4.8.

PROTECTION OF PERSONAL INFORMATION (SOCIÉTÉ DE TRANSPORT DE MONTRÉAL)

April 20, 2018

SUMMARY OF THE AUDIT

OBJECTIVE

The objective of the audit was to evaluate whether the controls put in place ensure the logical and physical security of the personal information (PI) held by the Société de transport de Montréal (STM) in a way that limits privacy breaches, theft or unauthorized access.

RESULTS

In addition to these results, we have formulated various recommendations for the business units of the STM.

The details of these recommendations and our conclusion are outlined in our audit report, presented in the following pages.

Note that the business units have had the opportunity to formulate their comments, which appear after the audit report recommendations.

Overall, we can conclude that the STM adequately protects the PI collected in the course of its activities.

Regarding governance:

- The STM has suitable corporate and management policies; responsibilities are clearly defined and accountability reporting is in place;
- Employees and managers are suitably aware of the importance of protecting PI;
- The STM has a PI inventory that meets the requirements of the *Act respecting Access to documents held by public bodies and the Protection of personal information* (AAD).

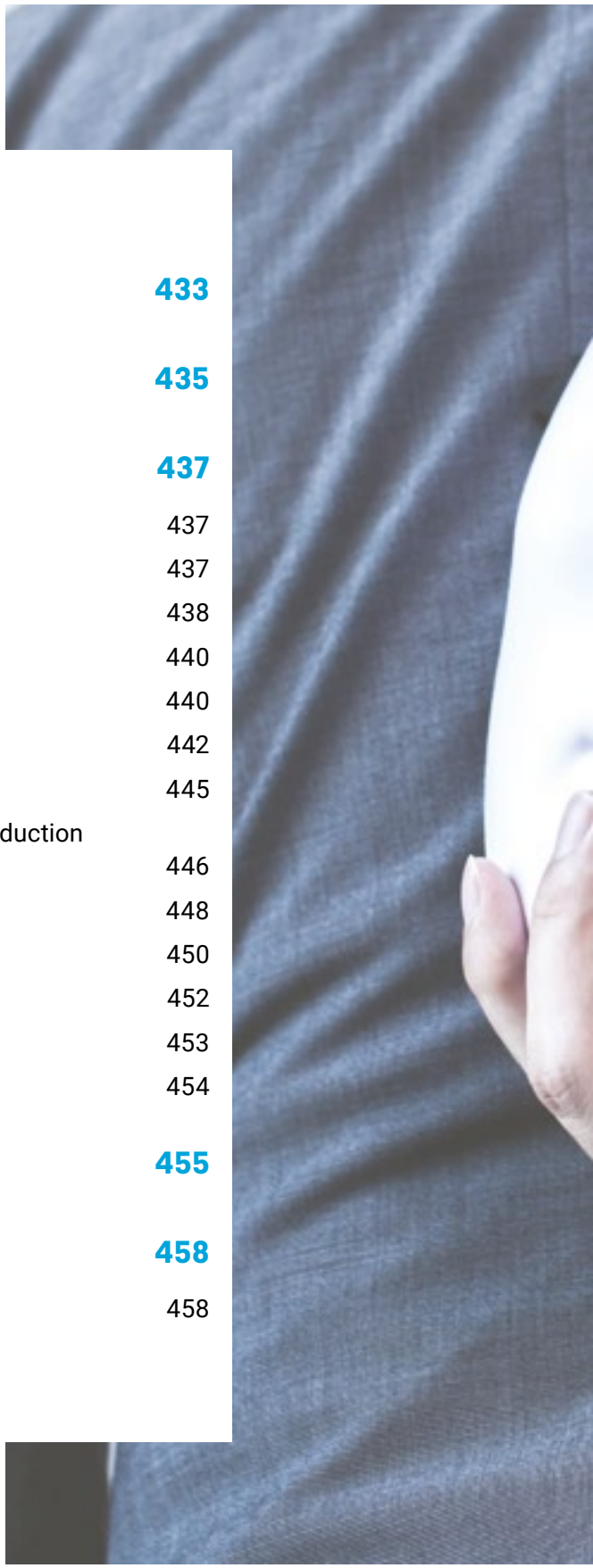
Regarding the retention and destruction of PI:

- A retention schedule has been established for PI in physical files and in the new systems. However, there are no retention guidelines for the five information systems audited;
- The destruction of PI in physical files is conducted by an outside firm in a secure manner;
- No destruction of PI is scheduled for three of the five information systems audited.

Regarding protection measures:

- Four of the five systems audited contain real PI in environments other than their production environments;
- One system presented a deficiency in terms of the review process for access rights; but logical access was managed properly in the other systems;
- Physical access to medical records is protected. Two locations where employee records, applicant files and paratransit forms are kept have combination door locks, which are not as secure as card reader door locks;
- The electronic transmission of PI to other transit agencies is secure. However, the transmission of applicant files to an external firm is not confidential;
- The incident management process includes the protection of PI;
- Penetration tests are conducted regularly to evaluate the security of systems containing PI.

TABLE OF CONTENTS



1. BACKGROUND 433

2. PURPOSE AND SCOPE OF THE AUDIT 435

3. AUDIT RESULTS 437

3.1. Governance 437

3.1.1. Policies 437

3.1.2. Employee Education Program 438

3.1.3. Assignment of Responsibilities 440

3.1.4. Inventory and Classification of Personal Information 440

3.2. Retention and Destruction of Personal Information 442

3.3. Protection Measures for Personal Information 445

3.3.1. Personal Information in Environments Other Than Production Environments 446

3.3.2. Logical Access 448

3.3.3. Physical Access 450

3.3.4. Transmission of Personal Information to Third Parties 452

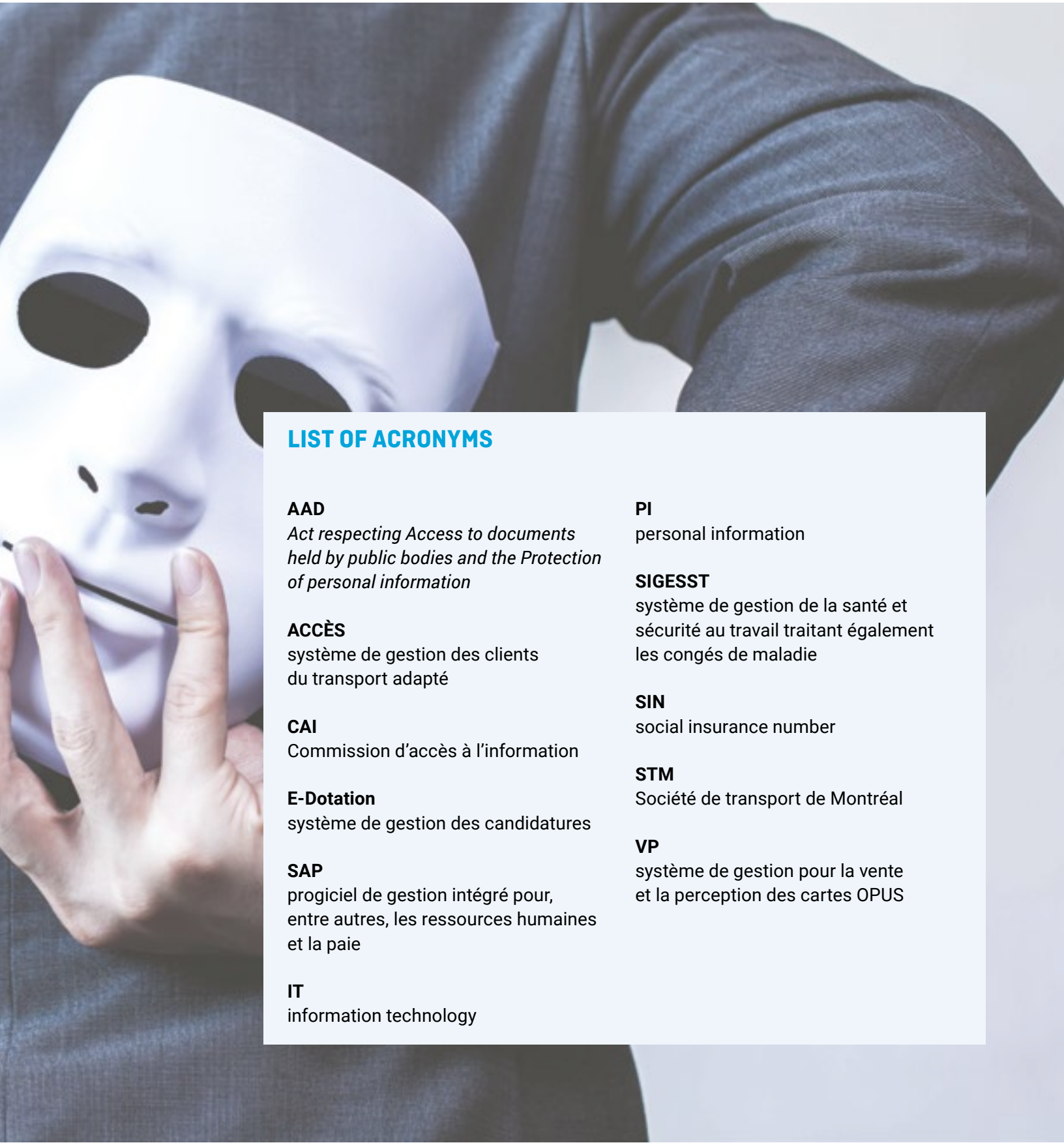
3.3.5. Incident Management 453

3.3.6. Penetration Test Program 454

4. CONCLUSION 455

5. APPENDIX 458

5.1. Assessment Criteria 458



LIST OF ACRONYMS

AAD
Act respecting Access to documents held by public bodies and the Protection of personal information

ACCÈS
système de gestion des clients du transport adapté

CAI
Commission d'accès à l'information

E-Dotation
système de gestion des candidatures

SAP
progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie

IT
information technology

PI
personal information

SIGESST
système de gestion de la santé et sécurité au travail traitant également les congés de maladie

SIN
social insurance number

STM
Société de transport de Montréal

VP
système de gestion pour la vente et la perception des cartes OPUS

1. BACKGROUND

Through its activities, the Société de transport de Montréal (STM) collects and processes a considerable amount of information concerning the private life of its customers and employees. The STM serves approximately 2.9 million customers who have a registered OPUS card, 30,000 customers who use paratransit; it also employs 9,700 people. The STM needs this information in order to provide quality service. The main activities for which the STM collects personal information (PI) are:

- The compilation of employee records, including their medical records;
- The collection of employee banking information for payroll purposes;
- Employment applications for staffing purposes;
- OPUS card registration (generally for reduced fare purposes);
- The collection of medical information on paratransit users.

In Canada, privacy is a fundamental right that is protected in a comprehensive manner by federal and provincial laws.

Adopted on June 27, 1975, Québec's *Charter of Human Rights and Freedoms* lists, among others, the following rights and freedoms of citizens:

- The right to the safeguard of dignity, honour and reputation;
- The right to respect of private life.

Over the past four decades, Québec has built a legislative model embodied by the Québec Commission d'accès à l'information (CAI). The CAI oversees the application of two acts:

- For the public sector: The *Act respecting Access to documents held by public bodies and the Protection of personal information*[1] (AAD);
- For the private sector: The *Act respecting the protection of personal information in the private sector*[2].

As a public body, the STM is subject to the AAD. This Act sets out two intrinsic rights: the right of access and the right of protection of PI.

It applies to all documents whether they are recorded in writing or print, on sound tape or film, in computerized form, or otherwise.

1 CQLR, chapter A-2.1.

2 CQLR, chapter P-39.1.

PI is defined as information that[3]:

- Identifies a natural person (as opposed to a corporate body);
- Helps identify an individual (as opposed to anonymized information);
- Is factual or subjective about a person regardless of its form or medium.

Given its nature, some PI is confidential. Examples include:

- Social insurance number (SIN);
- Health insurance number;
- Date of birth;
- Banking information;
- Medical records;
- Curriculum vitae.

However, some PI is not confidential given its public nature. Here are a few examples:

- Name, title, salary, workplace address and telephone number of a member of a public body or its board of directors;
- STM management staff.

Any loss, theft or unauthorized access involving confidential PI is not only against the law, it can also:

- lead to the disclosure of PI;
- make it possible for malicious individuals to steal identities;
- compromise a person's safety, given the sensitive nature of some of the information held;
- damage the organization's reputation;
- result in the loss of confidence by users;
- lead to lawsuits.

Given this context, the STM must absolutely protect its PI in order to reduce the risk of any of these events occurring.

3 In accordance with CQLR, chapter A-2.1, sections 1 and 54.

2. PURPOSE AND SCOPE OF THE AUDIT

In accordance with the provisions of the *Cities and Towns Act*, we have conducted a value-for-money audit of the protection of PI by the STM. This audit was performed in compliance with the Canadian Standards on Assurance Engagement (CSAE) 3001 of the CPA Canada Handbook – Assurance.

The objective of the audit was to evaluate the presence and efficiency of the controls put in place to ensure the adequate logical and physical security of the PI held by the STM in a way that limits privacy breaches, theft or unauthorized access.

The role of the Auditor General of Ville de Montréal is to provide a conclusion regarding the purpose of the audit. To do so, we have collected a sufficient amount of relevant evidence on which to base our conclusion and to obtain a reasonable level of assurance. Our evaluation is based on criteria we have deemed valid for the purpose of this audit. These are set out in the appendix.

The Auditor General of Ville de Montréal applies the *Canadian Standard on Quality Control* (CSQC 1) of the CPA Canada Handbook – Assurance and, consequently, maintains a comprehensive quality control system that includes documented policies and procedures with respect to compliance with ethical guidelines, professional standards and applicable legal and regulatory requirements. It also complies with regulations on independence and other ethical guidelines of the *Code of Ethics of Chartered Professional Accountants*, which is governed by fundamental principles of integrity, professional competence, diligence, confidentiality and professional conduct.

Our audit focused on PI found in the following:

- Physical supports:
  - Employee medical records;
  - Staffing (applications, employee records);
  - Paratransit (paratransit service request form, which includes medical information on customers).
- Information systems:
  - Progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie (SAP);
  - Système de gestion pour la vente et la perception des cartes OPUS (VP) primarily for students and people 65 years of age and over;
  - Système de gestion des candidatures (E-Dotation);
  - Système de gestion de la santé et sécurité au travail traitant également les congés de maladie (SIGESST);
  - Système de gestion des clients du transport adapté (ACCÈS).

We have excluded from our audit PI collected when issuing statements of offence and PI used for the purpose of managing pension plans, for the following reasons:

- Under the Act, courts, such as the municipal court of Ville de Montréal, are not considered a public body. Statements of offence issued in accordance with STM regulations 036 and 105 are collected by inspectors and other STM employees. The statements are then redirected to the municipal court system of Ville de Montréal. As such, legal statements of offence are accessible without restriction;
- Regarding pension plans, they are managed by an organization other than the STM;
- We have also excluded the following from our audit:
  - Logical access to the SAP and VP systems;
  - Physical security of server rooms;
  - Backup processes.

These aspects are evaluated during the audit of the general controls of information technology (IT) as part of the financial statements. For the 2017 fiscal year, they were found to provide a sufficiently robust control environment overall.

While the STM is required to comply with existing laws and regulations, this audit cannot be construed as a mandate to attest to the level of compliance of the STM with the AAD or with any other laws or standards to which the STM refers when developing its PI protection system.

Our audit was conducted from September 2017 to March 2018. The work consisted of conducting interviews with personnel, examining various documents and conducting surveys we considered appropriate with a view to obtaining probative information.

Upon completing our audit work, we presented a draft audit report to the managers of each of the audited business units for discussion purposes. The final report was then forwarded to the Director General of the STM and to each of the business units involved in the audit in order to obtain action plans and timetables for their implementation. A copy of the final report was also sent to the Chairman of the Board for information purposes.

3. AUDIT RESULTS

3.1. GOVERNANCE

3.1.A. BACKGROUND AND FINDINGS

Governance includes the frameworks and operating principles implemented by an organization to disseminate its strategic directions, establish rules of conduct and promote transparency and accountability within the organization.

Our first audit criterion addressed the STM's need to develop, document and communicate policies and procedures on PI and assign responsibility for ensuring compliance with these policies and procedures.

The STM is also required to comply with the AAD. In three of its sections on PI, the AAD stipulates that:

- *A public body must take the security measures necessary to ensure the protection of the personal information collected, used, released, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored* [s. 63.1];
- *No person may, on behalf of a public body, collect personal information if it is not necessary for the exercise of the rights and powers of the body or the implementation of a program under its management* [s. 64];
- *A public body must establish and keep up to date an inventory of its personal information files* [s. 76].

To comply with the AAD, the STM has developed several frameworks that define the parameters for the management of PI within the organization.

3.1.1. POLICIES

3.1.1.A. BACKGROUND AND FINDINGS

Frameworks are documents that determine the scope, the requirements and the roles and responsibilities of the different business units for any given issue. In the case of the STM, these documents take the form of corporate policies and management policies.

During our audit, the STM provided us with its policies on the protection of PI, which include one corporate policy and two management policies.

The corporate policy entitled "Sécurité informatique et protection de l'information" establishes the STM's position and strategic orientations on computer security and the protection of information. This policy, which was approved by the Board of Directors, outlines the general framework governing the efficient and effective management of risks involving computer systems and data processing.

The guiding principles presented in the policy require that:

- IT and information resources be administered in a manner that gives priority to the protection and security of these resources;
- the physical and logical access to IT and information assets be controlled in a way that efficiently prevents and counters intrusions and the unauthorized use of equipment, systems and data that make up these assets;
- the access, retention, transmission and destruction of files and documents be conducted in a way that complies with the ethical guidelines of the STM and the laws that apply to it.

The management policies, entitled "Protection de la confidentialité des renseignements personnels" and "Utilisation du patrimoine informatique," focus on the management of information. They have been approved by the Director General.

The first management policy defines the management framework governing the efficient control of activities involving PI. It sets out the basic principles on the access, retention and destruction of PI and its release to third parties.

The second policy, which deals with the use of IT assets, aims to guarantee the efficient, optimal and secure use of computer equipment and networks of the STM in a manner that respects individuals and protects the PI held by the STM. It includes the administrative rules and regulations on the retention, transmission and use of information along with access protocols and access rights. It also defines illegal and unacceptable behaviour.

We evaluated these frameworks and found them to be adequate. The corporate policy was issued in 2002 and is currently being updated. The management policies derived from the corporate policy will be addressed and amended at a later date. No recommendation is required.

3.1.2. EMPLOYEE EDUCATION PROGRAM

3.1.2.A. BACKGROUND AND FINDINGS

All employees play an active role in the protection of PI. Consequently, it is important for the STM to share with its employees the frameworks and their amendments pertaining to the protection of PI. In addition, there must be special education measures to make

employees aware of the issues related to privacy, confidentiality and the protection of PI. These measures must be documented. Moreover, disseminating these measures on a regular basis increases the level of vigilance of individuals.

We have evaluated the document on an information session entitled “Accès à l’information et protection des renseignements personnels.” The main topics covered during the session were:

- The scope of the AAD;
- Access to documents held by public bodies;
- The protection of PI;
- Access to PI;
- Protocols on access to information and PI;
- The role of the CAI;
- Penalties.

The training is offered at least twice a year. Since 2013, it has been held 19 times and presented to 177 participants. It is provided to employees in the following positions: executives, managers, office managers, advisors, holders of PI, administrative assistants and information and customer service employees.

A training session entitled “Ce qu’un gestionnaire d’exploitation devrait savoir au plan légal” is also offered to managers. It provides them with an overview of the laws and regulations governing the operations of the STM. The session includes a segment on the concepts of access to information contained in the documents held by the STM.

In addition, new employees must sign a document acknowledging that they have read the policy “Gestion sur l’utilisation du patrimoine informatique” and have agreed to abide by it.

Finally, in order to increase employee vigilance regarding PI, certain initiatives have been launched:

- The code of conduct of the STM is presented to new employees of the Division Planification et acquisition de talents upon being hired;
- Before accessing the corporate network of the STM, a warning reminds all users that they must comply with the requirements of the management policy “Utilisation du patrimoine informatique”.

After evaluating the various measures implemented, we concluded that these are adequate for educating employees and managers on issues related to the protection of PI. No recommendation is required.

3.1.3. ASSIGNMENT OF RESPONSIBILITIES

3.1.3.A. BACKGROUND AND FINDINGS

At the STM, the responsibility and accountability reporting regarding PI are formally assigned to an entity or department by the corporate policy "Sécurité de l'information et protection de l'information." The entity in charge must develop, document and implement the necessary measures and monitoring mechanisms that will allow it to demonstrate compliance with the requirements of the framework. The designated entity must have the highest authority.

During our audit, we noted that the responsibility has been suitably assigned to the Direction exécutive – Technologies de l'information et innovation and to the Secrétariat corporatif et direction affaires juridiques. These responsibilities have been delegated to the secrétaire corporatif (Secrétariat corporatif et direction affaires juridiques) and to the head of the division, Risques, sécurité et conformité (TI et innovation). The staff from these divisions work together on applying the policy.

The top two employees responsible in this respect participate in committees on the protection of PI and related issues.

The first committee is the "Comité de gestion de ressources et actifs informationnels". It focuses on recommended orientations to deal with the main risks faced by the STM and evaluates the main risk incidents involving information assets that have occurred at the STM and in the area of public transit.

A second committee, which is attended by the secrétaire corporatif, compiles the annual statistical listing of access to information requests and their processing. This listing is also presented to the "Gouvernance, éthique et développement durable" committee of the Board of Directors and can be found in one of the sections of the STM's annual report.

After assessing these aspects, we concluded that the responsibilities for protecting PI have been properly assigned and that accountability reporting is in place and functions adequately. No recommendation is required.

3.1.4. INVENTORY AND CLASSIFICATION OF PERSONAL INFORMATION

3.1.4.A. BACKGROUND AND FINDINGS

This last portion of our audit work on governance is specifically defined in the AAD. Section 76, mentions that "*a public body must establish and keep up to date an inventory of its personal information files*".

According to this section, the inventory must contain the following information:

- The title of each file, the classes of information it contains, the purposes for which the information is kept and the method used to manage each file;
- The sources of the information entered in each file;
- The categories of persons to whom the information in each file relates;
- The categories of person who have access to each file in carrying out their duties;
- The security measures taken to ensure the protection of PI.

A person has a right of access to the inventory on request, except as regards information confirmation of the existence of which may be refused under this Act.

In addition, setting up a PI inventory and classification system for all manual and computer processes used in handling PI provides an overview of the situation that facilitates procedures on:

- Risk analyses by the STM;
- Implementation on control measures to ensure the protection of PI.

The STM has inventoried its PI in table format. For each of its corporate divisions, the table identifies the following information, as required by the AAD:

- The classes of information;
- The source of the information;
- The category of persons to whom the information relates;
- The category of persons who have access to this information;
- The security measures taken to ensure the protection of PI.

The STM has also established a document classification plan by subject based on a logical hierarchy that reflects its main activities. Among them, let us note the following categories related to the management of PI:

- Information and communication management;
- Human resources management (staffing, human resource file, health and safety).

The STM uses the information contained in these two documents to inform its annual risk analysis process, which includes the protection of PI and establishes mitigation and control measures.

However, while the PI inventory may seem comprehensive, we note that the table does not specify each type of PI contained in the computer systems or physical files.

For example, for the SIGESST system (health and safety, sick leave), the E-Dotation system (external applicants) and the ACCÈS system (paratransit customers), the exact nature of the PI contained and the PI recorded on an optional basis are not known.

Moreover, the number of files or items related to the classes of information is not specified, even as an estimate. These statistical data would enhance the risk analysis process.

While this information is not required under the AAD, it could nevertheless facilitate the STM's decision-making on the mitigation and control measures required.

RECOMMENDATION

3.1.4.B. **We recommend that the Secrétariat corporatif et direction affaires juridiques add the following information to the personal information inventory:**

- **All the types of personal information held, whether optional or required, for each physical and/or electronic system;**
- **The number of files or items held for each type of personal information.**

BUSINESS UNIT'S RESPONSE

3.1.4.B. ***Société de transport de Montréal***

[TRANSLATION] Given the low level of residual risk, here is one of the actions we propose:

- *Expand the inventory of personal information for all new files by creating a subcategory to specify the types of personal information and the number of related files.* ***(Planned completion: December 2018)***

3.2. RETENTION AND DESTRUCTION OF PERSONAL INFORMATION

3.2.A. BACKGROUND AND FINDINGS

Regarding the retention and destruction of PI, the AAD stipulates in section 63.1 that:

> *A public body must take the security measures necessary to ensure the protection of the personal information collected, used, released, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.*

The retention of PI must comply with the *Archives Act*[4]: it must be based on formally defined retention schedules and any access granted must be restricted solely to authorized persons through the use of physical and logical protection measures. A retention schedule generally specifies the number of years each type of PI must be kept. At the STM, the schedule is presented as index cards. Each specifies the number of years for active and semi-active files.

When PI is destroyed, measures must be taken to protect the confidentiality of the information. For example:

- By defining and applying a policy on the destruction of media and documents containing PI;
- When using the services of a specialized company, drawing up a contract that contains clauses related to the protection of PI. This company must follow industry standards to ensure the confidentiality of the PI upon destroying documents.

For the purpose of our audit, we have evaluated two of the actions involved: the retention and destruction of PI.

RETENTION

The aim of our work was to ensure that the PI collected was kept only as long as needed to fulfill the purposes for which it was gathered.

For PI contained in physical files, we made sure that there were index cards indicating the retention period for the following files:

- Employee records including their medical records;
- Employees on work-related accident leave;
- Eligibility to paratransit;
- External applicants.

Furthermore, when analyzing the computer systems, we noted that for newly implemented software applications, the STM specifies retention rules for electronic data in an index card annexed to the PI table. However, the STM does not have any index cards for older computer systems such as VP, SAP, SIGESST, ACCÈS and E-Dotation. It is therefore difficult to know if the rules that apply to physical files must also be applied here. Let us note, however, that for the VP system, the information on the retention period can be found in the system's procedures.

4 CQLR, chapter A-21.1.

Without a comprehensive overview of PI retention periods including both physical files and computer files, the STM faces the risk of having retention rules applied in a random fashion, which could lead to breaches in confidentiality of PI, given that the information might be kept for longer than required by its operational needs.

It would seem advisable to produce a summary containing the PI retention schedules for all media (paper and computer) as this would make it easier to monitor the retention and destruction periods for all PI.

DESTRUCTION

Information that is no longer required must be made anonymous or destroyed to prevent its loss, theft, misuse or unauthorized access.

In the case of physical files, we noted that an external firm ensures the archiving of semi-active files. This firm is also responsible for the destruction of these files. It has undertaken to respect the confidentiality of the information it receives. We noted that the requirements for the services provided are listed in the quote and include the management of the inventory (file transfers). The firm is certified NAID AAA (*National Association for Information Destruction*), attesting that the destruction of paper and computer data is done in a secure manner. Once the firm completes the destruction, it provides the STM with a certificate.

For computer files, data is destroyed only in the VP and ACCÈS systems. We have obtained reports indicating that the PI in these systems has been destroyed.

For the E-Dotation, SIGESST and SAP, the STM has confirmed to us that PI is not being destroyed. Failing to destroy PI found in these systems can lead to it being kept longer than necessary, thus increasing the likelihood of disclosure.

RECOMMENDATION

3.2.B. **We recommend that the Secrétariat corporatif et direction affaires juridiques, in collaboration with the Direction exécutive des technologies de l'information et innovation, establish:**

- **retention rules for computer systems, except the most recent, in order to obtain a comprehensive overview of all personal information;**
- **procedures on the destruction of personal information in the following systems: the Système de gestion des candidatures (E-Dotation), the Système de gestion de la santé et sécurité au travail traitant également les congés de maladie (SIGESST) and the progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie (SAP).**

BUSINESS UNIT'S RESPONSE

3.2.B. ***Société de transport de Montréal***

[TRANSLATION] Catalogue the systems that require retention rules. Establish retention rules with the stakeholders of the catalogued systems. Have the rules approved by the required authorities. Define a destruction procedure for personal information with the stakeholders for each catalogued system. Implement the destruction procedure periodically. ***(Planned completion: June 2019)***

3.3. PROTECTION MEASURES FOR PERSONAL INFORMATION

A protection measure is any process, mechanism or action that limits the risk of someone seizing PI in any number of ways without proper authorization. Among these measures, we find:

- the management of physical and logical access to computer equipment and systems;
- the deletion or redaction (blacking out) of PI in environments other than its production environment;
- the management of incidents for a timely response in the event of a security breach;
- the encryption of data being sent to a third party;
- the performance of penetration tests to identify vulnerabilities.

The disclosure, unauthorized access or loss of confidentiality involving PI could lead to:

- the breach of personal security;
- identity theft;
- the theft or disclosure of PI or medical information on employees;
- the theft or disclosure of PI on clients;
- damage to the reputation of the STM or loss of user confidence;
- lawsuits.

To ensure that the STM is adequately protecting PI from all such risks, we evaluated:

- The procedures on PI found in environments other than its production environment;
- The procedures on the management of computer system access;
- The physical access to files containing PI;
- The control mechanisms involving the transmission of PI to third parties;
- The management of incidents;
- The existence and operation of a penetration test program.

3.3.1. PERSONAL INFORMATION IN ENVIRONMENTS OTHER THAN PRODUCTION ENVIRONMENTS

3.3.1.A. BACKGROUND AND FINDINGS

For this portion of our audit, we wanted to verify whether there were mechanisms in place to avoid the use of PI found in the STM's information system environments other than production environments.

Information systems generally have several distinct environments. There is the production environment, which is used by employees in the course of their work, and which contains real data that is required to meet business needs. Then there are the environments that are used for other purposes, for example:

- Development environments: these are used by IT specialists to develop or improve the functionalities of applications;
- Test environments: these are used by groups of users and computer analysts to ensure that changes made to the applications function properly;
- Training environments: these enable employees to acquire the expertise needed to effectively use the information systems.

However, without exception, in environments other than production, the use of real data is not necessary, especially if these data are confidential, as is the case with PI. Good industry practices recommend that dummy records be used in environments other than production.

During our audit, we noted that the VP system does not contain real PI in its three non-production environments. Instead, it uses a combination of false or amended data (e.g., date of birth).

However, in the information systems below, we found that real PI was being copied, in whole or in part, from production environments to various test and development environments. In addition, no systematic PI deletion procedure was being applied once the test or development work was completed.

- **SAP**: Four in five environments use real PI (pre-production, quality assurance, development, project) from the production environment, including last name, first name, SIN, date of birth, banking information, home address and home telephone number.
- **E-Dotation**: In three environments (development, quality assurance and pre-production), all production data are imported, including PI such as last name, first name, home address, personal telephone number, personal email, driver's license number (if applicable), gender, group membership (e.g., visible minority) and disability indicator (yes or no).

- **SIGESST**: In the pre-production environment, employees with access to it use real PI from the production environment, including last name, first name, SIN, date of birth, gender, home telephone number and email.
- **ACCÈS**: Four environments (development, quality assurance pre-production and training) use real PI from the production environment, such as last name, first name, SIN, date of birth, home address and home telephone number; the last name, first name and, if relevant, date of birth of accompanying children under the age of 14.

Allowing real PI to be used outside production environments could result in the PI of all employees, customers and applicants being stolen and disclosed to unauthorized individuals. With such information, malicious individuals could commit fraudulent acts, such as theft or identity theft. In all cases, this would seriously harm the STM's reputation.

RECOMMENDATION

3.3.1.B. **We recommend that the Direction exécutive des technologies de l'information et innovation:**

- **delete real personal information from the data environments other than production environments (e.g., through redaction or anonymization) for the following information systems:**
  - **Progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie (SAP);**
  - **Système de gestion de la santé et sécurité au travail traitant également les congés de maladie (SIGESST);**
  - **Système de gestion des clients du transport adapté (ACCÈS);**
  - **Système de gestion des candidatures (E-Dotation);**
- **Implement a systematic process for the deletion of personal information.**

BUSINESS UNIT'S RESPONSE

3.3.1.B. ***Société de transport de Montréal***

[TRANSLATION] For each identified system, in collaboration with the system owner, conduct an analysis to identify the solutions that will mitigate the risk related to the use of personal information in non-production environments and also meet development and quality assurance needs. Given the related level of risk, prioritize the analysis of the progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie.

- *Prioritize and deliver the analysis for the progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie.* ***(Planned completion: September 2018)***
- *Deliver the analyses for the other identified systems:* ***(Planned completion: March 2019)***
  - *Système de gestion de la santé et sécurité au travail traitant également les congés de maladie;*
  - *Système de gestion des clients du transport adapté; and*
  - *Système de gestion des candidatures.*
- *Develop an implementation plan for the solutions identified through the analyses.* ***(Planned completion: To be determined)***

3.3.2. LOGICAL ACCESS

3.3.2.A. BACKGROUND AND FINDINGS

For this second portion on protection measures, we evaluated the procedures in place used to restrict the logical access to PI only to authorized persons. This assessment included three components: access rights given to users and administrators, the review of these access rights and the parameters used to ensure robust passwords.

We noted that for the ACCÈS, SIGESST and E-Dotation systems, the passwords were sufficiently robust since the following parameters were used:

- Minimum of 8 characters in length;
- Activation of password complexity;
- Expiry deadline of 90 days;
- History to prevent the reuse of the last five passwords.

For the ACCÈS and SIGESST systems, the access rights granted to users and administrators is well-founded and based on their current responsibilities. In addition, an access request form has been signed by a person in authority. These access rights are subject to a formal periodic review.

However, access to the E-Dotation system is not subject to such a review. While conducting tests on the administrative accounts in E Dotation, we found that two accounts in the list of access were still active even though the users had left the STM. E-Dotation contains the following PI:

- Last name and first name;
- Home address;
- Personal telephone number;
- Personal email address;
- Driver's licence number (if applicable);
- Gender.

It should be mentioned that the E-Dotation system is expected to be replaced in December 2018. However, E Dotation will retain for at least three years data collected in more than 200,000 files for operational purposes; for instance, many candidates apply more than once and their PI must be recovered. During the replacement, access to the old E-Dotation system will be limited to two or three users in read-only mode.

Without an access review process, the STM faces the risk of former employees still having access to the E-Dotation system or of current employees in new positions still maintaining old access rights that do not reflect their new duties and responsibilities. This could lead to the loss of confidentiality of PI held by the STM.

RECOMMENDATION

3.3.2.B. **We recommend that the Direction expertise ressources humaines, in collaboration with the Direction exécutive des technologies de l'information et innovation, implement a recurring review process of access rights and related privileges for the Système de gestion des candidatures (E-Dotation) until its replacement. This same process will need to be implemented for the new system.**

BUSINESS UNIT'S RESPONSE

3.3.2.B. ***Société de transport de Montréal***

[TRANSLATION] Establish the annual access review process for the Système de gestion des candidatures.
(Planned completion: September 2018)

Ensure the annual access review process is in place for the Solution de Gestion des Talents (a new solution that will replace the Système de gestion des candidatures). ***(Planned completion: December 2018)***

3.3.3. PHYSICAL ACCESS

3.3.3.A. BACKGROUND AND FINDINGS

To ensure that the security procedures and mechanisms put in place restrict physical access to PI only to authorized persons, we evaluated whether the offices protecting files containing PI had adequate security mechanisms and whether the persons accessing these offices did so legitimately.

Based on good industry practices and in the spirit of the AAD, offices that contain sensitive information must be protected by containment mechanisms to prevent unauthorized physical access. These mechanisms can be, for example, an area reserved for the storage of files or doors installed to separate hallways from the offices. These doors should be fitted with card reader door locks. Card reader access systems are capable of tracing the users entering an office and restricting access only to authorized persons.

Our audit focused on the following three offices:

- Human resources: contains employee and applicant records;
- Paratransit: contains medical information on customers provided on request forms for paratransit;
- Health office: contains employee medical records.

During our evaluation, we found that only the health office, where employee medical records are kept, has a card reader door lock. Access rights are reviewed several times a year. We found no discrepancies in the management of these access rights.

The other two offices (human resources and paratransit) are equipped with a five-digit combination lock. This type of lock does not provide the identity of the person entering the office or the date and time of entry.

Here is the main PI at risk of exposure:

- Human resources: employee and applicant files:
  - Last name, first name;
  - Home address;
  - Personal telephone number;
  - SIN;
  - Date of birth;
  - Driver’s licence (for some employment categories, such as bus drivers);
  - Curriculum vitae;

- Paratransit: Application for admission to Transport adapté :
  - Last name, first name;
  - Home address;
  - Personal telephone number;
  - Date of birth;
  - Email address;
  - Medical data;
  - Gender;
  - Weight;
  - Height;
  - Last name, first name and date of birth of accompanying children under the age of 14.

While combination locks are safer than standard locks, they cannot ensure that only authorized persons are accessing the premises. Whether or not access codes are modified on a regular basis, persons who do not necessarily need access for the performance of their duties can nevertheless find out what the code is. Moreover, in the event of fraudulent acts (e.g., theft of PI), it would be impossible to determine who was present on the premises at the time of the incident.

A malicious employee could have access to PI and steal it by consulting certain pay records, applications or paratransit request forms.

RECOMMENDATION

3.3.3.B. **We recommend that the Directions expertise ressources humaines and transport adapté replace the combination locks with card reader door locks on the doors of the following offices:**

- **Human resources;**
- **Paratransit.**

BUSINESS UNIT'S RESPONSE

3.3.3.B. ***Société de transport de Montréal***

[TRANSLATION] Install card reader door locks on the door to the Human Resources office. ***(Planned completion: December 2018)***

Install card reader door locks on the door to the Paratransit office. ***(Planned completion: December 2018)***

3.3.4. TRANSMISSION OF PERSONAL INFORMATION TO THIRD PARTIES

3.3.4.A. BACKGROUND AND FINDINGS

Here, we were looking to evaluate the tools and mechanisms put in place to protect PI when sending it to external third parties by email or other means.

When sending PI, the holder (or guardian) of the information is under the obligation to protect the PI in a way suited to the communication channel used (e.g., mail, email, fax).

During our audit, we identified three types of information being sent to third parties.

For the VP application, customer data reports are shared with other transit agencies that use the OPUS card, including the Réseau de transport métropolitain (RTM), Réseau de transport de Longueuil (RTL), Société de transport de Laval (STL) and Réseau de transport de la Capitale (RTC). Our audit found that the data transmitted are encrypted making it impossible to identify the customers referred to in the reports.

In the case of paratransit, the vast majority of transport is provided by external taxi companies. Only the last name, first name and home address of customers are sent by email to the drivers. We nevertheless consider this to be adequate, since this type of PI is not critical and the risk of identity theft is very low.

In the area of human resources (applicants), the pre-employment screening forms are sent by email to a company, which conducts a background check on criminal records, employment references and academic diplomas, as part of the STM's hiring process. The process is carried out with the applicant's consent. The company providing the service has agreed to the STM's clauses on confidentiality and PI protection. In addition to last name, first name, address and personal telephone number, information such as date of birth, SIN and driver's licence number (e.g., in the case of candidates applying for a bus driver position) are transmitted. The information sent by email is not protected in any way, such as encryption.

By not adequately protecting employment application forms sent by email, malicious individuals could steal the PI of applicants and use it to steal a person's identity.

RECOMMENDATION

3.3.4.B. **We recommend that the Direction expertise ressources humaines, in collaboration with the Direction exécutive des technologies de l'information et innovation, implement a protection measure when transmitting personal information on applicants to the external firm.**

BUSINESS UNIT'S RESPONSE

3.3.4.B. ***Société de transport de Montréal***

[TRANSLATION] Analyse and set up a mechanism to protect personal information during transmission to the provider for applicant background checks. ***(Planned completion: December 2018)***

3.3.5. INCIDENT MANAGEMENT

3.3.5.A. BACKGROUND AND FINDINGS

By evaluating the incident management process it is possible to identify security breaches involving PI and assess whether the appropriate corrective measures have been implemented. Incident management activities must include detection and escalation procedures specific to PI. Lastly, these activities must be appropriately documented and retained for audit purposes.

We obtained the documents indicating that an incident management process has been implemented. These included a flow chart on the « processus de communication – incident majeur », a summary of the overall process of the Service aux utilisateurs featuring the incident management and security request management process. A dashboard of security incidents is produced and presented monthly to the management committee of the Direction exécutive des technologies de l'information et innovation and to the comité trimestriel de gestion de ressources et actifs informationnels.

To support the incident management process, there are also detailed procedures pertaining to security events, such as:

- Unauthorized access;
- Social engineering;
- Equipment theft or loss;
- Data loss, theft or leaks.

A review of this document allowed us to conclude that the procedures in place are adequate for the proper management of incidents involving PI. No recommendation is required.

3.3.6. PENETRATION TEST PROGRAM

3.3.6.A. BACKGROUND AND FINDINGS

A penetration test program helps an organization determine its vulnerabilities in terms of data leaks or unauthorized access to PI by external sources. This type of program is meant to identify potential weaknesses in an organization's system so it may act quickly to repair security breaches, thus limiting risks.

Our audit involved reviewing the penetration test program; it featured three main items: the methodology used, test reports and action plans.

We noted that the STM conducts two types of penetration tests:

- First, penetration tests are conducted on new IT projects just before deployment. We evaluated the methodology used on a new project and the test report, which presents recommendations to address the vulnerabilities found. We noted that this report is then used to develop an action plan.
- The second type of penetration test is performed on the STM's operational systems once a year and simulates an external attack. We reviewed the methodology of this category of test, which included the objective, scope, targets and intervention protocol. We then reviewed the penetration test report, which presented the results of the tests. We noted that the vulnerabilities identified and the corrective measures to be implemented were then included in an action plan.

After reviewing the penetration test program, we were able to conclude that the methodology in place is adequate for the proper management of system vulnerabilities, thus limiting risks. No recommendation is required.

4. CONCLUSION

Overall, we can conclude that the Société de transport de Montréal adequately protects the confidentiality of personal information collected as part of its activities through the implementation of effective control measures that limit the risk of security breaches, theft or unauthorized access.

The following evaluation criteria were used:

Assessment Criteria – Governance:

- The Société de transport de Montréal has adequate corporate and management policies that govern the protection of personal information;
- Responsibilities are clearly established and assigned to the appropriate persons;
- Various measures, such as training sessions and presentations for employees and managers, are in place to make them aware of the importance of protecting personal information;
- There is accountability reporting to address issues related to the protection of personal information;
- The Société de transport de Montréal has a personal information inventory that meets the requirements of the *Act respecting Access to documents held by public bodies and the Protection of personal information*. However, even if not required, the types of personal information and the number of files are not inventoried.

We believe that if the Société de transport de Montréal added to the inventory the types of personal information and the number of files held for each type of personal information, its risk analysis process would be improved.

Assessment Criteria – Retention and Destruction of Personal Information:

- A retention schedule has been established for personal information in physical files and for the new systems. However, there are no retention guidelines for the following information systems:
  - Système de gestion pour la vente et la perception des cartes OPUS;
  - Progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie;
  - Système de gestion de la santé et sécurité au travail traitant également les congés de maladie;
  - Système de gestion des clients du transport adapté;
  - Système de gestion des candidatures;
- The destruction of personal information in physical files is conducted by an outside firm in a secure manner;

- In terms of computer systems, the destruction of personal information is only carried out for the Système de gestion pour la vente et la perception des cartes OPUS and Système de gestion des clients du transport adapté systems. There is nothing in the works for the Système de gestion des candidatures, Système de gestion de la santé et sécurité au travail traitant également les congés de maladie and progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie.

We believe that if the Société de transport de Montréal implements retention rules and destruction procedures for personal information in the above-mentioned systems, personal information would be destroyed as soon as it was no longer needed by the Société de transport de Montréal for the conduct of its operations.

Assessment Criteria – Protection Measures for Personal Information:

- The système de gestion pour la vente et la perception des cartes OPUS system only contains personal information in its production environment. In the case of the Système de gestion des clients du transport adapté, Système de gestion de la santé et sécurité au travail traitant également les congés de maladie, progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie and Système de gestion des candidatures, real personal information is present in environments other than production environments;
- The management of logical access is adequate for the Système de gestion des clients du transport adapté and Système de gestion de la santé et sécurité au travail traitant également les congés de maladie. There were discrepancies in the Système de gestion des candidatures in terms of the review of access rights;
- The office where medical records are kept has a card reader door lock, which restrict physical access only to authorized personnel. The two locations where employee and applicant files are kept along with paratransit forms have combination door locks, which are not as secure as card reader door locks;
- The electronic transmission of personal information to other transit agencies is secure; However, the transmission of applicant files to an external firm is not confidential, since it is not encrypted;
- An incident management process is in place and includes the protection of personal information;
- Penetration tests are conducted regularly to demonstrate the reliability of systems containing personal information and gaps are corrected, as needed.

We believe that the Société de transport de Montréal could increase the effectiveness of protection measures for personal information by:

- deleting real personal information from information system environments other than production (e.g., using redaction) and implementing a systematic process for the deletion of personal information once the tests or development work is completed;
- implementing a process for the recurring review of access rights and related privileges for the Système de gestion des candidatures;
- replacing both combination locks with card-reader doors locks on the doors of offices where human resources and paratransit records are kept;
- implementing a protection mechanism when sending personal information about applicants to the external firm hired to conduct pre-employment background checks.

5. APPENDIX

5.1. ASSESSMENT CRITERIA

Our audit is based on the following assessment criteria in these three areas:

- **Governance:**
  - **Policies**: The Société de transport de Montréal has frameworks defining the requirements on the sound management of personal information applicable to all business units;
  - **Employee education program**: Employees are made aware of the issues and risks associated with personal information making them better able to comply with the security rules governing its protection;
  - **Assignment of responsibilities**: The Société de transport de Montréal has formally assigned responsibility and accountability reporting to a directorate which is in charge of developing, documenting and implementing the requirements of personal information protection policies;
  - **Inventory and classification of personal information**: There is a comprehensive, up-to-date inventory of personal information that provides the Société de transport de Montréal with an overview of data to be protected to ensure their confidentiality. The protection of personal information is included in the risk analysis process.

- **Retention and Destruction of Personal Information:**
  - Personal information is retained in keeping with a pre-established schedule. When personal information is no longer required, it is destroyed in a manner that prevents it from being reassembled in order to avoid all fraudulent use.

- **Protection Measures for Personal Information:**
  - **Personal information in Environments other than Production Environments**: Mechanisms are in place to prohibit the use of real personal information in information system environments other than production;
  - **Logical Access**: Access rights are granted in a manner that only authorized persons can access the information systems containing personal information when this access is required by their position. The security parameters (e.g., passwords) are sufficiently robust to prevent unauthorized access to personal information;
  - **Physical Access**: Mechanisms are in place to limit access to personal information in physical media (e.g., medical or employee records) only to authorized personnel;

- **Transmission of Personal Information to Third Parties**: Personal information sent to third parties protected by security mechanisms to safeguard the confidentiality of the information being transmitted;
- **Incident Management**: Should a major event involving the massive disclosure of personal information occurs, the Société de transport de Montréal has in place an incident management procedure enabling it to respond in a timely manner, thus limiting the real and potential repercussions, and take the necessary measures to resolve the incident;
- **Penetration Test Program**: There is a penetration test program that includes personal information and measures the vulnerabilities of information systems to cyberattacks.