Attachment 2: Practical Security Checklist

[This Checklist is adapted from Sharon D. Nelson, David G. Ries and John W. Simek, *Locked Down: Practical Information Security for Lawyers, Second Edition* (American Bar Association 2016).]

This checklist supplements the Comprehensive Cybersecurity Program Checklist and covers practical measures to implement a cybersecurity program. While checklists are helpful for cybersecurity programs, it important to use them appropriately. Security is not a "check the box" or "set it and forget it" process. It is important to devote continuing attention to security and to periodically review and update cybersecurity programs.

□ **Use secure, common configurations for servers, desktops, laptops, and mobile devices.**

- This includes settings like automatic logoff or shut down after *x* minutes of inactivity and locking or wiping after *x* failed logon attempts.
- Follow security configuration recommendations from Microsoft, Apple and device manufactures.
- For more comprehensive recommendations, see the Center for Internet Security's CIS Benchmarks, www.cisecurity.org/cis- benchmarks.
- Most attorneys will need technical assistance with secure configuration of servers.

□ **Control use of administrative privileges.**

- Windows and Mac computers have two kinds of user accounts: administrator and standard user accounts.
- Administrator access is needed for some functions like installing or removing software and devices.
- Some malware can run only in an administrator account.
- Use a standard user account for regular use of a computer.

□ **Use strong passwords or passphrases and a password manager.**

□ **Use multifactor authentication, particularly for administrator accounts and remote access.**

□ **Segment networks and limit access to sensitive data.**

□ **Promptly patch the operating system, firmware, all applications, and all plug-ins.**

- Malware often takes advantage of vulnerabilities in operating systems, applications and plug-ins. Updates and patches are developed to protect against such vulnerabilities after they are known.
- Patches should be promptly applied to protect against vulnerabilities.
- Computers are often compromised by malware for which patches are available but have not been applied.

□ **Provide for secure electronic communications.**

- It has now reached the point where attorneys should have access to encrypted e-mail for use when appropriate.
- There are now multiple options for encrypted e-mail that are inexpensive and easy to use.
- Examples include business versions of Microsoft 365 (Office 365) and Google's G Suite and services like ZixMail and Citrix FileShare.

□ **Use strong encryption.**

- Business versions of Windows have built-in encryption called BitLocker. It is activated by turning it on and saving a recovery key. BitLocker works best on business grade desktops and laptops that have a TPM (Trusted Platform Module) security chip. For consumer versions of Windows, encryption software is available from the publishers of standard security software like Symantec, McAfee, Norton and Sophos. Standalone encryption software is available from providers like Dell and WinMagic.
- Apple computers have built-in encryption called FileVault (currently FileVault 2). It is activated by turning it on and saving a recovery key.
- iPhones and iPads have built-in encryption that is automatically enabled when a passcode is set.
- Newer Android devices work the same way as iPhones and iPads, with encryption automatically enabled when a PIN, passcode, or swipe pattern is set.
- Older Android devices require encryption to be enabled by checking a box or pressing an onscreen button. If you are enabling encryption on an Android device that is already in use, follow the onscreen instructions, including plugging the device into a charger.
- After encryption is enabled, the device is automatically encrypted when a user logs off or the device is shut down. It is automatically decrypted when a user enters his or her logon credentials.

□ **Use only secure wireless networks.**

  - Securely configure law office wireless networks and home wireless networks used for work and use only ones with WPA2 or WPA3 security. Do not use wireless clouds with outdated WEP or WPA security.
  - Do not use public wireless networks unless you confirm that you have a secure connection by using a VPN (Virtual Private Network) or other secure communication channel.

□ **Use strong security appliances and software and keep them up to date.**

□ **Use email filtering and website filtering.**

□ **Conduct vulnerability assessment and remediation.**

□ **Back up important files and data.**

  - Files should be backed up at least daily.
  - Backups should be configured in a way that they won't be immediately compromised by malware that impacts the operating computer or network. This is particularly important for ransomware.
  - Test backups.

□ **Address third party security risks.**

  - It's important to conduct due diligence to determine that the level of security and the terms of service are appropriate.
  - Attorneys should require by contract that the services will be provided in a way that is consistent with the attorney's ethical duties, particularly confidentiality.
  - Attorneys should also engage in appropriate monitoring or supervision.

□ **Consider using secure cloud service providers.**

  - Service providers like business and enterprise versions of Microsoft Office 365 and Google's G Suite and secure case management platforms can generally provide a higher level of security than all but very large law firms.
  - Business versions of services like Dropbox and Box provide stronger control and security than consumer versions.
  - It's important to conduct due diligence to determine that the level of security and the terms of service are appropriate.

□ **Provide for secure disposal of electronic data and paper.**

  - Paper records should be shredded or incinerated.
  - Electronic data should be wiped or deleted with secure deletion software.

  - Devices that can’t be securely wiped with software should be physically destroyed.

□ **Address security for new, current, and departing employees.**