University Policy
University Procedure
Operating Standard
Guideline/Form

Privacy Breach, Procedure for Responding to a

Classification Information Management	**Table of Contents** 1 Purpose ..... 1 2 Scope ..... 1 3 Definitions ..... 1 4 Procedure ..... 1 5 Parent Policy ..... 2 6 Related Guidelines/Forms ..... 2 7 References ..... 2 8 History 2
Approval Authority General Counsel	
Implementation Authority FOIP Coordinator	
Effective Date December 1, 2008	
Last Revision N/A	

1 Purpose

The purpose of this procedure is to outline the steps taken in response to a breach of privacy.

2 Scope

This procedure applies to employees of the University of Calgary and includes individuals working for the University as volunteers or contractors.

3 Definitions

In this procedure:

a) "Privacy Breach" refers to the unauthorized access to or collection, use, disclosure or disposition of personal or health information. Such activity is considered to be 'unauthorized' if it occurs in contravention of the *Freedom of Information and Protection of Privacy Act*, the *Health Information Act*, or the University of Calgary's Privacy Policy.

4 Procedure

First Responder

4.1 Immediately identify the nature of the privacy breach and take steps to contain the damage. This may involve:

a) Stopping an unauthorized practice;
b) Recovering records;
c) Moving records to a secure facility;
d) Changing door locks;
e) Revoking an individual's access to the Electronic Communication System;
f) Temporarily shutting down a server;
g) Removing a file or record from a public website; or
h) Changing a password to a protected file or server.

If unable to contain the breach, contact the FOIP Coordinator without delay.

4.2 Report the breach of privacy to the FOIP Coordinator as soon as possible but no later than the end of the day on which the breach is discovered. Contact the FOIP Coordinator by email at foip@ucalgary.ca or by phone at (403) 210-7952.

4.3 Complete the Privacy Breach Incident Report Form within 24 hours of discovering the breach and submit it to the FOIP Coordinator.

4.4 Take remedial action if required.

FOIP Coordinator

4.5 Report the breach of privacy to others within the organization as appropriate. Consider, in particular, if the Director of Campus Security and the Information Security Officer need to be involved in the investigation and response.

4.6 Preserve the evidence.

4.7 Involve the Office of the Information and Privacy Commissioner (OIPC) if necessary.

4.8 Conduct further in-depth investigation into the cause and extent of the breach if required. Evaluate the risks associated with the breach of privacy.

4.9 Determine if notification of affected individuals is warranted. Consult with General Counsel when necessary.

4.10 Conduct the notification of affected individuals if it is determined that notification is warranted.

4.11 Review investigative findings with the program area and others within the organization as appropriate. Develop and implement prevention strategies.

5 Parent Policy Privacy Policy

6 Related Guidelines/Forms Privacy Breach Incident Report Form

7 References Freedom of Information and Protection of Privacy Act, RSA 2000, c F-25
Health Information Act, RSA 2000, c H-5

8 History

December 1, 2008	Approved and Effective.
April 6, 2017	Editorial Revision.
January 1, 2020	Editorial Revision. Updated format and links.