Privacy Breach/Complaint Protocol

CONTEXT

A. Protocol Statement

In managing information, the Department of Justice has the responsibility to:

1) be accountable to the public for the information it collects and manages; and

2) protect the privacy of each individual whose information it holds, and to allow the individual access to that information.

B. Protocol Objectives

This protocol is divided into two parts. It is intended to assist employees in their response to
1) their discovery of a privacy breach or a breach of sensitive information (Part I); and
2) a complaint from an individual about an alleged privacy breach or breach of sensitive information (Part II).

C. Definitions

"Sensitive Information" means information which if disclosed could result in harm, disruption of government affairs or other negative consequences but does not include personal information. (Personal Information has its own definition.)

See the Department of Justice Privacy Policy for additional definitions.

D. Directive: Security Arrangements

The Department of Justice is responsible for protecting personal and sensitive information by making reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure or disposal.

E. Accountability

Employees are accountable for adhering to this Protocol.

Employees who are involved in the engagement of external agents or contractors by the DOJ are accountable for advising these parties that any breach or potential breach of personal or sensitive information must be immediately reported that employee.

Managers and supervisors are responsible for monitoring compliance with this Protocol and should address comments or concerns to both their immediate supervisor and the Information Access and Privacy (IAP) Administrator.

PART I

F. Procedures for Managing and Reporting a Privacy Breach

Step 1 – Identify the Breach and take Immediate Action to Contain or Remedy It
Step 2 – Notify the appropriate people about the Breach
Step 3 – Manage the Breach
Step 4 – Investigate and Document the Breach
Step 5 – Follow-up and Long Term Action

Step 1 – Identify the Breach and take immediate action to contain or remedy it

The employee responsible for the breach or the employee who discovers the breach must do his or her best to both identify what happened and to contain, minimize and remedy the damage from the breach. Some examples are as follows:

a) If an electronic data device is stolen the employee must notify security staff immediately.

b) If a fax is sent to the wrong number, the employee must call the recipient and ask them to destroy the document and any copies that were made.

c) If an e-mail is sent to the wrong person, the employee must call the recipient and ask them to securely destroy any e-mail printouts that were made and delete the e-mail. If the e-mail is sent through the GroupWise system, and has not been opened, the sender may delete the e-mail from the recipient's mailbox.

d) If an unauthorized person has or may have access to a database or computer system, notify the IT HelpDesk who can disable accounts or change passwords and identification numbers.

Step 2 – Notify the appropriate people about the Breach

The employee should report the incident as follows:

- To the police if a theft or other crime has occurred (*e.g.* office break-in, laptop or Blackberry stolen from car);
- To the employee's immediate supervisor;
- To the IAP Administrator who will help manage the breach;
- To legal counsel if it is a theft or other crime or if legal counsel have an interest in the documents or information at issue (court papers, sensitive documents);

- To the IT HelpDesk to have passwords reset or to have a lost or stolen device wiped;
- To the Finance and Administration Division if there has been a loss of a government asset (*e.g.* laptop).

Step 3 - Manage the Breach

The IAP Administrator is responsible for coordinating a departmental response to the incident and for making a decision, after appropriate consultation (for example, with legal counsel) whether to notify the Deputy Minister, Director of Communications and/or the individual(s) whose personal information was the subject of the breach.

Employees involved in the breach (or their supervisor) should stay in contact with the IAP Administrator.

Step 4 – Investigate and Document the Breach

The employee's supervisor must:

- document the breach (see the suggested form at the end of this Appendix);
- Follow-up on the breach which may include documenting:
    - recovery of the record or data device
    - identification of any additional loss of information.

Step 5 - Follow-up and long term action

The IAP Administrator will review the circumstances of the breach to determine if policies, procedures or work practices are adequate to protect personal and sensitive information and to prevent future breaches.

Together with staff, the IAP Administrator will determine what, if any, follow-up and long-term remedial action is necessary to prevent the breach from occurring again. This includes considering whether the privacy breach protocol was followed and whether any new or amended policies, procedures or work practices are required or if any training is required to prevent reoccurrence of the breach.

PART II

G. Privacy Complaint Protocol

Employees may receive a call, email or letter from a citizen or another employee complaining of an alleged breach to that person's personal information or a breach of sensitive information. Getting as much detail as possible and notifying the right people is the key to handling this type of communication.

Step 1 - Receive and Document the complaint

a) When a complaint is received by telephone or in person, discuss the details of the alleged breach with the complainant and document what the complainant believes has happened. This is a critical first step and should be completed in writing so that it can form part of the Department's record response to the complaint. (For a suggestion of information to gather, see the form at the end of this Appendix.)

b) When a complaint is received by email or letter, or once you have captured in writing the details given to you by phone or in person, forward the complaint to your supervisor for appropriate action.

Step 2 – Notify the appropriate people

The supervisor should report the complaint to the IAP Administrator.

The IAP Administrator will coordinate a departmental response and will make a decision, after appropriate consultation, whether to notify the Deputy Minister, Director of Communications or others.

Step 3 - Complainant Communication

Communication with the complainant should be done in consultation with the IAP Administrator. The Supervisor or other employee responsible for responding to the complaint (for example, the Director or Executive Director) should incorporate the following into the complaint procedure:

a) Send written acknowledgement to the complainant, restating the details presented by the complainant and indicating who will be performing an investigation.

b) If necessary, send a written update of progress of the investigation (stage of investigation, follow-up activities, expected or updated time frames, etc.). Do this after no more than two months has elapsed since the initial acknowledgement.

c) Generate a report of the results of the investigation. At a minimum, the report should include:
- Verification of the breach
- Mitigating activities
- Other follow-up activities

Step 4 – Continue to keep the IAP Administrator informed of any follow up correspondence (from you or the complainant) and any progress on promised or anticipated changes to policies, procedures or work practices.

Information Breach Reporting Form

Please complete this document and provide the completed and signed document to the Information Access and Privacy (IAP) Administrator. Treat the information you collect about a breach as highly confidential. You do not want to further the breach by sharing the information more broadly than absolutely required.

1. **Breach of (check one):**

   ❍ Personal Information
   ❍ Sensitive Information
   ❍ Both

2. **Documented by:**

3. **Date and time of breach:**

4. **Breach reported by:**

5. **Person responsible for breach**:

6. **Details of breach:**

7. **If personal information was involved in breach, please provide details:**

9. **Location of breach:**

10. **Notifications to individuals:** (include name and date):

11. **Notes of discussions:**

12. **Follow-up:**

13. **Signatures**

Completed by	**Date**
Employee responsible for breach	**Date**
Supervisor/Manager	**Date**

TO BE COMPLETED BY THE
INFORMATION ACCESS AND PRIVACY (IAP) ADMINISTRATOR

Outcome:

Date Closed:

_____

Signature Date