THE UNIVERSITY OF BRITISH COLUMBIA

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

Records Management Office
Phone: 604 827 3952
http://recordsmanagement.ubc.ca
records.management@ubc.ca

Security of Paper Records

A RECORDS MANAGEMENT OFFICE GUIDELINE

Introduction

Under UBC Policy GA4, 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."

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). 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. The purpose of this Guideline 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?

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.

The University has an Information Security Standard on the Security Classification of UBC Electronic Information; the principles of this document can also help you determine the sensitivity of information found in paper records and the level of control that should be implemented to protect it throughout its lifecycle. A summary of the sensitivity level of different forms of personal information can be found below.

CONFIDENTIAL	SENSITIVE	PUBLIC
Personal information such as SIN, home address, or medical history	Research data that does not contain any personal information	Employee business contact details

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

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	Records are stored in locked file cabinets, desks, closets, or offices		Records are stored in open shelves, drawers, or 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	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	Confidential 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

Glossary

Term	*Definition*
controlled access areas	Areas restricted to authorized employees or members of the public under close supervision
publicly accessible areas	Areas that members of the public are permitted to enter without close supervision

References

Freedom of Information and Protection of Privacy Act, RSBC 1996, c. 165. Retrieved March 31, 2021, from https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00

UBC Board of Governors. Records Management Policy (Policy No. GA4) [PDF]. Retrieved March 31, 2021, from https://universitycounsel-2015.sites.olt.ubc.ca/files/2019/08/Records-Management-Policy_GA4.pdf

UBC Office of the CIO. (2021). *Information Security Standard U1: Security Classification of UBC Electronic Information.* UBC Office of the CIO Policy, Standards & Resources. Retrieved March 31, 2021, from https://cio.ubc.ca/information-security-standards/U1

DOCUMENT CONTROL		
Revision	Issued For	Date
0	Use	2013
1	Updated style, format, and links	20210406