Law is also considered as outlined. Listed below is an overview of each program.

Cybersecurity Maturity Model Certification (CMMC 2.0)

-Primarily for Government Contracting

Level 1 includes security requirements in the following categories:

- ·Access Control
- Identification & Authentication
- Media Protection
- Physical Protection
- System Communication Protection
- System and Information Integrity



CMMC Model 2.0

	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information: Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment

National Institute of Standards and Technology (NIST) Cybersecurity Framework

IDENTIFY

Identify – Determine risks, create policy and procedure

PROTECT

Protect – Limit access, implement physical and digital security

DETECT

Detect – Anti-virus, log monitoring, threat management

RESPOND

Respond – Public and private response plan

RECOVER

Recover – Backup strategy, disaster recovery, insurance, process improvements

SC Title 39 Trade and Commerce- Section 39- 1- 90- SC Breach of Security Business Data Law

NOTE:

The content and instruction in this presentation is meant as a guideline for you to define your cybersecurity practices.
It cannot prevent a breach on its own, nor will specific information about your company, your legal liability or your computing assets be addressed.
It is recommended you consult a cybersecurity or IT specialist to address specific questions regarding your unique cybersecurity strategy.
It may also be advisable to seek legal assistance regarding questions of legal liability.

South Carolina’s Breach of Security Business Data Law

(SC code § 39-1-90 et seq.)

What You Need to Know

If you conduct business in South Carolina and own or license personal identifying information on South Carolina residents, you are required to notify South Carolina residents when their personal identifying information has been accessed or acquired by an unauthorized person who compromises the security, confidentiality or integrity of the information, and is or is reasonably likely to use the information illegally or in a way that creates a material risk of harm to the residents.

What is Personal Identifying Information?

The categories listed below must be associated with a South Carolina resident’s first name or initial and last name in combination with any of the following categories with the required password or security code:

- Social Security Number
- Driver’s License Number
- Financial Account Number
- Credit or Debit Card Number
- Other numbers or information used to access financial accounts
- Numbers or information issued by a governmental or regulatory entity that uniquely identifies an individual.

What Timing is Required?

Disclosure to affected residents must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.

Are There Exceptions?

Disclosure of data breach is not required to South Carolina residents whose personal identifying information had been rendered unusable prior to the breach through encryption redaction, or other methods. Also, good faith acquisition of personal identifying information by your employee or agent for the purposes of your business is not a breach of security of the system if the information is not used or subject to further unauthorized disclosure. The notification law doesn’t apply to financial institutions that are subject to and in compliance with the privacy and security provisions of the Gram-Leach-Bliley Act.

How is Notice to be Made?

- Written notice, mailed or hand delivered to the affected residents;
- Electronic notice, if your primary method of communication with the resident is by electronic means or is consistent with federal electronic records and signature laws;
- Telephonic notice; or
- Substitute notice, under certain conditions set forth in the statute.
- Internal notification procedures that are part of your information security policy may also be available for use under certain conditions set forth in the statute.
- If notice is made to more than 1,000 residents at one time, you will also have to notify the South Carolina Department of Consumer Affairs and the consumer reporting agencies.

South Carolina’s Breach of Security Business Data Law (continued)

Data Breach Response: Secure Your Operations

Following a data breach, you are required to quickly secure your systems and fix the vulnerabilities that may have caused the breach.

The Federal Trade Commission (FTC) has established guidelines that can help you make smart, sound decisions.

- Assemble a team of experts to conduct a comprehensive breach response which may include forensics, legal, information security, information technology, operations, human resources, communications, investor relations and management.
- Secure physical areas potentially related to the breach.
- Stop additional data loss.
- Remove improperly posted information from the web.
- Interview people who discovered the breach.
- Do not destroy the evidence.
- Have a communications plan.

What About Vendors?

- A vendor must notify the owner or licensee of personal identifying information of South Carolina residents immediately following discover that the information was, or is reasonably believed to have been, acquired by an unauthorized person.

What Else Should I Know?

- The statute provides residents who are injured by a violation of Section 39-1-90 certain rights, including limited private rights of action to sue you, and to recover attorneys; fees and court costs.

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.

For more information:

- SC Title 39 Trade and Commerce – Section 39-1-90 — https://www.scstatehouse.gov/code/title39.php
- NIST Protection Framework — https://www.nist.gov/cyberframework

Reaching Cyber Awareness Training Workbook

Why YOU are the target…

What is your initial assessment of your business' cybersecurity? (circle one)

No Cybersecurity   Factory Default Security   Passive Security   Active Security   Contracted Professionals

List the data you possess that would be of most interest to a cyber criminal

____

____

____

____

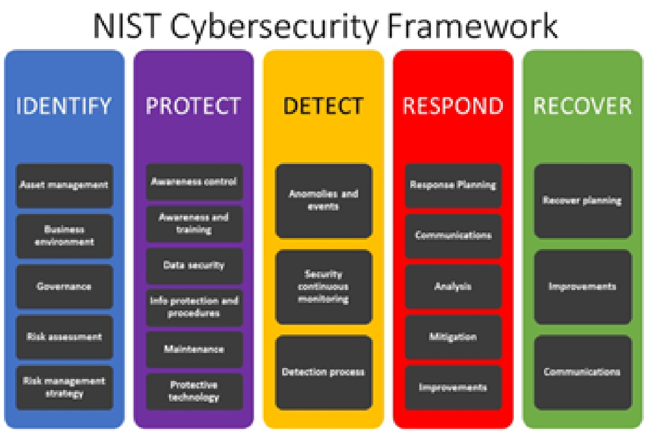
Weaknesses within Small Business—Some of your biggest threats

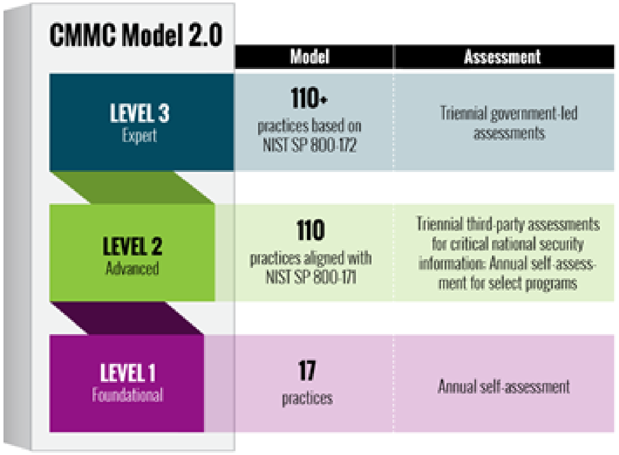
List what you feel are your greatest weaknesses and likely threats regarding cybersecurity

____

____

____





CMMC Model 2.0

	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment

CMMC 2.0 Level 1

Level 1 Maturity is accomplished by Performance – NOT just a documented processes – You must be capable of demonstrating intentional, consistent and auditable security actions

You MUST go beyond a policy manual

Most processes are doable in-house at minimal cost

It may still be advisable to use a professional cybersecurity resource

____

____

____

CMMC AC.1.001 – Log-in Credentials: “Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).“

IDENTIFY

____

____

____

CMMC AC.1.002 – Assign Permissions: “Limit information system access to the types of transactions and functions that authorized users are permitted to execute.”

PROTECT

____

____

____

CMMC AC.1.003 – Exclusive Networks: “Verify and control/limit connections to and use of external information systems.”

PROTECT

____

____

____

CMMC AC.1.004 – No data sharing: “Control information posted or processed on publicly accessible information systems.”

PROTECT

____

____

CMMC IA.1.076 – No Group Log-ins: “Identify information system users, processes acting on behalf of users, or devices.”

IDENTIFY

____

____

CMMC IA.1.077 – No default passwords: “Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.”

IDENTIFY

____

____

CMMC MP.1.118 – Secure trash: “Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.”

PROTECT

____

____

Business Process Paperless Flow

List paper processes in your business that need to be secured.

____

____

CMMC PE.1.131 – Physical Security: “Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.”

IDENTIFY

____

____

DETECT

CMMC PE.1.132 – Track visitors: “Escort visitors and monitor visitor activity.”

____

____

____

DETECT

CMMC PE.1.133 – Archive access history: “Maintain audit logs of physical access.”

____

____

____

DETECT

CMMC PE.1.134 – Keys/badges/codes: “Control and manage physical access devices.”

____

____

Business Process—Hiring and Firing

IDENTIFY

List enhancements needed to incorporate cybersecurity into your onboarding and exit procedures:

____

____

CMMC SC.1.175 – Stay behind firewall: “Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.“

PROTECT

____

____

____

CMMC SC.1.176 – Diversify web access: “Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.”

PROTECT

____

____

_

CMMC SI.1.210 – Install updates!: “Identify, report, and correct information and information system flaws in a timely manner.”

PROTECT

____

____

____

CMMC SI.1.211 – Maintain Antivirus: “Provide protection from malicious code at appropriate locations within organizational information systems.”

PROTECT

____

____

____

CMMC SI.1.212 – Subscriptions: “Update malicious code protection mechanisms when new releases are available.”

IDENTIFY

____

____

____

CMMC SI.1.213 – Full, Regular Scans: “Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.”

DETECT

____

____

____

Employee Behavior—Training

PROTECT

Type of Training	Who Should Attend	Frequency
____________________	____________________	____________________
____________________	____________________	____________________
____________________	____________________	____________________
____________________	____________________	____________________
____________________	____________________	____________________

Low Cost Software Solutions

PROTECT

List what solutions you need to research further for your business:

Type of Software	Brand / Manufacturer	Urgency
______________________________	______________________________	______________________________
______________________________	______________________________	______________________________
______________________________	______________________________	______________________________
______________________________	______________________________	______________________________
______________________________	______________________________	______________________________

Response Planning

RESPOND

User Level
System Level
Internal
External
Learn & Adapt

____

____

____

____

____

____

Back up Planning

RECOVER

Type of Backup	Storage Location	Frequency
______________________________	______________________________	______________________________
______________________________	______________________________	______________________________
______________________________	______________________________	______________________________
______________________________	______________________________	______________________________
______________________________	______________________________	______________________________

Last Back up Recovery Test: _________________________ (Date)

Insurance as a Defense

RECOVER

First Party Cyber Liability Provider

____

Third Party Cyber Risk Provider

____

Basic Cybersecurity Guidelines for Small Business

The following outline provides the beginnings for a small business cybersecurity plan. Consult an IT professional or your SC SBDC consultant for more details on each topic.

Assess Your Vulnerabilities

- Personnel
- Hardware (Inventory)
- Software
- Suppliers, Vendors, Third Parties

Create a Cybersecurity Policy

- Internal Personnel
- Vendors, Suppliers
- Social Media
- BYOD – Bring Your Own Device
- Data Management
- Set Personnel Expectations

Implement a Password Maintenance Program

- Secure Password Creation Guidelines
- Periodic Forced Update
- Multi-Factor/Dual Authentication
- (Also see "Control Access")

Create a Backup Process

- What gets backed u
- Frequency of back ups
- Location of backups
- Testing of backups

Update and Maintain Software

- Encryption software
- Virtual Private Network (VPN)
- List Approved Software
- Auto Update Settings

Install/Update Anti-Virus/Malware Protection

- Desktop, mobile and smart devices
- Monitor Activity

Implement Hardware/Software Firewalls

- Hardware settings, updates, physical security
- Software settings, permissions and traffic monitoring

Control Access

- Assess Personnel Access Needs
- Physical Access to Equipment
- Set up Software to Accommodate Multi-Level Permissions (Also see Password Maintenance Program)

Test the Hardware, Software and Personnel

- Run phishing, malware and access testing regularly
- Focus on Personnel – the weakest link
- Stress test networks, websites
- Regularly review social media traffic

Monitor Device and Network Activity

- Review activity logs (login times, excessive activity, web traffic, etc.)
- Regular reboot, power cycling
- Remote access activity
- Wi-Fi device connections
- Intrusion Detection

Implement Vendor/Supplier Policy and Monitor/Test Performance

- Establish similar guidelines as these for non-personnel
- Outline clear consequences, in writing with acknowledging signature

Establish Internal and External Communications Plan

- Regular internal updates regarding threats
- Updates to personnel changes
- Make resources accessible and create a culture unafraid to report issues
- Implement a PR plan to face the media, work with authorities

Create and Test a Recovery Plan

- Legal and Reporting Responsibilities
- Disaster Plan
- Recovery from breach
- Recovery from data loss
- Brand Protection
- Insurance

Set up Regular and Timely Training for ALL Personnel

General Information and Resources

Warning Signs of a Possible Compromise

- Slow laptop/computer without anti-virus
- Non-biz browsing history
- Freely logging on to public Wi-Fi
- Employees volunteer info without verification
- Customer information laying out in open
- Guest login for Wi-Fi without a password
- Not using dual authentication
- Customers contact you with difficulties accessing your information, especially involving security alerts

Resources

General Software

- Email Filtering (Office 365, Gmail, SonicWALL)
- Anti-Virus (AVDefender, AVG Anti-Virus, Symantec SEP, McAfee, Malwarebytes, Trend Micro)
- Online Cyber Courses (YouTube, Lynda, KnowBe4.com)
- Find my phone – App to locate phone
- Website Protection (Cloudflare, Incapsula, Akamai, Amazon Web Services)
- Cloud Storage (Microsoft One Drive, Google Drive, Dropbox, Box, Amazon AWS Storage, Barracuda, Storagecraft.com, Veeam.com, Crash Plan, Carbonite)
- Virtual Private Networks – VPN (IPVanish, Avast Secureline TunnelBear, Nord – Beware of caps and throttling)
- Data Loss Prevention (Symantec, Trustwave, WatchGuard, Digital Guardian, Proofpoint, Lookout.com)
- Software Firewalls (Avast, Norton, McAfee, BitDefender)
- Password Managers (Dashlane, Keepass, mSecure, LastPass, 1Password)

Other Resources

- NIST – nist.gov/cyberframework
- Federal Trade Commission - ftc.gov/tips-advice/business-center/small-businesses/cybersecurity
- SBA Guidelines - sba.gov/business-guide/manage-your-business/small-business-cybersecurity
- US Computer Emergency Readiness Team (US CERT) – us-cert.gov
- FCC.gov - fcc.gov/cyberplanner
- Knowbe4.com—Testing and security simulations
- Website Protection (Cloudflare, Incapsula, Akamai, Amazon Web Services)
- Hardware Firewalls (Cisco, Sophos, WatchGuard, Juniper, Checkpoint)
- Security Policy Templates - sans.org/information-security-policy/
- Stay Safe Online - staysafeonline.org/cybersecure-business/
- Have I Been “Pawned?” - haveibeenpwned.com/
- SmallBusinessBigThreat.com
- SBDC360Cyber.com – Co-sponsored cybersecurity insurance through ASBDC

Cybersecurity Glossary

Admin or Admin Level Access – Typically the highest level of access that can be given to a user on a computer network or software package. An Admin User would be able to make wide-sweeping changes within any area of a system.

Anomaly – Unusual traffic or cyber activity that falls outside the normal access or movement of data from point to point.

Antivirus – Software specifically designed to detect and mitigate attacks originating from data transfer activity.

Backup – The practice of making regular, updated copies of data, programs and other digital property and storing it in a safe location.

Bluetooth – A networking technology that allows devices to communicate with other devices nearby (normally within 30 ft. but some devices can connect at 350 ft.)

Breach or Data Breach – The term commonly used to describe a successful hack of an organizations network and/or computer systems or devices.

BYOD (Bring Your Own Device) – An acronym used to describe all personal devices normally found on workplace networks.

Cloud Storage – A remote storage location, normally on the internet used to maintain data for real-time use or backup purposes. Examples might include: Dropbox, Google Drive, OneDrive, etc.

CMMC (Cybersecurity Maturity Model Certification) – The current standard (utilizing the NIST framework) used by the Department of Defense and other organization to measure the degree of cybersecurity awareness a contractor, vendor or small business has in place.

Cybersecurity – The effort and resources put in use to protect a business from criminal or unauthorized use of digital assets.

DoD (Department of Defense) – The government entity currently driving minimal cybersecurity measures in order to conduct business within their contracts.

Encryption – The process of converting human legible data into complex computer code to prevent unauthorized access.

Firewall – A hardware or software device used to monitor network traffic and prevent unwanted content.
Forensics – Scientific tests or techniques used to detect and/or investigate the cause of a crime.

Hardware – Equipment associated with conducting digital work such as laptops, computers, mobile devices and networking devices.

HIPAA (Health Insurance Portability and Accountability Act) – Law that outlines the requirements to maintain the privacy of medical and health records.

Host – The computer or internet service providing the digital space to hold data, files and software for daily operations. Common hosts might include GoDaddy, Amazon, HostGator, BlueHost, etc.

IoT (Internet of Thinks) – Commonly refers to any device other than a traditional computer that is connected and able to communicate over the internet. Examples may be, cameras and security systems, manufacturing equipment or household thermostats.

IP (Intellectual Property) – An original creation such as an invention, literary or artistic work whether tangible or digital in form.

Intrusion Detection – In the context of cybersecurity, normally software or hardware set up to note unwanted or unusual digital traffic or by physical access.

Malware – Software designed to disrupt, damage or gain unauthorized access to digital systems.

Cybersecurity Glossary

NIST or NIST Framework – National Institute of Standards and Technology guidelines for security measures to help prevent, detect and respond to cyber attacks.

PCI (Payment Card Industy) Compliance – Standards in place to secure and protect credit card data as it is exchanged.

Permissions – The level of access granted a person using network or computing device. Normally limits the data that can be seen or the software functions allowed.

PII (Personal Identity Information) – Information that directly and specifically identifies an individual. Examples may include: name, address, social security number, employee number, phone number, etc.)

Server – Usually the primary location for all software and data within a networked computer system. There may be one or several servers in any network.

Social Media – Websites that allow users to create and share content while networking with friends and peers.

Software – Programs or instructions used by computers to conduct the tasks requested by users.

URL (Universal Resource Locator) – Web page address. Example: SCSBDC.com

Virus – Malware capable of copying itself across one or more computer networks with the intent to do harm.

VPN (Virtual Private Network) – A software solution that provides an encrypted, secure access to remote devices across the internet.

Wi-Fi – Short range wireless connection between two devices over the internet.

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 U.S. Small Business Administration

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