NACB CYBERSECURITY CHECKLIST

STANDARD 3 — SIGNIFICANCE AND PURPOSE

Y /N

- ☐ ☐ Has Organization identified what information assets to protect?
  - Customer records
  - Intellectual property
- ☐ ☐ Has Organization identified sources of vulnerabilities?
  - Public Wi-Fi by employees
  - Security of paper records
  - Connected smart devices
  - Email/phishing
- ☐ ☐ Has Organization conducted a risk, threat, vulnerability assessment?
  - Identify
  - Describe
  - Analyze
- ☐ ☐ Has Organization identified critical information assets?
  - What security measures and controls are in place?
- ☐ ☐ Has Organization created a written standard operating procedure that all pertinent employees can understand?
  - Who has the best knowledge of the organization's activity and internal structure (best person to help write SOPs)?

  What are the security measures and controls in place?
- ☐ ☐ Is a Computer Security Incident Response Team in place? CSIRT
  - Who do the employees call if something happens with the network?
- ☐ ☐ Is the number easily accessible?
- ☐ ☐ Is there a landline at the business?

How often do you conduct simulated breaches?
When was the last time a simulated breach exercise happened?
Who is in charge of evaluating and improving the existing protocol?

STANDARD 5 — ACCEPTABLE USE POLICY

- ☐ ☐ Is the accepted use policy clearly communicated to employees?

  What types of uses are directly related to the employees job function?
- ☐ ☐ Can sensitive files be segregated, or password protected?
- ☐ ☐ Does the manager know which employees have which level of access?

STANDARD 6 — PASSWORDS

- ☐ ☐ Does the Organization use a password generator?
- ☐ ☐ Have any employees revealed a personal password to anyone else?
- ☐ ☐ How often does Organization mandate password changes?
- ☐ ☐ Recommended at least every 90-180 days.
- ☐ ☐ Has multi-factor authentication been enabled?
- ☐ ☐ Has Organization identified the high value accounts?
- ☐ ☐ Are those accounts protected with a physical hardware token?
- ☐ ☐ Are all employee passwords at least 15 characters long, with a mixture of lowercase, uppercase, special symbols, and numbers?
- ☐ ☐ Are the company passwords kept in a safe place?
- ☐ ☐ Does Organization have a reporting system to catalog compromises?

STANDARD 7 — CONFIDENTIAL DATA POLICY

- ☐ ☐ Does Organization have a secure place to store:
- ☐ ☐ Personally identifiable information?
- ☐ ☐ Customer credit card information?
- ☐ ☐ Business decision support system information?
- ☐ ☐ Medical patient information?

Y /N

- ☐ ☐ Has Organization identified, classified, and segregated all PII, PCI, DSS, and ePHI?
- ☐ ☐ Does Organization have any media that contains patient ePHI?
- ☐ ☐ Has Organization identified systems, devices, and media that house collect, store, or process sensitive information?
- ☐ ☐ Has Organization documented ownership, responsibility, and function of each of these systems?

STANDARD 7 — CONFIDENTIAL DATA POLICY

- ☐ ☐ Is Organizational handling of the sensitive information compliant with regulations pertaining to health re cords and financial records confidentiality requirements?
- ☐ ☐ Is Organization's system capable of remote access?
  - Who has remote access?
- ☐ ☐ Is Organization equipped to handle confidential information? (Storage, transmission, destruction)
  - Who has access?
  - How many copies?
  - Is any stored in the cloud?
  - Does Organization use encryption?
  - Does Organization have a firewall
  - Does Organization use a secure server?
  - Does organization destroy confidential information?
  - Does organization have policy for retention of data?
- ☐ ☐ Can data be recovered once it has been destroyed? (Digital paper shredder)
- ☐ ☐ Is Organization's system of handling confidential information up-to-date with current standard operating systems and security procedures?
  - When was the last upgrade?
- ☐ ☐ Has Organization been clear about how the third-party is limited in its use of the confidential data?
  - How and when will the third-party destroy the data?

STANDARD 8 — MOBILE DEVICE POLICY

- ☐ ☐ Any company phones lost or stolen? What are the data security controls on the phone?
- ☐ ☐ Are the phones encrypted?
- ☐ ☐ Is any organizational data available on any personal mobile device?
- ☐ ☐ Is any removable media used?
- ☐ ☐ Is it encrypted?
- ☐ ☐ Assuming employees are using different Wi-Fi systems with different levels of security, can the business provide devices or laptops for remote use?
- ☐ ☐ Has Organization instructed employees to never connect their company device to a free wireless hotspot? (aka—No working from Starbucks).
- ☐ ☐ When did Organization conduct the most recent review of policy compliance?
- ☐ ☐ When did Organization conduct the most recent inspection of mobile devices?

STANDARD 9 — RETENTION POLICY

- ☐ ☐ Is there a data retention policy in place?
- ☐ ☐ Is Organization anticipating any litigation?
- ☐ ☐ How often does Organization recycle security footage?
- ☐ ☐ Has Organization identified and segregated operational data?
- ☐ ☐ Does company Wi-Fi automatically pair with new devices when they enter the range?

STANDARD 10 — EMAIL POLICY

- ☐ ☐ Are employees clear about use of personal email at work?
- ☐ ☐ Does anyone send confidential information via email?
  - If so, is the email containing the sensitive info encrypted?
  - *See Confidential Data policy for email.*
- ☐ ☐ How long does Organization keep company emails?
  - What is required in the jurisdiction?

Y /N

- ☐ ☐ Have all email accounts of former employees been disabled?
- ☐ ☐ Does Organization trace who handles classified data?
- ☐ ☐ Have any employees emailed sensitive data to personal email accounts?

STANDARD 11 — BACKUP POLICY

- ☐ ☐ Has critical data been identified and segregated?
  Policy to backup data?
- ☐ ☐ Does Organization measure the burden of backup?
- ☐ ☐ On users?
- ☐ ☐ On network resources?
- ☐ ☐ On backup administrator?
- ☐ ☐ Do you frequently back up data?
- ☐ ☐ Is there a set schedule for backup of data?
- ☐ ☐ Have the changes been tested?
- ☐ ☐ Does Organization screen new employees?
- ☐ ☐ Has the new employee read and signed the Acceptable Use Policy?
- ☐ ☐ Does the Organization change the initial setup password for each new employee?
- ☐ ☐ Does an administrator know the employee passwords?
- ☐ ☐ Is a role-based access control system in place?
- ☐ ☐ Is it documented?
- ☐ ☐ Where is it stored?
- ☐ ☐ Does the system incorporate a default "denyall" setting for new or unrecognized users?
- ☐ ☐ Is a password management system in place?
- ☐ ☐ Is it encrypted?
  How does the Organization handle failed login attempts?
- ☐ ☐ Does the system lock a user out after 3-5 failed login attempts, prevent another attempt for 30 minutes, or require a manual reset?
- ☐ ☐ How often is the log of failed attempts reviewed?
- ☐ ☐ Is a multifactor authentication process in place?

STANDARD 12 — WORKFORCE SECURITY POLICY

- ☐ ☐ Are all of the Organization's job descriptions in writing?
- ☐ ☐ Has the Organization identified which positions will handle ePHI?
- ☐ ☐ Do employees have the required skills and qualifications to perform according to their job descriptions?
- ☐ ☐ Is an employee training program in place?
- ☐ ☐ Does the Organization have multiple levels of security clearance?
- ☐ ☐ Does organization have procedure for disabling access when an employee is terminated or resigns?

STANDARD 13 — INCIDENT RESPONSE POLICY

- ☐ ☐ Are unauthorized devices accessing the network?
- ☐ ☐ Has the Organization lost any laptops or devices by accident or theft?
- ☐ ☐ Has the Organization lost any hard copies of sensitive documents?
- ☐ ☐ Who is in charge of responding to a security incident?
- ☐ ☐ Does the organization conduct simulated incident response exercises?
- ☐ ☐ Does the jurisdiction have industry or governmental regulations that outline a compliant response policy?
- ☐ ☐ If there has been a breach, has all at-risk information been treated as confidential information?
- ☐ ☐ How is information of the breach shared with media or customers?
  Electronic Incidents:
- ☐ ☐ Was damage limited?
- ☐ ☐ Was network secured?
- ☐ ☐ Was evidence of the incident preserved?
- ☐ ☐ Was compromised device removed from the network?
- ☐ ☐ Was incident reported to the IT department?
- ☐ ☐ Has the compromised system been physically secured?
  Note: Do NOT power down the entire system
- ☐ ☐ Did the Organization's policy operate as intended during the incident?
- ☐ ☐ Does Organization conduct a quarterly audit for lost or stolen devices that contain Organization data?

Y /N

STANDARD 14 — EXTERNAL CONNECTION POLICY

☐ ☐ Does Organization use "Strong encryption"
(i.e., encryption algorithms meet or exceed current industry standards).
☐ ☐ Does Organization use "Strong authentication":
☐ ☐ Strong password.
☐ ☐ Pre-shared key.
☐ ☐ Certificate.
☐ ☐ Verify identity of remote user.
☐ ☐ Implementation
☐ ☐ "Principle of Least Access"
☐ ☐ Access only what is required for business purposes
☐ ☐ Set up in a Demilitarized zone.
☐ ☐ Does Organization manage the VPN gateways, or does a third-party?
☐ ☐ Logging/Monitoring:
☐ ☐ Links to third-parties:
Organization should use a higher security standard than intra-Organization.

STANDARD 15 — GUEST ACCESS POLICY

☐ ☐ Has Guest signed the Acceptable User Policy agreement?
☐ ☐ Is Guest access separated from the corporate network (logically or physically).
☐ ☐ Guest access should be monitored for appropriate use.
☐ ☐ Guest is not a trusted user.
☐ ☐ Are Organization's interests protected?
☐ ☐ Are security policies followed?

STANDARD 16 — WIRELESS ACCESS POLICY

☐ ☐ Is Media Access Control (MAC) Address filtering available?
☐ ☐ Limit network connections to known Network Interface Controllers (NICs)

STANDARD 17 — NETWORK SECURITY POLICY

☐ ☐ Are password for network security devices more complex than user passwords?
☐ ☐ Do network security devices utilize multi factor authentication?
☐ ☐ Does Organization lock a user's account after 5 failed login attempts?
☐ ☐ Does Organization utilize technology to enforce password policies?
☐ ☐ Does Organization log activity on network-level devices to the fullest degree possible?
☐ ☐ Does Organization maintain a chronological trail of audits?
☐ ☐ Are audit results retained for a time period dictated by business or compliance requirements?
☐ ☐ Does Organization record:
☐ ☐ User ID?
☐ ☐ Event types (including date and time)?
☐ ☐ Identity or name of affected data
☐ ☐ Origination
☐ ☐ Success/failure indicators
☐ ☐ System components
☐ ☐ Details of potential compromises
☐ ☐ Does Organization secure audit trails to prevent attackers from covering their tracks?
☐ ☐ Does firewall's default setting block inbound access from external sources?
☐ ☐ Are firewall rules as restrictive as possible without affected legitimate access?
☐ ☐ Does firewall utilize strong encryption surrounding administrative access?
☐ ☐ Does firewall limit management access to networks where management connections originate?
☐ ☐ Does organization use a hardened system or pre-hardened appliances for firewall platforms?
☐ ☐ Firewall is properly configured and that all rules are regularly audited.
☐ ☐ Secure remote access points and users.
☐ ☐ Block any unused or unneeded open network ports.
☐ ☐ Disable and remove unnecessary protocols and services.
☐ ☐ Implement access lists.
☐ ☐ Encrypt network traffic.

Y /N

- ☐ ☐ Are firewall rule sets audited every six months?
  - ☐ ☐ Details of each rule.
  - ☐ ☐ Business justification for services/protocols.
  - ☐ ☐ Documentation of insecure protocols.
    - ☐ ☐ Mitigation features used to remedy.
  - ☐ ☐ Scrutinize each rule.
  - ☐ ☐ Documentation maintained by IT Person.
- ☐ ☐ Is firewall configured to filter inbound and outbound traffic?
  - ☐ ☐ Is permitted outbound traffic specified?
  - ☐ ☐ Is restricted outbound traffic blocked from leaving the network?
- ☐ ☐ Does Organization use consistent network hardware?
  - ☐ ☐ Routers.
  - ☐ ☐ Switches.
  - ☐ ☐ Bridges.
  - ☐ ☐ Access points.
- ☐ ☐ Network server protocol:
  - ☐ ☐ For intended business functions, isolate necessary from unnecessary:
    - ☐ ☐ Services.
    - ☐ ☐ Daemons.
    - ☐ ☐ Protocols.
    - ☐ ☐ Scripts.
    - ☐ ☐ Drivers.
    - ☐ ☐ Features.
  - ☐ ☐ Disable the unnecessary ones.
  - ☐ ☐ Does Organization utilize appropriate server-hardening guidelines?
  - ☐ ☐ Are network servers protected by a firewall or access control list?
  - ☐ ☐ Is each server limited to one primary function?
- ☐ ☐ What is the security review timeline?
- ☐ ☐ Security review includes:
  - ☐ ☐ Network and network architecture.
  - ☐ ☐ Infrastructure.
  - ☐ ☐ Security processes.
  - ☐ ☐ Capability of personnel.
  - ☐ ☐ Data flow diagrams up-to-date.
  - ☐ ☐ Compliance with data protection regulations.
- ☐ ☐ How often is a security test conducted?
  - ☐ ☐ Does the test involve relevant stakeholders?
  - ☐ ☐ Has Organization mitigated any security or compliance issues?
  - ☐ ☐ Is the vulnerability test score acceptable in relation to the CVSS?
- ☐ ☐ Is the antivirus/anti-malware software up-to-date on all devices with access to the network?
- ☐ ☐ Is the operating system up-to-date with all available Security Patches and Critical Updates?
- ☐ ☐ Does Organization have a Software Use Policy?
  - ☐ ☐ Is software tested for vulnerabilities and misconfigurations?
- ☐ ☐ Does Organization maintain a “change log”?
  - ☐ ☐ Hardware and/or configuration changes.
  - ☐ ☐ Notify relevant stakeholders of reasons, risks, and rollback strategies for changes.

STANDARD 18 — ENCRYPTION POLICY

- ☐ ☐ Is Organization aware of current industry standards regarding encryption algorithms?
- ☐ ☐ Is Organization aware of any government regulations applicable to encryption?
- ☐ ☐ Does Organization use “Strong Encryption”?
- ☐ ☐ Is remote access to Organization network encrypted?
- ☐ ☐ Has encryption been initiated before administrative password was changed?
- ☐ ☐ Do all mobile devices store Organization data on an encrypted partition?
  - ☐ ☐ Use whole disk encryption where sensitive data is on the device.
- ☐ ☐ When confidential information is transmitted via email, is it encrypted?
  - ☐ ☐ Never send sensitive data via end-user messaging technology.
- ☐ ☐ Has Organization stored confidential data in encrypted form?