RIT | Information Security

Desktop and Portable Computer Standard Security Checklist for Systems Administrators

Computer identification and location: ____

Completed by (please print): ________________________ Date: ______________

Signature: __________________________ Next scheduled review date: ______________

Manager's signature: __________________________ Date: ______________

All computers that connect to the RIT network require the following:	*Ref.*	**Initials**
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. An ISO-approved Host Intrusion Prevention System has been installed and enabled.	*(5)*	
7. An ISO-approved host-based vulnerability management software is installed and enabled. (Requirement pending product selection.)	*(6)*	
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? (**Y/N**) ____________ If **No**, skip to number **14**.		
12. 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. 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? (**Y/N**) ____________ If **Yes**, who is the dean or VP that has authorized the privileges? ___________________________	*(10)*	

RIT Information Security
infosec@rit.edu
https://www.rit.edu/security