



Privacy, Records Management and Information Security at the University of Victoria

A YEAR IN REVIEW 2015

Chief Information Officer, University Systems | Chief Privacy Officer,
Office of the University Secretary | University Archivist, UVic Libraries

February, 2016

A. Introduction

Technology presents new challenges and new opportunities. The pace and the intensity of technological advancement—our ability to create, store, use and share mass amounts of digital information and data—are really at the heart of some of the biggest challenges facing privacy and access to information today. We've moved from a paper-based system to an era where most records are "born digital".

OIPC Commissioner's Briefing: Freedom of Information and Protection of Privacy Act

– Hansard, Special Committee to Review the Freedom of Information and Protection of Privacy Act, July 21, 2015, page 19

This is the third annual report to the university community providing an overview of the privacy, records management and information security activities at the University of Victoria for 2015.

Good privacy, security and records management practices are key to a healthy organization. Privacy, security and records management work is closely linked. Open and constant communication among these areas is vital to a successful governance model for any organization.

Privacy is the right of an individual to control his or her personal information. Records management is the systematic control of university records, both paper and electronic. Information security is the protection of university electronic information and supporting systems from risks such as unauthorized creation, collection, access, use, disclosure, disruption, modification or destruction.

Privacy, records management and information security activities at the University of Victoria during 2015 included:

- distributing a training video to over 1085 new employees, as well as existing employees in 15 offices, selected because of the sensitivity and volume of personal information those offices hold;
- developing and testing three new training modules on privacy breaches, email management and records retention;
- ongoing use of privacy impact assessment tools and process;
- continuing the renewal of the Directory of Records;
- finalizing new electronic records management best practices;
- commencing a comprehensive review of UVic's privacy, information security and records management policies and procedures;
- conducting 4 site visits to departments selected because of the sensitivity and volume of personal information;
- planning for a 2016-2017 privacy, information security and records management assessment of confidential and highly confidential records containing personal information;
- enhancing the information security program;
- improving the overall university security posture;
- completing a second external security vulnerability assessment; and
- improving privacy and security assessments and processes within University Systems.

B. Accountability

During 2015 the structure for the coordination and reporting of privacy, information security and records management at the university was in full operation. The Coordinating Committee—consisting of the University Secretary (chair), Vice-President Finance and Operations, University Librarian, Associate Vice-President Faculty Relations and Academic Administration, and a Dean—oversaw the development and implementation of integrated privacy, records management and information security work plans, including activities such as education and training, risk assessment, policy and procedural review, and reporting. This committee, which coordinates reporting to the Board, President and university community, met four times in 2015.

In addition, the Advisory Committee on Privacy, Records Management and Personal Information Security met to provide input and advice on these matters. The Advisory Committee, which met three times in 2015, is composed of people from across the university with key responsibilities, experience and expertise in the areas of privacy, security and records management. The committee's discussions included topics such as out-of-country storage of personal information, educational technology in the classroom and management of email.

The Coordinating Committee has established a sub-committee to consider the changes to the Directory of Records (the University-wide records classification, retention and disposition plan). The Directory of Records (DOR) sub-committee, chaired by the university Archivist and including the university General Counsel, Chief Information Officer and the Chief Privacy Officer met three times during 2015. The sub-committee has met to review proposed changes to records classifications within the Financial Management, Governance, Human Resources and Student Services sections, and to discuss related issues affecting the ongoing management of university records and information.

C. Cross-portfolio activities

2016-2017 Privacy and Information Security Assessment of confidential and highly confidential records

During 2013-2014, a report was issued on the assessment of confidential and highly confidential records that was conducted in 2012-2013 covering all administrative offices across the university, as well as deans' and departmental offices. Over 170 offices, including research centres, responded to questions about their electronic and paper records.

One lesson from the 2012-2013 assessment was that it can never be said that an organization is 100 percent secure; we must continue to take steps to reduce exposure and manage risk on an ongoing basis.

As a next step, we have started planning for an update of the campus-wide records assessment for 2016-2017. The purpose of this project is to update through a streamlined self-assessment process our documentation and assessment of how administrative and academic units and research centres within the University collect, use, disclose, retain, and dispose of personal information contained in electronic and paper records. During 2016/2017 we plan to provide units and centres with an assessment tool, to assist in assessing their record handling practices. The results of this self-assessment will help to identify remaining privacy and security risks which need mitigation. The project will make recommendations so that privacy, security, and records management best practices, policies, regulatory and legislative requirements are properly implemented. In addition, the project will reinforce training and awareness to units' and centres' employees about best information management practices. This update is part of the continuous improvement of records handling, both electronic and paper, by units of the university.

Site Visits

Site visits are an opportunity to assist units in improving their privacy, security and records management practices through awareness-raising, training and the use of a questionnaire. The site visits allow for continued improvement in key units of the university while the 2016-2017 records assessment is being planned. The questions prepared for the site visits complement the records assessment questions. Four site visits have been conducted in 2015 and six are planned for the next year.

Education and training

Education and training are an important part of the toolkit for privacy, security and records management. A basic training video has been developed for new and existing employees. This supplements ongoing in-person training and a campus-wide awareness campaign.

In 2015 this video was sent to 1085 new employees. Employees hired through UVic Careers were notified about the training video as part of the required on-boarding. New employees hired outside of UVic Careers were notified by email.

Eight new privacy fact sheets have been drafted and tested. These cover topics including safe email practices and an office privacy checklist. The fact sheets will be posted and disseminated in the coming months.

In-person training was offered for several groups in 2015. In-person training continues to be provided for administrative officers and research staff in selected research centres. Specific sessions were presented to faculty councils, departmental meetings and sessionals. Records management training has been offered to specific units on campus.

Three new modules for online training covering privacy breaches, email management and records retention have been developed and tested. These modules will be available in 2016. In addition, we have conducted focus groups with faculty to discuss effective methods of online training.

Privacy impact assessment

A privacy impact assessment (PIA) is an assessment that is conducted by a public body to determine if a current or proposed system, project, program or activity meets or will meet the privacy requirements of the *Freedom of Information and Protection of Privacy Act* (FIPPA).

In the past, the most prevalent approach to such assessments has been compliance-based, resulting in institutions checking a series of boxes. At UVic risk-based instruments have been developed and tested. These identify potential privacy and security issues and impacts, allowing for correction and mitigation and thus avoiding costly program, service or process redesign.

The first tool measures the preliminary, overall risk and determines when a PIA is needed. This shorter risk assessment tool has been designed to determine whether a project exceeds a risk threshold, triggering project staff to complete the more detailed PIA.

The full PIA is a comprehensive assessment that reviews the proposed system and determines possible privacy and security risks and uses privacy and security controls to support, mitigate or eliminate the risks, or alternatively assist in determining whether the risk is acceptable.

The UVic instruments have been integrated into the University Systems project management process.

Policy review

In 2009, the university introduced an integrated suite of information management policies and procedures building upon prior policies. Since then, the policies and procedures have been tested and several changes have occurred.

A comprehensive review of all privacy, security and records management policies and associated procedures is underway and will be completed in 2016.

Providing privacy and security awareness in learning and teaching

As a result of the development of the Technology Integrated Learning department, the university's approach to the use of technology in the classroom continues to be enhanced and standardized. Privacy and security considerations are important components of this new work.

Educational technology issues have also been considered by the Senate Committee on Learning and Teaching. It has established a Working Group on Educational Technology. This working group considered questions related to the use of technology in the classroom. Privacy and security were incorporated into its discussions.

Integration of Records Management into Systems development

The University is in the process of transitioning existing SharePoint sites to Connect. The governance framework for Connect (SharePoint 2013) advises departments to consult with Records Management regarding the disposition of records not being converted to the new version. Records Management is reflected in the University Systems' Project Plan template to be used for all SharePoint migrations. The Connect onboarding projects are another opportunity to proactively bring good records management practices to the attention of unit staff. Records Information bulletins on the transition process and the organization of records on new sites are being drafted.

D. Specific portfolio activities

In addition to the cross-portfolio activities described above, the following activities have taken place:

Privacy activities

Over the past year the Chief Privacy Officer has provided ongoing privacy advice to administrative and academic units. The advice ranged from the creation of consent forms for student admission to advice on the purchase of new systems and software. As part of his ongoing work, units are given advice on the collection and use of student and employee personal information and the disclosure of personal information in specific cases.

An important part of privacy work is responding to complaints and investigating campus concerns about privacy issues. Over the past year these have included concerns about the use of cloud computing; the security of mobile devices; and misdirected email.

The increasing use of cloud-based services poses complex privacy, security and records management challenges for organizations, including the higher-education sector. The Chief Privacy Officer and the Chief Information Officer have devoted considerable attention to these and initiated a number of activities; for example, the preparation and implementation of standard questions to assess the risk of cloud-based services.

Records management activities

The major Records Management activities for 2015 included updates to the DOR. The DOR sub-committee has met to review proposed changes to classifications within the Financial Management, Governance, Human Resources and Student Services sections, and to discuss related issues affecting the ongoing management of university records and information.

Over the past year the Records Management staff has continued to provide advice to units to assist in their records management practices. This covered such matters as: reviewing requests for disposition, including transfer to Archives; email and shared drive management advice; and secure destruction of records.

The decision has been made to disseminate advice on Electronic Records Management as a Best Practices document, being a collection of principles for email management, document naming and organization of electronic information.

Information security

Over the past year Systems has contributed to improving both security and privacy through investments in existing and new processes and services.

A number of projects are currently underway, or have already been completed to improve information security:

- Updated information security operations methodology which is a component of UVic's Information Security Program and consists of the definition of roles and processes that manage IT security operational processes (monitoring, responding, reporting) at the university.
- Completed a second external security vulnerability testing.
- Developed a security program to provide strategy and guidance on institutional IT security.
- Implemented internal and external IT controls related audit recommendations.

E. Conclusion and priorities for the next year

The work over the past year has demonstrated our commitment to maintaining strong and comprehensive privacy, records management and information security programs in support of the university's strategic direction and priorities. The university continues to integrate these programs, and work on issues of shared concern.

Over the next year, priorities in the areas of privacy, security and records management include:

- A. Cross-portfolio:
 - i) Carry out site visits of 6 units.
 - ii) Implement and communicate changes to the privacy, information security and records management policies and procedures.
 - iii) Complete further online training packages for advanced training.
 - iv) Continue to integrate the PIA tools into the university processes.
 - v) Continue the planning for the 2016-2017 records assessment project of confidential and highly confidential records containing personal information.
- B. Privacy:
 - i) Develop and distribute further materials on the use of cloud technology.
 - ii) Renewed privacy website.
- C. Records Management:
 - i) DOR revision (with priority given to the sections that must be updated prior to the 2016/17 Assessment Project)
 - ii) A revised stand-alone records management website
 - iii) Continued development of electronic records management resources for the campus.
- D. Security:
 - i) Continue to improve security posture.
 - ii) Increase maturity in IT controls for security and privacy.
 - iii) Deploy security awareness and education across campus.
 - iv) Focus on implementing the Security Program

In conclusion, privacy, records management and information security will continue to collaborate over the course of 2016 to maintain and strengthen privacy and security in this rapidly changing higher education and technological environment.