Saskatchewan
Apprenticeship and
Trade Certification
Commission

Privacy Breach Policy and Procedures

Effective Date: May 2, 2011
Revised Date: August 1, 2014

INTENT

The purpose of this policy is to outline the steps to be followed when a possible breach of privacy is identified to ensure the impact is contained and minimized. The policy also articulates the measures to be taken to develop and implement strategies to prevent similar breaches from recurring.

DEFINITIONS

Privacy Breach: A privacy breach occurs when there is unauthorized collection, use or disclosure of personal information.

Personal Information: Personal information can be generally described as any information about an identifiable individual, and can be as simple as a person's name and address, or name and telephone number. For a complete description of personal information, please refer to Section 24 of *The Access to Information and Protection of Privacy Act* at www.oipc.sk.ca

Personal Health Information: Personal health information is generally described as any information about an identifiable individual living or deceased which is related to their physical or mental health, any health services provided, and registration information. For a complete description of personal health information, please refer to Section 2(m) of *The Health Information and Protection Act* at www.oipc.sk.ca

AUTHORITIES

Under the two pieces of legislation listed below, the SATCC is accountable for the collection, use, storage and destruction of personal information and personal health information in the possession or control of the Commission.

The Freedom of Information and Protection of Privacy Act (FOIP)
The Health Information Protection Act (HIPA)

POLICY AND PROCEDURES

POLICY

Any breach of privacy is not acceptable and will not be tolerated at SATCC. Any real or suspected privacy breach will be investigated and addressed in accordance with the following guidelines.

PROCEDURES

Upon learning that a potential privacy breach has occurred, immediate action must be taken. Any staff member who learns of a potential privacy breach must report this immediately to their Manager, Director, or Executive Director who will report to the Access and Privacy Officer. The Access and Privacy Officer will notify the SATCC Senior Management Team (SMT) who, in conjunction with the Access and Privacy Officer, will act as the lead on all actions taken towards resolution, steps to prevent a recurrence, and preparation of the necessary documents as required (e.g., OIPC reports, briefing notes, etc).

Many of the following steps need to be carried out simultaneously or in quick succession.

STEP 1: CONTAIN

Take **immediate** action to contain the breach, including:

- Take appropriate steps to avoid further harm (e.g., stop the practice, shut down the system(s) that caused the potential breach, revoke access to records, etc).
- Immediately report the incident to your Manager, Director, or Executive Director and the Access and Privacy Officer. The Access and Privacy Officer will notify the SATCC SMT.
- Recover any records which may be held by unauthorized persons.
- For further guidelines related to notification of involved individuals, please see STEP 3 below.

STEP 2: INVESTIGATE THE BREACH[1]

When the breach has been contained, an internal investigation will be initiated. The investigation will be led by the Manager, Director or Executive Director and the SATCC's Access and Privacy Officer.

All privacy breach investigations will address the incident on a systematic basis and will include the following elements:

- Individuals with information about the breach will document details of the privacy breach and provide them to the Manager who will then provide

[1] Privacy Breach Guidelines, www.OIPC.sk.ca/resources

them to their Director or Executive Director and Access and Privacy Officer.
- The Access and Privacy Officer, in conjunction with the CEO, may notify the Office of the Information and Privacy Commissioner (OIPC) and will provide ongoing liaison with them.
- The immediate and ongoing risks will be evaluated.
- Standard policies and procedures, as well as the safeguards in place prior to the breach and the circumstances that led to the breach will be critically assessed.

STEP 3: NOTIFICATION OF AFFECTED INDIVIDUALS

Notification of affected individuals should occur if it is necessary to avoid, mitigate or address harm to them. Notifications should occur as soon as possible. However, if law enforcement authorities have been contacted, those authorities should be consulted re: the timing of any notification. Responsibility for notification and the process for notification will be determined by the SATCC Board Chair, the CEO and the Access and Privacy Officer on a case by case basis.

ALL DISCUSSIONS RELATED TO NOTIFICATION SHOULD BE DATED AND DOCUMENTED.

For further information about when notification is required, when and how to notify individuals and what should be said, please refer to the Privacy Breach Guidelines at www.oipc.sk.ca/resources

STEP 4: ASSESS AND ANALYZE THE BREACH AND ASSOCIATED RISKS

When the breach has been contained and the investigation is underway, the following will be critically examined:
- Is personal information and/or personal health information involved?
- What is the cause and extent of the breach?
- How many individuals are affected by the breach? Who are the individuals?
- What is the foreseeable harm resulting from the breach?

A 'Review of Privacy Breach' report will be completed which will include:
- a summary of the incident;
- a chronology of events and steps taken to contain the breach;
- a review of safeguards and protocols;
- a summary of possible solutions and recommendations; and
- a detailed description of the next steps including identification of who is responsible for implementing the timelines.

The SATCC's Access and Privacy Officer will finalize the report, facilitate approval by the CEO and may provide the final report to the OIPC.

The Access and Privacy Officer will facilitate all follow-up reports as required.

For further detail on the assessment and analysis of associated risk please refer to the Privacy Breach Guidelines at www.oipc.sk.ca

STEP 5: PREVENTION

A plan to avoid similar future breaches will be developed by the Manager, Director or Executive Director with the support of the SATCC Access and Privacy Officer. This plan will include all identified procedural and policy changes aimed at ensuring, to the highest level possible, compliance with the privacy legislation.

Audits will be conducted following implementation of procedural and/or policy changes to ensure the prevention plan has been fully implemented. Ongoing audits may be conducted at the discretion of the CEO, Executive Director, Director or the SATCC Access and Privacy Officer.

ADDITIONAL INFORMATION RELATED TO THE COLLECTION, USE, STORAGE AND PROTECTION OF PRIVACY

Additional related information can be accessed on the web:

- The Office of the Information and Privacy Commissioner: www.oipc.sk.ca
- Ministry of Justice and Attorney General: www.justice.gov.sk.ca/accessandprivacy

Revision Approved by: Jeff Ritter
Date Approved: July 28, 2014

Original Approved by: Joe Black, CEO
May 2, 2011