Security Standard: Desktop and Portable Computers

Scope

This standard applies to any computers that access RIT information resources.

Requirements

The following security controls are required to be implemented on computers based on their type:

	RIT-owned desktop/laptop	**Lab computers, Grant-funded computers**	**Personally-owned computers (student, visitor, home)**
1. Anti-virus	Centrally managed	Centrally managed	X
2. Endpoint Firewall	X	X	X
3. Supported Software with Up-to-date security patches	X	X	X
4. Log out/lock out	X	X	X
5. Host-based Intrusion Prevention System (HIPS)	X	X	
6. Host-based vulnerability management software	Pending product selection	Pending product selection	
7. PI management software	X	Storage of Private Information Is prohibited	Storage of Private Information Is prohibited
8. Full-disk encryption	If accessing Private Information		
9. Centralized Desktop Management	X	X	
10. Administrative privileges	At the discretion of VP/Dean		

Other computing devices (e.g. tablets, smartphones, copiers, device controllers) should employ these controls to the extent possible commensurate with the risk of the information that is accessed or stored on them. Storage of Private information is prohibited on these devices.

All required security controls are required to be installed, up-to-date and enabled.

1. **Anti-virus software**: Should have anti-virus with malware signature, heuristic, anti-spyware, and reputation awareness capabilities

2. **Endpoint firewall**

3. **Supported software with up-to-date security patches:** Operating system and application software should be supported with up-to-date security patches.

4. **Log out/lockout:**
   - 4.1. Users should either log out or lock the interactive session before leaving the session or computer unattended.
   - 4.2. For RIT-owned computers, administrators should set a minimum automatic lockout commensurate with the use and risk of the information, e.g., a lockout after 15 minutes is recommended for typical office use.

5. **Host Intrusion Prevention System (HIPS):** Required on Windows operating systems. Recommended Host Intrusion Prevention Systems solutions can be found at https://www.rit.edu/security/content/technical-resources.

6. **Host-based vulnerability management software:** The recommended host-based vulnerability management software solution can be found at https://www.rit.edu/security/content/technical-resources. NOTE: The requirement for host-based vulnerability management software is pending product selection.

7. **Private information management software:**
   - **7.1.** The software should complete scans monthly.
   - **7.2.** Users should not be storing private information on any endpoint and should immediately remediate any identified private information.
   - **7.3.** The software should report results to a centralized management console controlled by ITS.
   - **7.4.** The recommended Private Information management software can be found at http://www.rit.edu/security/content/securing-your-computer

8. **Full Disk Encryption:**
   - 8.1. If computers are used to access private information, then the computer should have full disk encryption. The encryption solution should validate that the product was installed and operating correctly.
   - 8.2. User-configurable settings should not be capable of interfering with the encryption software.
   - 8.3. Encryption software and policies should be controlled by centralized security personnel.
   - 8.4. The recommended full disk encryption solution can be found at https://www.rit.edu/security/content/encryption-rit.

9. **Centralized Desktop Management:** Computers should be auditable from centralized configuration management software. This audit capability should include an inventory of applications and current patch level.

10. **Administrative privileges:** Use of limited vs. administrative privileges is determined by the divisional VP or dean.

For additional information and product recommendations, please see
http://www.rit.edu/security/content/securing-your-computer

Effective Date: January 23, 2015

Standard History:
May 5, 2005
May 15, 2009
November 11, 2013
October 19, 2015