Tompkins County Public Library
Payment Card Industry Data Security Standard (PCI DSS) Compliance Policy

Payment Card Industry Data Security Standard (PCI DSS) compliance are security and business practice guidelines adopted by Visa, MasterCard, American Express, Discover Card, and JCB to establish a "minimum security standard" to protect customer's payment card information. It is a requirement for all merchants that store, transmit, or process payment card information.

The Tompkins County Public Library (TCPL) complies with all PCI standards regarding the storage, processing and transmission of customer credit card information for payment that we process through our Circulation Desk. The Finger Lakes Library System is PCI DSS compliant for patrons who make account payments on the TCPL website. The Tompkins County Public Library Foundation uses a service that is PCI DSS compliant for patrons that make online donations on the Foundation's website.

Terms

Cardholder Data: At a minimum, cardholder data consists of the full primary account number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

Information Security: Protection of information to insure confidentiality, integrity, and availability.

PAN: Acronym for "primary account number" (or "account number"). This is a unique payment card number (typically for credit or debit cards) that identifies the issuer and PCI: Acronym for "Payment Card Industry."

POS: Acronym for "Point of Sale."

Terminal: The device used to manually process the credit cards.

Payment Location: Payments handled at the TCPL service desks at Circulation, Adult Services, and Youth Services

Guidelines

a. This policy applies to all Library employees and to contractors and consultants who have access to cardholder data.
b. All employees who have access to cardholder data must attend security awareness training and acknowledge in writing that they have read and understand the Library's Information Security Policy. This policy will be reviewed with applicable staff annually.
c. The Library uses a POS terminal not connected to the Internet. It uses a dedicated phone line for transactions.
d. The Library accepts payments via telephone. The telephone is within close proximity to the credit card terminal so there is usually no need to write down card information because it can be entered directly into the terminal. If a staff person from another department writes down credit card information to enter into the terminal, they immediately shred the information once the transaction is finished.
e. No cardholder data shall be entered or stored under any circumstance. This includes:
    i. The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card).
    ii. The personal identification number (PIN) or the encrypted PIN block.
    iii. The contents of the payment card magnetic stripe (track data) on any media whatsoever.
f. Cardholder data may not be transmitted via email.
g. No more than the last four digits of a PAN shall be printed on either the Library copy or the customer copy of any receipts or reports.
h. All Circulation Clerks are issued a clerk number that is recorded with the Head of Access Services. Clerks must include their clerk number when entering their transaction into the register. This number is also written on the credit card slip before it is placed in the register drawer.
i. Credit card receipt copies are sent to the Business Office and retained following the Federal Record Retention Requirements. After this time, the receipts are sent to a professional shredding service to be destroyed.

Reporting an Incident

The Head of Access Services should be notified immediately of any suspected or real security incidents involving cardholder data:

a. Contact the Head of Access Services (HAS) who will contact the Business Manager to report any suspected or actual incidents. Staff should contact the HAS if it occurs during non-business hours.

b. Document any information you know while waiting for the HAS to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.
c. No one should communicate with anyone outside of their supervisor(s) or the Business Manager about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the Business Manager.

Incident Response Policy (Handled by HAS and Business Manager)

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, and recovery resulting in improvement of security controls.

Contain, Eradicate, and Recover

1. Notify applicable card associations.

   #### VISA Steps

   If the data security compromise involves credit card account numbers, implement the following procedure:

   i. Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
   ii. Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.
   iii. Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
   iv. For more Information visit: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if _ compromised.html

   #### MasterCard Steps

   i. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
   ii. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to compromised_account_team@mastercard.com.
   iii. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.

iv. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
v. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
vi. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
vii. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Discover Card Steps

i. Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102
ii. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
iii. Prepare a list of all known compromised account numbers
iv. Obtain additional specific requirements from Discover Card

2. Alert all necessary parties. Be sure to notify:

a. Merchant bank
b. Local FBI Office
c. U.S. Secret Service (if Visa payment data is compromised)
d. Local authorities (if appropriate)

3. Collect and protect information associated with the intrusion.
4. Eliminate the intruder's means of access and any related vulnerabilities.
5. Research potential risks related to or damage caused by intrusion method used.

Payment Location: Payments handled at the public print release station

Jamex supplies TCPL with the device that accepts credit card payments at the print release station. According to their document titled, "NetPad Touch for Credit Card End to End Encryption E2EE,"

> *NetPad Touch for Credit Card has been implemented to provide maximum PCI security. By partnering with CreditCall, a global payments company with offices in North America and Europe, the NetPad provides state of the art encryption from card swipe through completion of transaction."*
>
> *CreditCall is a validated PCI DSS Level 1 Service Provider. This is the industry's highest level of certification. Reviewed annually, an intensive onsite audit ensures the highest compliance levels are maintained and adhered to. To comply with the strictest security measures, CreditCall does not store raw magnetic stripe (track 2), card validation codes or PIN block data.*
>
> *The NetPad touch uses an encrypted card reader that can only be decrypted by CreditCall.*
>
> *All communications from the NetPad Touch are outbound over HTTPS to the CreditCall server. The use of an encrypted reader in conjunction with direct communication only to the CreditCall server provides a PCI DSS compliant solution.*
>
> [content confirmed with Jamex 3/18/21]

Please contact the Business Manager at the Tompkins County Public Library if you would like a copy of the complete document.

Payment Location: Payments made through online catalog for fines and fees

The Finger Lakes Library System maintains TCPL's online catalog and handles online payments made through it. Below is the Finger Lakes Library System Privacy Policy for Credit Card Transactions:

> *All credit card transactions are conducted on the PayPal PayFlowLink gateway hosted pages ensuring Payment Card Industry (PCI) compliance standards. We use a 2048 bit SSL Certificate from a recognized Certificate Authority (CA) for all public facing pages where personally identifiable information (PII) is stored. Since all credit card transactions occur on the PayFlowLink hosted pages,* ***we don't have access to or store any credit card numbers****. The lock icon indicates that your browser is communicating over a secure link.*
>
> *Refunds will* ***not*** *be issued via the online credit card web page. Overdue fines can only be refunded by the library (check or cash) where the fine was incurred. Any returned items that were Lost and then Paid must seek the refund from the Library that owns the item. The period of time that a Library may issue a Refund is governed by the owning library only. This period ranges from 1 month to 1 year depending on the owning library policy.*
>
> [content confirmed with the Finger Lakes Library System 3/15/21]

Payment Location: Donations made to the Tompkins County Public Library Foundation

The Tompkins County Public Library Foundation http://www.tcplfoundation.org uses a third-party vendor called Blackbaud to take online payments. Blackbaud is PCI compliant and their statement can be found at https://www.blackbaud.com/security/pci-compliance.

Payments mailed to the Foundation office are retained in a secure area and follow the Federal Record Retention Requirements. After this time, the receipts are sent to a professional shredding service to be destroyed.

[content updated and confirmed by the TCPL Foundation 3/18/21]

Revision History

Changes	Approving Staff Member	Date
Initial publication	Jennifer Schlossberg	10/26/16
Added Jamex NetPad Touch wording and reformatted	Jennifer Schlossberg	11/1/16
Edits received from Library Services & Policy Committee	Jennifer Schlossberg	11/1/16
Minor edits related to going Fine-Free and not charging for meeting rooms	Jennifer Schlossberg	1/2/2019
Updated	Jennifer Schlossberg	3/24/2021
Approved	Library Board of Trustees	7-27-21