INFORMATION INCIDENT CHECKLIST FOR EMPLOYEES

Information incidents occur when unwanted or unexpected events threaten privacy or information security. They can be accidental or deliberate and include the theft, loss, alteration of destruction of information.

An information incident can be especially serious when it is a **privacy breach**, which occurs when the compromised data includes personal information such as names, birthdates, health or financial details, or social insurance numbers. An information incident can also involve information technology, such as lost or stolen devices (e.g. laptops, cellular phones), IT system related issues, viruses and/or exposures of confidential government information (e.g. cabinet confidences, legal opinion information, etc).

The following checklist provides high-level guidance to employees for responding to information incidents (For more detailed information, see the *Information Incident Management Process* and the *Process for Responding to Privacy Breaches* at http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-incidents).

What to expect

After you report an information incident to the Shared Services BC Service Desk, you will be contacted by an investigator, who will gather information from you and will provide guidance and advice on actions that need to be taken to resolve the incident. The investigator will be seeking information and providing guidance focused on:

- Containing the incident (and recovering the information wherever possible);
- Assessing the potential harm to individual(s) who may be affected by the information incident and whether those person(s) may need to be notified about the incident; and
- Preventing similar incidents from occurring in future.

The ministry or business area responsible for the incident is responsible for taking action to contain the incident, notify where appropriate, and prevent similar incidents from occurring in future. The ministry or business area is also responsible for working collaboratively with the investigator and for keeping and maintain records regarding the information incident itself and the steps taken to revolve it.

Common actions that can help prevent similar incidents from occurring in future include:

- Having staff take mandatory and refresher training on information management topics such as privacy, access, and records management;
- Coaching staff who may have made an error that caused an incident on steps they can take to avoid a similar error;
- Identifying and correcting weaknesses that contribute to information incidents;
- Updating or developing new policy, procedures guidance for staff, and/or business processes; and
- Implementing recommendations from your investigator.

Any questions you have, including questions about information management training should be directed to your investigator.

Employee/Supervisors (including Service Providers)

- ☐ Employees notify supervisors, and supervisors provide direction with regard to the information incident. This is an urgent priority.
- ☐ The supervisor or employee immediately reports the information incident to the Shared Services BC Service Desk by calling 250 387-7000 or toll free at 1-866-660-0811 (available 24 hours a day) and selecting Option 3.

  Indicate that you are reporting a suspected information incident or privacy breach (where the incident involves personal information). You will receive a callback shortly by an investigator who will seek further information.

  The requirement for immediate reporting applies at *all times (24x7, 365 days a year)*, including after-hours, weekends and holidays.

- ☐ Take steps to contain the information incident, including recovering the information, wherever possible. Among other actions, this can also include suspending the activity that led to the incident or correcting the physical weakness that led to the incident.

  If the information incident involves information technology (i.e. IT system related issues, lost electronic devices, etc.), wait until contacted by an investigator before taking any action.

- ☐ Notify your Ministry Chief Information Officer.
- ☐ Ensure that the Risk Management Branch receives the General Incident Loss Report (GILR) within 24 hours (http://gilr.gov.bc.ca).
- ☐ Gather details regarding the information incident (the type of information affected and its sensitivity, whether the information was recovered, cause and extent of incident including how many individuals affected, dates of occurrence, business area involved, foreseeable harms and/or risks to individuals).
- ☐ Record the information incident file number provided to you by the investigator, **including the investigation case file # provided to you**. Keep all records, including both physical and electronic records, related to the information incident (including the steps taken to resolve the incident) stored in a single, confidential location.
- ☐ Complete additional responsibilities listed in the *Information Incident Management Process*[1].

[1] http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-incidents