# Data Security Policy

## Description and Purpose

The activities of Call2Recycle Canada Inc. ("**Call2Recycle**") largely depend on information that is processed, produced and transmitted. Like any other organization, Call2Recycle may face threats to its confidentiality, integrity and availability of information. These threats include identity theft and theft of confidential information, fraud, industrial espionage, theft of intellectual property, the use, disclosure and destruction of information, technical failures, natural events and human error.

To meet its regulatory and legislative obligations, Call2Recycle hereby adopts, implements, maintains, and enforces this data security policy that establishes the implementation of formal data security processes to ensure risk management, access management and incident management of its confidential and personal information.

## General Provisions

1. Objective

    a. This policy is one of the key elements to ensure the realization of the mission and the business objectives of Call2Recycle, to maintain its reputation and to comply with the applicable legal, regulatory, and contractual requirements.

    b. The main objective of this policy is to communicate Call2Recycle's determination and commitment to managing data security risks effectively and efficiently. The approach adopted is aimed at identifying the stakeholders and defining their roles and raising user awareness of the risks of designing and implementing measures to effectively safeguard the security of information assets.

2. Scope

    a. This policy applies to all natural persons or legal persons who use or access the information resources of Call2Recycle.

    b. This policy applies to all data that Call2Recycle holds while carrying out its functions or that it safeguards, throughout its lifecycle, regardless of the form, medium and location.

3. Guidelines

    a. The principles that orient Call2Recycle's approach, the distribution of responsibilities and the nature of actions and means put forth are as follows:

i. Availability
To the best of its abilities, Call2Recycle ensures the availability of the data it holds, so this information can be accessed in a timely fashion, and in the manner required by any authorized person.

ii. Integrity
To the best of its abilities, Call2Recycle ensures the integrity of information so that it cannot be destroyed or altered without authorization, and so that the information medium provides appropriate stability and durability.

iii. Confidentiality
Call2Recycle ensures that the disclosure of information is limited to those authorized to access it, thus ensuring strict confidentiality. To this end, Call2Recycle collects and retains only the information stated in its Privacy Policy; implements access control and profiles to ensure that only those persons, objects or technological entities identified as entitled and authorized shall have access to the information, in accordance with laws and regulations; and ensures that information, documents, equipment, or materials destined for disposal, declared as surplus property, containing out-of-date or unnecessary data or turned over to a service provider for maintenance, recycling, destruction, or other purposes are handled in accordance with the applicable processing and destruction procedure.

iv. Accountability
Call2Recycle's accountability applies to information assets, processes and systems under the owner's responsibility or control, including that delegated to a third party.

v. Proportionality
Call2Recycle puts reasonable measures in place to guarantee the confidentiality, integrity, and availability of information assets, at a cost proportionate to the sensitivity of the information and to the underlying risks.

vi. Awareness
Call2Recycle shall ensure that its employees are informed of risks and threats that may affect data security, enabling them to recognize potential incidents and risks and to understand their roles and responsibilities with respect to data security by developing appropriate skills and competencies.

**Particular Provisions**

4. Roles and responsibilities

    a. In this policy and its application, the following mandates are assigned to different stakeholders:

        i. Board of Directors: adopts this policy as well as any amendment thereto.

        ii. Board of Directors: acts as the primary forum for consultation on data security matters for Call2Recycle; formulates recommendations on the management framework, action plans and reviews; formulates proposals for action in matters of data security; formulates the data security policy and its updates, and coordinates its implementation; is involved in the implementation of data risk measures; develops and implements formal data security processes; formulates and implements data security awareness programs.

        iii. Privacy Officer: supervises the data security risk management process and the application of this policy; ensures the adequacy of the data security measures in effect, in relation to the risks incurred; ensures that measures are in place to reduce data security risks to a level deemed acceptable for the organization; is informed of Call2Recycle's actions in the area of data security; assists management in determining strategic orientations and intervention priorities; assists in implementation of the normative framework for information resources and risk mitigation measures; is Call2Recycle's first respondent for data security; is responsible for reporting, in compliance with legislative and regulatory requirements.

        iv. Human Resources Department: as applicable, conducts background checks of prospective candidates before hiring and of staff members involved with data security; ensures that the responsibilities of stakeholders concerning data security and compliance with this policy, as well as the normative framework for information resources, are included in the job descriptions of staff members; informs and obtains from all new employees of Call2Recycle their commitment to respect this policy; imposes appropriate sanctions when policies, rules and the code of conduct concerning data security are violated;

        v. IT Department: ensures the security of information assets, throughout their lifecycle, by deploying appropriate security measures; develops, integrates, and maintains safeguards appropriate to the level of sensitivity of the information concerned, as well as to other applicable business, legal, regulatory or contractual requirements, in the conduct of a development project or the acquisition of an information system.

vi. Users: comply with this data security policy and any guidelines pertaining to data security and the use of information assets; comply with security measures in effect, without seeking to circumvent, disable or modify them.

**Administrative Measures and Sanctions**

5. In the event of violation of this policy:

a. The user shall be personally responsible for any violation of this policy, as shall be any person who, whether through negligence or omission, causes information to be inadequately protected.

b. Any employee of Call2Recycle who violates the legal framework, this policy or data security measures stemming from it shall be subject to sanctions depending on the nature, seriousness, and repercussions of the violation, under the law or applicable internal disciplinary rules, up to and including dismissal.

c. Similarly, any violation by a supplier, partner, guest, consultant, or external organization shall be subject to sanctions as stipulated by contract with Call2Recycle or under the provisions of applicable law.

d. When an audit gives reason to believe that a law or regulation has been violated, the Privacy Officer may refer the file to any other competent authority to verify whether there are grounds for prosecution, among other things. The Privacy Officer may transmit to this authority any information collected during the verification or investigation.

e. In addition to the measures provided for in laws, regulations, policies or agreements, any violation of this policy may result, without limitation, in the following consequences, depending on the nature, seriousness and repercussions of the act or omission:
   i. Cancellation of access privileges to Call2Recycle's information assets. Such cancellation may be effective without notice depending on the nature and seriousness of the violation.
   ii. The obligation to reimburse Call2Recycle for any amount that the latter is obliged to pay because of unauthorized, fraudulent, or illicit use of its services or information assets.

**Final Dispositions**

6. Review

This policy shall be revised as needed, or in accordance with ongoing changes to legislative and regulatory obligations, considering new governmental orientations as well as the evolution of data security practices.

7. Policy application and monitoring

The Privacy Officer is responsible for the application of this policy.

8. Entry into force

This policy comes into effect on June 1, 2023.