



# Plain English Guide to the Information Access and Protection Standard

RIT has issued new requirements for Information Access and Protection in order to safeguard RIT information. The requirements were developed and reviewed by a team representing the RIT community. This Plain English Guide provides explanation and illustration of the Standard and is provided as an aid to help you understand and implement the requirements of the Standard. The Standard itself is authoritative. The standard is effective on **December 15, 2005**.

## Why we issued this standard

Information is most valuable or useful when it is known to be accurate and can be accessed by authorized users. Conversely, information is most protected when it can not be accessed. This standard provides requirements for handling sensitive information that create a balance between accessibility and protection and ensure that information is not improperly changed, inadvertently or by design. The standard requires RIT departments to adopt a plan to ensure information access and protection.

The standard addresses both the confidentiality of information to protect against unauthorized or unplanned exposure, and the integrity/reliability of the information to protect against unplanned changes or deletion.

These requirements are also necessary because:

- Federal and state regulations require access controls for confidential information.
- Federal and state regulations often require assurance that the integrity of record information (e.g., financial records) is maintained.
- State laws require disclosure of information security breaches.
- The risk of significant information compromise has increased along with the advances of data storage technology that allow large amounts of information to be stored easily on portable devices such as portable USB drives, PDAs, cell phones, iPods, etc.
- The availability of Operationally Critical information must be ensured.

## Who do the requirements apply to?

The requirements apply to RIT employees, student employees, volunteers, and external business associates who handle specific classes of RIT information—sensitive information, such as RIT Confidential and RIT Internal Use Only, and information whose integrity must be maintained, such as Operationally Critical. Confidentiality and integrity categories are not mutually exclusive. For example, information may be both RIT Confidential and Operationally Critical. It may not be both RIT Confidential and RIT Internal Use Only.

Information of a scholarly nature (such as research materials) is generally excluded from the requirements of the standard. However, this exclusion does not extend to student record information, information that RIT is obligated to protect by contract, or information that is being developed at RIT that is intellectual property such as pre-patent information.

## What do I have to do?

The standard requires departments to develop and communicate a written Information Access and Protection Plan and train employees who handle RIT information categorized as RIT Confidential, RIT Internal Use Only, or Operationally Critical. Each department must designate an individual to develop the Plan. The Plan must include processes for storing and handling information in both electronic and non electronic forms. The Plan must contain the following elements:

- Information identification
- Information handling processes and safeguards, including transfer of sensitive information outside the department
- Communications and training
- Plan maintenance

Plans for higher level organizational units may be adopted if the information access and protection requirements are applied uniformly.

The Information Security Office will support plan creation by providing the following:

- Plan template
- Plan creation workshop
- Individualized Plan creation assistance and review

Development of the Information Access and Protection Plan requires a review of information owned or handled by the department, identification of information that should be categorized, and development and documentation of procedures for handling that information from creation to destruction. The Plan should ensure that the right information reaches only the right audience. The Plan may identify changes to implement in daily departmental activities.

## Where do I go for more information?

Visit our website at <http://security.rit.edu> to read the standard and obtain a copy of the Plan template. For more information or assistance with the Information Access and Protection Plan, contact RIT Information Security at [infosec@rit.edu](mailto:infosec@rit.edu).