Information Security Checklist for Small Businesses

Management

- ☐ Do you have written security policies and have they been reviewed and signed by all employees?
- ☐ Do you have onboarding/out-processing documents/checklists for hiring and terminating employees?
- ☐ Do you have a disaster recovery plan?
- ☐ Do you have a computer software and hardware asset inventory list and network diagram?
- ☐ Are there industry standards for which your firm must be compliant, such as PCI, HIPAA, HITECH or Sarbanes-Oxley?
- ☐ Do you have a list of third-party vendors that your business is using, including infrastructure access and contact information?
- ☐ Do your employees receive annual training on information security and safe computing practices?
- ☐ Do you have a Bring Your Own Device (BYOD) policy?
- ☐ Do you have a Bring Your Own Network (BYON) policy?
- ☐ Do you have an Incident Response Plan in the event of a data breach or a disaster?

Technology

- ☐ Are your systems protected by enterprise grade security software?
- ☐ Is the security software up-to-date, license current, and actively scanning on a regular basis?
- ☐ Are all of the Windows-based firewalls enabled?

- ☐ Is your e-mail being filtered to protect users from spam, viruses and phishing attempts?
- ☐ Is a password policy in place requiring strong, 14-character or longer passwords? Are passwords, especially network log-in passwords, required to be changed every 30 days? Is password reuse prohibited via technology for 12 months or longer?
- ☐ Are computer systems up-to-date with security patches?
- ☐ Is software being updated on a regular basis and with updates from the manufacturer?
- ☐ Have you upgraded all software that is no longer supported?
- ☐ Is your data getting backed up on a regular basis? Are you performing test restorations of backups?
- ☐ Is your backup engineered so that it cannot be encrypted by ransomware?
- ☐ Is data on mobile devices encrypted (smartphones, laptops, tablets)?
- ☐ Do you require passphrases/PINs on mobile devices that connect to your network?
- ☐ Are your mobile devices protected with security software?
- ☐ Is your wireless network using WPA2 encryption?
- ☐ Do you have a guest wireless network so you can restrict access to your business data?
- ☐ Have the default usernames and passwords for your computers, equipment and software been changed?
- ☐ Are your computers running Microsoft Windows 7 or newer, servers Microsoft Server 2008 or newer?
- ☐ Do you have a redundant/backup Internet connection, in the event your business loses connectivity?
- ☐ Can you remotely wipe data from mobile devices if they are lost or stolen?

If you find yourself needing assistance with answering the questions in this checklist, and/or would like to set up a complimentary one-hour security meeting to go over the results of this checklist, please contact:

Michael Maschke, CISSP
Sensei Enterprises, Inc.
Chief Executive Officer
Phone: (703)359-0700
E-mail: mmaschke@senseient.com

Sensei Enterprises, Inc. is a nationally known digital forensics, information security and information technology company located in Fairfax, Virginia. Sensei provides complimentary one-hour security informational meetings, as well as security assessments and recommendations for all types of businesses.