PRIVACY BREACH MANAGEMENT PROTOCOL

OBJECTIVES AND RATIONALE

This protocol outlines the steps to be taken as soon as an employee at the university learns of a privacy incident. The protocol is intended to guide the immediate, short-term, and long-term privacy breach management activities. Every breach is different; the nature of the response will dictate the specific actions required.

Following this protocol will help the university:

1) Implement immediate remedial measures to mitigate any harm caused by a breach; and
2) Take steps to prevent a similar breach from happening again.

DEFINITIONS

Privacy breach: an event in which there is unauthorized access to, collection, use, disclosure, or disposal of personal information by ECU, its vendors, or its employees. Activities are unauthorized if they contravene BC's *Freedom of Information and Protection of Privacy Act* or ECU's related confidentiality and privacy policies. Breaches may be the result of theft, purposeful behavior, or inadvertent behavior.

Personal information: recorded information about an identifiable individual other than business contact information. This includes student names, ID numbers, emails, addresses, phone numbers, credit card information, employment history, educational history, medical history, financial history, and more.

Records: includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records;

SCOPE AND APPLICATION

This protocol applies to all university employees, volunteers and service providers engaged in a sanctioned university activity that involves the handling of personal information in the custody or under the control of the university. With respect to service providers, this protocol applies only during the term of their contract with the university.

This protocol should be followed following the discovery of a privacy breach, as defined above. **For clarity, action items are denoted with this symbol: »**

SECURITY INCIDENTS INVOLVING PERSONAL INFORMATION

If the university's electronic systems are compromised, notify and work with IT Services to manage the breach. Examples of a compromised electronic system include: phishing attempts, hackers, malware infections, ransomware attacks, copyright infringement.

If unsure of which plan to follow, individuals should contact both the Privacy Office and IT Services, and further guidance will be provided.

Privacy Office	privacy@ecuad.ca
IT Services	ithelp@ecuad.ca

PROCEDURES

STEP 1: IDENTIFY AND CONTAIN THE INCIDENT [SAME DAY]

A privacy breach is **unauthorized access to or collection, use, disclosure or disposition of personal information.** Examples of a privacy breach include stolen computers containing personal information of ECU students or employees, personal information emailed to the wrong organization or person, lost memory devices that contain personal information, and other situations.

Privacy incidents may be identified in many ways, including but not limited to:

- Responding to a privacy complaint
- Monitoring systems on campus
- Responding to an information security breach
- Reporting from an external source

Anyone (staff, administrator, faculty, etc.) who is made aware of any privacy incident or privacy breach must:

» Immediately **notify their direct supervisor or director/dean**.

As well, the employee and their supervisor or director/dean should immediately take action to contain the breach if technically able to, or ask for assistance to do so.

» **Contain the breach** by, for example, stopping the unauthorized practice, recovering the records, temporarily shutting down the system that was breached, revoking or changing computer access codes/passwords or correcting weaknesses in physical security.

STEP 2: INTERNAL REPORTING [SAME DAY]

» **Notify the Privacy Office** who will advise on what further steps to take, and send the Privacy Breach Reporting Form for the employee to complete. The form captures the types of personal information breached, but do not include any information about an identifiable individual. Provide as much information as possible since it helps with the preliminary assessment.
» **Notify IT Services** if you suspect it may be a security incident.
» **Notify Campus Security** if you believe personal information was stolen.

Breach Checklist – to be completed on the same day as discovery:

- ☐ Immediately contain the breach if possible
  - Ask IT for assistance if necessary
- ☐ Notify your direct supervisor or director/dean
- ☐ Notify the Privacy Office (privacy@ecuad.ca)
- ☐ Notify IT Services if it may be a security incident (ithelp@ecuad.ca)
- ☐ Report to Campus Security if you believe personal information was stolen (e.g., an office was broken into and computers stolen)

STEP 3: PRELIMINARY ASSESSMENT + PRIVACY BREACH RESPONSE TEAM

» The Privacy Office (with IT Services, if appropriate) will conduct a preliminary assessment. The preliminary assessment should involve the following:
- The type of personal information affected
- An estimate of the number of individuals affected
- If there was a known cause of the breach
- If the information was encrypted or otherwise not accessible
- Has any information been recovered
- Is this a systemic problem or an isolated incident
- Is there foreseeable harm from the breach; if so, what type and how severe

» Upon completing the preliminary assessment, the Privacy Office will determine how to escalate the incident.
1) If the risks appear to be Low/Medium, the Privacy Office will work directly with the affected department to contain, manage and document the breach.
2) If the risks appear to be Medium/High, the Privacy Office will alert the President. It may be necessary to contact the RCMP if there is a high risk of foreseeable harm.

» **For Medium/High risk incidents**, the President or the Privacy Office will create a Breach Response Team comprised of the employees representing the departments necessary for the assessment and resolution of each specific privacy incident. The Breach Response Team will depend on the nature and severity of the breach. The President can also be a member of the Breach Response Team if necessary. The team may include one or more of the following positions and departments:
- Chief Information Officer, ITS
- Privacy Officer (HR)
- University Secretary
- Director, Communications and Marketing
- Vice President, Finance + Administration
- Department(s) and employee(s) where the incident occurred, and departments affected by the incident
- Outside agencies, as necessary.

» The Privacy Office will begin the Breach Checklist found in Appendix 1.

Breach Checklist – to be completed within 2 days of the breach:
- ☐ Privacy Office and/or IT Services to complete preliminary assessment of the risks and cause of the breach
- ☐ Privacy Office and/or IT Services to escalate the incident as necessary (e.g., to the President if Medium/High risk)
  - ☐ Privacy Breach Response Team is assembled
  - ☐ Contact the RCMP if necessary
  - ☐ Take further containment steps if necessary

STEP 4: INVESTIGATION

Note: If the incident is a security incident (that involves PI), the incident response should be managed in conjunction with IT Services. In these cases, the CIO and Privacy Office will work together to determine which office is most appropriate to lead response tasks (e.g., investigations, assessments, notifications).

The Breach Response Team will:

- Ensure actions are (or have been) taken to further contain the privacy incident (e.g., stop the practice, shut down affected systems, revoke access, correct weaknesses in physical security, etc.)
- With reference to the preliminary assessment, conduct and document a risk assessment. The assessment includes the following:
  - Personal information involved
  - Cause and extent of the breach
  - Identify the individuals affected by the breach
  - Foreseeable harm from the breach
  - Refer to more details on pgs. 5-6 of the OIPC Privacy Breaches: Tools and Resources document.
- Based on the risk assessment, determine the notifications necessary and the internal and external reporting requirements. See "Step 5 Notification" below.

Breach Checklist – to be completed within 1 week of the breach:

☐ Breach Response Team to conduct a risk assessment (see Appendix 2)

STEP 5: NOTIFICATION

- The Breach Response Team will determine whether notification is required in accordance with the BC Privacy Commissioner's Privacy Breaches: Tools and Resources (https://www.oipc.bc.ca/guidance-documents/1428). Notification of affected individuals and the Commissioner's Office is generally required where any of the following factors is present:
  - Legislation requires notification
  - Notification is required to meet professional standards or certification standards
  - Contractual obligation to notify
  - Risk of identity theft
  - Risk of physical harm
  - Risk of hurt, humiliation, damage to reputation
  - Risk of loss of business or employment opportunities

If notification is required, a **notification response team** will be formed.

1) For low severity breaches, this team will generally constitute only the Privacy Office, and the affected unit.
2) For higher severity breaches, the team will also include other support/stakeholder units including the President, Communications + Marketing, and the relevant Vice-President(s).

The notification response team will:

» Develop and finalize a communication plan for notification (email, web, press release, etc.) – note that notification itself is generally delivered by the affected unit
» Determine supporting infrastructure (e.g., contact web page, responding to questions)
» Determine other supporting resources/compensation (e.g., credit monitoring, specialized assistance)
» Assign spokesperson (if appropriate)
» Oversee notification process
» Assist with post-incident review as required

Refer to Appendix 3 for the Components of a Notification Letter.

EXTERNAL REPORTING TO THE OIPC

The Breach Response Team will decide if it is necessary that the University report a privacy breach to the Office of the Information and Privacy Commissioner for British Columbia (OIPC). The Breach Response Team will make this decision upon considering:

- the circumstances that caused the privacy breach;
- the type, quantity and sensitivity of the personal information involved;
- the number of individuals affected;
- the number of unauthorized recipients;
- the media on which the personal information was stored and transmitted;
- the location where it was stored; and
- any other relevant factors.

» The Privacy Officer will be the point of contact with the OIPC.

EXTERNAL REPORTING AS APPROPRIATE

The Breach Response Team should consider whether the following authorities or organizations should also be informed of the breach:

- Law enforcement if theft or other crime is suspected (note: the police may request a temporary delay in notifying individuals, for investigative purposes)
- Professional or regulatory bodies, if standards require notification

- Technology suppliers if the breach was due to a technical failure
- Insurance agencies

Breach Checklist – to be completed within 1-2 weeks of the breach:

- ☐ Breach Response Team to determine if notification to the OIPC is necessary
  - If necessary, the Privacy Office will report the breach to the OIPC and act as the point of contact with their office
- ☐ Breach Response Team to determine whether notification to affected individuals is necessary, specifically:
  - Which individuals to notify
  - Manner of notification (email, direct mail, phone, etc.)
  - Responsibilities for drafting, finalizing and approving communications related to notification
  - Timeline of notification
- ☐ Notification response team is formed
- ☐ Notification response team drafts, finalizes and sends the notification letter. The affected department and/or the Privacy Office will respond to questions from affected individuals.
- ☐ Contact other parties as appropriate

STEP 6: PREVENTION + REMEDIATION

These activities may take place in parallel with Step 5, Notification.

The Breach Response Team will:

- Finalize the notifications process with the conclusion of the internal and external reporting.
- Determine if further, in-depth investigation is needed.
  - Further investigate the cause and extent of the breach as appropriate
  - This may require a security audit of both physical and technical security. As a result of this evaluation, determine if there are any new or updated safeguards necessary to prevent future breaches.
- Review investigation findings and improve prevention strategies.
  - Any prevention plans should be monitored and reported on (or audited) to ensure implementation. Ensure that ECU's business practices are improved where necessary to prevent such future incidents
  - Safeguards can be:
    - Administrative (policies, procedures, training and education)
    - Technical (new security features or requirements)
    - Physical (additional locks, physical access requirements)
- Complete the Privacy Breach checklist (Appendix 1).

- The Privacy Breach Management Protocol should be reviewed and updated to reflect the lessons learned from each incident.

Breach Checklist – to be completed within 3 months of the breach:

- ☐ Breach Response Team to determine if notification to the OIPC is necessary
  - If necessary, the Privacy Office will report the breach to the OIPC and act as the point of contact with their office
- ☐ Breach Response Team to determine whether notification to affected individuals is necessary, specifically:
  - Which individuals to notify
  - Manner of notification (email, direct mail, phone, etc.)
  - Responsibilities for drafting, finalizing and approving communications related to notification
  - Timeline of notification
- ☐ Notification response team drafts, finalizes and sends the notification letter. The affected department and/or the Privacy Office will respond to questions from affected individuals.
- ☐ Contact other parties as appropriate
- ☐ Review and update the Privacy Breach Management Protocol

APPENDIX 1: PRIVACY BREACH CHECKLIST

	Action Required	Responsibility	Recommended Timelines
Step 1	Contain the breach	Affected program area	Immediately
Step 2	Report the breach to the Privacy Office	Program area staff	Day of breach discovery
	Notify IT Services if it might be a security incident	Program area staff or Privacy Office	Day of breach discovery
	Report to Campus Security if you believe personal information was stolen	Program area staff	Day of breach discovery
Step 3	Complete preliminary assessment of the risks and cause of the breach. Determine if preliminary risk is low, medium, or high.	Privacy Office and/or IT Services	Within 2 days of breach discovery
	Escalate the incident as necessary (if medium/high risk: President, VPs, maybe RCMP)	Privacy Office and/or IT Services	Within 2 days of breach discovery
	Privacy Breach Response Team is assembled (if applicable)	President	Within 2 days of breach discovery
	Take further containment steps (if necessary)	Program area, Privacy Office and/or IT Services	Within 1 week of the breach
Step 4	Conduct a risk assessment	Breach Response Team	Within 1 week of the breach
Step 5	Determine whether to notify the BC Privacy Commissioner	Breach Response Team	Within 1 week of the breach
	Determine whether to notify affected parties	Breach Response Team	Within 1-2 weeks of the breach
	Notify affected parties as determined	Notification Response Team	Within 1-2 weeks of the breach
	Contact other parties as appropriate	Notification Response Team	As needed
Step 6	Determine whether further, in- depth investigation is needed	Breach Response Team	Within 2-3 weeks of the breach
	Further investigate the cause and extent of breach if appropriate	Breach Response Team	Within 3 months of the breach
	Review investigation findings and improve prevention strategies	Breach Response Team	Within 3 months of the breach
	Implement prevention strategies/ improvements	Program area	Depends on the prevention strategy
	Review and update this Privacy Breach Management Protocol to reflect the lessons learned from each incident	Breach Response Team, Privacy Office	Within 3 months of the breach

APPENDIX 2: TOOLS AND RESOURCES

» OIPC Privacy Breaches: Tools and Resources: https://www.oipc.bc.ca/guidance-documents/1428
  - See pages 5-6 for conducting a Risk Assessment
  - See pages 20-24 for the Breach Notification Assessment Tool

» Report a privacy breach to the OIPC: https://www.oipc.bc.ca/forms/public-bodies/online-privacy-breach-report-form/

APPENDIX 3: COMPONENTS OF A NOTIFICATION LETTER

In the event of a privacy breach, determine who should be notified, and include the following elements in the notification letter:

- ✓ Date of the notification letter
- ✓ Date the breach occurred
- ✓ The department, school, or office in which the breach occurred
- ✓ Description and nature of the breach (e.g., computer theft, inappropriate release of information, lost memory device, etc.)
- ✓ Description of the information that was stolen, lost, released, etc.
- ✓ Risks or possible consequences to the person or group/organization whose information
- ✓ was breached (the "information owner")
- ✓ Steps taken so far, and further steps to be taken regarding this incident, to control or mitigate the possible harm
- ✓ Further steps planned or in process to prevent future privacy breaches
- ✓ Actions the information owner can take to prevent or reduce the possible harm
- ✓ Contact information for British Columbia's Office of the Information and Privacy Commissioner
- ✓ Contact information for the ECU Privacy Office.

Add additional comments (such as regrets) or other relevant information as appropriate.

Assistance with a template is available from the Privacy Office (privacy@ecuad.ca).