Security Standard: Desktop and Portable Computing Devices

Introduction and Scope

RIT uses many types of computing devices, physical and virtual (desktop, portable, tablet, smartphone, etc.), to access RIT information resources. This standard provides requirements for these computing devices to ensure that RIT information resources are accessed securely.

Requirements

OVERVIEW

The following security controls are required as detailed in the table. See the notes following the table for more information about each requirement.

	RIT-owned desktop/laptop, Grant-funded computers	**Lab computers**	**Personally-owned computers (student, visitor, home)**	**Other Computing Devices**
1. **Endpoint Protection/Anti-malware**	Must be centrally managed	Must be centrally managed	Yes	Yes
2. **Endpoint Firewall**	Yes	Yes	Yes	Required if RIT-owned device when solution available from RIT. Recommended if personally-owned device.
3.**Host-based Intrusion Prevention System (HIPS)**	Yes	Yes		

	RIT-owned desktop/laptop, Grant-funded computers	Lab computers	Personally-owned computers (student, visitor, home)	Other Computing Devices
4.**Supported Software/Apps with up-to-date security patches**	Yes	Yes	Yes	Yes
5.**Log out/lock out**	Yes	Yes	Yes	Yes
6.**PI management software**	Yes	Storage of private information is prohibited	Storage of private information is prohibited	Storage of private information is prohibited
7.**Full-disk encryption**	Required, if accessing private information			
8.**Centralized Desktop/Device Management**	Yes	Yes		Required if RIT-owned device when solution available from RIT. Recommended if personally-owned device.
9.**Administrative privileges**	Administrative privileges granted only at the discretion of VP/Dean			Jail-broken or rooted devices are prohibited from accessing Confidential or Private Information.
10. Backups (data)	Required (centrally managed preferred)		Recommended	Recommended

DETAILS

All required security controls must 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. Anti-virus software is available for most computing devices.
2. **Endpoint firewall:** Not needed with Android or iOS devices unless rooted or jail-broken.
3. **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.
4. **Supported software/applications with up-to-date security patches:** Operating system and application software must install up-to-date security patches.
5. **Log out/lockout:**
   5.1. Users should either log out or lock the interactive session before leaving the session, computer, or device unattended.
   5.2. 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.
   5.3. For personally-owned devices, we recommend an automatic lockout period of 2-15 minutes.
6. **Private information management software:**
   6.1. The software should complete scans monthly.
   6.2. Users should not be storing private information on any endpoint and should immediately remediate any identified private information.
   6.3. The software should report results to a centralized management console controlled by ITS.
   6.4. The recommended Private Information management software can be found at http://www.rit.edu/security/content/securing-your-computer
   6.5. PI software licensing may not extend to grant-funded computers
7. **Full Disk Encryption:**
   7.1. 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.
   7.2. User-configurable settings should not be capable of interfering with the encryption software.
   7.3. Encryption software and policies should be controlled by centralized security personnel.
   7.4. The minimum recommended full disk encryption levels can be found at https://www.rit.edu/security/content/encryption-rit.
8. **Centralized Desktop Management:** RIT-owned, lab computers, and grant-funded computing devices should be auditable from centralized configuration management software. This audit capability should include an inventory of applications and current patch level.

9. **Administrative privileges:** Use of limited vs. administrative privileges is determined by the divisional VP or dean.
10. **Backups:** RIT data and research data should be backed up. Backups shall enable computers/devices to be restored to a recent point in time before the incident requiring backup. Centrally-managed backups are preferred.
    10.1. For usage where data is stored on the network, a disk image is an acceptable backup.
    10.2. For situations where data is stored locally, the backup should be able to restore that data. (We recommend that data not be stored locally.)

Resources/Related Information

- Standards Lexicon (definitions of terms used in standards)
- Roles and Responsibilities in relation to specific standards
- Exceptions/Non-Compliance—use of non-compliant portable media requires an exception request approved by the information trustee and the RIT Information Security Office.
- Related RIT Policies
    - Information Access and Protection Standard
    - Portable Media Standard

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

Effective Date: June 1, 2019

Standard History:

- May 5, 2005
- May 15, 2009
- November 11, 2013
- October 19, 2015
- October 24, 2017