Original Approval Date: November 7, 2013
Most Recent Approval: November 7, 2013
Editorial Amendments: June 4, 2026

Parent Policy: Information Technology Use and Management Policy

Privacy and Information Security Incident Reporting and Response Procedure

Office of Administrative Responsibility:	Information, Privacy and Records Management Office
Approving Authority:	Provost and Vice-President (Academic)

Purpose

As a public body under the Alberta *Access to Information Act* (ATIA) and *Protection of Privacy Act* (POPA), the University of Alberta must protect Personal Information, Data Derived from Personal Information, Non-personal Data, Sensitive or Confidential Information and Research Records under its custody or control against such risks as unauthorized access, collection, use, disclosure or destruction.

From time to time through the business, service and research functions of the university, the university may gain access to Health Information as defined in the Alberta *Health Information Act* (HIA). In these relationships, the university must also protect such information against unauthorized access, collection, use disclosure or destruction in accordance with the provisions of the HIA.

The purpose of this procedure is to provide the steps necessary for identifying, containing, investigating, assessing, analyzing, reporting, and notifying in the event of a Privacy and/or Information Security Incident, as well as preventing future Incidents.

Definitions

The attached definitions table outlines the terms used in this procedure that are not otherwise defined herein and any specific rules of interpretation that apply.

Scope

This procedure applies to all members of the University Community participating in activities or functions governed by this procedure and its parent policy.

Procedure

1. CONTAIN AND DOCUMENT

Any member of the University Community who becomes aware that a Privacy and/or Information Security Incident (the Incident) has occurred must:

1.1. Take immediate action to stop and contain the Incident and secure the affected information, records, systems or web-sites, revoking access and correcting vulnerabilities in physical and/or technical security.

1.2. **Immediately report the Incident to the Information, Privacy and Records Management Office (IPRMO) and the Office of the Chief Information Security Officer (CISO)** within 24 hours of detecting an Incident, by submitting a completed Privacy and/or Information Security Incident Report Form and providing any further information as may be required by the IPRMO and/or CISO.

1.3. The Privacy and/or Information Security Incident Report Form includes all the required fields to initially report an Incident in compliance with POPA. If the Incident involves Research Records, contact the approving research ethics board.

2. RISK ASSESSMENT

In most cases, the more Sensitive the information (Personal or Confidential Information), the greater the potential harm to the individuals affected from a Privacy and/or Information Security Incident.

Upon notification of an Incident, the IPRMO and CISO will determine the risks associated with the Incident and the required next steps.

If a Privacy and/or Information Security Incident occurs involving the loss of, unauthorized access to, or unauthorized disclosure of Personal Information in the custody or under the control of a public body, a Privacy Breach under POPA has occurred. Where a reasonable person would consider that there exists a Real Risk of Significant Harm (RROSH) to an individual as a result of the Privacy Breach, the University must give notice, without unreasonable delay, of the Incident to the following:

2.1. the individual to whom there exists a real risk of significant harm;

2.2. the Information and Privacy Commissioner; and

2.3. the Minister (responsible for POPA).

To determine whether a RROSH to an individual exists as a result of the loss of, unauthorized access to, or unauthorized disclosure of Personal Information, the University must consider each of the following factors, in addition to any other relevant factors:

2.4. whether there is a reasonable basis to believe that the Personal Information has been misused or will be misused;

2.5. whether the loss of, unauthorized access to or unauthorized disclosure of the Personal Information occurred as a result of malicious intent;

2.6. the sensitivity of the personal information that was lost or accessed or disclosed without authorization; mitigating measures taken or other factors that reduce the risk of significant harm.

3. NOTIFICATION

3.1. Based on the results of the RROSH assessment above, the IPRMO and CISO will advise whether to notify individuals affected by the Privacy Breach, when and how they will be notified, and what information will be included in the notification.

3.2. The IPRMO and CISO will consult with the General Counsel, the Office of Provost and VIce-President (Academic) and other relevant University offices when making the decision to notify affected individuals.

3.3. Depending on the circumstances, notification must include:

3.3.1. description of the circumstances of the Privacy Breach including the date or period during which the Incident is thought to have occurred;

3.3.2. general description of the type of Personal Information that was lost or that was the subject of the unauthorized access or disclosure;

3.3.3. steps taken so far to reduce the risk of harm to the individual and future steps planned to prevent further Privacy Breaches;

3.3.4. additional information as to how individuals can protect themselves against identity theft or fraud;

3.3.5. contact information of an individual (including position title) within the University who can respond to questions or provide further information about the Privacy Breach.

3.3.6. In the case of the notice to impacted individuals, the individuals' right to request a review by the Information and Privacy Commissioner in accordance with POPA; and

3.3.7. any other information as required under POPA and that the University considers relevant.

4. PREVENTION

4.1. Once immediate steps have been taken to contain the Privacy Breach and mitigate risks associated with the breach, steps must be taken to prevent future occurrences. The IPRMO and CISO may:

4.1.1. conduct a security audit of both operational, physical and technical security;

4.1.2. develop policies and procedures for the collection use, access and security of Personal and Sensitive or Confidential Information; and

4.1.3. conduct staff training to ensure the protection and prevention plan has been implemented.

Definitions

Any definitions listed here apply to this procedure only with no implied or intended institution-wide use. Capitalized words and phrases used in this procedure that are not otherwise defined herein shall have the same meanings ascribed to them in the Information Technology Use and Management Policy.	
Access to Information Act **(ATIA)**	The *Access to Information Act,* SA 2024, c A-1.4 and associated regulations, as amended from time to time.
Personal Information	Personal Information means recorded information about an identifiable individual, including but not limited to: ● the individual's name, home or business address, home or business telephone number, home or business email address, or other contact information, except where the individual has provided the information on behalf of the individual's employer or principal in the individual's capacity as an employee or agent, ● the individual's race, national or ethnic origin, colour or religious or political beliefs or associations, ● the individual's age, gender identity, sex, sexual orientation, marital status or family status, ● an identifying number, symbol or other particular assigned to the individual, ● the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics, ● information about the individual's health and health care history, including information about the individual's physical or mental health, ● information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given, ● anyone else's opinions about the individual, and ● the individual's personal views or opinions, except if they are about someone else.
Privacy and/or Information Security Incident	A Privacy and/or Information Security Incident is an event that *may* lead to a data leak, or a compromise of a system, or the unauthorized access to or collection, use, disclosure, or disposal of Personal Information that is in the custody or under the control of a public body but has not been confirmed yet.

Privacy Breach	A Privacy Breach occurs when a Privacy and/or Security Incident is confirmed to have resulted in the unauthorized access, collection, use, disclosure, or disposal of Personal or Health Information within the Custody or Control of a public body. Examples may include: ● Information collected in error; ● Information used or disclosed for a purpose NOT consistent with the original collection; ● Lost or misplaced Personal Information; ● Stolen or displaced files, laptops, data drives or disks or thumb drives; ● Hacking of databases; ● Accidental or deliberate disclosure of Personal Information to unauthorized persons or groups; ● Accidental or deliberate disclosure of Personal Information in email or other electronic communications.
***Protection of Privacy Act* (POPA)**	The *Protection of Privacy Act*, SA 2024, c P-28.5 and associated regulations, as amended from time to time.
Sensitive or Confidential Information	Sensitive or Confidential Information (including but not limited to Personal Information) refers to all information that has been collected or compiled in the conduct of operating the programs and services of the University and may include, but is not limited to: ● Confidential business information of third parties; ● Confidential Information collected or compiled in the process of hiring or evaluating employees of the University; ● Information collected or compiled in the process of law enforcement investigations; ● Advice, proposals or recommendations, consultations or deliberations of the governing and administrative authorities of the University; ● Information, the disclosure of which would harm the economic interests of the University; ● Any information to which legal privilege including client-solicitor privilege may apply.

University Community	Academic, excluded and support staff, academic colleagues and postdoctoral scholars as outlined and defined in the *Recruitment Policy Appendix A: Definitions and Categories of Staff*; undergraduate, graduate, continuing education students and post-graduate learners; emeriti; contractors; visitors; volunteers; and members of the Board of Governors.

Parent Policy Suite

- Information Technology Use and Management Policy
- Information Technology Use and Management Policy Appendix A: Examples of Unacceptable Use
- Email Forwarding Restriction Procedure
- Official Email List Procedure
- Privacy and Information Security Reporting and Response Procedure

Related Policy Documents

- Access to Information and Protection of Privacy Policy
- Information Technology Security Policy

Related Links

- *Access to Information Act*
- *Protection of Privacy Act*
- Information, Privacy and Records Management Office
- *Post-secondary Learning Act*

History

November 7, 2013	Approved.
September 19, 2024	Editorial amendment. Formatting and links.
June 4, 2026	Editorial amendment. Formatting and numbering, definition clarification, legislative reference updates and alignment. Renamed from *Responding to and Reporting of Information Security Breaches Procedure*.

For questions surrounding policy document interpretation or implementation, please contact the Office of Administrative Responsibility.

The official version of this document may be obtained from https://www.ualberta.ca/policies-procedures/index.html