Attachment 3: Common Security Configuration 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 provides more details for implementing one of the measures in the Practical Security Checklist. 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.

- ❑ **Follow set up instructions for operating system and device**
- ❑ **Set up administrator and standard user accounts**
- ❑ **Use a strong pass word / passphrase**
- ❑ **Set up auto lock after *x* mins of inactivity**
- ❑ **Set up lock after x incorrect log on attempts**
- ❑ **Enable encryption (+ save recovery key)**
- ❑ **Turn on firewall**
- ❑ **Use current operating system and apps**
  - with all current updates (auto update where available)
- ❑ **Install security software (auto update)**
- ❑ **Secure Internet browser**
- ❑ **Turn off unneeded services**

More details are available in:

- NIST's, National Checklists Program, https://nvd.nist.gov/ncp/repository, and
- The Center for Internet Security's CIS Benchmarks, www.cisecurity.org/cis- benchmarks, and
- Microsoft's Security Baselines, https://techcommunity.microsoft.com/t5/microsoft-security-baselines/bg-p/Microsoft-Security-Baselines.