Audit

Account Management:

- ☐ Modify the passwords/authentication if any of the following apply:
  - ☐ Passwords are insecure or have been compromised
  - ☐ Usernames/addresses are not in line with company policy
  - ☐ Employees have lost control of an account due to leaving the business
- ☐ Does every employee have a company email account
- ☐ Does the system have more or fewer user accounts than employees
- ☐ Is all authentication methods current

Access control:

- ☐ Require all user/admin accounts to have 2-factor verification
- ☐ Require all user/admin accounts to have an associated phone number
- ☐ Ensure that access is only possible through company computers
- ☐ Ensure that company computers fit company guides and do not have any unauthorized software
- ☐ Do you perform weekly security check-ups
- ☐ Are there any holes or vulnerabilities in their current authentication program

Information Control / Sharing:

- ☐ When communicating with users outside of the organization, verify their identities
- ☐ Do not connect to unauthorized domains
- ☐ Examine the source addresses of any unknown information

- ☐ Do not open personal emails on company computers
- ☐ Do not disclose company information outside of company grounds
- ☐ Ensure that employees are aware of basic phishing attacks
- ☐ Ensure that employees are aware of the dangers of clicking unknown URLs
- ☐ Inform employees of the type of information that must not be publicly accessible
- ☐ Does their system provide software to identify threats
- ☐ Are there any holes or vulnerabilities in their current software
- ☐ Do admins have ways of monitoring activity from users on their systems/domain

Policy/Procedures:

- ☐ Develop a proper recovery system for the business
- ☐ Enforce internal and external ways of protecting secure information
- ☐ Does the business have an up-to-date recovery plan for their system
- ☐ Do they have a response plan when systems are compromised
- ☐ Are employees aware of how to protect themselves from social engineering tactics
- ☐ Does the company have a proper company profile
- ☐ Is the company aware of what domains users can access via their system
- ☐ Have employees been made aware of how to identify security threats
- ☐ Are employees up-to-date with recovery procedures
- ☐ Do employees understand steps to take in the event of a security breach
- ☐ Do employees take steps to protect their identity when conducting business on public networks

Incident/reporting:

- ☐ Does the business have a proper system of alerting management when they believe they've witness an incident
- ☐ Does the business have a form of anti-virus software installed on all business laptops/desktops
- ☐ Do employees know how to identify an emergency cyber threat versus non-emergency cyber threats?
- ☐ Have all personnel been properly trained on how to respond to and report a threat