



# Desktop and Portable Computer Standard Security Checklist for End-Users

**Computer identification and location:** \_\_\_\_\_

Completed by (please print): \_\_\_\_\_

Date: \_\_\_\_\_

Signature: \_\_\_\_\_

Next scheduled review date: \_\_\_\_\_

Manager's signature: \_\_\_\_\_

Date: \_\_\_\_\_

<b>All computers that connect to the RIT network require the following:</b>	<i>Ref.</i>	<b>Initials</b>
1. Anti-virus software (with malware signature, heuristic, anti-spyware, reputation awareness) installed and enabled.	(1)	
2. A firewall, software or hardware, is installed and enabled.	(2)	
3. All operating system and application security patches are up to date.	(3)	
4. Users are aware that they should not leave their computer unattended without logging off or locking the computer first.	(4.1)	
5. Computer is set to automatically lock the screen when inactive for more than 15 minutes.	(4.2)	
6. Have you confirmed with your systems administrator that an ISO-approved Host Intrusion Prevention System is installed and enabled on your machine?	(5)	
7. Have you confirmed with your systems administrator that ISO-approved host-based vulnerability management software is installed and enabled on your machine? (Requirement pending product selection.)		NA
8. Have you confirmed with your systems administrator that ISO-approved private information management software is installed and enabled on your machine?	(7, 7.4)	
9. Scans are allowed to complete monthly and results are reported (by the software) to ISO.	(7.1, 7.3)	
10. No private information is stored on the computer. If the software reports any private information, it is immediately remediated.	(7.2)	
11. Do you access private information on this computer? <b>(Y/N)</b> _____ If <b>No</b> , skip to number 14.		
12. Have you confirmed with your systems administrator that whole-disk encryption is installed and enabled, and that no user-configurable settings are interfering with the software?	(8.1 – 8.2, 8.4)	
13. The encryption software and its policies are being managed by centralized ISO-approved security personnel.	(8.3)	
14. Have you confirmed with your systems administrator that this computer can be audited from centralized and ISO-approved configuration and software management tools, and that the audit is configured to include applications and patch inventory?	(9)	
15. Are administrator privileges being used on this computer? <b>(Y/N)</b> _____ If <b>Yes</b> , who is the dean or VP that has authorized the privileges? _____	(10)	

RIT Information Security  
[infosec@rit.edu](mailto:infosec@rit.edu)  
<https://www.rit.edu/security>