

Security Standard: Desktop and Portable Computers

Effective **August 1, 2009**

1.0 Purpose

This standard is the first step towards making all computers connecting to the RIT network more secure and protecting the data that they access. Adherence to the standard will both increase the security of personal computers and help safeguard RIT network resources to meet the significant and growing internal and external threats from among others:

- Criminals who are testing the vulnerability of RIT computers
- Inbound network-based attacks
- Liability associated with outbound network mapping or attacks
- Undetermined system anomalies that might hinder availability or access to critical resources and applications
- Eavesdropping programs designed to relay sensitive information

2.0 Scope

This standard applies to:

- All RIT-owned or leased computers.
- Any computer (physical or virtual) connecting to the RIT network through a physical, wireless, dial-up, or VPN connection.

The standard *does not* apply to:

- Computers used only to access RIT web pages, Webmail, etc. from off campus.
- Cell phones, pagers, PDAs, and other special purpose devices that connect to the Institute network solely through Web, portal, or application access.

3.0 Audience

The audience for this standard is all users connecting directly to the Institute network. *The Code of Conduct for Computer and Network Use* mandates “self-protection” and this standard further defines that mandate.

4.0 Definitions

Authorized User – Anyone who has been granted permission to read or access a given set of data or system. This may or may not entail the modification of the data or system.

Host-based Intrusion Prevention System (HIPS) – A security application which typically resides on an individual computer or system. Its main purpose is to monitor system activities—particularly those relating to network connections—for malicious or unwanted behavior and react in real time to block or prevent those compromises.

Privileged Access – A computer access level that enables an individual to take actions which may affect computing systems, network communications, or the accounts, files, data, or processes of other users.

5.0 Minimum Standard

The following security controls must be applied to, enabled, and operating on computers that connect directly to the Institute network, on **August 1, 2009** and all times thereafter:

- 5.1 All computers that connect to the RIT network require:
 - 5.1.1 Anti-virus software, with up-to-date signatures
 - 5.1.2 Up-to-date Operating System and application security patches
 - 5.1.3 Hardware or software that provides memory protection (e.g., buffer overflow protection, Data Execution Prevention (DEP))
 - 5.1.4 A personal firewall (software or hardware)
 - 5.1.5 Anti-spyware software, with up-to-date signatures
- 5.2 Additional requirements for RIT-owned or leased computers:
 - 5.2.1 Laptops must employ whole-disk encryption
 - 5.2.1.1 The encryption solution must validate that the product was installed and operating correctly.
 - 5.2.1.2 User-configurable settings must not interfere with the encryption software.
 - 5.2.1.2.1 Laptops must be set to hibernate, rather than standby, when inactive for more than 30 minutes.
 - 5.2.1.3 Encryption software and policies must be controlled by centralized ISO-approved security personnel.
 - 5.2.1.4 Encryption on Mac and Linux laptops will be required when the centralized solution becomes available.
 - 5.2.2 Automated audit ability
 - 5.2.2.1 Wherever possible, RIT-owned or leased computers must be auditable from centralized ISO-approved configuration and software management tools.
 - 5.2.2.1.1 This audit must include applications and patch inventory.
 - 5.2.3 Anti-phishing controls
 - 5.2.3.1 Anti-phishing controls must be used. Recommendations may be found at <http://security.rit.edu/dsd/bestpractices/phishing.html>.
 - 5.2.4 Log out/locking of unattended computers
 - 5.2.4.1 Users must log out of or lock computers before leaving them unattended.
 - 5.2.5 Administrative privileges
 - 5.2.5.1 Use of limited vs. administrative privileges is determined by the divisional VP or dean.
 - 5.2.6 Host Intrusion Prevention System (HIPS)
 - 5.2.6.1 RIT-owned or leased computers must employ a Host Intrusion Prevention System. A list of ISO-approved Host Intrusion Prevention Systems can be found at <http://security.rit.edu/essentials.html>.

If products are not available from reputable commercial or reliable open source communities for a specific requirement, then the specific requirement is waived until an appropriate solution is available. A current list of appropriate software is maintained on the Information Security website <http://security.rit.edu/essentials.html>.

Anti-virus software is available without cost to RIT faculty, staff, and students at <http://http://www.rit.edu/its/services/security/>. Firewall software is also available at no cost for use on RIT-owned or leased computers through the same site.

A “Plain English Guide” providing explanation and illustration of this standard may be found at <http://security.rit.edu/desktop.html>. In all cases, it is the standard itself, and not the “Plain English Guide,” which is authoritative.

Note: Additional security precautions and recommendations for desktop and portable computers can be found at: <http://security.rit.edu/essentials.html>.

6.0 Roles and Responsibilities

This section identifies the roles and responsibilities for implementation and compliance.

- **Information Security Office**—Issues security standards based on threats and the needs of the Institute for protection. The ISO champions implementation efforts, offers acceptable alternatives, and provides exceptions as appropriate. The staff of the Information Security Office provides communication and training materials as appropriate. The ISO will be available for participation in Institute disciplinary processes.
- **Information Trustee (Divisional VP or Dean)**—Comprehends the risks associated with the security standard and provides direction to appropriate students, faculty, and/or staff to ensure full compliance with the *Standard* and wherever possible the associated *Best Practices*.
 - **Institute Audit, Compliance & Advisement (IACA)**—reviews compliance with this Security Standard (and all Security Standards) as part of departmental audits.
- **End User**—Ensures that all assigned RIT-owned or leased desktop and portable computers that connect to the Institute network meet the minimum standards set forth above. In order to enhance compliance with the Desktop Standard, end users may engage support personnel, such as systems administrators. The burden for compliance with this standard falls on each end user, unless a systems or network administrator has agreed to assume some or all of the responsibility.
- **Systems or Network Administrator**—Ensures that all existing RIT-owned or leased supported desktop or portable computers are configured to support the minimum standards set forth above, or that an alternate plan for risk management is provided to their Information Trustee in accordance with the Exception Process below.

7.0 Non-Compliance and Exceptions

For all individuals with administrator access—if any of the *Minimum Standards* contained within this document cannot be met on systems you use or support, an Exception Process must be initiated that includes reporting the non-compliance to the Information Security Office and providing an alternate plan for risk management. For more, see <http://security.rit.edu/process/exceptions.pdf>.

Anyone not complying with the standard is subject to sanctions including suspension of computer and network privileges and/or current Institute personnel and student disciplinary processes.

8.0 Related RIT Policies, Procedures, Best Practices and Applicable Laws (not all-inclusive)

- RIT Information Security Policy (C8.1)
<http://http://www.rit.edu/~620www/Manual/sectionC/C81.html>
- RIT's Code of Conduct for Computer and Network Use (C8.2)
<http://http://www.rit.edu/~620www/Manual/sectionC/C82.html>
- RIT Password Security Standard
<http://security.rit.edu/password.html>
- RIT Information Access and Protection Security Standard
<http://security.rit.edu/iap.html>
- RIT Server Security Standard
<http://security.rit.edu/server.html>
- RIT Portable Media Security Standard
<http://security.rit.edu/portablemedia.html>
- RIT's Information Security Exception Process
<http://security.rit.edu/process/exceptions.pdf>

Date Issued: May 5, 2005

Revised: May 15, 2009