Privacy Breach Procedure

Purpose:

The EPS acknowledges the importance of protecting personal information and recognizes that occasionally personal information may be mistakenly or intentionally collected, retained, used, disclosed, or disposed of in ways that are not in accordance with the *Access to Information Act (ATIA)*. The guidance provided in this protocol ensures that when these privacy breaches occur, they are quickly contained, and future privacy breaches are prevented from occurring.

This procedure applies to all sworn and civilian EPS employees and establishes guidelines for managing the improper (inadvertent or deliberate) disclosure of personal information, including providing guidance to employees in relation to reporting, investigating, documenting, and determining the severity of privacy breaches.

Definitions:

Definitions listed in this section apply to this document only with no implied or intended organization-wide or EPS Policy and Procedure Manual wide use.

Personal Information – Personal information is defined in section 1(n) of the *ATIA.* It is defined as recorded information about an identifiable individual, including (but not limited to) the individual's name, home or business address or home or business telephone number, the individual's race, national or ethnic origin, religious or political beliefs or associations, the individual's age, sex, marital or family status, information about the individual's educational, financial, employment or criminal history, anyone else's opinions about the individual, etc.

Privacy Breach – The loss, unauthorized access, or unauthorized disclosure of personal information or individually identifying health information. A breach may be the result of inadvertent errors or deliberate actions by employees, agents, contractors, third parties, partners in information sharing agreements, or intruders. Breaches also encompass the improper disposal of any printed or digital documents related to the personal information listed above. The EPS categorizes privacy breaches into three levels:

1. **Low Level Breach** – Basic personal information such as name, picture, date of birth, or salary the release of which, while causing annoyance or inconvenience, is unlikely to result in significant or lasting harm. Low level breaches are breaches that only involve EPS employees and the release of personal information internally (within EPS only).

2. **Medium Level Breach** – Sensitive personal information including, but not limited to, personnel records, minor health information or financial records that may result in significant harm. This level of privacy breach is characterized by the information listed above getting shared externally.

3. **High Level Breach** – Comprehensive, detailed personal information such as:

    a. banking records, social insurance number, payroll information, detailed health information, family information, etc.

    b. Release and/or use of criminal information, including but not limited to, the disclosure of criminal record checks and release of information from criminal intelligence databases (CPIC, JOIN, NICHE, INet viewer).

    Often this level of privacy breach is characterized by information being shared externally and usually involves the release of a significant amount of personal information and/or involves many individuals.

Procedure:

A. General

1. Circumstances that could lead to a real or potential privacy breach include, but are not limited to:

    a. Theft loss or disappearance of equipment or devices containing personal information (e.g. cellphones, personal computers, laptops, external memory drives, USB memory sticks, electronic devices, photocopiers, CD-ROMS, file cabinets, briefcases, and fax machines).

    b. Release and/or use of personal information to an unintended or inappropriate recipient or group. Examples include but are not limited to:

        i. Accessing file information in the RMS without an appropriate investigative or administrative reason,

        ii. allowing file/report information displayed on a monitor to be read by third parties (without an appropriate investigative or administrative reason), or

        iii. allowing another person to use one's username and password to sign-on to the EPS network.

    c. The use of equipment or devices to transport/store personal information outside the office without adequate security measures.

d. Intrusions that result in unauthorized access to personal information held in buildings, file storage containers, computer applications, systems, or other equipment and devices holding personal information.

e. Faulty departmental procedures or operational breakdowns.

f. Insufficient controls in place to protect personal information in paper and electronic files.

2. If a breach is discovered, it will be reported to the Information and Privacy Unit (IAPU). IAPU will keep a record of the breach for tracking and training purposes and refer the matter to Human Resources Division (HRD) if it involves civilian employees or Professional Standards Branch (PSB) if it involves sworn members.

3. Following the resolution of any privacy breach, IAPU will conduct a review and determine what steps to take to reduce or eliminate a similar breach from reoccurring. IAPU, however, will not conduct investigations into privacy breaches.

B. Employee Responsibilities

Upon learning of or discovering an actual or potential privacy breach, and regardless of whether the matter seems minor, employees must report it to their supervisor or manager as soon as possible. In addition, the employees must take steps to try and contain the breach. These steps may include but are not limited to following:

1. The supervisor or manager will confirm that a privacy breach has occurred and will follow **Appendix E - Privacy Breach Internal Guidance**, including notifying EPS's Information and Privacy Coordinator.

2. In the absence of the Information and Privacy Coordinator, the notification can be made to the Manager i/c Administrative Police Information Section or any Senior IAPU Analyst.

3. The privacy breach level of seriousness (low, medium, or high) will be determined by the Information and Privacy Coordinator (or their designate) in consultation with the affected area.

4. Supervisors and managers are responsible for preventing further breaches in relation to the affected information. Breaches determined to be high level (and in some cases medium level) must be mitigated as soon as possible.

5. Supervisors and managers will work with the Information and Privacy Coordinator in determining any notification requirements in relation to those affected by medium or high-level breaches. Efforts will be made to

notify the affected individuals or groups as soon as possible. Low level breach notifications to affected parties will be done in consultation with the Information and Privacy Coordinator, as soon as practicable.

C. Further Escalations

1. The Information and Privacy Coordinator will determine if the Chief of Police should be notified of a privacy breach.

2. EPS is not required by law to notify the Office of the Information and Privacy Commissioner (OIPC); however, the OIPC does advise public bodies to voluntarily report privacy breaches to the Commissioner. The Information and Privacy Coordinator will work with the Manager i/c Administrative Police Information Section to determine if the OIPC should be notified.

D. Monitoring Trends

1. The Information and Privacy Coordinator is responsible for monitoring of privacy breach trends upon review of resolved cases. Training provided by IAPU will be adjusted based on review of these trends to prevent future breaches.

2. If PSB and HRD identify trends resulting from their investigations, they must share them with IAPU to improve privacy training and awareness.

Review:	Revision Date:	No.:
	2024 April 04	**SD24-007**
	2025 July 31	
	2026 September 08	**SD26-019**

Related Information:

Forms:	Privacy Breach Reporting Form
Appendices:	IS - Appendix E - Privacy Breach Internal Guidance