

## Security Standard: Portable Storage Devices and Media

Effective September 1, 2008

### 1.0 Purpose

This standard defines the minimum requirements for the secure use of portable storage devices/media (portable media) that store or transport Private, Confidential, or Operationally Critical information. The standard addresses growing internal and external risks including, but not limited to loss or compromise of Private, Confidential, or Operationally Critical information contained on the media due to theft, irrecoverable data, or unauthorized access.

### 2.0 Scope

This standard applies to:

- All portable media (RIT-owned and privately-owned) that store or transport computerized Private, Confidential or Operationally Critical information
- The standard applies irrespective of the Operating System on the device or File System on the portable media.
- Portable media includes but is not limited to CDs, DVDs, Flash Memory, portable hard drives, backup tapes, and any future portable media.

This standard does not apply to:

- Non-digital forms of media including paper, audio or video tapes, etc. However, if this non-digital media contains Private or Confidential information it must be handled in accordance with the Information Access and Protection Standard.

The NYS Security Breach and Notification Act (Dec. 2005) applies to all computerized data containing personal and private information irrespective of whether it is maintained on RIT-owned or personally-owned media. If Private or Confidential information resides on personally-owned storage media, the owner of the media must follow the requirements of this standard.

Classification of RIT information is defined in *Security Standard: Institute Information Access and Protection*

<http://security.rit.edu/docs/informationprotection.pdf>

Private and Confidential information must be handled in accordance with the Information Access and Protection Standard. Requirements of this standard that are more stringent supersede any less stringent requirements in departmental Information Access and Protection Plans.

### 3.0 Audience

The audience for this standard is anyone who uses portable media to store or transport Private or Confidential information.

## 4.0 Definitions

### Portable hard drive

A portable hard drive is any disk drive that is plugged into an external port on a computer such as USB or FireWire. For laptops, the PC Card slot may be used to connect a cable to a full-size drive, or the hard disk may be contained entirely inside the PC Card.

## 5.0 Minimum Standard

The following security controls must be applied to, enabled, and/or operating on all portable or removable media that store or transport Private or Confidential information no later than **September 1, 2008**.

### 5.1 General

5.1.1 All new portable media must support ISO-Approved Encryption Methods.

5.1.1.1 A list of acceptable encryption methods is available on the RIT Information Security website at <http://security.rit.edu/portablemedia.html>

5.1.2 RIT Confidential Information must be encrypted on portable media used for backups, archives, and transport.

5.1.3 Portable media containing RIT Confidential Information must be given reasonable physical protection from unauthorized use or theft.

5.1.4 RIT Confidential Information on media that is to be disposed of or transitioned to another user must be overwritten so that the information is no longer recoverable.

5.1.4.1 Disposal of RIT Confidential Information may require destruction of the media.

### 5.2 Operationally Critical Data

5.2.1 Operationally critical data shall not be placed solely on portable media

5.3 Loss of portable media whose contents are unknown or that contain Private or Confidential information must be reported through the Incident Handling process

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

## 6.0 Roles and Responsibilities

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

- **Information Security Officer**—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 (VP or Provost)**—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 personally owned portable media that may contain Private or Confidential information meet the minimum standards set forth above and follows the Information Access and Protection Standard. In order to enhance compliance with the Standards, end users may engage support personnel such as systems administrators. The burden for compliance with this standard falls on each end user. The end user must report loss or compromise of portable media containing Private or Confidential information in accordance with the Computer Incident Handling Process standard.
- **Systems or Network Administrator**—ensures that all existing RIT-owned *supported* portable media that may contain Private or Confidential information 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

If any of the *Minimum Standards* contained within this document cannot be met on portable media you use or support that transports or stores Private or Confidential information, 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>

The Information Security Office will determine applicability of the standard to any portable media not specifically listed in the standard.

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://www.rit.edu/~620www/Manual/sectionC/C81.html>
- RIT's Code of Conduct for Computer and Network Use (C8.2)  
<http://www.rit.edu/~620www/Manual/sectionC/C82.html>
- Security Standard: Institute Information Access and Protection (2009)  
<http://security.rit.edu/docs/informationprotection.pdf>

- RIT's Information Security Exception Process  
<http://security.rit.edu/process/exceptions.pdf>
- Security Standard: Desktop and Portable Computers, RIT-owned or Leased  
<http://security.rit.edu/articles/desktopstandard.pdf>
- Security Standard – RIT User Account Passwords  
[http://security.rit.edu/standards/passwordstandard\\_users.pdf](http://security.rit.edu/standards/passwordstandard_users.pdf)
- Security Standard: Computer Incident Handling Process  
<http://security.rit.edu/articles/incidenthandling.pdf>

**RIT Information Security Office**

**Date Issued: May 15, 2008**

**Revised: March 8, 2010**