CAPILANO UNIVERSITY	PROCEDURE		
Procedure No.	Officer Responsible		
B.700.1	**Vice President, Finance and Administration**		
Procedure Name			
Personal Information Incident Management Procedure			
Policy This Procedure is Under			Date of Next Policy Review
B.700 Privacy and Access to Information Policy			**February 2025**
Date Issued	Date Revised	Responsible Director	
February, 2023	**NEW**	Designated Privacy Officer	

1 PURPOSE

To describe the process for managing Personal Information Incidents (often described as privacy breaches), setting out employees' obligation to report, and assigning responsibilities and timelines for investigation and response.

This procedure has been designed to meet the requirements of the *Freedom of Information and Protection of Privacy Act* (FIPPA). Where the Personal Information Incident has an extraterritorial element compliance with international privacy regulations such as the California Consumer Privacy Act (CCPA) or the General Data Protection Regulation (GDPR) will be taken into consideration, to the extent of applicability. In the event of a conflict between this policy and FIPPA or other applicable law, the legislation will govern.

2 DEFINITIONS

Personal Information - recorded information about an identifiable individual excluding business contact information.

Personal Information Incident– an incident involving the theft, loss or unauthorized access to; or any collection, use, disclosure or disposition of Personal Information that is in contravention of the *Freedom of Information and Protection of Privacy Act* ("FIPPA"), the University's Privacy and Access to Information Policy or other applicable law. Personal Information Incidents are often referred to colloquially as privacy breaches in reference to breaching FIPPA.

3 SCOPE

This procedure applies:

a. when there is unauthorized access to, or collection, use, disclosure, or disposal of Personal Information
b. to anyone employed by the University and to contracted service providers and their subcontractors

4 PROCEDURE

4.1 Initial Identification and Actions

Employees who discover a Personal Information Incident should immediately:

a. suspend any processes or activities causing the incident to occur/continue that are in their immediate control; and

b. contact Security or IT if the incident involves an imminent threat to the security of an individual, University property or electronic systems and then notify their supervisor/manager or the chair and/or coordinator of their department ("the Manager") of the incident as soon as possible.

4.2 Internal Reporting

The Manager will report the incident without unreasonable delay and, where feasible, not later than 24 hours after having become aware of the incident to:

a. the Privacy Officer;
b. Campus Security if It is possible that the incident could lead to unauthorized entry to University premises;
c. IT Services if the security of electronic systems may have been compromised;
d. Risk Management if any devices or equipment have been lost or destroyed, or if a claim is possible; and
e. their department or faculty Administrator

Reports should include the nature of the incident, the type of Personal Information involved, the number of people potentially affected, and any initial action taken.

4.3 Containment

The Manager will then, with the guidance of the Privacy Officer, Security, IT Services or Risk Management:

a. Immediately take any remedial actions possible, for example shutting down compromised applications, removing access, recalling emails, destroying inappropriately printed documents, changing passwords, etc;
b. Identify the Personal Information involved and the scope of the incident;
c. If Personal Information has been inappropriately disclosed, make all reasonable efforts to recover the Personal Information or ensure that it is destroyed confidentially and not further disclosed. A template letter is available from the Privacy Officer that can be sent to third party organizations requesting that the information be returned to the University, electronic copies deleted and/or paper records confidentially destroyed and confirming that no copies of the information have been retained; and
d. Start a log to record actions taken prior to, during and after the incident.

4.3 External Reporting

The Privacy Officer will consult with Risk Management as to whether a report should be made to the University, College and Institute Protection Program (UCIPP), to any cyber insurance providers or to specialist third party services including legal counsel as applicable.

The Privacy Officer will determine whether to report the privacy breach to the Office of the Information and Privacy Commissioner (OIPC) in consultation with legal counsel as appropriate. In determining whether to notify the OIPC the following factors will be considered:

a. the sensitivity of the Personal Information;
b. whether the breached information could result in significant harm including identity theft; bodily harm; embarrassment or humiliation; damage to reputation or relationships; loss of employment, business or professional opportunities; financial loss; damage to a credit record; or damage to or loss of property.
c. the amount of people affected by the breach;
d. whether the information has been fully recovered; and
e. if the breach is the result of a systemic problem or a similar breach has occurred before; and
f. any other factors required by FIPPA or other applicable law.

The University will comply with notification requirements in accordance with FIPPA or other applicable law. If the Incident involves The Privacy Officer should determine whether

4.2 Notice to Affected Individuals

The Privacy Officer will, in consultation with legal counsel as appropriate, identify the most appropriate University officer to notify the individual(s) affected. The contents of any notice will be appropriate to the facts and may include:

a. the date of the incident;
b. a description of the incident;
c. the type (e.g., name, address, financial information, medical history, credit card number, etc.) and volume of Personal Information involved;
d. an explanation of the steps taken to recover any information disclosed, stolen, or lost (if applicable);
e. the steps that an affected individual may take to further protect themselves (if identity theft or other potential risks to the individual are suspected);
f. the contact information for the Privacy Officer who can respond to enquiries regarding the incident and
g. a statement about the right to complain to the Office of the Information and Privacy Commissioner (OIPC)

Notification must **not** include:

a. Personal Information about others or any information that could result in further exposure of personal information
b. information that could be used to circumvent security measures or negatively impact an ongoing investigation

Notice to the affected individuals should be completed as soon as possible in accordance with FIPPA. If any affected individual is resident outside of Canada, the notification requirements of applicable regulations (for example GDPR or CCPA) should be followed as applicable.

Notice should be made in writing whenever possible. If law enforcement authorities have been contacted it may be appropriate to coordinate the notification process to ensure that any ongoing investigation is not impacted.

4.3 Investigation and Follow Up

The Privacy Officer will coordinate Personal Information Incident investigations, working with department management and dependent on the nature of the incident, Campus Security, IT, HR, legal or other specialists. The aim of the investigation is to:

a. review and document the circumstances surrounding the incident.
b. make sure that there is no ongoing exposure or loss of Personal Information and that all affected individuals have been notified.
c. review the adequacy of existing physical, procedural, and technical security measures used to protect Personal Information and recommend changes if required.

When the investigation is concluded, the Privacy Officer will taking into account advice from legal counsel, write a report on the incident including:

a. how and why the incident occurred, the remedial steps taken, and the outcome;
b. the investigation findings and recommendations to the Director of the area affected and
c. any further recommendations including broader process changes and additional training to be provided to other teams to reduce the potential of future incidents.

The Privacy Officer will support department managers in providing or accessing privacy training as needed. Where information security issues are identified training will be provided by IT Services.

The Privacy Officer will at an agreed point in time confirm with department Administration that recommendations have been actioned and risks addressed.

Where incident investigations highlight systemic issues that may lead to future incidents or if a need to provide additional University wide privacy awareness raising and training is identified the Privacy Officer will make recommendations for action to be taken to University leadership.

The Privacy Officer will periodically provide reports to the Audit and Risk Committee on the Personal Information Incidents that have occurred, recommendations at department and University level and the actions taken as a result.

5 ADMINISTRATIVE RESPONSIBILITY FOR THESE PROCEDURES

5.1 The Vice-President Finance and Administration or the designated Privacy Officer is responsible for managing and administering these procedures