EX36.9

TORONTO

REPORT FOR ACTION

PCI Compliance and records management

Date: June 29, 2018
To: Executive Committee
From: City Clerk, Chief Information Officer, Treasurer
Wards: All Wards

SUMMARY

The City must become Payment Card Industry (PCI) compliant by December 31, 2018 or risk its ability to use credit cards to process payment transactions. It further risks breaching contract terms with Moneris, the City's payment card processing services provider, and be subject to increasing penalties and fines as a result.

One of the PCI standards that the City must meet, is to guarantee that no credit card information of any kind is stored anywhere on the City's network. In conducting an audit of the City's network and systems, unredacted credit card information was found on the SilverDane Archive (SilverDane). SilverDane cannot be searched for credit card information nor can the credit card information be removed in order, to satisfy the PCI requirements.

SilverDane contains emails, attachments, calendars and notes from the City's legacy GroupWise system including relatively recent documents from 2011-15. The system's search capability cannot meet the PCI compliance requirements to remove all credit card. The only option available is to 'unplug' the system from the City's network which could cause the system to fail and the loss of the records contained in it.

The City is under statutory obligations to preserve, and make accessible, records until they are scheduled for destruction under Section 201 of the City of Toronto Act, 2006 and Municipal Code Chapter 217, Schedule A. SilverDane contains records that are scheduled with various retention periods into the future. Staff is seeking authority from Council, to change the various retention periods to one retention period for SilverDane content, as listed in Appendix 1, in order for the City to become PCI compliant.

RECOMMENDATIONS

The City Clerk, Treasurer and Chief Information Officer recommend that:

1. City Council authorize the amendments to Schedule A of Municipal Code Chapter 217, Records, Corporate (City), necessary for the purposes of completing the migration, as required, of City records currently contained in the SilverDane archive to secure archival resources, and decommissioning of the City's current SilverDane archive application, as listed in Attachment 1 to this report; and

2. City Council authorize the City Solicitor to prepare the necessary Bills for introduction in Council to implement recommendation 1 above, subject to such stylistic and technical changes to the draft bills as may be required.

FINANCIAL IMPACT

There is no net financial impact arising from the approval of this report.

The Interim Chief Financial Officer has reviewed this report and agrees with the financial impact information.

DECISION HISTORY

There is no decision history for this report.

COMMENTS

The City must become PCI compliant by December 31, 2018 or risk its ability to use credit cards to process payment transactions. During the City's efforts to become fully compliant with Payment Card Industry (PCI) standards, a barrier to becoming compliant was discovered. There are instances of unredacted credit card information in SilverDane as certain Divisions had received credit card information through email in prior years, even though this process was discouraged. Although all Divisions now have processes in place to protect credit card information in a PCI compliant manner, the presence of any credit card information in the SilverDane archive, hosted on the City's network, prevents the City from being certified as PCI compliant.

The PCI Data Security Standards apply to any organization that accepts credit cards. As the City accepts approximately $750 million in card payments each year, the City is a level 1 merchant, subject to standards higher than any other Canadian city. The City is on track to become certified as PCI compliant in 2018, with SilverDane as the last system issue to be addressed. The proposed solution that is being planned and scoped, will disconnect SilverDane from the City's network, and will reconnect it for limited times, for retrieval and management of information in a PCI compliant manner if and when required.

SilverDane Solution

City staff confirmed that there is no technology solution available to remove the emails or attachments containing credit card information or move all of the contents of SilverDane into another system. SilverDane is an old legacy technology that is no longer supported since the vendor ceased operations a number of years ago. Much of the hardware infrastructure is very old and cannot be replaced. Without vendor support, the solution will ultimately fail. When it does fail, staff will be unable to fix or restore the solution.

However, much of the data in the SilverDane solution is also stored off-site on backup tapes. Furthermore, when the City migrated from its older email system (between 2014 and 2015), much of the same data from that system was copied into the current email solution. A SilverDane Risk Assessment conducted by Internal Audit Division in June 2018, highlighted the technological risk of failure associated with this legacy solution.

Records retention

Records created or received by City staff are City records. They are relied upon to document actions and deliver City services. The City's legislative requirements to preserve and make City records accessible to the public, is as follows:

The *City of Toronto Act, 2006*, requires that City records be stored securely and in an accessible manner. It allows for the destruction of City records only after their authorized retention period has expired, or if the record is a copy. The *Municipal Freedom of Information and Protection of Privacy Act* requires the City to institute reasonable measures to preserve records under the applicable statutes and policies. Authorized retention periods are set out in the City's Records Retention Schedule, (Municipal Code Chapter 217, Schedule A). MFIPPA was amended recently to include a fine for wilfully altering, concealing or destroying records subject to a Freedom of Information request.

In order to be PCI compliant, SilverDane must be taken off the City's network risking system failure and the loss of the contents. Staff are requesting Council's authority to amend the retention schedule for the records in SilverDane to allow for its destruction following the City's best efforts to extract essential emails. By having an authorized retention schedule for the records stored in SilverDane, the City can proceed to migrate records from this SilverDane application as required, while becoming fully PCI compliant, and permitting the decommissioning of this legacy system.

The City has advised the Information and Privacy Commission on our approach to email retention in SilverDane. Legal Services has been consulted in preparation of this report.

CONTACT

Daphne Gaby Donaldson
Deputy City Clerk, Corporate Information Management Services
416-392-9683 Daphne.GabyDonaldson@toronto.ca

SIGNATURE

Ulli S. Watkiss
City Clerk

Rob Meikle
Chief Information Officer

Mike St. Amant
Treasurer

ATTACHMENTS

Appendix 1- Amendments to Chapter 217, Schedule A

Appendix 1- Amendments to Chapter 217, Schedule A

1. Schedule A of Municipal Code Chapter 217, Records, Corporate (City), is amended by adding the two following record series in alphanumerical order by code number, under the Information, Communications, and Administration functional category:

Code	Records Title	Originating Office	Retention				Comments/ Legislation
			A	I	Total	Disposition	
I5011	SilverDane Archival Collection (excluding Credit Card information) Records stored in the City's current SilverDane archive application. Records are accessed for where required for business operations, and other archived copies are not retained. Records consist of archived copies of e-mail correspondence, including attachments, sent or received by City staff from 2011-2015, in addition to any copies of the records maintained in current e-mail system, or other storage mediums.	Common	6M	0	6M	D	Comments: Retention applies to Electronic Records. Active retention period is terminated upon completion of SilverDane mitigation and decommissioning process, or failure of SilverDane archive application where restoration of records affected by the failure would unreasonably adversely impact City operations or would require the utilization of computer hardware, computer software, technical expertise, or other information storage equipment not normally used by the City ("SilverDane Technical Failure").

Code	Records Title	Originating Office	Retention				Comments/ Legislation
			A	I	Total	Disposition	
I5012	Records containing Credit Card information contained in SilverDane Archival Collection Records stored in the City's current SilverDane archive application, such as e- mails or attachments containing machine-readable receipts, payment balancing stubs, invoices documenting the receipt of payment or issuance of refunds which contain information related to a specific credit card payment, credit or account.	Common	90 DY	0	90 DY	D	Comments: Retention applies to Electronic Records. Active retention period is terminated upon creation of duplicative record, including duplicative record redacting Credit Card information; or the completion of SilverDane mitigation and decommissioning process, or SilverDane Technical Failure.

Retention Legend: A = Active; AP = Archival and Permanent; I = Inactive; AR = Archival Review; C = Current Year; DY = Days; D = Destroy; M = Month(s); OPI = Office of Primary Interest - "The division that has primary interest in and responsibility for the disposal of the master copies of a category or class of records"; P = Permanent; P/AR = Permanent/Archival Review; S = Superseded; T = Termination – based on specific criteria