REPORT FOR ACTION

New Policy Resolutions for Payment Card Industry Data Security Standard (PCI DSS) Compliance

Date: November 19, 2020
To: Board of Directors, Toronto Parking Authority
From: Acting President, Toronto Parking Authority
Wards: All

SUMMARY

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.

Toronto Parking Authority (TPA) is seeking to certify as a Level 1 Merchant in order to continue working with major payment card brands. A requirement is to develop and implement policies to protect cardholder data.

This report seeks the Board's approval of two new policies:

- Policy Resolution 5-14: Protect Credit Cardholder Data; and
- Policy Resolution 4-34: Visitor Policy

RECOMMENDATIONS

The Acting President, Toronto Parking Authority recommends that:

1. The Board of Directors of Toronto Parking Authority approve two new policy resolutions:

- Policy Resolution 5-14: Protect Credit Cardholder Data; and
- Policy Resolution 4-34: Visitor Policy; and

direct staff to enact these Policy Resolutions as approved.

FINANCIAL IMPACT

There is no financial impact resulting from the adoption of the recommendation in this report.

DECISION HISTORY

There is no prior decision history relating to this topic.

COMMENTS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.

As an organization processing greater than 6 million credit or debit card transactions a year, Toronto Parking Authority (TPA) is seeking to certify as a Level 1 Merchant in order to continue working with major payment card brands. TPA has identified a requirement to develop and implement policies to protect credit cardholder data and restrict visitor access to sensitive areas.

Two new policies are proposed:

- Protect Credit Cardholder Data Policy
- Visitor Policy

Protect Credit Cardholder Data Policy
The purpose of this new policy is to define the Toronto Parking Authority policy with respect to the protection of the cardholder data from potential compromise throughout its lifecycle. This policy adheres to the requirements set out in the Payment Card Industry Data Security Standard (PCI DSS). The policy will apply to all TPA employees, contractors and third parties who have access to or can impact the security of cardholder data.

Visitor Policy
The purpose of this new policy is to ensure all employees and visitors to the facilities and office are safe, while safeguarding property, assets, confidential data and restricted information. All employees and visitors have a responsibility in satisfying the requirements of this policy and in following the applicable procedures. The policy will assist in ensuring that TPA is aware, at all times, of external parties on premise. In relation to compliance to PCI DSS, visitors to TPA premises will be monitored and access to areas that may impact credit cardholder data will be restricted.

TPA is committed to protecting the cardholder data in accordance with the PCI DSS requirements, and the implementation of these new policies is a key factor in establishing the expectations for the organization.

CONTACT

Phyllis Gallagher, Acting Vice President, Finance, Toronto Parking Authority, 416-393-7296, Phyllis.Gallagher@toronto.ca

Arlene Yam Fritz, Vice President of Human Resources and Transformation, Toronto Parking Authority, 416-393-7283, arlene.yam.fritz@toronto.ca

SIGNATURE

Robin Oliphant, Acting President
Toronto Parking Authority

ATTACHMENTS

Attachment 1: Proposed Toronto Parking Authority Policy Resolution 5-14 Protect Credit Cardholder Data

Attachment 2: Proposed Toronto Parking Authority Policy Resolution 4-34 Visitor Policy

ATTACHMENT 1:

PROPOSED TORONTO PARKING AUTHORITY POLICY RESOLUTION 5-14 PROTECT CREDIT CARDHOLDER DATA

TORONTO PARKING AUTHORITY

5-14

POLICY RESOLUTION

ITEM: Protect Credit Cardholder Data PAGE 1 of 3

PURPOSE	To define the Toronto Parking Authority policy with respect to the protection of the cardholder data from potential compromise throughout its lifecycle. This policy adheres to the requirements set out in the Payment Card Industry Data Security Standard (PCI DSS).
APPLICATION	This policy applies to all TPA personnel, contractors and third parties who have access to or can impact the security of the cardholder data.
DEFINITION	This section outlines some of the related standard acronyms used in this policy document: • CID – Card Identification Data, 3 digits on front of the card. • CVV2 – Card Verification Value, 3 digits on back of the card. • IT – Information Technology. • PIN – Personal Identification Number. • PAN – Primary Account Number, a commonly used acronym for credit card number in the Payment Card Industry Data Security Standard manual. • PCI DSS – Payment Card Industry Data Security Standard, a payment card industry regulatory body co-founded by card brands such as Visa Inc, MasterCard, AmEx, Discover Financial Services and Japan Credit Bureau. • SOP – Standard Operating Procedures. • TPA – Toronto Parking Authority.
POLICY	1. The Toronto Parking Authority is committed to protecting the cardholder data in accordance with the PCI DSS requirements: • *Render the PAN (Primary Account Number) unreadable anywhere it is stored.* • *Never send unprotected PANs by end-user messaging technologies.* • *Sensitive Authentication Data (CVV2, CID, etc.) should never be stored* 2. All employees of the TPA as stated in the policy above, must never send unencrypted cardholder data, and/or other sensitive information such as CID, CVV2 and PIN over unsecured and non-compliant channels. Refer to the Standard Operating Procedures (SOP) *Credit Card Payment Channels* for more information on PCI compliant and non-PCI compliant channels. 3. The TPA strictly prohibits storage of the unencrypted cardholder data, and/or other sensitive information, as stated above, in all media formats (i.e. paper or electronic media).

FIRST ADOPTED: xxx xx, 2020
LAST AMENDED: MINUTE NUMBER:
LAST REVIEWED: MINUTE NUMBER:

ITEM: Protect Credit Cardholder Data PAGE 2 of 3

Refer to the TPA *Encryption Standard* and *Media and Sanitization Standard*.

4. The TPA strictly prohibits the acceptance of the cardholder data via any non-PCI compliance payment channels. Refer to the Standard Operating Procedures (SOP) *Credit Card Payment Channels* for more information on PCI compliant and non-PCI compliant payment channels.

5. Any exceptions to this policy must be in accordance with the TPA *Exception Handling Process Standard*.

6. Report any non-compliance to IT Management. Refer to the TPA policy *Reporting Information Security Incidents*.

7. In recognition of this principle and in accordance with PCI DSS compliance and standards, TPA will review this policy annually.

ITEM: Appendix - REFERENCES

Industry Standards	The TPA as a level 1 merchant and service provider shall comply with Payment Card Industry Data Security Standard (PCI DSS) requirement *Protect Credit Cardholder Data* by: • *Encrypting transmission of cardholder data across open, public networks.* • *Physically securing all media; store media back-ups in a secure location.* • *Maintaining strict control over the storage and accessibility of media.* • *Destroying media when it is no longer needed for business or legal reasons.* • *Maintaining a security policy that addresses information security for all personnel.*
Other Organizational Policies	The existing related TPA organizational policies on PCI DSS requirement (PCI DSS) *Protect Credit Cardholder Data are*: • *8-1 Information Security Program* • *8-3 Information Security Risk Management Process* • *8-12 Reporting Information Security Incidents*

FIRST ADOPTED: xxx xx, 2020
LAST AMENDED: MINUTE NUMBER:
LAST REVIEWED: MINUTE NUMBER:

Additional Standards, Procedures and Guidelines	The existing related TPA standards, procedures and guidelines on PCI DSS requirement (PCI DSS) *Protect Credit Cardholder Data are*: • *Encryption Standard* • *Media and Sanitization Standard* • *Exception Handling Process Standard*

FIRST ADOPTED: xxx xx, 2020
LAST AMENDED: MINUTE NUMBER:
LAST REVIEWED: MINUTE NUMBER:

ATTACHMENT 2:

PROPOSED TORONTO PARKING AUTHORITY POLICY RESOLUTION 4-34 VISITOR POLICY

TORONTO PARKING AUTHORITY

4-34

POLICY RESOLUTION

ITEM: Visitor Policy PAGE 1 of 4

PURPOSE	Toronto Parking Authority (TPA) is accountable to ensure all employees and visitors to the facilities and office are safe, while safeguarding property, assets, confidential data and restricted information. All employees and visitors have a responsibility in satisfying the requirements of this policy and in following the applicable procedures. The policy will assist in ensuring that TPA is aware, at all times, of external parties on premise.
APPLICATION	This policy applies to and must be followed by all TPA employees, contractors and visitors.
DEFINITION	Refer to the Glossary for definitions of key terms.
POLICY	*Visitor Requirements* It is the expectation of all visitors to behave in a manner that is professional and respectful towards TPA staff, members of the public and other visitors. Where a violation of this policy or other applicable policy has occurred, a visitor will be asked to leave TPA property immediately. Visitors are expected to work in a safe manner while on TPA property and must be familiar with the circumstances of and work in full compliance with their respective duties and responsibilities under the *Occupational Health and Safety Act, other relevant acts, standards and regulations*. Visitors to TPA's office or facilities must, at all times, clearly display their visitor pass or permit and follow applicable procedures. Visitors must abide by TPA's policies, which are made available to visitors upon arrival or upon issuing a visitor permit. Visitors must only enter areas they have been granted access to. When unsure, visitors should refer to their visiting TPA employee for clarification. Visitors are prohibited from connecting their electronic devices, both manually and using WIFI, to TPA networks, unless pre-authorized to do so. Upon arrival to head office, a visitor pass will be issued. Unless otherwise requested, all visitor passes expire at the end of the date of

FIRST ADOPTED:
LAST AMENDED: MINUTE NUMBER:
LAST REVIEWED: MINUTE NUMBER:

issue. Passes are non-transferrable and are the property of Toronto Parking Authority.

Employee Requirements

Employees of TPA have an obligation to ensure precautions are made to protect assets, property and information and to promote a safe work environment.

Employees are prohibited from entering sensitive / restricted areas without pre-approval, based on business need.

Employees working at head office will be issued a security fob or pass and/or key for their corresponding location of work in the building. Employees whose normal work location is not head office will be required to obtain a visitor pass upon arrival to the building.
It is the responsibility of any employee who is expecting a visitor to receive the visitor at the pre-determined meeting location and validate the visitor upon arrival.

Employees receiving a visitor are accountable to ensure the applicable procedures are followed. The Vice President or designee may, on an exception basis, require a visitor to be escorted by a TPA employee at all times in sensitive / restricted areas. Employees must not allow access into any sensitive / restricted area to unauthorized visitors, including personal guests. Personal guests are to be treated as visitors under this policy.

It is every employee's responsibility to keep watch for unknown persons. A TPA employee should request to see a visitor's pass or permit, if applicable, if it is not prominently displayed. Employees must notify their Supervisor immediately upon learning of an unauthorized visitor. The Supervisor shall investigate immediately, and where applicable, ensure the proper visitor process is followed.

Annual Policy Acknowledgment by TPA Employees

All employees are required to acknowledge their understanding of this policy on an annual basis.

Violation of Policy

It is imperative that employees and visitors understand the importance of this policy. Failure to comply with this policy may result in significant ramifications, including security and safety risks.

Any visitor who contravenes this policy will be asked to leave TPA property immediately and may be prohibited from future entrance to TPA property, depending on the severity of the violation.

All employees of TPA are required to follow this policy. Any employee found to have not followed this policy may be subject to corrective action.

The following corrective measures may be considered depending on the severity of the particular incident:

a) training;
b) formal reprimand;
c) suspension; and/or
d) discharge

GLOSSARY

Visitor:	Visitors to TPA head office or operational facilities may include, but are not limited to, vendors, contractors, business affiliates and stakeholders, or any external third-party requiring access to a restricted area. A visitor is not a member of the public requiring access to public areas unless clearly stipulated by signage.
Employee:	A person employed on a part time or full-time basis by TPA.
Escort:	A TPA employee receiving a visitor. The escort may, in certain situations, be required to accompany a visitor while in sensitive restricted areas.
Contractor:	Any individual representing a vendor, subcontractor, supplier or consultant, who, conducts business with Toronto Parking Authority.
Restricted Area:	Any area whereby sensitive data, security and/or safety can be compromised. Restricted areas can only be accessed by authorized individuals.

FIRST ADOPTED:
LAST AMENDED: MINUTE NUMBER:
LAST REVIEWED: MINUTE NUMBER:

	Head Office:	TPA's corporate office.
	Facility:	Any outside carpark structure or operation owned or maintained by TPA where restricted areas are present.
POLICY ACCOUNTABILITY	Human Resources is accountable for the requirements under this policy.	

FIRST ADOPTED:
LAST AMENDED: MINUTE NUMBER:
LAST REVIEWED: MINUTE NUMBER: