

## **BAILIFF SERVICES INC. PRIVACY BREACH POLICY**

A privacy breach is an incident involving the unauthorized disclosure of personal information in the custody or control of BSI. This would include personal information being lost, stolen, or accessed by unauthorized persons. This plan outlines the best practices for responding to a privacy breach in four steps:

### **STEP 1: RESPOND AND CONTAIN**

### **STEP 2: NOTIFY**

### **STEP 3: INVESTIGATE**

### **STEP 4: IMPLEMENT CHANGE**

---

### **STEP 1: RESPOND AND CONTAIN**

#### **There's been a possible breach...what next?**

In the event of a possible breach of privacy, the first step is to **respond** to the potential breach. Once we respond and determine whether an actual breach has occurred, **containment** of the situation must follow. In order to accomplish **STEP 1** efficiently, there are five critical actions that need to be taken as soon as possible following the discovery of a possible incident:

1. **REPORT**
2. **ASSESS**
3. **CONTAIN**
4. **DOCUMENT**
5. **BRIEF**

#### **REPORT**

Even if a breach is only suspected and has not yet been verified, it must be **reported** to the appropriate individuals upon notification. Notification can come from either an internal source (i.e. a BSI employee) or an external source (i.e. a client or debtor).

**If reporting internally, a privacy breach or suspected breach needs to be reported to:**

- (a) the BSI Manager of the branch affected by the breach (or the next available level of management); and
- (b) BSI Privacy Officers (Chris Davis or Darren Horne)

Provide as much information as possible when providing notification. Some points that should be included are: what happened, when the incident occurred, how the breach was discovered, and whether any corrective action has already been taken. Any additional information we have on the incident should be included (i.e. did we have to involve law enforcement?)

## **ASSESS**

Once you have reported the situation to the appropriate people, an **assessment** of the situation will be carried out to determine whether a privacy breach has indeed occurred. Two important questions are asked during an assessment, so be sure to have as much information available that can help.

### **1. Is personal information involved?**

Not all data in the custody or control of an institution is personal information. Therefore, the first part of our assessment is to identify the type of information affected by the incident in order to determine whether a breach has occurred.

- **Personal information** is recorded information about an identifiable individual (i.e., natural person) and includes, but is not limited to: date of birth, address, telephone number, financial information, identifying numbers. This list is not exhaustive – BSI may have other types of personal information in its custody or control which may include information that is not recorded (e.g., a verbal disclosure). Also, if there is a reasonable expectation that an individual can be identified from the information disclosed (either alone or when combined with other information), such information will likely qualify as personal information.

### **2. Has an unauthorized disclosure occurred?**

Unauthorized disclosure is the defining characteristic of a privacy breach. Whether it is intentional, inadvertent or as a result of criminal activity, an unauthorized disclosure constitutes a privacy breach.

**If the answer to both questions is “yes”, a privacy breach has occurred, and we need to follow the rest of the privacy breach response protocol outlined in this Plan.**

Once it has been determined that a privacy breach has occurred, containment must follow. This involves taking corrective action such as retrieving the personal information that has been released if the breach involved a hard copy, or isolating/suspending the activity, process or system if it was an electronic breach, etc. The main goal is to alleviate any consequences for the individual(s) whose personal information was involved, the Client, and BSI.

## CONTAIN

Documenting the details of a privacy breach and our **containment** strategy allows the Client involved to assist with the implementation of correct remedial measures, respond to any investigation by the Office of the Information and Privacy Commissioner (IPC), and evaluate our response so areas for possible improvement may be identified.

## DOCUMENT

**Documenting** the details of a privacy breach and our containment strategy allows the Client to assist with the implementation of correct remedial measures, respond to an investigation by the IPC, and evaluate your response so areas for possible improvement may be identified.

**If we find ourselves in a breach situation, here are some things we should document:**

- What happened (e.g., staff disclosed personal information without authority, intruder, third party service provider alert, equipment containing personal information lost or stolen, etc.), when and how the breach was discovered, and what corrective action was taken.
- If the breach was identified by an external source (e.g., applicant, courier, Client), document the information provided, including contact information for follow-ups, and any instructions given to the reporting party (e.g., asking caller to mail back documents sent to wrong address).
- **If you're the BSI Branch Manager:** Ensure details of breach and corrective action are appropriately documented and report them to BSI's Privacy Officers (Chris Davis or Darren Horne).

## BRIEF

The following information will be included when the Privacy Officers files a report to the Client:

- ✓ The nature and scope of the privacy breach (e.g., how many people are affected, what type of personal information is involved, the extent to which you have contained the breach) or, if the nature and scope are not known at the time of the briefing, that they are still to be determined.
- ✓ What steps you have already taken, or will be taking, to manage the privacy breach.
- ✓ Our plans to notify the individuals affected by the privacy breach and, if appropriate, other parties.
- ✓ Our timetable for providing senior management with regular updates about the breach and the ongoing management of it.

**NO EMPLOYEE NAMES ARE EVER GIVEN TO THE CLIENT IN BREACH REPORTS YOUR IDENTITY WILL REMAIN CONFIDENTIAL.**

---

## STEP 2: NOTIFY

### Ok, so we definitely have a breach...now what?

Following a full response and containment of the situation as outlined in **STEP 1**, we must now notify the individual(s) whose personal information was affected by the privacy breach, except in situations when notice is not appropriate or possible (e.g. identities of individuals affected by the breach are unknown, contact information is unavailable, or if notice would interfere with a law enforcement investigation).

The purpose of providing notice of a privacy breach to the affected individual(s) is to provide them with sufficient information about:

- ✓ What happened and when;
- ✓ If possible, a generic description of the types of personal information involved in the breach, including whether any unique identifiers or sensitive personal information were involved in the breach;
- ✓ The nature of potential or actual risks of harm;
- ✓ What action we have taken to address the situation.

Try and notify the individual(s) as soon as reasonably possible. During the notification process, there are many factors and details to be considered, some of which will be situation specific. Examples include;

- ✓ ensuring that we only provide notification when the facts of the situation have been confirmed and well documented to avoid passing on faulty information and making the situation worse;
- ✓ making sure notice is being provided to the right person;
- ✓ determining if a personal representative or other authorized parties need to be notified if the individual(s) in question cannot receive the notification for any reason (capacity, age, language, etc.);
- ✓ if notifying by telephone create a script so the same information is always given ensuring accuracy and consistency and be sure to clearly identify BSI and contact information (toll-free number, website address, postal, etc.); or
- ✓ if notifying in writing, make the letter clear and concise, use BSI's letter head and envelopes, and send by mail to the last known mailing address, deliver it personally, or send by means that can prove receipt of mail such as requiring a "signature upon receipt"

By keeping the individual(s) affected by the breach aware of the situation by notifying them, we fulfill our collective responsibility to protect the privacy of individuals with respect to personal information. Be sure to advise the individual(s) of their right to contact the Client directly about BSI's handling of their information and provide contact information for the individuals at the Client that were notified of the breach, should they wish to pursue matters.

### STEP 3: INVESTIGATE

#### What went wrong?

After we've responded to and contained the breach, an investigation is the next step. In most circumstances BSI will be responsible for investigating its own privacy breaches. An internal investigation must:

1. **identify and analyze** the events that led to the privacy breach;
2. **evaluate** what we did to contain it; and
3. **recommend** remedial action to help prevent future breaches.

The BSI Privacy Officers (Chris Davis or Darren Horne) will handle the documentation at this point. Any assistance you can give during the investigation to help fulfill the above requirements should be provided to the BSI Privacy Officers.

There are instances in which BSI may not be responsible for the investigation and an external inquiry will be carried out. In these cases the Client may dictate who will be conducting the process. In the event that the Client has one of their representatives conduct the process to investigate our privacy breach, cooperate fully with their efforts and provide all relevant information.

---

### STEP 4 IMPLEMENT CHANGE

#### We know what went wrong...now how can we fix it?

The most vital outcome of any privacy breach should be an understanding of what went wrong and how to prevent and avoid breaches in the future. The BSI Privacy Officers (Chris Davis and Darren Horne) will take part in this process.

A meeting with all parties involved in the breach process will follow any breach once it has been fully contained, documented, and investigated. This will help the BSI Privacy Officers evaluate our existing

Privacy/security measures and our incident-handling process, while identifying areas and conduct needing change and improvement.

When determining what changes and remedial action needs to be implemented, some improvements may require us to:

- ✓ review our relevant information management systems to enhance compliance;
- ✓ amend or reinforce our existing policies and practices for managing and safeguarding personal information;
- ✓ develop and implement new security or privacy measures;
- ✓ train our staff on legislative requirements, security and privacy policies, practices and procedures to reduce the potential of future breaches; or
- ✓ test and evaluate remedial actions to determine if they have been implemented
- ✓ Correctly, and if our policies and practices need to be modified.

In addition, whether the notice provided to the affected individual(s) was effective will also be evaluated. The BSI Privacy Officers will discuss whether the notice was done in a reasonably timely manner, whether the tone and content of the notice was appropriate, and if there was sufficient support provided to data subjects.

Chris Davis  
chris@bailiffservicesinc.ca

Last update: January 26,2021