Records and Information Management (RIM) is responsible for guiding University departmental efforts to safeguard official records and informational assets through the management, access, retention, storage, protection, and disposition of those assets. RIM also provides training and operational assistance for all University departments concerning their records retention and secure information management practices.

This past June, Jeff Clark, Program Manager for Security & Policy for the Connecticut Board of Regents was at SCSU to present a seminar entitled “Information Security and Data Management Awareness.” Charged with presenting this information to all four sister universities and 17 community colleges, the goals of the seminar were to make staff aware that information security is everyone’s responsibility, to educate them about how data breaches can occur, and to offer recommendations on how to avoid damaging incidents.

Jeff began by informing staff that not only is information security everyone’s responsibility, it’s simply good business because data breaches can damage both an institution’s reputation and result in serious financial consequences. He then gave several examples of breaches that occurred at Connecticut colleges and universities and told how one Connecticut institution will spend almost $1 million to rectify a breach that occurred when a personal computer was infected by malware which sent confidential data offsite.

Major threats to SCSU information include cyber-threats (viruses, worms, Trojans); physical theft of data or equipment; improper disposal of data; fire, water or other physical damage; people who want to prove they can hack into a network just for fun; customers or employees with grudges to settle; authorized users who lose data, grant access to unauthorized users, or send unencrypted e-mails with confidential data; and the over 6 billion people who now have access to the Internet because, unfortunately, these people include sophisticated organized crime networks who steal identity and financial data for profit.

Finally, Jeff recommended that SCSU staff and faculty help prevent information and data breaches by adhering to the following:

- Know and maintain best practices for protecting information and data
- Avoid risky behavior
- Be alert for vulnerabilities and potential breaches
- Report potential problems and breaches
- Cooperate with investigators
PROTECTING THE PRIVACY OF RECORDS AND INFORMATION—

What does privacy have to do with records management? Simply put — a lot.

Individuals expect their privacy to be respected and their personal information to be protected by the organizations with which they do business. Colleges and universities like SCSU deal with enormous volumes and varieties of personal information. This fact—along with the wide range of faculty, staff, and student activities, the decentralized nature of operations, and a growing reliance on technologies that collect and centrally store data—present significant privacy and security challenges. Consequently, it is critical that everyone take steps to ensure that the records and information they are responsible for remains secure.

Like good records management, good privacy is good business. As business and technology become increasingly complex and sophisticated, Personally Identifiable Information (PII) becomes more vulnerable to unauthorized access and disclosure. PII is any information that can be used to identify, contact, or locate a single person or that can be used with other sources to identify a single individual. Examples of PII include name, maiden name, address, date of birth, and driver’s license, credit card, bank account, or social security numbers, the loss of which may result in substantial personal or financial harm, embarrassment, or inconvenience to an individual.

Privacy advocates recommend the following best practices to help protect not only PII, but all of an organization’s information:

BEST PRACTICES:

1. If you have an office, lock your office door whenever you leave.
2. If you work in a cubicle or in an open setup, lock your desk whenever you leave your area. Lock your desk AND any cabinets before you leave for the day.
3. Do not leave keys dangling in desks and filing cabinets while you are working.
4. Lock your computer whenever you leave your desk. Do not rely on your screensaver to hide the screen.
5. If you are provided with a laptop, keep it locked away when you are not using it. Never leave it in your car.
7. Keep your passwords secure. Do not write them on sticky notes that are then stuck under the keyboard, under the desk, or under some other object on the desk.
8. Do not leave papers with sensitive or confidential information (student transcripts or financial information, invoices, checks, contracts, etc.) on desktops.
9. Do not leave sensitive or confidential information in meeting areas. Check the area before you leave to be sure you have gathered all meeting materials.
10. Do not put sensitive or confidential information in trash cans or recycle bins. SHRED IT!!
11. Do not place sensitive or confidential information in mail slots. Hand deliver it.
12. Do not leave sensitive or confidential information in printers, copiers, and fax machines. Always check the equipment before you leave.
13. Keep all storage rooms locked.
14. Do not leave or “prop” outside doors open so that anyone can enter a secured area.
Get To Know Your ARMLO—

Connecticut’s Office of the Public Records Administrator (OPRA) mandates that each state agency designate an individual to serve as its Records Management Liaison Officer (RMLO). OPRA also recommends that each agency designate a sufficient number of individuals to serve as Assistant Records Management Liaison Officers (ARMLO) whose primary responsibility is to assist the RMLO in implementing a comprehensive, agency-wide records management program. Southern’s ARMLOs function as their division’s “authority” for all issues pertaining to records management—records retention, disposition, policies and procedures, etc.

Linda Robinson, CSU Administrative Assistant to the Provost serves as the ARMLO for the Division of Academic Affairs. In this capacity, she assists departments directly reporting to Academic Affairs with their records management issues to ensure that all state records retention requirements are adhered to and that records are properly managed.

Linda has worked at Southern for almost 10 years, and just joined Academic Affairs in August after 9 and a half years in the Office of Institutional Advancement. She is now enjoying the challenge of keeping up with a very busy Provost as well as the multifaceted aspects of Academic Affairs, especially those that bring opportunities to work with students and faculty.

Linda has been married for 25 years and has two grown children. A traveler and diehard beach lover, in recent years, she has visited the shores of Bermuda, Jamaica, and Mexico. However, most special to her is a 2009 European trip to Italy where she and her family took a Mediterranean cruise and became newly acquainted with Italian relatives in the small town where her grandfather was from.

SCSU Records Spotlight—

Office of the Registrar
Wintergreen Building
Kim Laing, Interim Registrar

According to Kim Laing, Interim Registrar, “The Office of the Registrar is here to help students succeed.”

Located in the Wintergreen Building, the Registrar’s Office services students’ registration needs and houses the paper and electronic records of every student who attended SCSU whether or not they actually graduated. A staff of 9 people provide face to face, telephone, and online customer service and student records processing including transcript requests, address changes, grade changes, undergraduate/graduate graduation auditing, and the printing and issuance of diplomas. They also set up registration rules, provide campus reporting services, and work closely with other campus offices such as Undergraduate and Graduate Admissions, Academic Advisement, and First Year Experience.

In addition, the Registrar’s Office is the gatekeeper of all paper and electronic student records for which they must comply with all State of Connecticut records retention requirements. And, because a student transcript must be retained permanently, they must also comply with the State’s storage requirements for permanent records which mandate that a backup copy of every record is to remain accessible at all times. To that end, the Registrar’s Office is transitioning to Banner’s Document Management System (BDMS). Student records are being scanned into the system where they will then be periodically backed up in Banner. BDMS will enable better records management and improved customer service, both of which ultimately translate into student success!
**NEW STATE OF CT RECORDS MANAGEMENT POLICY**

Recently, the Connecticut Office of the Public Records Administrator issued *Public Records Policy 05: Disposition of Public Records*. In accordance with this policy, state agencies must provide all employees with a copy of the state’s policy on records retention and disposition, obtain a signed acknowledgement of receipt (or equivalent) from each employee, and keep the signed acknowledgement on file. The Office of Human Resources originally distributed the policy in conjunction with records retention training. However, due to a technical glitch, the records retention training has not been available for several weeks. Consequently, to ensure compliance with Public Records Policy 05, the Office of Human Resources will be redistributing both the policy and the Certificate of Acknowledgement to those employees who did not have an opportunity to access these documents for the period when the training course was unavailable.

In addition to the redistribution of the Public Records policy that will be rolled out shortly, the Human Resources Office has announced that the records retention training course is now up and running. If you would like to learn more about records retention and destruction, please visit the [Human Resources Online Training Portal](#), click on the Courses tab, and select course number **120-2012 Records and Information Retention and Destruction**.

For questions, please contact Paula Rice in Human Resources at x25568.

---

**SCSU RECORDS AND INFORMATION MANAGEMENT BEST PRACTICE TIPS**

- Use resources only for their intended and specified purpose.
- Prevent the disclosure of any and all confidential information.
- Only access information that is relevant to your official responsibilities.
- Be aware of information security threats such as viruses, spyware, etc.
- **ALWAYS SHRED** documents that contain confidential information.
- **ALWAYS SECURE** documents that contain confidential information.

**and finally....**

*When In Doubt, Assume It’s A Record!*

---

**REMEMBER** — OPRA requires all state agencies to obtain approval before disposing of official records by completing an [RC-108 Records Disposition Authorization for State Agencies](#). Once approval has been received, all official public records must be shredded in a secure manner. In addition, a certificate of destruction issued by the shredding vendor must be maintained by the state agency.

Shred-It, Inc., under contract with the State, is the vendor SCSU uses to dispose of old records. To access SCSU’s shredding policies and procedures, see [Disposing of Old Records](#) on SCSU’s Records and Information Management’s website. If you would like more information on records management, retention, or disposition, please contact the ARMLO for your area or call Phil Koslowski at x26205.