North Star
Small Business Data/Cyber Protection Awareness

Cybersecurity Checklist

Why Cybersecurity is Important...

Small businesses have never transacted more business online than they are today. With the growth of technology, it has given small businesses the ability to compete directly with medium and large firms. However, with this comes greater risk for the small business since they represent an opportunity for hackers and cyber criminals to exploit vulnerabilities easier due to lack of expensive security infrastructure. Due to this threat, Federal, State, and Industry regulators have started putting regulatory demands in place to protect business and client data. This is not just a matter of following the rules, nor illustrating to your clients and customers that their safety and security matters, but it is a matter of outright survival of your company should it experience a breach. Many businesses cannot afford the legal, regulatory, and forensic hassles that accompany a breach of systems exposing client or internal information, let alone the loss of trust from a client or customer base.

Why Small Businesses are a Target:

Little to no cybersecurity protocols in place.

Maintain desirable data:

- Payment Card Information (PCI)
- Private Health Information (PHI)
- Personal Identifiable Information (PII)
- Federal Contract Information (FCI)
- Controlled Unclassified Information (CUI)

Have access to larger companies' and government systems.

Framework Foundation

The North Star follows the newly developed Cybersecurity Maturity Model Certification (CMMC) framework. The CMMC framework was designed by the Department of Defense (DoD) to protect sensitive unclassified information and follows the best practice standards derived from multiple sources like the NIST CS Framework. The North Star helps small businesses get the benefit of the latest cybersecurity methodology without a "certification" requirement. Our methodology follows the CMMC Level 1 model that has 15 basic cybersecurity practices that are easy to understand and implement and reduces a company's overall cybersecurity risk.

Purpose

The North Star "Cybersecurity Checklist" provides insights on your cybersecurity and where it may be weak and can help create a task list to complete. As a bonus for companies with DoD contracts, this checklist (if followed correctly) can serve as an internal readiness guide if your small business needs to become CMMC Level 1 compliant. Seemingly complicated at first, this checklist includes basic cybersecurity practices directly out of the CMMC Level 1 documentation that will help any small business protect sensitive data. Our subject matter experts have also included other cybersecurity measures that are necessary for a basic cybersecurity program within a small business.

This checklist will require adjustments going forward, and may also need expansion or modification based upon a small business' unique circumstances. Please note, this checklist is a starting point to develop a cybersecurity program. This program should become a culture and push company personnel, especially leadership, to develop a security mindset and approach in day-to-day operations.

This is a confidential document. Keep it secure.

AMERICA'S SBDC

Domain

ACCESS CONTROL

Access refers to the ability people or devices have to gain entry and use your data processing systems. You control access by granting or denying requests to use your Information, process data or enter into a network or facility. The goal should be to only provide access to authorized users, or processes implemented by authorized users, devices or other data processing systems. Controls should also include the ability to limit data exposure and processes to only the needed areas within the business and its data processing systems.

Access Control

Measure	Standard	Yes	No	N/A	Notes
Do you use passphrases for system and software access?	AC.1.001				
Do you authenticate users before allowing access?	AC.1.001				
Are logins required to gain access vs. group or shared access?	AC.1.001				
Are new account requests authorized before system access is granted?	AC.1.001				
Do you use access control lists to limit access to systems, applications, and data based on role/identity?	AC.1.002				
Can you separate and enforce access control rights within your systems?	AC.1.002				
Do you limit external access to only authorized individuals?	AC.1.003				
Are you providing guidelines/restrictions on personal or external system access?	AC.1.003				
Have external systems with access been verified to meet guide-lines/restrictions?	AC.1.003				
Are you limiting the number of system access points for better management of inbound/outbound traffic?	AC.1.003				
Are you controlling who posts information to publicly accessible systems?	AC.1.004				
Do employees receive training on what is classified or protected information that cannot be publicly posted?	AC.1.004				
Is there a review process for all public postings to ensure non-public information is not posted?	AC.1.004				

Best Practice

Measure	Yes	No	N/A	Notes
Are there any devices used by both employees and clients?				
Who owns the mobile devices used within the company?				
Do you allow employees to use personal devices to access company data (BYOD)?				
Who has access and authorization to distribute web/social media content?				
Does the company own and manage all web property and social media accounts internally?				
Can the company remotely lock / wipe a lost device?				
Does someone monitor login activity?				
Do all employees have web access and is it monitored?				

Role Based Access Control (RBAC) of Data

If you are a solopreneur, you probably don't need to implement a data segregation plan. However for even the smallest companies, putting your data into various places that are restricted to only those who need the information is a great idea.

You should determine who needs access to that data. Take your time and think through this process, because it can be very tempting to just say "everyone needs everything". This is seldom the case – especially with HR information including payroll. Write down all the users that have access to your data and the level of that users access (do they have read only access or admin access).

User Identities

Username	Users 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
			Y / N	Y / N	Y / N
			Y / N	Y / N	Y / N
			Y / N	Y / N	Y / N
			Y / N	Y / N	Y / N

Domain

IDENTITY & AUTHENTICATION

Identification and Authentication (IA) is the most basic defense put in place to stop unauthorized access to data resources within a business. Done properly it verifies the identity of a user, process or device and determines what data and systems are approved for access. IA also provides a means of tracking each individual along their passage within a network or system. Normally, identity of a user is authenticated using a combination of a passphrase, a device only the user has access to, and a biometric input (fingerprint, facial recognition, voice pattern). Care should be taken to not only verify identity at the point of entry but to maintain that the person originally verified continues to be the same person throughout the user session.

Identity & Authentication

Measure	Standard	Yes	No	N/A	Notes
Do you assign accounts for unique access by individuals?	IA.1.076				
Have you separated duties of those who assign permissions from those who assign access?	IA.1.076				
Is there a centralized account management process that can delete/lock accounts when needed?	IA.1.076				
Have you centralized account management into a central identity management system?	IA.1.077				
Is there an account provisioning (set-up) process in place?	IA.1.077				
Do you assign unique accounts to new employees, contractors and subcontractors?	IA.1.077				
Is there a random passphrase generated for each new account and is a passphrase reset required upon first access?	IA.1.077				
Does your passphrase policy include at least 12 characters with upper/lower case, numbers and special characters?	IA.1.077				

Best Practice

Measure	Yes	No	N/A	Notes
Can employees reset any passphrases or lock out owners from any device, in any way?				
Is hardware/software maintained internally?				
How many users have admin level access to their devices?				

Domain

MEDIA PROTECTION

Media Protection (MP) refers to both digital and non-digital data stored in formats such as internal/external hard-drives, thumb/flash drives, disks, film, and paper. Just like data systems, media should be protected with access controls through physical and digital security. Only authorized personnel should have physical or virtual access to digital and non-digital data. All media should remain in a controlled atmosphere until sanitized and/or disposed of properly.

Media Protection

Measure	Standard	Yes	No	N/A	Notes
Are you assigning unique inventory/asset control identifiers to all data processing equipment?	MP.1.118				
Have all removable media and mobile devices been marked and tracked?	MP.1.118				

Best Practice

Measure	Yes	No	N/A	Notes
Are cloud data storage services being used with limited access and sharing disabled?				
What non-data-processing equipment is connected to the internet via your network (IoT)?				
Is there a secure method for equipment / data / paper disposal?				
Is there an inventory of devices and software installed on each?				
Is there a regular accounting of data and where it is stored?				

Data Encryption | Encryption is something that is commonly overlooked, yet vital to secure data handling and storage. Some basic applications for encrypting data are as follows:

Encryption Checklist

Our Company Encrypts The Following:

- ☐ Database ☐ N/A
- ☐ Server Storage ☐ N/A
- ☐ Laptop Hard Drives ☐ N/A
- ☐ Mobile Devices ☐ N/A (devices not used for business)
- ☐ Email in Transit ☐ N/A
- ☐ Other .....

Domain

PHYSICAL ACCESS

Protecting the actual building, system and environment used to process your data is what Physical Access (PE) is all about. Normally we are talking about the facilities (building, room, data center, file cabinets, office, etc.) and the hardware (networks, computer cabinets, enclosures, etc.) Common threats within this category include unauthorized access, natural disasters, civil unrest, environmental fluctuations and human error. Controls range from simple door locks to complex redundant infrastructures with guarded access.

Physical Access

Measure	Standard	Yes	No	N/A	Notes
Have you identified sensitive areas within your locations and set up appropriate physical security to limit access to authorized personnel?	PE.1.131				
Do your printers and other output devices remain within physically secured areas?	PE.1.131				
Do you maintain a list of authorized personnel with appropriate access credentials for sensitive areas?	PE.1.131				
Are all visitors escorted by authorized personnel while on premises?	PE.1.132				
Are visitors provided security and access policies and monitored for compliance?	PE.1.132				
Are logs maintained on all personnel entering/leaving sensitive areas?	PE.1.133				
Are visitor access logs maintained and archived for future reference?	PE.1.133				
Do you use physical access devices (locks, card readers, biometrics) and are they checked regularly?	PE.1.134				
Is there a process to update access devices due to personnel changes?	PE.1.134				
Are all codes, keys and access devices secured and audited regularly?	PE.1.134				

Best Practice

Measure	Yes	No	N/A	Notes
Are networking and data processing equipment physically secured?				
Are hard copy files locked?				
Do you regularly audit/search facilities for passwords being left out?				

Domain

SYSTEMS & COMMUNICATION

Protections for Systems and Communication (SC) are both physical and virtual and involve protecting stored data and data in transit. Stored data can be protected by physically separating it from exposure to external networks. Data in transit can be encrypted and transmitted over virtual private networks as a form of protection. Creating boundaries with firewalls and restricted and monitored network access points would also fall into this category.

Systems & Communication

Measure	Standard	Yes	No	N/A	Notes
Have you established network communication limitations/boundaries?	PE.1.131				
Are there systems in place to monitor/manage communications across network boundaries?	PE.1.131				
Do policies exist to manage access points and acceptable server interfaces via gateways, routers, firewalls, VPNs?	PE.1.131				
Do you use subnetworks, perimeter networks or "demilitarized zones" to buffer internal networks from outside access?	PE.1.132				

Best Practice

Measure	Yes	No	N/A	Notes
Is a virtual private network (VPN) being used for remote access?				
Are devices set to auto connect to Bluetooth and WiFi networks?				

Approved Software

Software Name	Purpose	Owner	Version

Domain

SYSTEM & INFORMATION INTEGRITY

System and information (SI) integrity can be maintained by continuously monitoring for unusual activity, malware, and active attacks. Most companies will accomplish this through antivirus software, network monitoring services and regularly updating software and hardware to the latest security standards. Maintaining data integrity includes not only detecting and removing data abnormalities but also responding in an appropriate and timely manner. Reporting and correcting shortfalls within the security infrastructure is key to ongoing system and information integrity.

System & Information Integrity

Measure	Standard	Yes	No	N/A	Notes
Are there processes in place to identify, report and correct system flaws and security issues?	PE.1.131				
Do you perform software updates in a timely manner, in accordance with your system security plan (SSP)?	PE.1.131				
Have you turned on auto updates for security software and hardware?	PE.1.131				
Do you use malware detection on all inbound and outbound network traffic?	PE.1.132				
Have you loaded malware detection on all devices accessing your networks?	PE.1.132				
Are all malware, anti-virus and other protection systems updated within 5 days of update release?	PE.1.133				
Do you perform periodic scans for malware?	PE.1.133				
Are you scanning files from external sources in real-time as they are downloaded, opened or executed?	PE.1.134				
Does your malware protection automatically disinfect and/or quarantine suspect files?	PE.1.134				

Operating System Check

Our Company Has The Following:

- ☐ Windows Current Version(s): _____
- ☐ macOS Current Version(s): _____
- ☐ Linux Current Version(s): _____
- ☐ Other Current Version(s): _____

Best Practice

Measure	Yes	No	N/A	Notes
Is there a breach/data loss recovery plan in place?				
Is there a system security plan (SSP) in place?				
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?				
Does the company have a copy of applicable breach/incident reporting laws?				
Is there a backup plan identifying what data is backed up and the frequency of the backups?				
Are backups stored in a separate location?				
Does the company use cloud based back up services?				
Are hardware and software being used, less than 5 years old?				
Is encryption being used where applicable?				
Is there an inventory of all equipment?				
Are firewalls in place (hardware/software)?				
Are company owned devices encrypted?				
Has the company performed a test restoration of data lately?				
Does anyone monitor who is accessing/storing data remotely?				
Are regulatory guidelines being followed (HIPPA, DoD, PCI)?				
Has anyone been assigned to monitor web traffic for company information?				
Is web security in place for vendors, suppliers and international transactions?				

Identify Who is Responsible for Cybersecurity

Here is the simplest starting point. Who makes the calls when it comes to the security of the company? If you are filling out this workbook for a small company, chances are it is you, but there may be someone else who takes the security lead.

Name of Person Responsible for Cybersecurity:

Identify What Data You Collect & Where You Keep it

This is the root of a cybersecurity policy. What data do you maintain that could be useful or valuable to a bad actor?

Data can be stored on your devices (like a laptop or external storage devices), in cloud storage (like Google Drive), or in a service (like QuickBooks). Make note of what security requirements are used to access this data (passwords, multi-factor authentication, IP whitelisting, etc.)

Examples include:

- Personal Identifiable Information or PII (SSNs, DOBs, etc.)
- Payment Card Information (Credit Card Numbers)
- Personal Health Information
- HR Records that could contain Bank Account Information
- Business Plan Documents (Bank Statements, Taxes, etc.)
- Proprietary Schematics, Patent Applications, etc.

Data Inventory

Data Type	Location

How Secure Are Your Passwords?

The term 'Password' is not the best. It should really be 'Passphrase'. That alone should tell you a lot about password strength. Using passwords that have association with yourself, like a maiden name, birthday, favorite food, etc. are recipes for disaster.

Password Check

- ☐ Complex Passwords Required
  - ☐ Upper-Case Letters
  - ☐ Lower-Case Letters
  - ☐ Numbers
  - ☐ Symbols
- ☐ Length Standards Met (12 Characters Minimum)
- ☐ Change Frequency Every 180 Days or More Regularly
- ☐ No Reuse of Last 6 Passwords
- ☐ 15 Minute Lockout After 3 Unsuccessful Attempts
- ☐ Use of very long passphrases possible
- ☐ Mobile Devices Secured by a 6-Digit PIN at Minimum
- ☐ Mobile Devices Secured by a passphrase
- ☐ Additional Controls: _____

Identify What Devices Need Protecting

What devices are you using that could be used to compromise your sensitive data? Fill in the below table to create an inventory of devices that interact with sensitive data by any means. List every single device you can think of. Chances are the more specific the purpose of the device, the harder it is to protect and update (eg: printers).

Equipment/Device Inventory

Device Type	Owner	Location	ID Number

Endpoint Protection

If your business is more advanced and has a more sophisticated network or you store a high level of personal identification information, antivirus/antimalware might not be enough for you. You may need an endpoint protection software. A common misconception about endpoint protection is associated with the term 'Antivirus'. For the smaller mom and pop shops, this is most likely enough protection. However, more developed business networks need to be prepared for threats they can't predict.

Endpoint Protection Checks & Scanning

Our products cover the following categories:

- ☐ Antivirus/Antimalware
- ☐ Vulnerability Scanning
- ☐ Anomaly Detection
- ☐ Intrusion Detection
- ☐ Active Response
- ☐ Alerting/Notification
- ☐ Historical Analysis and Statistics
- ☐ Reporting
- ☐ Other

What Types of Backups Do You Run?

There are different types of backups that a small business can run in their environment. The level of sensitivity of the data and the importance of it, will dictate what type of backup up should be run. Check which backup types you run.

- ☐ **Full System Backup**: This backup will create an exact copy of the computer, including all operating system files. This can also be considered a mirror of your computer's hard drive.
- ☐ **File Level Backup**: This is a backup of only user created files on a system. This backup uses less space since it is not copying system files but it will have all of the user's data such as pictures, documents, etc.
- ☐ **Incremental Backup**: This backup scans the system for any file changes since the last Full System or File Level backup and only backs up the files that have changed, saving time and space during routine backups.

Backup Schema:

We Back Up Data On The Following Timeline:

☐ Daily ☐ Weekly ☐ Monthly ☐ Other

☐ Backups are version controlled

We Store Backups At The Following:

Who Is In Your Corner?

In the event of a data breach your business needs to move quickly and strategically. In order to do so you should put together an incident response team. An incident response team should be formed with all relevant business personnel. This team includes technical workers to investigate the breach along with your IT staff whether they are internal or an external company. You will also want to include your human resource personnel, intellectual property experts, a legal representative when customer data is involved, and your marketing team.

If you are a small business, chances are, you or one of your employees wears all the hats mentioned above. That is okay as long as you acknowledge that you know where to go for help in all the specified areas. A number of legal issues can arise around a data breach, so it is imperative that you seek legal advice as soon as a breach is discovered.

Incident Response Team

Name	Company/Department	Phone	Email

Additional Resources

The North Star CMM program offers many resources free of charge to all small businesses looking to become cyber secure. These resources range from simple cybersecurity checklists to more detailed industry specific workforce development. Below you will notice just a few of our resources with many more at www.americassbdc.org/cybersecurity

Cybersecurity Resources

Cyber Do's & Don'ts

Live Trainings

For More Information

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

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

Special Thanks

Thank you to the SBDC networks for their contribution to this document: Delaware, Michigan, Mississippi, Oregon, and South Carolina

North Star
Small Business Data/Cyber Protection Awareness

This is a confidential document. Keep it secure.

AMERICA'S SBDC