Desktop/Laptop/Mobile Devices Security Requirements When Accessing Sensitive Data

IT Security Requirements for Workstations/Mobile Devices with access to Personally Identifiable Information (PII) or Other Sensitive Information

1. Must have the latest Operating System security patches installed.

2. Must have automatic Operating System updates set to download and automatically install.

3. Must enabled Operating System firewall or equivalent.

4. User account must not have Local Administrative or Power User privileges (exceptions may be made in cases where an essential application requires elevated privileges).

5. Must change the default password for the Administrator and other pre-installed accounts.

6. Must disable and remove all unnecessary and unused accounts.

7. Must disable 'save password' feature, if applicable.

8. Must implement strong Operating System password rules: 8 or more characters in length including mix of alphanumeric and special characters.

9. Must enable password protected screen saver with inactivity threshold of 15 minutes.

10. Mobile devices (e.g., Blackberries, iPads and iPhones) must use passwords with inactivity thresholds of 5 minutes.

11. Must have managed version(s) of virus, spyware, malware protection software (e.g., Symantec) installed and actively monitored by the IT support department/group.

12. Must have a Management Agent software package (e.g., Altiris, SMS, etc.) resident, actively running on the computer and monitored by the IT support department/group. Note: A management agent provides IT personnel with the ability to periodically audit and do software inventory of machines.

13. If sensitive information is stored on the workstation (e.g., in the form of reports, spreadsheets, or other files), then the local hard drive and any external storage devices (such as USB drives) must be encrypted using software like the CUIT-supported Guardian Edge (can be obtained by emailing CUIT at askcuit@columbia.edu)

14. Must NOT install Peer-to-Peer file sharing software.

Desktop/Laptop/Mobile Devices Security Requirements When Accessing Sensitive Data

IT Security Requirements for Workstations/Mobile Devices with access to Personally Identifiable Information (PII) or Other Sensitive Information

15. The respective business/data owner(s) must enforce encryption (e.g., WinZip, 7-Zip, etc.) to secure attached confidential files/data sent by email.

16. Remote access is only allowed via the three options below:

    a. Personnel who have been provided CU issued and maintained laptops that adhere to the secure computer requirements outlined in this document, can gain remote access by using the CU VPN client software.

    b. Currently, CUIT approves remote desktop software that is bundled with Windows XP and above versions, configured according to our guidelines, to be an approved remote access solution.

    c. Citrix as configured by CUIT.

17. When a device becomes obsolete or the sensitive data saved on the device is no longer needed, all sensitive data must be effectively removed from the storage media before the devices are reused or discarded.

Any computing device containing multiple applications, which handle PII or other sensitive information, must adhere to applicable laws and regulatory requirements (e.g., PCI-DSS, PA-DSS, FERPA, GLBA, etc.) by implementing the most restrictive security controls (e.g., data encryption) in the event that multiple laws and regulatory requirements are applicable.