

Security Standard: Institute Information Access and Protection

Effective December 15, 2005

1.0 Purpose

The intent of this standard is to

- Establish common definitions and information classifications
- Facilitate the identification and management of sensitive information
- Facilitate the identification and management of information critical to the operations of the Institute
- Facilitate communications and training requirements to promote consistent handling of sensitive and critical information

2.0 Scope

This standard applies to the handling of Institute information that is non-public or supports the administrative business of the university. This standard does not apply to information whose primary purpose is scholarly (e.g., instructional material, research notes, etc.)

3.0 Audience

The audience is all faculty, staff, student employees, contractors, and external business associates and vendors working with RIT information or information systems.

4.0 Definitions:

For the purpose of this standard, information is defined by specific classifications related to either confidentiality or integrity/reliability. These classifications are not mutually exclusive. (E.g., information may be both RIT Confidential and Operationally Critical.)

Information Confidentiality Classifications

RIT Public Information—information that may be accessed or communicated by all RIT faculty, staff, students, alumni, contractors, and business associates without restriction.

RIT Internal Use Only—a suggested, but optional, categorization for information that may be accessed or communicated by all RIT faculty, staff, students, alumni, contractors, and business associates without restriction for the conduct of Institute business.

RIT Confidential—a more restrictive classification, that is required for information that is accessed or communicated on a need to know basis, that, because of legal, contractual, ethical, or other constraints, may not be accessed without specific authorization. RIT Confidential information may have many forms including, but not limited to, documents, data, stored audio, or video. The classification “RIT Confidential” also applies to information the

unauthorized disclosure of which could result in significant harm to the Institute, Institute processes, or to individuals.

Information Integrity/Reliability Related

Information/Data Integrity—the assurance that information/data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

Authoritative Source—the information source with the highest level of information verification or data integrity.

RIT Operationally Critical—a classification for information that requires a high level of information availability in addition to integrity. The classification “RIT Operationally Critical” refers to information that is essential to the daily operations of the Institute. This information must be identified and protected, not only for business continuity planning, but also as appropriate for information availability and integrity. It may be of any level of confidentiality/sensitivity.

5.0 Minimum Standard

By the effective date of this standard, each department (or higher level organizational unit if uniformity allows) must adopt a written Information Access and Protection Plan describing how it manages the handling, access and protection of RIT information that has confidentiality or integrity requirements. The Plan must be published and accessible to all employees in the department and must be made available to the Information Security Office upon request. Required components of the Plan are listed below.

5.1 Information inventory/identification

5.1.1 For all information handled and retained by the department, the plan must identify by type

5.1.1.1 All **RIT Confidential** information the *confidentiality of which* is legally regulated (i.e., regulated by FERPA, GLBA, or HIPAA, etc.)

5.1.1.2 All other **RIT Confidential** information documents or elements maintained by the department.

5.1.1.3 All **RIT Operationally Critical** information whose *integrity* is legally regulated (e.g., GLBA)

5.1.1.4 All other **RIT Operationally Critical** information documents or elements maintained by the department.

5.1.1.5 All information for which the department believes they are the *authoritative source* (i.e., the source of the most reliable information).

5.1.1.5.1 The plan must identify classes of recipients of information routinely shared through electronic data feeds.

- 5.1.1.6 Information shared with external business associates.
- 5.2 Information handling processes and safeguards
 - 5.2.1 For all RIT Confidential and RIT Operationally Critical information identified in 5.1, the Plan must describe
 - 5.2.1.1 How the department manages the confidentiality and integrity of information
 - 5.2.1.2 The use of confidentiality or disclosure agreements, internally and externally.
 - 5.2.1.3 How the department ensures confidentiality when transferring **RIT Confidential** information.
 - 5.2.1.4 Procedures for the retirement and destruction of **RIT Confidential** information maintained by the department.
 - 5.2.1.5 Procedures for the storage of **RIT Confidential** information, including appropriate restrictions relative to media with limited access control capabilities (e.g., flash drives, writable CD/DVDs, and Personal Digital Assistants).
 - 5.2.1.6 Procedures for the reuse or retirement of devices and media used to store **RIT Confidential** information.
 - 5.2.1.7 Procedures for ensuring the confidentiality and integrity of RIT information used by external business associates.
 - 5.2.1.8 Handling requirements and procedures for the use of RIT Confidential or Operationally Critical information off-site.
- 5.3 Training and communications requirements
 - 5.3.1 The Plan must specify how to communicate information access and protection requirements and train employees (regular and temporary).
- 5.4 Plan maintenance
 - 5.4.1 The Plan must be reviewed internally and updated at least once every 2 years.

5.0 Roles and Responsibilities

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

- **Information Security Officer**—issues standards based on legal context, threats and the needs of the Institute for confidentiality and integrity of Institute information. The ISO champions implementation efforts, facilitates recognition and communication of best practices, offers acceptable alternatives, and provides exceptions as appropriate. The staff of the Information Security Office provides communication and training materials as appropriate.

- **Information Trustee (VP or Provost)**—comprehends the risks associated with the **RIT Confidential** and **University Critical** information and provides direction to all faculty, staff, student employees, and contractors within his or her domain to ensure full compliance with the *Standard* and wherever possible the associated *Best Practices*. Information Trustees whose organizations are responsible for maintaining the authoritative source for elements of information have a responsibility to maintain a list of automated data feeds when they provide the information to other organizations.
- **Information Security Coordinator**—acts as an information security liaison to their colleges, divisions, or departments; responsible for information security project management, communications, and training for their constituents.
- **Systems or Network Administrator**—implements technical access control based on authorization provided through the departmental Information Access and Protection Plans; verifies the transition of data rights from departing or former employees or contractors to current employees or contractors; provides technical support for the information's integrity, business continuity, and electronic data retirement or destruction.
- **End-User**—follows guidance provided in the Plan, during new employee training, and in offsite locations. Thoughtfully communicates **RIT Confidential** information, wisely choosing the medium and the recipients.
- **External Business Associate**—accesses RIT Confidential or Operationally Critical information when authorized.

6.0 Non-compliance and Exceptions

If a department or other RIT entity is unable to meet the *Minimum Standards* contained within this document, an Exception Process must be initiated that includes reporting the non-compliance to the Information Security Office, along with a plan for risk assessment and management. For more, see: security.rit.edu/process/exceptions.pdf

Anyone not complying with the *Minimum Standards* is subject to sanctions, including the full range of current human resources and student judicial processes.

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

- RIT's Information Security Policy
Under RIT Governance review. Draft at:
http://security.rit.edu/policy/RIT_InfoSec_Policy.pdf
- RIT's Code of Conduct for Computer and Network Use (C10.0)
www.rit.edu/computerconduct

- RIT's Information Security Exception Process
security.rit.edu/process/exceptions.pdf
- Gramm-Leach-Bliley Act (GLBA)
- Federal Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)

Jim Moore, Information Security Officer, CISSP, IAM

Date Issued: August 31, 2005

Next Scheduled Review Date: August 31, 2006