Call2Recycle Canada, Inc.

Changing habits. Inspiring action.™

Policy for handling confidentiality incidents and confidentiality incident response plan

Purpose and scope

The purpose of this policy for handling confidentiality incidents and incident response plan is to ensure that Call2Recycle Canada Inc. ("**Call2Recycle**") is prepared to manage privacy incidents and cyberincidents in an effective manner and in accordance with the new obligations brought about by the "Act to modernize legislative provisions as regards the protection of personal information", commonly known as "Bill 25".

This document describes Call2Recycle's general policy for handling confidentiality incidents and confidentiality incident response plan. It defines the structure, roles and responsibilities, common types of incidents, and the approach to prepare for, identify, contain, and learn from privacy and cybersecurity incidents to minimize the impact of incidents.

The purpose of the policy and incident response plan is to ensure that Call2Recycle is organized to respond to privacy and/or cybersecurity incidents in an effective manner.

This policy and incident response plan apply to all Call2Recycle's networks, systems and data, as well as to stakeholders (including employees and third-party vendors) who access them.

This document defines incident handling and response capabilities and identifies the appropriate response to common cybersecurity incidents that will occur. This document is not intended to provide a detailed list of all activities to be performed in response to cybersecurity incidents, but rather a general overview of the essential steps to be followed in the event of a cyberincident.

Definitions

Confidentiality Incident: a confidentiality incident is defined as:

(1) access not authorized by law to personal information;
(2) use not authorized by law of personal information;
(3) communication not authorized by law of personal information; or
(4) loss of personal information or any other breach of the protection of such information.

Person in charge of the protection of personal information: the person in charge of the protection of personal information refers to the person exercising the highest authority shall see to ensuring that Bill 25 is implemented and complied with. That person shall exercise the function of person in charge of the protection of personal information; he or she may delegate all or part of that function in writing to any person.

Personal Information : any information which relates to a natural person and allows that person to be identified.

Malware: umbrella term that describes any malicious program or code that is harmful to systems.

Virus: a virus can infect the computer and other devices, but it can also reappear and infect the devices of other people, including those on a contact list.

Worm: malware that is not attached to a file and can self-activate to make copies without any action required.

Trojan Horse: malware disguised in legitimate software.

Spyware or adware: malware that collects personal information about the user's online activity for the benefit of a third party.

Ransomware: malware that locks the device and the data it contains in exchange for a sum of money or all data will be erased.

Contact Persons

The responsibility for the security of confidential information, including personal information, is everyone's business. In the event of a confidentiality incident the person responsible is:

Michael Partab
437-290-0096
privacy@call2recycle.ca

If the person responsible is unavailable, please contact:

Grace Wu
437-900-8546
gwu@call2recycle.ca

Computer firm mandated in case of IT problems:

Viviane Wans
416-307-2855
vwans@call2recycle.ca

In the event of a critical confidentiality incident, a crisis cell will meet quickly and is composed of the people mentioned in the table below.

Role	Name	Title	Telephone	Email
Privacy Officer	Michael Partab	Privacy Officer	437-290-0096	privacy@call2recycle.ca
Computer security / servers management	Viviane Wans	Director, Business Management	416-307-2855	vwans@call2recycle.ca
Communications management	Jon McQuaid	Vice President, Marketing, Communications, and Innovation	647-484-2672	jmcquaid@call2recycle.ca

Types of confidentiality incidents

A cybersecurity or confidentiality incident may not be immediately recognized; however, there are indicators that may be signs of a security breach, compromised system or unauthorized activity, or signs of misuse within your or your third-party service providers' environment.

Always be on the lookout for signs that a security incident has occurred or is in progress. Some of these indicators are described below:

1. Excessive or unusual login and system activity, especially from any inactive user IDs (user accounts).
2. Excessive or unusual remote access within your organization. This may include staff or third party vendors.
3. The appearance of any new wireless (wifi) network visible or accessible from your environment.
4. Unusual activity related to malware, suspicious files, or new or unapproved files and executable programs. This could be on your networks or systems, including web-based systems.
5. Hardware or software key loggers connected to or installed on systems.
6. Suspicious or unusual activity on or behavior of online systems, such as e-commerce sites.
7. Lost, stolen, or misplaced merchant copy receipts or other documentation showing the full payment card number or card security code (three or four digit number printed on the card).

8. Lost, stolen, or misplaced computers, hard disk drives, or other media that contain payment card data or other sensitive data.

Early prevention

The following recommendations should be followed:

- Use 2-factor authentication, or any other more secure authentication method, to access any server or software hosting confidential and/or sensitive data, including personal information.
- Perform privacy incident simulations.
- Prohibit the storage of documents on the computer's hard drive. Documents must be stored on appropriate cloud servers.
- Be on the lookout for any phishing attempts, fraudulent e-mails or e-mails with suspicious files, and ask employees to notify the privacy officer in such cases.
- Use a variety of passwords, alternating numbers, letters and symbols.
- Be careful not to use the same password repeatedly.
- Obtain approval from a company official before downloading software onto the computer.
- Provide training, if necessary, to equip employees to better spot suspicious e-mails or files.
- Validate which information needs to be archived and which can be destroyed.
- Properly destroy information that is no longer valid or necessary.
- Consider setting up an internal e-mail address so that employees can quickly identify and report cybersecurity problems, to prevent e-mails from becoming diluted.
- Take out insurance against cyber risks and breaches of confidentiality.
- Establish a model for communicating incidents when the regulator needs to be notified.

Incident severity levels

Category	Indicators	Scope
1 - Critical	Data loss/theft, malware	Generalized or with critical servers, or loss of data, stolen data, unauthorized access and use of data
2 – High	Theoretical threat becomes active	Generalized or with critical servers, or loss of data, stolen data, unauthorized access and use of data

3 – Moderate	Email phishing or infection by general propagation	Generalized
4 - Low	Localized phishing (often a financial request)	Individual host or person

Action plan

Event	Example	Procedure to follow	Severity level
Loss of an electronic device	Employee loses or has his cell phone or work computer stolen	Procedure A	Low to High
Unauthorized access or use	An individual gains unauthorized physical or computer access to the network, system or data (sending an e-mail to the wrong recipient)	Procedure B	Low to High
Malware	Installation of malware (e.g. virus, worm, Trojan horse or other code)	Procedure C	Critical
nability to access information (ransomware)	A specific type of malware that infects a computer and displays messages demanding payment of a sum of money in exchange for system recovery.	Procedure D	Moderate to High
Malicious unauthorized access	Theft of customer/employee personal data	Procedure E	Critical

Procedure A

1. Notify the Privacy Officer as soon as the loss or theft occurs.
2. Immediately change passwords for the employee's e-mail account and any cloud server, and ensure that 2-factor authentication or any other more secure authentication method is enabled.
3. Validate whether documents containing personal information were on the computer's hard drive.
    a. In the case of personal information:
        i. May serious harm be caused? To assess the damage: what is the sensitivity of the information concerned, the apprehended consequences of its use and the likelihood that it will be used for harmful

purposes? It is advisable to call in experts to determine whether there is a risk of serious harm.

ii. If there is risk of serious harm: notify the regulator and any concerned person (provided no investigation is hindered)

b. If no personal information was compromised, **go to step 4**.

c. If it is not possible to determine with certainty the type of information to which the individual has had access
   i. Treat the event as if it were personal information
   ii. May serious harm be caused? To assess the damage: what is the sensitivity of the information concerned, the apprehended consequences of its use and the likelihood that it will be used for harmful purposes? It is advisable to call in experts to determine whether there is a risk of serious harm.
   iii. If there is risk of serious harm: notify the regulator and any concerned person (provided no investigation is hindered).

4. Record the event in the confidentialty incident register without delay.
5. Be on the lookout for suspicious events or suspicious e-mails in the weeks or months following the loss/stolen device.
6. Implement reasonable preventive measures for any future situation.

Procedure B

1. Notify the Privacy Officer as soon as discovery is made that an individual has had unauthorized access.
2. Immediately block access to the individual concerned and/or ask such individual to delete all data obtained and obtain confirmation of destruction.
3. Determine what information has been subject to the confidentiality incident, if necessary by calling in a specialized IT firm.
   a. In the case of personal information:
      i. May serious harm be caused? To assess the damage: what is the sensitivity of the information concerned, the apprehended consequences of its use and the likelihood that it will be used for harmful purposes? It is advisable to call in experts to determine whether there is a risk of serious harm.
      ii. If there is risk of serious harm: notify the regulator and any concerned person (provided no investigation is hindered)

   b. If no personal information was compromised, **go to step 4**.

   c. If it is not possible to determine with certainty the type of information to which the individual has had access
      i. Treat the event as if it were personal information

ii. May serious harm be caused? To assess the damage: what is the sensitivity of the information concerned, the apprehended consequences of its use and the likelihood that it will be used for harmful purposes? It is advisable to call in experts to determine whether there is a risk of serious harm.
iii. If there is risk of serious harm: notify the regulator and any concerned person (provided no investigation is hindered).

4. Conduct internal follow-up to understand how the situation arose and implement reasonable preventive measures.
5. Record the event in the confidentialty incident register without delay.

Procedure C

1. Do not take any action (do not enter personal and/or banking information under any circumstances) and immediately notify the Privacy Officer.
2. The Privacy Officer immediately contacts an IT firm and follows its recommendations.
3. Notify employees of the computer attack in progress, and pass on the IT firm's recommendations without delay.
4. Determine which information was subject to the confidentiality incident with the help of the specialized IT firm.
    a. In the case of personal information:
        i. May serious harm be caused? To assess the damage: what is the sensitivity of the information concerned, the apprehended consequences of its use and the likelihood that it will be used for harmful purposes? It is advisable to call in experts to determine whether there is a risk of serious harm.
        ii. If there is risk of serious harm: notify the regulator and any concerned person (provided no investigation is hindered)

    b. If no personal information was compromised, **go to step 5**.

    c. If it is not possible to determine with certainty the type of information to which the individual has had access
        i. Treat the event as if it were personal information
        ii. May serious harm be caused? To assess the damage: what is the sensitivity of the information concerned, the apprehended consequences of its use and the likelihood that it will be used for harmful purposes? It is advisable to call in experts to determine whether there is a risk of serious harm.
        iii. If there is risk of serious harm: notify the regulator and any concerned person (provided no investigation is hindered).

5. Conduct internal follow-up to understand how the situation arose and implement reasonable preventive measures.

6. Record the event in the confidentialty incident register without delay.

Procedure D

1. Do not take any action (do not enter personal and/or banking information under any circumstances) and immediately notify the Privacy Officer.
2. The Privacy Officer immediately contacts an IT firm and follows its recommendations.
3. Warn employees that a ransomware attempt is underway, and ask them to be extremely vigilant.
4. Evaluate with the help of the IT firm whether personal information may have been compromised by the ransomware.
    a. In the case of personal information:
        i. May serious harm be caused? To assess the damage: what is the sensitivity of the information concerned, the apprehended consequences of its use and the likelihood that it will be used for harmful purposes? It is advisable to call in experts to determine whether there is a risk of serious harm.
        ii. If there is risk of serious harm: notify the regulator and any concerned person (provided no investigation is hindered)

    b. If no personal information was compromised, **go to step 5**.

    c. If it is not possible to determine with certainty the type of information to which the individual has had access
        i. Treat the event as if it were personal information
        ii. May serious harm be caused? To assess the damage: what is the sensitivity of the information concerned, the apprehended consequences of its use and the likelihood that it will be used for harmful purposes? It is advisable to call in experts to determine whether there is a risk of serious harm.
        iii. If there is risk of serious harm: notify the regulator and any concerned person (provided no investigation is hindered).

5. Conduct internal follow-up to understand how the situation arose and implement reasonable preventive measures.
6. Record the event in the confidentialty incident register without delay.

Procedure E

1. Immediately notify the Privacy Officer.
2. The Privacy Officer contacts the IT firm and, if necessary, the police to report the data theft.
3. Block computer access for all employees while secure access is re-established, and warn staff of the situation and to be vigilant.

4. Evaluate with the help of the IT firm whether personal information may have been compromised.
    a. In the case of personal information:
        i. May serious harm be caused? To assess the damage: what is the sensitivity of the information concerned, the apprehended consequences of its use and the likelihood that it will be used for harmful purposes? It is advisable to call in experts to determine whether there is a risk of serious harm.
        ii. If there is risk of serious harm: notify the regulator and any concerned person (provided no investigation is hindered)

    b. If no personal information was compromised, **go to step 5**.

    c. If it is not possible to determine with certainty the type of information to which the individual has had access

        i. Treat the event as if it were personal information
        ii. May serious harm be caused? To assess the damage: what is the sensitivity of the information concerned, the apprehended consequences of its use and the likelihood that it will be used for harmful purposes? It is advisable to call in experts to determine whether there is a risk of serious harm.
        iii. If there is risk of serious harm: notify the regulator and any concerned person (provided no investigation is hindered).

5. Conduct internal follow-up to understand how the situation arose and implement reasonable preventive measures.
6. Record the event in the confidentialty incident register without delay.
7. Take reasonable steps to improve IT security measures.
8. Prepare a communications plan in preparation for questions from customers and/or employees affected by the data theft.