Information Classification Policy

Purpose

All members of the Institute have the responsibility to protect information that is confidential in nature. The information in this policy is intended to educate the Institute community on the importance of protecting data, including guidelines on how defined categories of data should be stored, transmitted, and communicated to others.

Definitions

Classification category One of three groupings – confidential, internal use, or public – for identifying the general handling requirements for information.

Control statements Statements provided in addition to a classification category to further restrict or clarify how the information is to be handled. Examples include “To be opened by addressee only” and “Classified Public after mm/dd/yyyy”.

Information authority / data authority A person with responsibility for granting access to and ensuring appropriate use of the information.

Information steward / data steward A person with operational responsibility for the physical and electronic security of the information.

Information user / data user A person who needs and uses Rensselaer information as part of assigned duties or in fulfillment of assigned roles within the Rensselaer community.

Portable device Things including but is not limited to laptop and tablet computers, smart phones, external storage devices, flash drives, DVD, CD, and tape.

Handling Summary

Data will be classified into three categories:

1. Confidential Information
2. Internal Use Information
3. Public Information

Responsibilities

Rensselaer employees are responsible for handling information consistent with this policy’s requirements.

Rensselaer, for its part, has defined this policy to describe the need for and what constitutes proper information handling, it delivers training to individuals about information handling, and it makes available facilities and mechanisms in support of information handling consistent with this policy.

Scope and Enforcement

This policy applies to all personnel of Rensselaer while performing Institute employment duties, including student employees, visiting students, visiting faculty, and visiting researchers. The Vice President for Finance and the Chief Information Officer are jointly responsible for policy maintenance. Employees who violate the requirements of this policy are subject to disciplinary action, up to and including immediate termination of employment.

	Confidential	**Internal Use**	**Public**
Description	Information that, if disclosed, could violate the privacy of individuals or government regulations or statutes, could jeopardize the financial state of Rensselaer, could injure its reputation, or could reduce its competitive advantage.	Information intended for use by Rensselaer employees when conducting Rensselaer activities.	Information that has been made available for public distribution through authorized Rensselaer channels. Public information is not sensitive in context or content and requires no special protection.
Examples	Personnel file, social security number, date of birth, health records, email password, mother's maiden name, student grades, library patron browsing history.	Parking lot assignment, employee home address, course notes, portfolio performance plans.	Course catalog, research publication, *The Rensselaer Plan*.
Access	Rensselaer employees, contractors, and others with a business need to know who have signed confidentiality agreements and/or completed data classification training.	Rensselaer employees, contractors, and others with a business need to know.	No restrictions.

	Confidential	Internal Use	Public
Storing information on Rensselaer systems	Confidential information may be contained on portable devices, desktops or servers. Confidential information shall not be stored on portable devices unless it is secured (e.g. encrypted). Portable devices shall not be visible to the public when not attended to prevent disclosure and theft. Confidential information should be stored in secured databases or on secured file servers. It may also be stored in secured off-line media, such as CD, DVD and tape. Such media shall be encrypted, and stored in a secure location.	May be stored on portable devices. It is recommended the information be secured (e.g. encrypted).	No restrictions.
Storing information on personally owned equipment	Confidential information may not be stored on any personal equipment. Confidential information must not be directed to personal accounts.	Internal use information shall not be stored on any personally owned equipment unless it is secured (e.g. encrypted). Internal use information must not be directed to personal accounts.	No restrictions.
Labeling	Classification labels and controls statements should appear on the bottom of at least the first page of reports; they may be added on each subsequent page as desired. "Rensselaer Confidential" should appear on removable media labels.	Classification labels and control statements appear on the bottom of at least the first page of reports if determined necessary; they may be added on each subsequent page as desired. “Rensselaer Internal Use Only" should appear on removable media labels if determined necessary.	No requirements.

	Confidential	Internal Use	Public
Reproduction	Reproduction is discouraged and may be specifically prohibited by the control statement.	Reproduction is authorized if not prohibited by the control statement.	No restrictions.
Distribution	Distribution is only to those who have a business need-to-know and are Rensselaer employees, contractors, or vendors who have signed a confidentiality agreement.	Distribution is only to Rensselaer employees, contractors and vendors with a business need-to-know.	No restrictions.
Mail	Confidential information may be sent through intra-campus or U.S. Mail. The information must be in a sealed envelope clearly marked on the outside with appropriate statements such as “Confidential” or “To be Opened by Addressee Only".	May be sent through intra-campus or U.S. Mail with no special handling. If being sent via intra-campus mail, it should be placed in an interoffice envelope with no special marking.	No restrictions.
Electronic mail	May not be sent or forwarded unless protected by a sanctioned secure (e.g. encryption) package or algorithm.	May be sent or forwarded to those authorized for distribution.	No restrictions.
Data transmission	Data transmission over public networks requires protection by sanctioned secure (e.g. encryption) package or algorithm.	Data transmission permitted to those authorized for distribution.	No restrictions.
Facsimile	Faxing is authorized if not prohibited by the control statement. May not be sent to a public fax machines.	Faxing is authorized if not prohibited by the control statement. Should not be sent to public fax machines.	No restrictions.
Telephone	Conversations must be limited to other Rensselaer employees, contractors, and vendors covered by confidentiality agreement with a business need-to-know.	Conversations must be limited to other Rensselaer employees, contractors, and vendors covered by confidentiality agreement with a business need-to-know.	No restrictions.

	Confidential	Internal Use	Public
Visual disclosure	Ensure that documents and screens are positioned to prevent inadvertent disclosure. Do not leave documents and screens unattended and unsecured. Erase all white boards at the end of meetings.	Ensure that documents and screens are positioned to prevent inadvertent disclosure. Do not leave documents and screens unattended and unsecured. Erase all white boards at the end of meetings.	No restrictions.
Printed storage	Paper records must be stored in a locked enclosure when not in use. Media should not be left unattended on a desk.	Recommended that paper be stored in a locked enclosure or area when not in use. Media should not be left unattended on a desk.	No restrictions.
Backup	Backup media must be stored in a secured location. If transported outside the Institute, media shall be encrypted. Backups require the same care as originals to maintain confidentiality.	It is recommended the backup media containing internal use information be secured (e.g. encrypted) if transported outside the Institute. Backups require the same care as originals to maintain confidentiality.	No restrictions.
Record retention	Records of any type of medium must be retained and disposed as required by the record retention policy.	Records of any type of medium must be retained and disposed as required by the record retention policy.	Records of any type of medium must be retained and disposed as required by the record retention policy.
Disposal	Hard copy must be shredded; electronic storage media must be irretrievably erased or destroyed in accordance with the record retention and disposition policies.	Hard copy should be shredded. Re-writable electronic storage media may be erased using normal operating system commands for file deletion; other electronic media (e.g. CD and DVD) should be shredded or destroyed.	Normal waste disposal following the record retention policy.

	Confidential	Internal Use	Public
Inventory	All electronic repositories must be identified. Inventory must be reported annually to Information Security Office. Access controls must be reassessed annually.	All electronic repositories must be identified. Inventory must be reported annually to Information Security Office. Access controls should be reassessed annually.	No restrictions.
Re-/Declassify	The Institute may raise the classification of any information to Confidential. The Information Authority can reclassify or declassify confidential information.	The Institute may raise the classification of any information to Internal Use. The Information Authority can reclassify or declassify internal use information to public.	No requirements.
Certification	Employees with access to confidential information must complete annual training course covering data classification.	Employees should exercise reasonable care when handling and storing internal use information.	No requirements.

Credit

The production of this policy borrowed heavily from other sources, including The George Washington University, California State University at San Luis Obispo, and the SANS Institute