Professional Liability Insurance Program

Technology Privacy and Security Self Assessment: Primer and Recommended Minimum Practice (RMP)

1. Does your company have a **virus** protection program and a **firewall** in place?

RMP: Implement virus controls and filtering on all systems. Minimum controls include:

- Installing **antivirus software** on all systems.
- Implementing a process to keep antivirus programs up to date, utilizing automatic update of virus signatures if possible.
- Filtering e-mail attachments and downloads to reject files with the following extensions: .exe, .vbs, .bat, .pif, .scr.
- Disabling unneeded services and ports including: file transfer protocol (FTP) services and telnets (network protocols).
- Training employees not to open e-mail attachments unless they are expected and from a known and trusted source.
- Executing antivirus scans on all e-mail attachments, files and downloads before the file is opened.
- Running a commercially available product specifically designed to function as **antispyware software**. At a minimum, run a monthly full scan of all computers on your network.
- Disabling any non-essential network file sharing capabilities. If file sharing is necessary, create a dedicated directory for file sharing, password protect these shared files, and restrict use to "read only" if possible.

2. Does your company check for security software updates in a timely manner?

RMP: Subscribe to vendor **patch** notification services for all software and systems utilized, review and evaluate at least weekly, preferably daily. Where possible, enable automatic update capabilities. Test and install critical security **patches** and upgrades within 24 hours of availability, and all other **patches** within 30 days.

3. Does your company replace factory default settings to ensure that your information security systems are securely configured?

RMP: Implement policies regarding the configuration of all network security devices and systems.

- Avoid default configurations, and implement specific procedures for the management of strong administrative passwords for these devices and systems.
- Update policies as new **vulnerabilities** arise or network configurations change.
- Default policy for a **firewall** handling inbound traffic should be to block all **packets** and connections unless the traffic type and connections are specifically permitted.

4. Does your company control access to information that resides on company servers and computers?

RMP: In regard to confidential or sensitive information accessible within your company:

- Define access controls based on "need to know" or "least privilege", which refers to granting only the access required by users to perform their duties.
- Centrally administer access controls to limit access to confidential or sensitive information.
- Establish separation of duties to prevent individuals from subverting access controls.
- Implement written procedures to change user access privileges immediately upon changes in employee position or authority.
- Implement written procedures to terminate user access privileges when employment is terminated. If employment is being terminated for cause, revoke privileges concurrent with notifying the employee of termination.

5. Does your company have a policy on the creation and use of passwords?

RMP: Maintain an easily understandable written policy on creating and using passwords, and update the policy yearly to reflect current guidance.

6. Does your company use **authentication** and **encryption** to protect remote access to your network?

RMP: Authenticate and encrypt all remote access to your network, requiring user identification and strong passwords. While a **Virtual Private Network (VPN)** is the most common method to provide this protection, its use may not provide sufficient security when using offsite computers, networks or public Wi-Fi hotspots.

As part of your security policy, allow remote access only from other networks that meet your organization's security requirements.

7. Does your company monitor user accounts to identify and eliminate inactive accounts?

RMP: Maintain a written standard on required timeframes to eliminate inactive user accounts, and utilize software that automatically identifies and disables such accounts in accordance with the standard.

Over, please.

8. Does your company have the ability to monitor and control downloading of data to external storage devices such as flash drives, personal and tablet computers, and smart phones?

RMP: Maintain a written policy regarding storage of company data on portable devices, and utilize technical methods to prevent data leakage such as disabling or monitoring usage of USB ports, content filtering, and use of network monitoring software. All downloadable data should be encrypted.

Glossary

Antispyware Software
A program that specializes in detecting both **malware** and non-malware forms of **spyware**.

Antivirus Software
A program that monitors a computer or network to identify all major types of **malware** and prevent or contain **malware** incidents.

Authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Ciphertext
Data in its encrypted form.

Encryption
The process of changing **plaintext** into **ciphertext** for the purpose of security or privacy.

Firewall
A gateway that limits access between networks in accordance with local security policy.

Malware
A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

Packet
A short fixed-length section of data that is transmitted as a unit in an electronic communications network.

Patch
An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Plaintext
Unencrypted information.

Spyware
Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

Virtual Private Network (VPN)
A virtual network, built on top of existing physical networks, that provides a secure communications tunnel for data and other information transmitted between networks.

Virus
A self-replicating program that runs and spreads by modifying other programs or files.

Vulnerability
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Glossary Sources

Glossary of Key Information Security Terms, National Institute of Standards and Technology, February 2011. Merriam-Webster Dictionary, April 2013

Resource List

AICPA PrivacyDataProtection web site
www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/Pages/default.aspx

Alexa Huth, Michael Orlando and Linda Pesante, *Password Security, Protection and Management*, 2012, Department of Homeland Security United States Computer Emergency Readiness Team (US-CERT) www.us-cert.gov

General and updated information on information technology security is maintained by US-CERT at www.us-cert.gov

Endorsed by: AICPA®

Underwritten by: CNA

Nationally Administered by: AON

F-10515-113