a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

University Archives
Irving K. Barber Learning Centre
1961 East Mall
Vancouver, BC V6T 1Z1

University Records Manager
Phone: 604 827 3952
Fax: 604 822 9587
alan.doyle@ubc.ca

Information Security Fact Sheet

Security of Paper Records

Introduction

1. Under the University's Records Management Policy, the University Archives is responsible for providing leadership and advice concerning the management of records. Records are "recorded information, regardless of medium or characteristics, which the University creates, receives or maintains in connection with the conduct of the University's affairs."[1]

2. The University has a responsibility to protect confidential information (which includes personal information) from unauthorized viewing and use. Specifically, the *Freedom of Information and Protection of Privacy Act* (FIPPA) requires public bodies to implement "reasonable security arrangements" over personal information (in both electronic and paper format).[2] The Records Management Policy requires individual units to ensure that the appropriate security measures are observed for maintaining records containing personal or other confidential information.[3] The purpose of this Fact Sheet is to provide guidance for faculty members, staff, and other individuals on how to manage the University's paper records in a secure manner.

What records need to be protected and to what extent?

3. Owing to the significant volume of paper-based records that are handled by the University, it is not possible, nor required, to protect all records to the same extent. The University follows a risk-based approach, where the overall aim is to implement a reasonable level of control, taking into account the probability and impact of a security breach. More extensive safeguards are required for records containing (a) larger volumes of confidential information and (b) any information that is extremely confidential (e.g. Social Insurance Numbers or other information that could be used to commit identity fraud or otherwise harm the reputation of an individual). Therefore, the best practices described in this Fact Sheet should be considered in the context of the level of risk to the records that you handle.

Always take a risk-based approach to securing personal information.

4. The University has an Information Classification Scheme, which will help you determine the sensitivity of your information and the level of control that should be implemented to protect it throughout its lifecycle. A summary of this scheme is provided below; however, full details are available in section 1.2.1 of the UBC Information Security Manual.[4]

	Confidential	Sensitive	Public
Examples	Personal information such as SIN, home address, or medical history	Research data that does not contain personal information	Employee business contact details

[1] Policy 117, sections 2.2 and 3.3
[2] FIPPA, section 30
[3] Policy 117, section 2.4
[4] http://www.it.ubc.ca/sites/it.ubc.ca/files/uploads/__shared/assets/UBC_Information_Security_Manual.pdf

How do I protect the paper-based records I handle?

5. The best practices below provide guidance on the types of controls that should be considered to protect records throughout their lifecycle.

Storage of Records

	Confidential	Sensitive	Public
Storage in controlled access areas[5]	Records are stored in locked file cabinets, desks, closets or offices.		Records are stored on open shelves/ drawers/ cabinets.
Managing entry to controlled access areas	Individual(s) are assigned the authority to grant access to an area and someone is appointed to formally manage the physical access process (keys, fob/card, keypad access).		
Storage in publicly accessible areas[6]	Confidential records are never stored in publicly accessible areas.	Records are stored in locked file cabinets, desks, closets or offices.	

Transmission of Records

	Confidential	Sensitive	Public
Campus Mail	Large volumes of extremely confidential records (T4s, transcripts, medical records) are sent using the secure delivery service provided by Campus Mail.	Records are sent by regular Campus Mail.	
External mail	Records are sent by registered mail or courier.		Records are sent by regular mail.
Copiers, scanners and fax machines	Copiers, scanners and fax machines are located in a controlled access area, off-limits to unauthorized persons.		

Disposition/Destruction of Records

	Confidential	Sensitive	Public
Collecting records for destruction	Records are retained either in a locked room/area, or a locked, confidential shred bin.		Records may be retained in publicly accessible areas.
Destruction method	Records are cross-cut shredded. Simple straight-strip shredding is not adequate as there is always the possibility of reassembly.		Records are recycled.
Destruction confirmation	Commercial shredding companies are bonded and provide written confirmation of secure shredding.		n/a

[5] Areas restricted to authorized employees or members of the public under close supervision
[6] Areas that members of the public are permitted to enter without close supervision