Original Approval Date: November 7, 2013

Parent Policy: IT Use and Management Policy

Responding to and Reporting of Information Security Breaches Procedure

Office of Administrative Responsibility:	Information and Privacy Office
Approver:	Provost and Vice-President (Academic)
Scope:	Compliance with this University procedure extends to all members of the University community.

Overview

The University of Alberta as a public body under the ***Alberta Freedom of Information and Protection of Privacy Act* (FOIPPA)** must protect **personal information, health information, sensitive or confidential 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.

Purpose

The purpose of this procedure is to provide education about **information security breaches** of personal information, health information , sensitive and confidential information, or research records and the steps necessary in identifying, containing, investigating, assessing, analyzing, reporting, and notifying in the event of a breach, as well as education to prevention of privacy breaches from occurring.

PROCEDURE

1. CONTAIN AND DOCUMENT

   Any member of the University community who comes aware that an information security breach has occurred must:

   a. Take immediate action to stop and contain the breach and secure the affected records, systems or web-sites, revoking access and correcting weaknesses in physical security.

   b. Immediately contact the Information and Privacy Office and the Information Technology Security Officer (within 24 hours of detecting a breach)

   c. If the breach involves research records, contact the approving research ethics panel.

   d. Document the cause and circumstances that gave rise to the privacy breach. (See attached Information Security Breach Reporting Form)

   e. Produce a detailed inventory of the personal or sensitive or confidential information that was or may have been lost or compromised. (List all of the data elements of the personal information (including health information) or sensitive or confidential business information exposed through the breach.

   f. Identify the parties and individuals whose personal information or confidential information has been disclosed, accessed, stolen or lost as a result of the breach. (employees, students, research subjects, contractors, service providers, other organizations)

   g. Identify the office, department or faculty that is responsible for the administration of the personal or confidential information involved in the breach.

h. Include all other relevant information related to the breach or loss of information.

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 information security breach..

Upon notification of an information security breach, the Information and Privacy Office (IPO) and the Information Technology Security Officer (ITSO) will convene a process to determine the risks associated with the breach including consideration of the following elements and the need to notify affected individuals:

a. Is there a relationship between the unauthorized recipients and the data subjects?

b. What potential harm to the individuals will result from the breach?

i. Security risk

ii. Identity theft or fraud

iii. Loss of business or employment opportunity

iv. Hurt, humiliation, damage to reputation or relationships

v. Risk to public health or safety

c. What potential harm could result to the university?

i. Loss of trust in the university

ii. Loss of assets

iii. Financial or legal exposure

iv. Reputational damage?

3. NOTIFICATION

a. Based on the results of the risk assessment, the IPO and ITSO will recommend whether to notify individuals affected by the breach, when and how they will be notified, and what information will be included in the notification.

b. The IPO and ITSO will consult with General Counsel and Risk Management in the decision to notify affected individuals.

c. Depending on the circumstances, notification could include some or all of the following:

i. Description of the breach

ii. Specifics of the information inappropriately accessed, collected, used or disclosed

iii. Steps taken so far to address the breach and future steps planned to prevent further breaches

iv. Additional information as to how individuals can protect themselves against identity theft or fraud

v. Contact information of an individual (including position title) within the University who can answer questions or provide further information about the breach.

4. PREVENTION

a. Once immediate steps have been taken to contain the breach and mitigate risks associated with the breach, steps must be taken to prevent future occurrences. The IPO and ITSO:

i. may conduct a security audit of both operational, physical and technical security

ii. develop policies and procedures for the collection use, access and security of personal and sensitive or confidential information

iii. Conduct staff training to ensure the protection and prevention plan has been implemented

DEFINITIONS

Any definitions listed in the following table apply to this document only with no implied or intended institution-wide use. [▲Top]

Freedom of Information and Protection of Privacy Act	The *Freedom of Information and Protection of Privacy Act*, Statute of Alberta, Chapter F-25, as amended from time to time.
Personal information	Personal information is defined as per Section 1(n) of the *Act.*
Health information	Health information is defined in Section 1 (k) of the Health Information Act.
Health Information Act	Health Information Act, Statute of Alberta Chapter H-5 as amended from time to time.
Privacy Breach	A privacy breach has occurred when there is unauthorized access to or collection, use, disclosure, or disposal of personal or health information that is in the custody or under the control of a public body. Examples might be • Information collected in error • Information used or disclosed for a purpose NOT consistent with the original collection • Lost or misplaced PI • Stolen or displaced files, laptops, data drives or disks or thumb drives • Hacking of databases • Accidental or deliberate disclosure of PI to unauthorized persons or groups • Accidental or deliberate disclosure of PI in email or other electronic communications.
Sensitive or Confidential Information	Sensitive or confidential 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.

Research Records	Research information assets supporting both research and operational needs. This includes administrative information and records produced for analytic or evidentiary purposes. Research records include those documents and records and materials captured by or for a researcher that are necessary to document, reconstruct, evaluate, and validate research results and the events and processes leading to the acquisition of those results. Research records may be in many forms including but not limited to laboratory notebooks, survey documents, questionnaires, interview notes, transcripts, machine generated data or performance outputs, recruitment materials, consent forms, correspondence, other documents, computer files, audio or video recordings, photographs including negatives, slides, x-ray films, samples of compounds, and components of organisms. With regard to research involving human participants or animal use, research records usually relate to the data collected about the subjects of the research, but may also include genomic sequencing and similar genetic information about animals used in research.

FORMS

Should a link fail, please contact uappol@ualberta.ca. [▲Top]

Loss or Breach of Information Reporting Form

RELATED LINKS

Should a link fail, please contact uappol@ualberta.ca. [▲Top]

Access to Information and Protection of Privacy Policy
Alberta Freedom of Information and Protection of Privacy Act
Alberta Health Information Act
Alberta Post-Secondary Learning Act
Information Technology Security Policy

PUBLISHED PROCEDURES OF THIS POLICY

Information Technology Use and Management Policy Appendix A- Examples of Unacceptable Use
Official Email Lists Procedure
Email Forwarding Restriction Procedure