Corporate Policies and Procedures			
DEPARTMENT: INFORMATION TECHNOLOGY			**POLICY #:** IT-10
POLICY: Email Security and Breach Protocol			
DATE: AUG/2013	**REV. DATE:** April 2017	**COVERAGE:** All Employees	**PAGE #:** 1 of 5

POLICY STATEMENT:

This policy provides guidance to all County of Renfrew employees for the transmission, storage and encryption requirements when corporate data is transmitted or stored electronically outside of the County of Renfrew network. It is the responsibility of the Department Head to classify data for their department and respective divisions.

DEFINITIONS:

Highly Confidential Data

Highly Confidential Data is information protected by legislation. Information protected by the Personal Health Information Protection Act (PHIPA), Health Information Protection Act (HIPA), Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), Personal Information Protection and Electronic Documents Act (PIPEDA) or contract and shall only be disclosed as per the legislative direction. Disclosure must be authorized by a Department Head or delegate.

For more information regarding legislation please consult the following links:

- Personal Health Information Protection Act (PHIPA)
  https://www.ipc.on.ca/english/phipa/

- Health Information Protection Act (HIPA)
  http://www.ontla.on.ca/web/bills/bills_detail.do?locale=en&BillID=3438

- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
  https://www.ontario.ca/laws/statute/90m56

- Personal Information Protection and Electronic Documents Act (PIPEDA)
  https://www.priv.gc.ca/leg_c/leg_c_p_e.asp

Confidential Data

Confidential Data is information that must be protected from unauthorized access due to privacy considerations and or business operations of the County of Renfrew.

Public Data

Public data is information that is open to the general public which may be stored or accessed from any public website or cloud provider.

PROCEDURE TO TRANSMIT DATA VIA THE COUNTY EMAIL SYSTEM:

1. **Data classified as Highly Confidential:**

   - It is the responsibility of the **employee to ensure they are not transmitting highly confidential data. If unsure, the employee should consult with their** Department Head to determine if the data is classified as Highly Confidential
   - **SHALL ONLY** be transmitted through the County email system via secure email attachment using the following procedure:
     - All highly confidential data shall be encrypted using an Adobe PDF document attachment. If an encrypted Adobe PDF attachment is not possible the sender must password protect the attachment (i.e. MS Word, Excel, Power Point…) before transmission
     - No highly confidential information shall be contained in the subject line or body of the email message
     - It is the sender's responsibility to verify that the recipient is a known contact and their identify can be verified
     - It is the sender's responsibility to ensure the password is sent in a separate email message or relayed via telephone to the recipient directly or to their designate

2. **Data classified as Confidential:**

   - It is the responsibility of the Department Head to determine if the data is classified as Confidential
   - **SHALL BE PERMITTED** to be transmitted via the County email system in an non password protected format

3. **Data classified as Public Data:**

   - It is the responsibility of the Department Head to determine if the data is classified as Public
   - **No restrictions**

PROCEDURE TO TRANSMIT DATA OUTSIDE OF THE COUNTY EMAIL SYSTEM:

- It is the responsibility of the Department Head to determine the classification of data as Highly Confidential, Confidential or Public
- It is the responsibility of the Department Head to ensure Highly Confidential Data **SHALL NOT** be posted on public websites, intranets or public domain
- Highly Confidential Data **SHALL BE PERMITTED** to be transferred via encrypted USB drive delivered via courier with Department Head approval**. It is the responsibility of the Department Head that the USB drive must comply with policy IT-08 Mobile Data Protection.**
- Data classified as Confidential **CAN BE** posted to the County's password protected Intranet for sharing with County of Renfrew staff only with Department Head approval

PROCEDURE FOR EMAIL BREACH:

The following procedure must be taken swiftly to address any email related privacy breach of data classified as highly confidential or confidential. It details the steps which will be taken to limit, to the extent possible, harm to individuals whose personal information has been compromised. Upon identification of a privacy breach, the Director of Human Resources must be immediately notified.

1. When an employee discovers that they have caused a privacy breach, they must immediately contact the recipient by email and phone, if possible, to confirm that the email was sent in error and request that the email be destroyed and confirm in writing to the County that they have done so. The email breach is then disclosed immediately by the employee responsible to their immediate Supervisor and Department Head.

2. The Department Head immediately notifies the Director of Human Resources and the Information Technology Manager. Any breach related to the Personal Health Information Protection Act or the Health Information Protection Act requires notification also be made to either the Director of Emergency Services, the Director of Long Term Care or the Director of Social Services as applicable.

3. The Director of Human Resources, **in consultation with the affected Department Head,** conducts an investigation to determine:

    - How many individuals' personal information was affected;
    - How many individuals received the personal information;
    - What type of information was disclosed, and what risks arise from the disclosure if one of the recipients were to misuse the information;
    - What type and extent of harm may arise for the affected individuals from the disclosure?
    - What factors contributed to the mistake – was it a system error, a lack of caution, or did it arise from other factors?

4. The Director of Human Resources determines whether the circumstances of the breach give rise to a real risk of significant harm. If so, the Director of Human Resources notifies affected individuals, and the Privacy Commissioner. If the circumstances do not give rise to a real risk of significant harm, the Director of Human Resources may decide to notify affected individuals and/or the Privacy Commissioner in any event.

5. The Director of Human Resources drafts notifications to the affected individuals as per SOP IT-88 Privacy Breach Response Protocol.

6. The Director of Human Resources then notifies the County's insurers and legal counsel.

7. The Director of Human Resources drafts a report of the breach, the investigation, notification, and remediation/mitigation steps for the privacy commissioner.

   The County takes any necessary steps to reduce the possibility of future similar breaches, such as revised policies and/or training for staff, improved technical safeguards or changes to system options where necessary.

Standard Operating Procedure			
SECTION: Information Technology			**SOP#:** IT-88
POLICY: PRIVACY BREACH RESPONSE PROTOCOL			
DATE: August 2016	**REV. DATE:** April 2017	**COVERAGE:** Human Resources & Information Technology	**PAGE #:** 1 of 5

Definition of a 'Privacy Breach': Unauthorized access to or collection, use, or disclosure of personal information. Activity is deemed "unauthorized" if it occurs in contravention of applicable privacy laws or regulations. A privacy breach may be a consequence of faulty business procedure, lack of a security safeguard, operational break-down, human error or deliberate action.

OPERATING PROCEDURE STATEMENT

This Policy is intended to guide The County of Renfrew (the "County") in taking swift and appropriate action to address any privacy breach. It details the steps which will be taken to limit, to the extent possible, harm to individuals whose personal information has been compromised. Upon identification of a privacy breach, the Director of Human Resources must be immediately notified.

STEPS FOR RESPONDING TO A PRIVACY BREACH

A. Breach Containment and Preliminary Assessment

Immediate steps will be taken to contain the breach and its consequences, including:

- Contain the breach, which may include: terminating the activity or practice resulting in the breach, shutting down the affected system, terminating access to computer systems, or restoring physical or electronic security.
- Identify the individual who will lead the investigation, both at the preliminary stage and at the more detailed stages, if required.
- Where necessary, assemble a breach response team, which may include representatives from various areas of the County, as well as external legal and/or technical supports.
- Identify who needs to be informed of the breach, internally and externally.
- Notify police if criminal activity is suspected.
- Preserve evidence of the breach. While containment is the priority, care should be taken to ensure that evidence of the breach is not lost. Evidence may be required both to investigate and address the breach, and in the event of litigation.

B. Investigation and Risk Assessment

An investigation will be conducted to determine the cause and extent of the breach.

- Determine the cause of the breach. This may require assistance from outside professionals, including for example IT forensic professionals.
- Determine whether there is a risk of further breaches or whether the breach was an isolated incident.
- Determine how many individuals were affected by the breach, and identify the affected individuals.
- Determine how much information was accessed, used or disclosed improperly, and the manner of that access, use or disclosure. Determine the probable extent of dissemination of the information in question.
- Identify the nature of the information which was accessed, used or disclosed improperly, in order to support an assessment of the risks and extent of probable harm arising from the breach.
- If possible, take all reasonable steps to recover personal information which was lost or disclosed. Contact the recipients of inadvertently disclosed personal information and ask them to delete the information.

The following factors will be considered in assessing the risks associated with the breach:

- The extent of the information disclosed or accessed;
- In the case of disclosure, the number of recipients and/or probability of public disclosure;
- The sensitivity of the information involved. Particularly sensitive information includes health information, social insurance numbers, drivers' license numbers, health card numbers, credit card numbers or other financial information.
- Whether or not the information was encrypted, partially or fully anonymized or whether it would otherwise be challenging in some way to misuse.
- The likelihood that information could be used for fraudulent purposes - for example, date of birth in combination with address and biographical information may increase the risk of identity theft.

- The nature of the harm which would result from public disclosure of the information: for example, fraud, reputational harm, or embarrassment.
- Whether recipients or individuals who have accessed the information improperly are likely to have disclosed or used further or whether their assurances of deletion and return of the information are reliable.
- Assess the likely effectiveness of steps taken to mitigate harm from the breach.

3. Individual Notification

Individuals affected by a privacy breach will be notified where the breach gives rise to a real risk of significant harm. "Significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property. The County will assess whether there is a "real risk" of such harm based on the factors set out above. The County may seek advice from outside experts in making the determination of whether notification is necessary. **Individuals will always be notified where there is any release of personal health information.**

(i) Procedure to Notify Individuals

After all necessary facts have been obtained, the County will make a proper determination as to whether individual notification is required.

Once it is determined that notifying individuals is necessary, notification of those affected shall occur as soon as reasonably possible after the County confirms the occurrence of the breach and concludes through investigation that it is required to give notice. If police are involved in the investigation, the County will take direction from police as to whether notification should be delayed to permit the police to conclude their investigation.

The County will determine in all the circumstances the appropriate manner for notification, with a view to the manner which is most likely to come to the attention of the affected individuals. One or more forms of notification may be appropriate. Direct notification of affected individuals by phone, letter and/or email is preferable where possible. Where direct notification would cause further harm or is otherwise not reasonably possible, indirect notification through the County's website or the media will be considered.

(ii) Content of Notification

The content of notifications will vary depending on the particular breach and the method of notification chosen. The notification must contain enough information to allow the individual to understand the significance of the breach to them and to take steps to mitigate that harm. The notice should include, as appropriate:

- A description of the incident and its timing.
- A description of the personal information involved in the breach.
- An account of what the County has done to control or reduce the harm.
- A description of how the County plans to assist individuals affected and what steps individuals can take to avoid or reduce the risk of harm. Possible actions include arranging for credit monitoring services
- Information designed to assist individuals in further protecting themselves against identity theft.
- Contact information of an individual within the County who can answer questions or provide further information.
- If applicable, information on whether the County has notified a privacy commissioner's office.
- Additional contact information for the individual to address any privacy concerns to the County, and
- Contact information for the appropriate privacy commissioner(s).

(iii) Others to Contact

(a) The County will notify its insurer of the breach as early as possible in accordance with any applicable provisions of its insurance policy.
(b) The County will notify the applicable Privacy Commissioner when there is a real risk of significant harm. The County may elect to notify the Privacy Commissioner even in other circumstances.
(c) If theft or other crime is suspected, the police will be notified.
(d) Where the breach involves health information and implicates a regulated health professional, the County may notify the regulatory body in accordance with statutory requirements under the applicable legislation and/or *PHIPA*.
(e) Where financial information is involved, credit card companies or financial institutions may be notified if their assistance is needed.
(f) Third parties who may be implicated in or affected by the breach, or other interested parties.

4. Prevention of Future Breaches

The County's investigation into the breach will include a consideration of what steps might be taken to prevent future breaches. These steps might include changes to the physical, technical, or administrative safeguards in place to protect the information, such as:

- Modifications to both physical and technical security;
- changes to policies and procedures and any changes to reflect the lessons learned from the incident and investigation (e.g., security policies, privacy policies, record retention policies, etc.); and
- additional training for employees.