Record Retention and Destruction, and Confidentiality Incidents Policy

Company Policy

TERMONT

Table of Contents

1 – PURPOSE

This Record Retention and Destruction, and Confidentiality Incidents Policy (the "Policy") serves various objectives. First, one purpose of this Policy is to ensure that necessary records and documents of TERMONT Montréal Inc. ("TERMONT") are adequately protected and maintained and to ensure that records that are no longer needed by TERMONT or are of no value are discarded at the proper time. This Policy is also for the purpose of aiding personnel in understanding their obligations in retaining paper and electronic documents - including e-mail, web files, text files, sound and movie files, PDF documents, and all Microsoft Office or other formatted files.

Second, another purpose of this Policy is to adopt a register to collect information regarding confidentiality incidents involving TERMONT.

The third objective of this Policy is to adopt a confidentiality response plan, integrated within TERMONT's current cyber response plan, for confidentiality incidents relating to personal information.

This Policy is adopted pursuant to certain provisions becoming effective on September 22, 2023, of the *Act to modernize legislative provisions as regards the protection of personal information*, SQ 2021, c. 25 (also known as "Bill 64" or "Act 25"), which received royal assent in Québec on September 22, 2021, modifying the *Act respecting the protection of personal information in the private sector*, CQLR, c. P-39.1 ("PPIPSA" or "ARPPIPS")). This Policy also ensures compliance with applicable provisions of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000. C. 5 ("PIPEDA") applicable to federally regulated entities.

2 – OTHER APPLICABLE POLICIES AND GUIDELINES

TERMONT adopted a Privacy Policy ("Privacy Policy") on November 21, 2018, as subsequently amended. The Privacy Policy summarizes the privacy practices of TERMONT relating to personal information collected and outlines the measures TERMONT takes with respect to the collection, use, disclosure, protection, and handling of personal information for compliance purposes with its obligations under privacy laws.

This Record Retention and Destruction, and Confidentiality Incidents Policy is to be read in conjunction with the Privacy Policy to ensure its full understanding, such that these two instruments can be harmonized without conflict.

3 – RECORD RETENTION SCHEDULE

Attached as Appendix A is a Record Retention Schedule that is approved as the initial maintenance, retention, and disposal schedule for physical records of TERMONT and the retention and disposal of paper and electronic documents.

TERMONT's Privacy Officer oversees the administration of this Policy and the implementation of processes and procedures to ensure that the Record Retention Schedule is followed. TERMONT's Privacy Officer is also authorized to:

- make modifications to the Record Retention Schedule from time to time to ensure that it is in compliance with local, provincial, and federal laws and includes the appropriate document and record categories for TERMONT;
- monitor local, provincial, and federal laws affecting record retention;
- annually review the record retention and disposal program; and
- monitor compliance with this Policy.

4 – SUSPENSION OF RECORD DISPOSAL IN THE EVENT OF LITIGATION OR CLAIMS

In the event TERMONT is served with any subpoena or request for documents or any individual becomes aware of a governmental investigation or audit concerning TERMONT or the commencement of any litigation against or concerning TERMONT, such individual shall inform TERMONT's Privacy Officer, and any further disposal of documents shall be suspended until such time as TERMONT's Privacy Officer, with the advice of counsel, determines otherwise. TERMONT's Privacy Officer shall take such steps as is necessary to promptly inform all personnel of any suspension in the further disposal of documents.

5 – REGISTER OF CONFIDENTIALITY INCIDENTS

Attached as Appendix B is a Register of Confidentiality Incidents that is approved for the recording of all confidentiality incidents involving TERMONT.

Confidentiality Incidents include any unauthorized access to personal information, any unauthorized use or communication of personal information, loss of personal information, or any other breach of the protection of such information.

Upon the occurrence of a confidentiality incident involving TERMONT, TERMONT's Privacy Officer is responsible for ensuring the Register of Confidentiality Incidents is completed with the required information and made available to regulators (where applicable).

-

6 – CONFIDENTIALITY INCIDENTS RESPONSE PLAN

Attached as Appendix C is TERMONT's Confidentiality Incidents Response Plan that is approved as an added module to TERMONT's existing Cyber Response Plan to address confidentiality incidents.

It is noted that confidentiality incidents may, or may not, result from a cyber incident and may, or may not, be criminal in nature. Therefore, certain insurance policies may, or may not, be applicable. The Confidentiality Incidents Response Plan contains information regarding TERMONT's cyber insurance policy applicable to cases where a confidentiality incident results from a cyber incident. Other insurance policies (such as general commercial liability policy or D&O) may be applicable in the case of a confidentiality incident.

7 – APPLICABILITY

This Policy applies to all physical records generated by TERMONT, including both original documents and reproductions. It also applies to the paper and electronic documents described above.

This Policy applies to all confidentiality incidents involving TERMONT.

8 – APPENDIX A – RECORD RETENTION SCHEDULE

The Record Retention Schedule is organized as follows:

- Employment Records

The Record Retention Schedule will be complemented on an ongoing basis further to legal and/or regulatory requirements and good practices.

RECORD RETENTION SCHEDULE
EMPLOYMENT RECORDS

NEW #	Former # that may be indicated on the boxes	Type of document	Recommended number of retention years	Comments
HR-1	2220/2250/2260	Candidates' applications, whether hired (curriculum vitae, criminal record check, medical or skills assessments, etc.)	4	Retention until the end of the hiring process plus 4 years. Triggered by the 3 years prescription + 1-year buffer
FIN -2	3520 to 3536	Payroll records, time sheets and vacations	7	In Quebec retention during the employment until termination + 3 years + 1-year buffer
HR-2	2320/2405/2430/ 2470/2610	Employment documents: employment contracts, dismissal letters, proof of disciplinary sanctions, etc.) excluding medical files	4	Retention during the employment until the end of the latest of these three events: a) Termination of the employment relationship; b) Payment of benefits, including pension benefits, where applicable; + prescription period (3 years) + 1-year buffer
HR-3	2220/2415	Information used for completing a pay equity plan	6	Retention prior to the posting of the results of a pay equity audit or any information used to conduct the pay equity audit plus 6
HR-4	2435/2445/2450/ 2455	Documents relating to employment insurance, including records of employment	7	Retention until the end of the year for which the documents in question were kept plus 7.
HR-5	2620	Training program and agreements, invoices and contracts related to training	7	Retention until the end of the last fiscal year to which training expenditures relate plus 7 years.
HR-6		Medical records of employees	41	The Act respecting Occupational Health & Safety provides that the public health director should keep worker's medical record for a period of not less than 20 years after the end of his employment or 40 years after the beginning of his employment, whichever is longer.

9 – APPENDIX B – REGISTER OF CONFIDENTIALITY INCIDENTS

The Register of Confidentiality Incidents requires the collection of the following information:

- Identification (Incident identification number; Regulator's file number, if any)
- Description (Brief description of incident; Categories of personal information; Date of incident; Date of awareness by the relevant entity; Number of individuals, Remediation measures)
- Assessment (Risk of serious harm or injury to individuals; Justification for absence of notice to regulators or individuals)
- Notification (where applicable) (Date of notice to regulator; Date of notice to individuals; Type of notice and justification)
- Governance (Name of person completing the register; Minimum retention time for record)

Register of confidentiality incidents	
This register is prepared pursuant to Canadian (PIPEDA) and Quebec (ARPPIPS) privacy legislation regarding incident notification. If affecting Quebec, it must be kept for five years following awareness. Otherwise, it must be kept for two years following awareness. **Always consult your breach coach/legal counsel before finalizing such register.**	
A confidentiality incident means ➤ an unauthorized access to personal information ➤ an unauthorized use or communication of personal information ➤ loss of personal information, or ➤ any other breach of the protection of such information.	
Brief description	*Provide a summary description and categorization (e.g. unauthorized access in the context of ransomware affecting the North American fileservers of the organization or loss of an unprotected corporate cellular phone). Avoid discussing the root cause / attack vector, (e.g. brute forced admin account with weak password exposed to the Internet or employee clicking on phishing link or employee intoxicated during a night out).*
Type of personal information	*Provide only categories of personal information, do not include the information itself (e.g. social insurance number, passport scans, physical addresses, employee performance evaluations, account passwords). If this information is unknown, briefly explain why.*
Date of incident	*Indicate the date or period of the incident, or approximation.*
Date of awareness	*Indicate the date or period of awareness of the incident, or approximation.*
Number of individuals	*Indicate the number or approximate number of affected individuals.*
Remediation measures	*Provide a summary description of measures taken to respond to the incident (e.g. internal investigation supported by external cybersecurity respondents immediately upon discovery, isolated compromised assets, deployed endpoint detection and response software to achieve 98% coverage, hard reset on all Office 365 passwords, engaged in Dark Web monitoring).*
Risk of serious harm (or injury) to the individuals	*Provide a summary description of the factors that led the organization to conclude that there is or is not a risk of serious harm (or injury) to the individuals concerned. In this regard, the law identifies the following factors:* *➤ the sensitivity of the personal information concerned;* *➤ the potential for misuse of the information;* *➤ the anticipated consequences of its use and the likelihood that such information will be used for harmful purposes.*
Notice to regulator	*Indicate the date that the notice to the Commission d'accès à l'information and/or the Office of the Privacy Commissioner of Canada or other regulatory body was made, or notices if more than one notice.*
Notice to individuals	*Indicate the date of the notice to affected individuals.*
Type of notice	*Indicate the type of notice (e.g. indirect on website, media, press release or direct by courier, email, phone, verbal, specifying remediation measures such as account resets, credit freezes, or complementary credit monitoring service).*
Retention date	*If the incident affected Québec personal information, you must keep the incident register five years following the date of awareness; if only Canada, two years following date of awareness.*

Register of confidentiality incidents

Identification		Information prescribed by regulation												
		Description						Assessment		Notification (where applicable)			Governance	
Incident identification number	Regulator's file number [if the incident was notifed]	Brief description of the incident	Categories of personal information	Date of incident	Date of awareness by the organization	Number of individuals	Remediation measures	Risk of serious harm (or injury) to the individuals	Justification for absence of notice to regulators / individuals	Date of notice to regulator	Date of notice to individuals	Type of notice and justification for indirect notice	Name of the person who completed the register	Minimum retention time for record
					9/1/2022									9/1/2027

10 – APPENDIX C – CONFIDENTIALITY INCIDENTS RESPONSE PLAN

The Confidentiality Incidents Response Plan identifies the following:

- The CORE Rapid Intervention Team and Key personnel for TERMONT
- Resources (Contact List; Summary of Cyber Policy Coverages (where applicable); Personal Information Inventory / Data Map)
- Breach Response Procedure (Evaluation; Escalation; Management; Post-Mortem; Claim Management)
- Confidentiality Breach Reporting Protocol
- Incident Assessment and Escalation Process (Breach Severity Rating)

AS ADOPTED BY THE BOARD OF DIRECTORS ON AUGUST 24, 2023, EFFECTIVE ON SEPTEMBER 22, 2023.