Policy Name: CIAS Records Management Policy (Reference RIT C22.0)

Section 1 - Policy Scope and Rationale

A. Scope:

The CIAS Records Management Policy applies to all personnel in the College. This policy is considered part of the conditions of employment for RIT personnel and is included in the CIAS Policies and Procedures Manual with reference to the Institute Polices and Procedures Manual.

B. Policy Statement:

In accordance with RIT policy C22.0, CIAS has developed a records management policy that fits the needs of the College. It references action items and procedures for the College from RIT Policy C22.0. This policy is available in the RIT Governance Policy Library (http://www.rit.edu/academicaffairs/policiesmanual/universitypolicies)

C. Rationale:

Compliance with the Records Management policy C22.0 ensures that CIAS handles information properly. The Information Security Office through the Information Access and Protection Standard (IAPS) requires departments to identify and maintain an inventory of private, confidential, and internal information. They are also required to handle, maintain and develop procedures to appropriately secure and protect information. Policy C22.0 demands consistent treatment of records. Personnel in designated official repositories must follow maintenance, retention, and disposal procedures for records systematically. This Policy is intended to ensure that RIT meets legal standards, preserves institutional history and properly destroys outdated and useless records.

Section 2 – Definitions

A. Definitions:

1. Information—any RIT knowledge, data or communication resident on information resources, including but not limited to, emails, documents, databases, photographs, stored audio or video. RIT and its users are responsible for information regardless of where it is stored.

2. Information Resources—Includes but are not limited to:
   a. RIT-owned or leased transmission lines, networks, wireless networks, servers, exchanges, Internet connections, terminals, applications and computers.
   b. Information owned by RIT or used by RIT under license or contract, in any form including, but not limited to, all types of electronic media, portable

media, all electronic hardware, software, network, communications device, system and paper.

c. Personal computers, servers, wireless networks, mobile devices, and other devices not owned by RIT but intentionally connected to RIT-owned information resources.

3. RIT Record—the original or copy of any record (paper or electronic) that is either an active record, archival record, or a record determined to be held for official business or regulatory purposes in accordance with the records retention schedule. Official repositories for these records are contained in the Records Management Policy. RIT Record does not include records, which are not created in the official course of business, serve no legitimate or necessary business purpose, or are created for personal purposes only.

4. Private Information—Private information is information that is confidential that could be used for identity theft. Private information also has additional requirements associated with its protection (e.g., state and federal mandates).

Section 3 — Secure Document Disposal

A. Paper Disposal

When a record containing confidential information is no longer needed (pursuant to the Records Management Policy), it must be disposed of in a manner that makes the confidential information no longer readable or recoverable. Disposal of paper records containing confidential information is accomplished by crosscut (or better) shredding or placement in secure document destruction bins located within each department. Recommended disposal methods are found at http://security.rit.edu/dsd/iap/disposal.html.

B. Electronic Storage and Disposal

Private information in electronic form must be stored in secure ISO-approved data centers or, if authorized, securely stored elsewhere in encrypted (not just password-protected) form. This information must not be stored on desktop, laptop, mobile devices or portable media without encryption or similar protection. Private information shall not be stored on systems that participate in cloud computing or grid computing. Private information in electronic form must be stored in secure ISO-approved data centers or, if authorized, securely stored elsewhere in encrypted (not just password-protected) form. Contact the Information Security Office for advice and assistance.

Section 4 — Procedures

A. Inventory and Classify Records

CIAS will develop information inventories in order to identify, classify and manage its information in accordance with the records management schedule for Policy C22.0.

B. Classifications:

1. Records required to be sent to RIT Archives;
2. Records recommended to be disposed;
3. Records required for disposal.

C. CIAS Document Destruction Process

As part of the document destruction process, CIAS will host at least two Document Destruction Days each calendar year. The basic structure of these days is that a central location will be designated where a certified third-party document destruction company can bring documents for collection. Records custodians will coordinate these days with their respective school or department. Additionally, on these days, representatives from the electronic document committee will be available to assist individuals with the proper disposal, retention or archival of electronic documents or documents stored on data storage medium (e.g. DVD, CD, etc.).

D. Paper Documents

1. Check with school or department records custodian (see Appendix B) for schedule and information on CIAS document destruction days.
2. Review records management schedule for your school or department. To review the CIAS records management schedule (see Appendix A).
3. Determine what paper documents need to be recycled, retained, or archived:
   a. Non-confidential recycled documents should be placed in designated receptacles within CIAS.
   b. Documents to be retained should be stored according to the CIAS records management schedule.
   c. Documents defined as "Archival" should be submitted to the RIT Archivist, Becky Simmons (raswml@rit.edu). Please refer to the CIAS records management schedule for the required list of archival documents.
   d. Confidential documents to be destroyed can be disposed of on document destruction day. Confidential documents/records include: employee records, student files, etc.
4. Contact your department or school Records Custodian if you have confidential materials or large quantities of documents needing disposal prior to the next scheduled CIAS document destruction day.

E. Electronic Documents

1. Electronic records are identified as maintained on a RIT network, email server, CD-ROM, hard drive or file server data storage. There are numerous sources that can contain electronic information at the desktop per machine. For example: Emails; Internet browser information (cached files, cookies, download records); word processing documents, spreadsheet, presentations;
2. Instant messaging/chat records; efaxes; electronic calendars; voicemail; text messages; blogs; chat room/bulletin board postings.

Section 5 — Responsible Officers

A. Responsible Officers:

The CIAS records manager is Betsy Saxe (mestpo@rit.edu). The primary role of the CIAS records manager is to:

1. Manage records custodians;
2. Ensure compliance with policy;
3. Facilitate records management process;
4. Liaison to Office of Legal Affairs.

B. The primary role of the CIAS records custodians (see appendix A) is to:

1. Educate respective department or school on RMP and ensure compliance with policy;
2. Review the Records Management Policy with new faculty and staff;
3. Report new categories for records management schedule;
4. Ensure appropriate destruction and retention of documents;
5. Ensure appropriate disposition of documents to RIT archives;
6. Participate in legal process, if applicable, including:
    a. Document certification
    b. Testimony

Responsible Office: Betsy Saxe, CIAS Dean's office
Effective Date: April 2014
Guideline History: April 2014

Appendix A

RECORDS MANAGEMENT SCHEDULE

I. RECORDS REQUIRED TO BE SENT TO RIT ARCHIVES

Item	Retention Period	Official Repository
Accreditation Reports and Supporting Documents	Permanent	Office of the Provost
Advisory Board, Committee and Task Force minutes, agenda and materials, including standing and ad hoc committees	Permanent	Appropriate Committee/Advisory Board
Affirmative Action Plans (including documentation)	Permanent	Office of Legal Affairs
College Strategic Planning Records	Permanent	Appropriate Colleges
Development and Alumni Relations Annual Reports, Materials, and Gift Records	Permanent	Development and Alumni Relations
Employee orientation & training materials	Permanent	Human Resources
Enrollment statistics	Permanent	Office of the Registrar
Governance Groups minutes, agenda and materials (including Student groups)	Permanent	Appropriate Governance Group
Institute publications (catalogs, handbooks, programs, etc.)	Permanent	Office of the Registrar
Lecture Series (documentation, advertisements, lectures)	Permanent	Appropriate College/Departments
News Content (internal and external)	Permanent	University News Services
Original Patents, Trademarks and Related Work Papers	Permanent	Intellectual Property Management Office
Periodicals and Newsletters (departmental, administrative, and student groups)	Permanent	Appropriate College/Departments
Policy and Mission Statements	Permanent	Human Resources
Real Estate Deeds	Permanent	Office of Sr. VP Finance & Administration
University Policies and Procedures Manual	Permanent	Human Resources

II. RECORDS RECOMMENDED TO BE DISPOSED

Item	Retention Period	Official Repository
Academic advisement files	1 year after graduation/last date of attendance	Appropriate Academic Departments
College/Department Office Student Files	1 year after graduation	Appropriate College/Department
Contracts files (including contracts with employees and consultants)	6 years after all obligations end	Appropriate Departments
Employee Medical Documentation	6 years from termination	Human Resources
Enrollment's Advanced Placement and Admissions Records (not otherwise listed for non-enrolled students)	2 years after application	Division of Enrollment Management
Equipment files (including maintenance records and leases)	6 years after disposition	Appropriate College/Departments
Faculty Student Files (including grades)	1 year after end of academic term	Appropriate Academic Departments
General Correspondence (including emails)	6 years	Appropriate Departments
Online Learning Materials	2 years after last use	Online Learning
Recruitment materials (for individual students)	Until date of enrollment	Division of Enrollment Management
Student Disciplinary Records (not responsible finding)	5 years	Student Affairs
Student Disciplinary Records (responsible finding)	Permanent	Student Affairs

III. RECORDS REQUIRED TO BE DISPOSED

Item	Retention Period	Official Repository
Auditor Documents	Permanent	Controller's Office
Bids (accepted and rejected)	6 years after all obligations end	Purchasing Department
Billing Records	6 years	Controller's Office
Bond Records	6 years after life of bond	Controller's Office
Capital Equipment Records	Life of Asset	Controller's Office
Certifications and Inspection Reports	6 years	Environmental Health and Safety
Employee Background Checks (including Controlled Substance Test Results)	6 years after employment ends	Human Resources
Employment applications and resumes – non-employees	3 years	Human Resources
Employment Records	6 years from date employment ends or death of eligible employee	Human Resources
Financial Records	6 years	Controller's Office
Invoices	6 years	Purchasing Department
Legal Records	6 years	Office of Legal Affairs
OSHA Records and Material Safety Data Sheets	40 years	Environmental Health and Safety
Purchase Orders	6 years	Purchasing Department
Search Committee Records	3 years	Human Resources
Student Employee Records (including applications and resumes)	6 years after employment ends	Student Employment Office
Tax Records	6 years after return is filed	Controller's Office
Training Records	6 years	Environmental Health and Safety
Unemployment Insurance Records	6 years	Human Resources
Workers Compensation Records	18 years	Human Resources

Responsible Office: Office of Legal Affairs
Effective Date: Approved May 13, 2009
Policy History:
Edited August 2010
Edited September 2012 (conversion edit)

Appendix B
CIAS Records Custodians
Betsy Saxe, CIAS Records Manager
Twyla Cummings, CIAS Assistant Records Manager

School/Department	Custodian (s)
Dean's Office	Grace Gladney, Teresa Merritt
Gallery r	Zerbe Sodervick
Bevier Gallery	Elizabeth Murkett
Image Permanence Institute	Lisa Cerra
Operations	Kevin Buck, Mike Dear, Bob Fleck, Brandi Patten, Jay Sullivan
School for American Crafts	Angela Carter
School of Art	Fran Chinnock
School of Design	Deb Weatherbee
School of Film and Animation	Mary Barnard
School of Photographic Arts and Sciences	Lisa DeRomanis, Chelsea O'Brien
School of Media Sciences	Marcia Carroll
Student Services	Sue Clark, Deb Kingsbury