Security Standard: Information Access and Protection

Scope

This Standard applies to everyone who accesses RIT Information Resources, whether affiliated with RIT or not, whether on campus or from remote locations, including but not limited to students, faculty, staff, contractors, consultants, temporary employees, alumni, guests, and volunteers. By accessing RIT Information Resources, these users agree to comply with this Standard.

Requirements for All Information

1. **Information Inventory**
   1.1. All RIT organizational units (departments, divisions, etc.) should identify and maintain an inventory (type, classification, location, accessibility) of all Private, Confidential, and Internal information they handle or maintain.

2. **Training**
   2.1. Divisional VPs and Deans are responsible for ensuring that mandatory information handling training is provided to any RIT employees (including adjuncts, temporaries and contractors), student employees, volunteers (including trustees, agents, members of affiliate groups, etc.) with access to Confidential or Private information.
   2.2. This training should be conducted on an appropriate periodic basis.

3. **Non-disclosures**
   3.1. Divisional VPs and Deans are responsible for ensuring that users comply with RIT non-disclosure requirements, which may include signing a non-disclosure agreement.
   3.2. Systems, applications, or web page administrators (including student employees) who administer information systems containing Confidential or Private information should sign the RIT Systems Support Personnel Non-Disclosure Agreement form located at https://www.rit.edu/security/content/forms-checklists-and-templates.

Requirements for Private Information

4. **Identification and Remediation**
   4.1. Every RIT organizational unit (department, division, etc.) shall participate in RIT-sanctioned Private information identification and remediation programs (e.g., Private Information Management @ RIT). Divisional VPs and Deans are responsible for developing inventories of private information through these programs.
   4.2. Alternatives to using Private information should be identified and used whenever possible. The University ID shall replace the Social Security Number as the primary identifier. Unless required by a VP-approved RIT business process, files should not contain Private information. Any Private information in the file shall be sanitized by redacting (removing) the Private information. This redaction should be done in a manner that permanently removes the Private

information from the files. Masking of the Private information is insufficient. Approved information sanitization practices may be found at https://www.rit.edu/security/content/information-access-protection-standard.

5. Access and Use

5.1. Private information should be used and disclosed to others only on a need-to-know basis to permit the individual faculty or staff member to perform their RIT functions for which the information was acquired and for which it is maintained. Access to Private information should be carefully safeguarded with documented technical and process controls that limit access to and use of Private information to locked and protected physical or electronic environments. The technical access controls should include use of a login trespassing banner where appropriate. Access and use of this information is restricted to specific departments.

5.2. It is the responsibility of Divisional VPs and Deans (Information Trustees) to protect Private information from disclosure to or unauthorized access by anyone who does not have a legitimate need to access the information to comply with requirements of the law or to carry on necessary University functions. Any business process that uses Private Information should be approved by the Divisional VP or Dean.

5.3. Disclosure of Private information to a third party agent or vendor is permitted only if the agent or vendor assumes a legally binding obligation to safeguard the use and disclosure of the information. Contact the Office of Legal Affairs for appropriate contractual language.

5.4. Access and use of Private information through clearinghouses (e.g., NCAA, National Student Clearinghouse, etc.) should follow the above requirements when possible.

5.5. Mandated federal, state and court reporting is excluded from this.

6. Storage

6.1. Private information in paper form and other portable media should be stored in locked areas when not in active use. Unless required by RIT business processes, copies of files containing Private information are prohibited.

6.2. Private information in electronic form should be stored in secure ISO-approved servers, or, if authorized to be stored elsewhere, only in encrypted (not just password-protected) form. It should not be stored on desktop, laptop, mobile devices or portable media without encryption or similar protection. Contact the Information Security Office for advice and assistance.

6.3. Private information shall not be posted in blogs, wikis, or other digital locations/repositories or social networks that do not use ISO-approved RIT authentication and authorization.

6.4. Private information shall not be stored on computer systems that share virtualized resources through the Internet (cloud computing) or a grid (distributed computing).

7. Transfer/Sharing

7.1. Any transfer or sharing of information should not include Private information unless essential to perform the function for which the communication is made. Transfer or sharing of Private information should be by ISO-approved methods such as:

- secure file transfer such as Tiger File Exchanger
- encrypted e-mail or other electronic transmission
- file-based encryption

7.2. Requiring use of Private Information to access a website is prohibited.

7.3. Portable media used to transfer information should be encrypted and comply with the RIT Portable Media Security Standard.

8. Printing

8.1. Avoid printing Private information unless necessary for business operations. (Documents sent to printers are usually transferred in an unencrypted fashion.) Printers used for Private information should be located in a secure area.

8.2. Printing Private Information on any material that is mailed to an individual, unless a State or federal law requires the Private information to be on the document being mailed, is prohibited. Notwithstanding the foregoing, Private Information can be mailed as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the Private Information. In these cases, Private Information should not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope being opened.

8.3. Printing, encoding, or embedding Private Information in or on any card, tag, or document required for an individual to access products, services, or benefits provided by the university is prohibited.

9. Disposal

9.1. When a record containing Private information is no longer needed (pursuant to the RIT Records Management Policy), it should be disposed of in a manner that makes the Private information no longer readable or recoverable. Disposal of paper records containing Private information should be accomplished by crosscut (or better) shredding, placement in a locked document destruction bin, or through vendor-supplied services under a contract approved by Purchasing. Recommended disposal methods may be found at https://www.rit.edu/security/content/media-disposal-recommendations.

Requirements for Confidential Information

10. Transfer/Sharing

10.1. If the intended recipient is unlikely to know the classification of the information received, then the sender should clearly label the information "Confidential" where possible. The words "Confidential" should be placed prominently on the information in a form appropriate to the medium in which it exists. The purpose of the label is to warn others that this information is Confidential and should be treated accordingly. Educational records governed by FERPA that are not defined as directory information are excluded from the marking requirement.

10.2. When possible, document creators should mark the document "Confidential". Recommended marking templates may be found at https://www.rit.edu/security/content/forms-checklists-and-templates.

11. Access and Use

11.1. Confidential information should be used and disclosed to others only on a need-to-know basis to permit the individual faculty or staff member to perform their RIT functions for which the information was acquired and for which it is maintained. Access to Confidential information should be carefully safeguarded with documented access controls, including a login banner where appropriate.

11.2. Disclosure of Confidential information to a third party agent or vendor is permitted only if the agent or vendor assumes a legally binding obligation to safeguard the use and disclosure of the information. Contact the Office of Legal Affairs for appropriate contractual language.

11.3. Mandated Federal and state reporting is excluded from this requirement.

12. Storage

12.1. Confidential information in paper form should be stored in locked areas.

12.2. Confidential information in electronic form should be stored using secure information technology resources with appropriate access controls. Passwords should comply with the Password and Authentication Provider Standards.

12.3. Confidential information shall not be posted in blogs, wikis, or other digital locations/repositories or social networks that do not use ISO-approved RIT authentication and authorization.

13. Disposal

13.1. When a record containing Confidential information is no longer needed (pursuant to the RIT Records Management Policy), it should be disposed of in a manner that makes the Confidential information no longer readable or recoverable. Disposal of paper records containing Confidential information should be accomplished by crosscut (or better) shredding, placement in a locked document destruction bin, or through vendor-supplied services under a contract approved by Purchasing. Recommended disposal methods may be found at https://www.rit.edu/security/content/media-disposal-recommendations.

Requirements for Internal and Public Information

14. Internal Information

14.1. Internal information in electronic form should be stored, transferred or shared using secure information technology resources with appropriate access controls. Passwords should comply with the Password and Authentication Provider Standards.

15. Public Information

15.1. Public information is information that is available to anyone.

Effective Date: February 1, 2010

Standard History:
August 31, 2005
November 11, 2013