City and County of San Francisco

Payment Card Processing and Data Security Standard Compliance Policy

Version 1.2

Applicable to ALL City and County of San Francisco employees including contractors, interns, volunteers, and suppliers as well as non-employees acting as agents of the City who handle, process, support, or manage payment card transactions.

Table of Contents

Applicable to ALL City and County of San Francisco employees including contractors, interns, volunteers, and suppliers as well as non-employees acting as agents of the City who handle, process, support, or manage payment card transactions.

City and County of San Francisco

Payment Card Processing and Data Security Standard Compliance Policy

Version 1.2

Applicable to ALL City and County of San Francisco employees including contractors, interns, volunteers, and suppliers as well as non-employees acting as agents of the City who handle, process, support, or manage payment card transactions.

Overview

The PCI (Payment Card Industry) DSS (Data Security Standard) is a mandated set of requirements agreed upon by the five major credit card companies: VISA. MasterCard, Discover, American Express and JCB. These security requirements apply to all transactions surrounding the payment card industry and the merchants/organizations that accept these cards as forms of payment. Further details about PCI can be found at the PCI Security Standards Council website.

City and County of San Francisco, hereinafter referred to as "City", have a fiduciary responsibility to their customers and payment card processors to comply with the PCI-DSS when handling payment card transactions. Non-compliance can result in serious consequences for the City (see Section 4). To reduce the City's risk associated with the administration of credit card payments, departments/agencies must ensure proper internal control and compliance with the PCI-DSS. The objectives of this policy are to:

- Update, publish and make publicly available information security policies and processes to relevant personnel (including vendors and business partners) on an annual basis.
- Ensure compliance with PCI-DSS and other applicable policies and standards
- Establish the governing structure for payment card processing and compliance activities at the City
- Define responsibilities for payment card services to various City department/agencies including constituents
- Provide general guidelines regarding the handling of cardholder data and acceptable use of the technologies for credit card capture and processing.
- Ensure compliance with PCI-DSS and other applicable policies and standards, according to PCI DSS Requirement 9.9.x for payment capture devices.

To accept and process credit card payments, the City must prove and maintain compliance with the PCI-DSS. This policy provides the requirements for the processing, transmission, storage and disposal of cardholder data of payment card transactions:

PCI-DSS REQUIREMENTS:

Build and Maintain a Secure Network	1. Install and maintain a firewall and router configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program Implement Strong Access Control Measures	5. Use and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications. 7. Restrict access to cardholder data by business need-to-know. 8. Assign a unique ID to each person with computer access while implementing secure authentication controls through such methods as password restrictions and guidelines, passphrase or two-factor authentication. 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors.

Purpose

To provide the City with clear and manageable procedures to protect customer cardholder data and to protect the City from a cardholder breach by complying with Payment Card Industry (PCI) Data Security Standards (DSS).

Applicability

This policy applies to City employees including contractors, interns, volunteers and suppliers of all City departments/agencies as well as non-employees acting as agents of the City who maintain the processing of payment cardholder data.

The City requires those who handle, process, support, or manage payment card transactions received by the City departments/agencies to comply with the current version of the PCI-DSS. All persons are expected to use the technologies for capturing, transmitting and processing payment card data in the intended and authorized manner which supports the city's business.

Consequence of Non-Compliance

Non-compliance can result in serious consequences for the City, including reputational damage, loss of customers, litigation, substantial fines, and other financial costs.

All City employees including temporary workers, contractors, suppliers, interns, or volunteers impacted by PCI-DSS requirements are responsible for complying with this policy. Failure to comply with this policy and/or applicable policies, standards, and procedures carries severe consequences which may include:

- loss of the ability to process payment card transactions,
- departmental repayment of financial costs imposed on the City, and
- employee disciplinary action, which can include termination of employment.

The City's PCI Steering Committee (PSC) has the authority to restrict and/or terminate merchant account status for non-compliance.

Terms and Definitions

Term	Definition
Security Incident	A vulnerability which may compromise the security of city resources has been discovered and is underway. Generally, this means a weakness in intrusion prevention has been found, an attempted exploit has taken place, or reconnaissance by a hacker has been thwarted. Examples include systematic unsuccessful attempts to gain entry, a PC or workstation infected with a virus, worm, Trojan, botnet, or other malware that has been discovered and removed.
Security Compromise	An escalation of a security incident where the attacker has gained control of a city account, system, or device, and is leveraging that position to control and utilize compromised resources for unauthorized acquisitions. At this point, it has been determined that data has not been compromised or stolen.
Security Breach	A confirmed, unauthorized acquisition, modification or destruction of City or private data has taken place. At this point, a breach has been forensically determined and evidence supports that data was compromised.
Private Data	Data about individuals that is classified by law as private or confidential and is maintained by the city in electronic

format or medium. "Private data" means data classified as not public and available to the subject of the data, and "confidential data" means data classified as not public but not available to the subject of the data.

Unauthorized Acquisition
For the purposes of this plan, this means that a person has obtained city data without statutory authority or the consent of the individual who is the subject of the data, and with the intent to use the data for non-City purposes.

Systematic Unsuccessful Attempts
Continual probes, scans, or login attempts where the perpetrators obvious intent is to discover a vulnerability and inappropriately access and compromise that device.

City Resources or Systems
Includes all city-owned computers, peripherals, networks, and related equipment and software, and the voice and data communications infrastructure.

Payment Card Industry Data Security Standards (PCI-DSS)
The security requirements defined by the Payment Card Industry Security Standards Council and the 5 major Payment Card Brands: Visa, MasterCard, American Express, Discover, JCB.

Cardholder
Someone who owns and benefits from the use of a membership card, particularly a payment card.

Card Holder Data (CHD)
Those elements of payment card information that are required to be protected. These elements include Primary Account Number (PAN), Cardholder Name, Expiration Date and the Card Identification Number (CID).

Primary Account Number (PAN)
Number code of 14 or 16 digits embossed on a bank or payment card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device

Payment Card
Refers to both credit, debit cards, and City purchase or p-cards.

Merchant
Refers to the City department or agency that has applied for and been approved to accept credit/debit card payments by TTX. A merchant is assigned a specific merchant account (MID), which is used to process all credit/debit card transactions via City-approved payment card processor

Payment Card Processor
The entity engaged by a merchant to handle payment card transactions on its behalf and can also be referred to as a

"payment gateway". Payment processors are not considered acquirers

Point of Sale (POS)

This is the location where payment card information is taken to complete a purchase by the cardholder

Point of Interaction (POI)

Point of Interaction (POI) Devices; the initial point where data is read from a card. POI transactions are typically integrated circuit (chip) and/or magnetic-stripe card-based payment transactions.

Service Provider

Any company that stores, processes, or transmits cardholder data on behalf of another entity is defined to be a Service Provider by the PCI guidelines.

PCI Scope

PCI in-scope cards include any debit, credit, and pre-paid cards branded with one of the five card association/brand logos that participate in the PCI SSC - American Express, Discover, JCB, MasterCard, and Visa International. PCI Scope includes Payment Gateways that connect a merchant to the bank or processor that is acting as the front-end connection to the Card Brands. They are called gateways because they take many inputs from a variety of different applications and route those inputs to the appropriate bank or processor. Gateways communicate with the bank or processor using dial-up connections, Web-based connections or privately held leased lines.

SAQ

PCI DSS self-assessment questionnaires (SAQs) are validation tools intended to assist merchants and service providers report the results of their PCI-DSS self-assessment.

Acquiring Bank

A financial institution that processes payment card transactions for merchants. It is defined by a payment brand as an acquirer.

Magnetic Stripe/Chip Data (or Full Track Data)

Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.

CAV2, CVC2, CID, or CVV2 data

Three-digit or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

Merchant Department

Any department/agency or unit (can be a group of departments/agencies or a subset of a department/agency) which has been approved by the City to accept payment cards and has been assigned a Merchant identification number.

Merchant Department Primary Contact (MDPC) An individual within the department who has primary authority and responsibility within that department for payment card transactions.

Roles and Responsibilities

PCI Steering Committee (PSC) (TTX)

This cross-functional committee is the principal decision-making body at the City in matters regarding PCI compliance. Members of the committee may vary from time to time but employees from the following departments will always be its senior members: Office of the Controller (CON), Office of the Treasurer & Tax Collector (TTX), and Department of Technology (DT). TTX may designate working groups or subcommittees to accomplish these responsibilities, but the TTX retains ultimate responsibility for PCI compliance.

The TTX is responsible for the following:

- Managing relationship with citywide 3rd party PCI contractor and budget
- Managing the relationship with citywide credit card "gateway" provider
- Creating effective lines of accountability, responsibility and authority for compliance with the PCI-DSS and Payment Application Data Security Standards (PA-DSS).
- Approving business policies, procedures, and guidelines related to PCI-DSS compliance, including providing leadership support in the event of a data breach (per Section 6.6 above).
- Providing input in the City's Emergency Management Plan in the event of a data breach.
- Approving new merchant departments who wish to begin accepting credit card payments to be PCI compliant before accepting payment card transactions. TTX will follow up to review and approve all applications for new merchant accounts and any variances to normal merchant operations for existing merchants.
- Facilitating and collaborating with CON and City Cybersecurity Team in scheduling ongoing network scanning and penetration testing for applicable merchants.
- Working with the City Cybersecurity Team in Implementing new mandates issued by the PCI Security Standards Council and conforming to the evolving PCI-DSS.
- Assisting merchant departments in reducing their PCI scope to minimize the chance of a data breach.
- Assisting the Office of the Controller (CON) in bringing non-responsive, non-compliant merchant departments

into compliance prior to their payment card privilege being terminated.

- Working with the City Cybersecurity Team to provide annual security awareness & inventory of POI devices and inspection training programs.

Departmental Chief Information Officer (CIO) and Information Security Officer (ISO)

Departmental IT (Information Technology) is responsible for the following:

- Creating, maintaining, and disseminating CCSF security policies and requirements that address PCI-DSS requirements, including incident response and escalation procedures, per COIT Cybersecurity Policy and Department of Technology Cybersecurity Requirements.
- Developing and implementing Departmental procedures to address CCSF security policies and requirements, including analyzing security alerts and distributing information to appropriate information security and business unit management personnel as needed, per COIT Cybersecurity Policy and Department of Technology Cybersecurity Requirements.
- Testing the City's infrastructure and network environment with the assistance of the City Cybersecurity team.
- Assisting the TTX in completing the technical sections of the annual PCI-DSS self-assessment questionnaire (SAQ) of merchant departments.
- Configuring and managing applications and infrastructure that store, process or transmit cardholder data in compliance with PCI-DSS including CCSF cybersecurity requirements, including administration of user accounts and authentication.
- Establishing appropriate limits for access to IT resources and sensitive data, including monitoring and controlling all access to cardholder data, in accordance with PCI-DSS requirements.
- Partnering with TTX in conducting citywide annual security awareness training
- Assisting the departments on their remediation plan and implementation on technical requirements for PCI compliance
- Creating, maintaining and disseminating CCSF security

policies and requirements that address PCI-DSS requirements, including POI management policies and processes for inventory, substitution and tamper check.

- Developing and implementing Departmental procedures to address CCSF security policies and requirements, including POI management policies and processes for inventory, substitution, and tamper check, as well as provide content for required training.

Department's Finance

Department's Finance Team is responsible for the following:

- Ensuring the department utilizes the merchant service provider contracted by TTX for the City.
- Previewing merchant applications before submission to the TTX.
- Collaborating with TTX in the initial setup and overseeing the ongoing administration of its own merchant accounts.
- Reviewing the department's third-party credit card processing vendors and service providers for compliance. Providing TTX with a diagram of the "flow of funds"
- Reconciling credit card merchant and settlement bank accounts regularly per CON policy and procedure

Merchant Departments

Merchant Departments are responsible for the following:

- Appropriate use of all technologies for capturing, transmitting and processing payment card data in the intended and authorized manner which supports the city's business, as directed by TTX, DT and / or department leadership.
- Overseeing the building and maintaining of secure networks, payment applications, systems and related infrastructure.
- Ensuring that all business process documents for accepting, processing, retaining, and disposing of cardholder data are updated and in compliance with the PCI-DSS Policy and all other applicable policies and standards.
- Performing an annual PCI-DSS self-assessment.
- Ensuring adherence with this policy, and that all inventory, substitution and tamper check procedures are followed, and required evidence is generated and

	retained.
Department Employees	Department employees who are involved in the storing, processing, transmitting, or have access to cardholder data are responsible for: - Appropriate use of all technologies for capturing, transmitting and processing payment card data in the intended and authorized manner which supports the city's business, as directed by TTX, DT and / or department leadership. - Completing PCI-DSS training upon hire and at least annually thereafter. All employees will acknowledge reading and understanding these security policies and procedures, and will comply with these policies. - Ensuring adherence with this policy, and that all inventory, substitution and tamper check procedures are followed, and required evidence is generated and retained.

Policy

In order for a department/agency, or any other entity at the City, to process credit/debit card transactions, it must be established as a merchant department and issued a merchant account through the Office of the Treasurer and Tax Collector (TTX). City departments or agencies may accept VISA, MasterCard, Discover, American Express, and debit cards with a VISA or MasterCard logo. All departments at the City are required to use the merchant service provider(s) contracted by TTX. Departments wishing to obtain an exception to this requirement must refer to Section 8, "Policy Exception", of this guideline.

6.1 Credit Card Brand Standard

Each card brand has its own program for compliance validation levels and enforcement. Merchants Departments should be familiar with all the individual credit card brand standards (American Express, Discover Financial Services, MasterCard Worldwide, and Visa Inc.) and refer to them periodically. More information about compliance with specific credit card brands can be found at the web addresses listed in Section 9 "Related URLs" of this guideline.

6.2 Payment Card Acceptance and Handling

6.2.1: All credit card processing is subject to audit by CON. This includes credit card payments received via: web forms, walk-in, phone calls, or mail; and off-site events.

6.2.2: POS (point of sale) or card swipe terminals must be approved by TTX.

6.2.3: Employees, including contractors, interns, volunteers and other non-employees acting as agents of the City handling cardholder information go through a background check. Employees should not have access to cardholder information. Anyone handling cardholder information will be required to attend security awareness training on an annual basis.

6.2.4: The opening of a new merchant account for accepting and processing payment cards is done on a case by case basis. Any fees associated with the acceptance of the payment card processing in that department/agency will be charged back to that department/agency. Interested departments should contact TTX to begin the process of accepting payment cards. Steps include:

- Completion of a Credit Card Payment Acceptance Application that can be obtained by contacting TTX at TTX.BankingTreasuryAccounting@sfgov.org to become a "Merchant Department".
- Read and sign-off attesting to their understanding of this policy and its requirements. The attestation statement must be included in the Application submitted above.
- Applications are submitted to TTX for review and approval / rejection.

6.2.5: Any department accepting payment cards on its behalf must designate an individual within the department who will have primary authority and responsibility within that department for payment card transactions. This individual is referred to as the Merchant Department Primary Contact (MDPC). The department should also specify a back-up, or person of secondary responsibility, should matters arise when the MDPC is unavailable.

6.2.6: Merchant Account Fees for City Departments: The department which owns the merchant account and receives the benefit of the revenue is responsible for all costs associated with payment card processing. These costs include, but are not limited to, merchant account setup and administrative fees, equipment purchases, recurring monthly costs, and fees based on a percentage of every transaction from each credit card brand.

6.2.7: Card Acceptance

Merchant departments accepting cards as payment must:

- Obtain the signature of the cardholder on the receipt.
- Verify signature of cardholder at the time of the transaction for card-present transactions.
- Verify that the payment card's expiration date is valid.
- Verify that only the last four digits of the payment card number are printed on the receipt and provide a duplicate copy to the cardholder.
- Review payment card charges as not exceeding the transaction amount of purchase.
- Ensure that refunds are made to the payment card that was used during the transaction. No transactions should be refunded in cash or to a different

payment card.

- Refrain from accepting cardholder data that utilized end-user messaging technologies (e.g., e-mail, voicemail, instant messaging, and text messaging).

6.2.8: Annual PCI DSS Self-Assessment: TTX with partnership from CON will contact each department/agency to schedule their annual self-assessment. Each department/merchant must complete an annual self-assessment questionnaire to attest compliance with this policy, PCI-DSS, and other applicable standards and policies. Merchant departments found not in compliance will work with their departmental IT and CON to implement the appropriate remediation activities.

6.2.9: Specific details regarding processing and reconciliation will depend upon the method of payment card acceptance and type of merchant account. Detailed instructions will be provided when the merchant account is established and will be also available by contacting TTX @ TTX.BankingTreasuryAccounting@sfgov.org.

6.3 Cardholder Data Processing & Collection

6.3.1: Collected cardholder data must be restricted only to those users who need the data to perform their jobs. Each merchant department must maintain a current list of employees with access to it and review the list monthly.

6.3.2: All equipment used to collect data must be secured against unauthorized use or tampering in accordance with the PCI-DSS requirements. All computing platforms used for entering cardholder information into online web forms must be locked-down in accordance with the CCSF Cybersecurity Requirements.

6.3.3: Email should not be used to transmit payment card or personal payment information, nor should it be accepted as a method to supply such information. If payment card data is received in an email:

- The email should be replied to immediately with the payment card number deleted stating that the City does not accept payment card data via email as it is not a secure method of transmitting cardholder data. The reply email should not include the cardholder information.
- The email should be deleted from the inbox and the trash folder.

6.4 Cardholder Data Storage and Destruction

The goal of the PCI-DSS is to protect cardholder data and sensitive authentication data wherever it is processed, stored or transmitted. The security controls and processes required by PCI-DSS are vital for protecting all payment card account data, including the PAN - the Primary Account Number - printed on the front of a payment card. Merchants, service providers, and other entities involved with payment card processing must never store sensitive authentication data after authorization. This includes the 3 or 4 digits security code printed on the front or back of a card, the data stored on a card's magnetic stripe or chip (also called "Full Track Data") and personal identification numbers (PINs) entered by the cardholder.

6.4.1: Cardholder data, whether collected on paper or electronically, must be protected against unauthorized access. Any media, including paper copies that contain cardholder information, must be treated as confidential. Electronic cardholder data should not be retained either in electronic / paper form.

6.4.2: Physical security controls must be in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents or electronic files containing cardholder data. Access must be authorized and based on individual job function, and be revoked immediately upon termination, including, but not limited to, the recovery or disabling of all keys, access cards, etc. Any paper copies of cardholder information must be securely stored in a locked location when not in use.

Physical storage of electronic and physical media containing payment cardholder data must be done in a secure environment which includes locked containers according to CCSF Cybersecurity Requirements.

6.4.3: Portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited to, the following: laptops, tablets, media disks, flash drives, and portable external hard drives. CCSF policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. Devices should be stored in a safe/secured place.

6.4.4: Cardholder data should not be retained any longer than a documented business need; after which, it must be deleted or destroyed immediately following the required retention period. The maximum period the data may be retained is for a maximum of three years. A quarterly schedule of deleting or destroying data should be established in the merchant department to ensure that no cardholder data is kept beyond the record retention requirements.

6.4.5: Purchasing Card data shall be protected in a similar manner and institute the above components, particularly in regard to storage and disposal of cardholder data.

6.4.6: In the event manual credit card payment slips that include credit card processing data are processed, these must be hand delivered to the merchant department's Finance Unit on the same day using a secure envelope and a procedure for verifying delivery.

6.4.7: Do not publicly display cardholder information or leave it unattended; do not disclose cardholder information to others.

6.4.8: When paper copies of cardholder information are no longer necessary, they must be shredded using a PCI-compliant crosscut shredder.

6.4.9: Encryption key management (if applicable) should be protected according to CCSF Cybersecurity Requirements.

6.5 PCI DSS Training

Department of Technology and TTX will ensure that security awareness training is provided to all relevant city staff, and Department Leadership will identify agency staff, as well as associated third-parties (as applicable). Training materials may be provided either by the City Cybersecurity Team, or contracted third-party security resources, as determined by TTX. TTX will coordinate the training, and the Departmental Information Security Officer/ Liaison will:

- Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security. The program may include web-based, pre-recorded and in-person formal training, as well as notifications to employees on security topics, such as malware outbreaks and phishing scams. This training satisfies PCI DSS requirement 12.6.1.
- Coordinate training for personnel to be aware of attempted tampering or replacement of devices. This will be required for any departments that utilize equipment that can directly interact with a card, even if not utilized specifically for that purpose. Common examples of POS systems are USB-connected readers, or any readers incorporated into POS terminals, as well as POI swipe devices. This training satisfies PCI DSS requirement 9.9.
- Train staff with security breach response responsibilities on an annual basis, including how to communicate a data breach, potential or confirmed. (See below). This training satisfies PCI DSS requirement 12.10.4.
- Communicate new hires in a timely manner such that appropriate security training can be provided in accordance with this policy.
- Provide training to personnel upon hire, and annually thereafter. Employees will be required to acknowledge, in writing or electronically and at least annually, that they have read and understand the information security policy. Department Leadership will retain evidence of personnel acknowledgment for at least (1) year, which may be subject for audit by TTX.

6.6 Cardholder Data Breach

6.6.1: Anyone who learns of an actual or potential cardholder data security breach, including the suspicion that payment card data has been exposed, lost, stolen, or misused, must immediately inform the Director of Treasury Services at TTX, City Cybersecurity Team, their Department's CFO, and the Departmental IT Director/Head. The Director of Treasury Services at TTX (primary) will alert all necessary parties immediately, including:

- the designated BAMS Business Consultant (identified by TTX) to initiate the BAMS Merchant Incident Response Team (MIRT).
  - The MIRT would then engage with CCSF Personnel to obtain information and determine next steps
- Local law enforcement and/or the local office of the United States Secret Service

The BAMS procedure: "What to do in the event of a Suspected Data Breach" (see Appendix B) should be followed, and CCSF staff should be prepared to work with BAMS MIRT during the incident.

6.6.2: Indications that such an investigation may be necessary include, but are not limited to, the following:

- A computer or device involved in credit card processing is compromised. You may observe a virus or other malware installed on the system or that unauthorized configuration changes have been made that cannot be adequately explained.
- Vulnerability is discovered that could be used to gain unauthorized access to cardholder data.
- An external report is received that indicates that the City may be a source of fraudulent transactions, or that cardholder data from the City has been accessed without authorization.
- Paper, tapes, USB-keys, laptops, or other media containing cardholder data has been lost or cannot be accounted for.
- Cardholder data has been discussed in public or overheard without authorization.
- Any of the above that occurs with a service provider or other third party involved in payment card processing for the City.

6.6.3: In the event a cardholder data breach involving non-electronic resources (for example, paper documents) is suspected, the Director of Treasury Services at TTX, Department CFO, and CON must be notified immediately.

6.6.4: If you suspect credit card fraud, notify the Director of Treasury Services at TTX, your Department CFO, and CON immediately.

6.7 PCI Risk Assessment

Annually, TTX, in partnership with CON and Departmental IT, will facilitate a formal Risk assessment process in which current threats and vulnerabilities to the City's PCI networking and processing environment are analyzed according to CCSF Cybersecurity Requirements. The CON will prepare a report including recommendations and deliver to TTX, City Cybersecurity Team and Departmental IT who will review the report and develop a corrective action plan.

6.8 Ongoing Compliance Monitoring

Periodic reviews of safeguarding and storing of payment card information are conducted by the CON, and payment card handling procedures are subject to audit. In addition, the Department's IT in partnership with the CON and City Cybersecurity Team periodically conducts assessments of security controls put in place to safeguard technology implementations, including, but not limited to, periodic network-based vulnerability scans.

All transaction and activity logs from relevant and critical systems within the cardholder environment shall be stored using City Cybersecurity approved log management system and shall be reviewed weekly. Logs from these systems shall be retained for one year from their creation date. Logs include, but are not limited to, user identification, type of event, date and time, success or failure indication, origination of event, identity or system component of affected data, or resources. Where a system allows, audit trails shall be implemented and kept to link all access to system components to individual users.

City departments or agencies with Merchant Account Numbers that do not comply with this policy and approved protection, storage, and processing procedures may lose the privilege to serve as a payment card merchant and the ability to accept card payments.

Individuals in violation of this policy are subject to the full range of sanctions. Refer to Section 4 "Consequence of Non-Compliance" for details.

6.9 Third Party Vendors and Service Providers

All service providers and third-party vendors contracted by the City who provide payment card services must process payment cards and handle cardholder data according to the PCI-DSS. Departments who work directly with third-party service providers must maintain a list of their service providers and:

- Ensure contracts include language that states that the service provider or third-party vendor is PCI compliant and will protect all cardholder data.
- Annually audit the PCI compliance status of all service providers and third-party vendors, including request for current evidence of PCI compliance. such as a PCI Attestation of Compliance (AOC). Note that a lapse in PCI compliance puts CCSF at risk, and could result in termination of the vendor relationship.

The City reserves the right at any time to request proof of PCI DSS compliance via an attestation of compliance verifying that the vendor/service provider uses secure standard financial industry practices in its financial transactions. All Remote Access should be turned off when not in use. Alternately, the vendor is considered compliant if they appear on one of the global registries listed below:

- VISA Global Registry of Service Providers
- MasterCard Compliant Service Provider List

6.10 Inventory of POI devices and Inspection for tampering and substitution

All CCSF agencies using credit card payment capture (Point of Interaction; "POI") devices for processing customer transactions must ensure that all POI devices are secured in accordance with documented physical security methods, including inventory checkpoints, and regular inspections to monitor for substitution or tampering of the POI devices.

CCSF agency personnel will maintain an up-to-date inventory of the devices in their possession, and in operations per the process indicated in this document. POI device inspections will be completed according to the process indicated in this document.

Agency personnel are required to report lost or stolen POI devices, as well as POI devices suspected of being compromised.

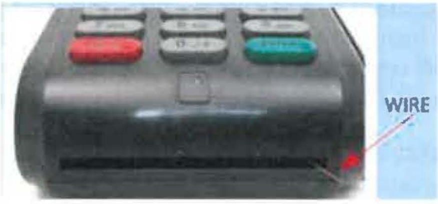
Completing POI Device Inventory and Substitution and Tampering Inspection

PURPOSE / OBJECTIVE

- Provide awareness of the vulnerabilities associated with the use of the POI devices in use by each CCSF agency.

- Provide direction for proactive physical security of the associated POI devices using an inventory process, to ensure that there have been no substitutions of correct devices with malicious devices.
- Provide guidance[1] on how to identify if the devices used in your retail location or in Storage (see note[2]) have been compromised. Compromised devices include those that have been tampered with (including, but not limited to, installation of skimming devices).

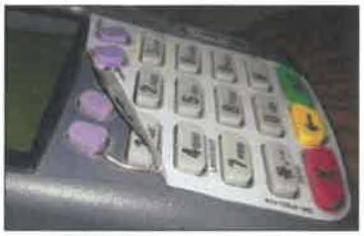
    - Skimming is the unauthorized capture and transfer of payment data to another source for fraudulent purposes and is different than mass data-compromise breaches. Skimming can capture payment data directly from the magnetic-stripe of the consumer's payment card via a compromised swipe terminal with an unauthorized data capture device inserted the card slot. This may be noticed with an unknown wire sticking out of the card slot.



    - Staff should also be aware of the addition of keypad overlays, which can be as simple as sticker that forms to the device and covers the keyboard area. Overlays may hide damage due to tampering, conceal wires intended for logging keystrokes such as for PINs.

[1] Additional resources: PCI PIN Transaction Security Program Requirements - https://www.pcisecuritystandards.org/documents/Skimming%20Prevention%20BP%20for%20Merchants%20Sept2014.pdf

[2] Applicable for those agencies who store devices on premises, or where a third party is used for offsite storage.



- What to look for in your POI devices – General:
  - Any indicator of physical condition outside of "normal use".
    - For example: scratching of the device in places where there shouldn't be regular contact with surfaces, and / or scratching associated with the removal of screws or forced entry.
  - Indicator of an installed skimming device (see above)

DEVICE INVENTORY PROCESS

On a semi-annual basis, agencies should verify the inventory of the devices (either in the retail location, or in storage) by documenting the Serial Number (SN) on each device and comparing the information to what was previously recorded when the device was deployed, or with the identifier in any corporate asset management system. Pending how the SN is recorded, Retail staff may need to simply report the information to the TTX Treasury/Banking Team for their verification using the appropriate application.

DEVICE SUBSTITUTION AND TAMPER CHECK PROCESS

On a semi-annual basis, agencies should verify the state of the devices (either in the retail location, or in storage) by following the appropriate steps for the devices used by your agency. Document the outcome of the effort, noting if any substitution or tampering has occurred on each device. Report any observations of substitution or tampering immediately to the TTX Treasury/Banking Team for action to be taken as needed, and in accordance with applicable Incident Response procedures. Please utilize the documentation provided to your agency by TTX, and / or the Department of Technology.

AWARENESS OF SUSPICOUS BEHAVIOR

It is understood that many of the POI devices in use by the agencies are intended for direct use by CCSF customers. However, there are several devices that are intended for facilitated use by a CCSF employee to assist customers in payment processing.

Where customers are intended to interact directly POI devices in publicly accessible locations, suspicious behavior might include:

- Lingering around the device without evidence of intended use. For example, not actually interacting with the devices, but waiting around for when they might be able to manipulate the device when no one is looking.
- Manipulating the device, including using hand tools, in an attempt to physically alter the device

and / or take it apart.

Where customers NOT are intended to interact directly with the POI device, and the operators are intended to be CCSF staff only, suspicious behavior might include:

- Attempts to gain access, or successfully access, to employee-only areas, such as behind a customer service window, or counter.
- Lingering around CCSF employee entrance points to back office locations.

IDENTIFICATION OF REPAIR / MAINTENANCE PERSONNEL

Agency's liaisons are expected to report to TTX Treasury/Banking any required repair or maintenance on their POI devices furnished by the City's Merchant Services Provider. TTX will coordinate with the service provider for the appropriate repair or maintenance.

Policy Exception (or Waiver)

Any request for exception (or waiver) to this policy must be submitted in writing and will be reviewed on a case by case basis. Exceptions shall be permitted only after written pre-approval from the TTX and final approval from the department director or designee are made. Waiver Requests are documented, stored, monitored, and tracked. All waivers are reviewed annually for extension purposes and cancelled as required.

Related URLs

- Payment Card Industry Data Security Standard (PCI DSS)
- PCI PIN Transaction Security Program Requirements / Skimming Prevention
- American Express
- Discover Financial Services
- MasterCard Worldwide
- Visa Incorporated
- SF City COIT Policies
- PCI Security Standards Document Library
- PCI Security Standards P2PE Solutions
- PCI Security Standards Network Segmentation Guidelines

City and County of San Francisco

Payment Card Processing and Data Security Standard Compliance Policy

Version 1.2

Applicable to ALL City and County of San Francisco employees including contractors, interns, volunteers, and suppliers as well as non-employees acting as agents of the City who handle, process, support, or manage payment card transactions.

Policy Revision History

Date	Version	Author	Comments
10/12/2018	1.0	Evelyn Mora	
10/28/2019	1.1	Evelyn Mora	Updated email address on page 11 + 12; and URL on page 21
02/10/2020	1.2	Evelyn Mora	Changed retention time from 90 days to 3 years in Section 6.4.4, page 14.

Policy Location:

The CCSF PCI DSS policy can be found at the Office of the Treasurer & Tax Collector website at https://sftreasurer.org/banking-investments/banking-services-city-departments under **Electronic Payments** tab.

Policy Approvals

Jose Cisneros	Treasurer		
Print Name	Title	Signature	Date
Tajel Shah	Chief Assistant Treasurer		2/22/2020
Print Name	Title	Signature	Date

Appendix A: BAMS - What to do if compromised

A Guide Provided by Bank of America Merchant Services

Bank of America
Merchant Services

A data security breach can lead to a data compromise; a prompt response may reduce a merchant's financial losses.
The card organization rules and regulations require that all data security breaches involving card holder information be reported.

The following step-by-step instructions are recommended when a merchant suspects they have experienced a data security breach:
1. Immediately contain and limit the exposure. Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information. To preserve evidence and facilitate the investigation:
• Do not access or alter compromised systems (i.e., don't log on to the machine and change passwords, do not log in as ROOT).
• Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable).
• Preserve logs and electronic evidence.
• Log all actions taken.
• If using a wireless network, change the Service Set IDentifier (SSID) on any access point or any other devices that may be using this connection with the exception of any systems believed to be compromised.
• Be on "high" alert and monitor all systems with cardholder data.
2. Alert all necessary parties immediately. Be sure to contact:
• Bank of America Merchant Services through:
o Customer Service at 1.800.228.5882 if no designated Relationship Manager
o Relationship Manager, if applicable
• Local law enforcement and/or the local office of the United States Secret Service
3. Be prepared to provide all compromised card accounts to Bank of America Merchant Services upon request.
4. Provide an Incident Response Report within three business days of the reported compromise.
5. Contain/control the event per Visa's Cardholder Information Security Protection (CISP) and MasterCard's Site Data Protection (SDP) program guidelines.
6. Be prepared to hire a certified third-party vendor to conduct forensic investigation if

required. Upon request, forward forensic investigation report to Bank of America Merchant Services.

7. Schedule validation of PCI examination and system scan. The scan must be conducted quarterly. Upon request, be prepared to forward results to Bank of America Merchant Services.

To obtain information on the PCI DSS go to: www.pcisecuritystandards.org.

Appendix B: Employee Policy Acknowledgement

I have read and acknowledge understanding of the content in this document: PCI-DSS Policy, which includes expectations for completion of POI Device Inventory and Substitution and Tampering Inspection.

Additionally, I acknowledge that I am responsible to follow the policy and process steps outlined herein at the agency location where I am staffed.

I also understand and have been instructed that if I have any questions during my employment that I should contact my supervisor/manager or IT Dept. If at any time I fail to uphold the security precautions detailed herein or any other company policies or procedures, it may be grounds for disciplinary action up to and including immediate termination.

Employee (Print Name)

Date

Employee Signature

Agency Office Location

Agency Manager (Print Name)

Agency Manager Signature