

Payment Card Industry (PCI) Governance Policy

Contents

- I. Background & Purpose ..... 3**
  - A. Background ..... 3*
  - B. Purpose ..... 3*
- II. Scope & Applicability ..... 3**
- III. Custody of PCI Data ..... 4**
- IV. Policy Directives ..... 4**
  - A. Compliance Required ..... 4*
  - B. System Requirements ..... 4*
  - C. Training Requirements ..... 4*
  - D. Capture Device Protection Measures ..... 4*
  - E. Regular Inspection of Capture Devices ..... 4*
  - F. Prohibition on Transmission of Data ..... 5*
  - G. Custodian Responsibilities ..... 5*
  - H. Prohibition on Sale or Purchase of Payment Card-Related Information ..... 5*
  - I. Pre-Hire Background Check ..... 5*
  - J. Acknowledgment ..... 5*
  - K. Retention Policy ..... 5*
- V. Prohibition on Incidental Use ..... 6**
- VI. Roles and Responsibilities ..... 6**
  - A. Appointment of PCI-DSS Compliance Officer as Central Coordinator ..... 6*
  - B. Responsibilities of Central Coordinator ..... 6*
  - C. Department Compliance Responsibilities ..... 6*
  - D. Approval of Payment Card Processing Software and Equipment ..... 6*
- VII. Enforcement ..... 6**
  - A. Policy Statement ..... 6*
  - B. Enforcement Action ..... 6*
- VIII. Auditing ..... 7**

*A. Systems Monitoring*..... 7

*B. Reporting*..... 7

*C. Provision of Systems Monitoring Information to Law Enforcement*..... 7

**IX. Reporting** ..... 7

**X. Security Exemption Process** ..... 7

**XI. Reference** ..... 7

**PCI Governance Policy Acknowledgment** ..... 8

## **I. Background & Purpose**

### ***A. Background***

Napa County accepts credit/debit card payments as a convenience to our residents and customers. Departments may accept Visa, MasterCard, Discover, American Express and debit cards with a Visa or MasterCard logo. Departments that process credit/debit card payments are assigned unique merchant accounts. Credit/debit card merchants at Napa County are required by this policy to follow strict procedures to protect customer payment card data as PCI-DSS (Payment Card Industry Data Security Standard) compliance is required of all merchants. Accordingly, controls must be in place for handling and restricting of payment card information, computer and internet security, as well as the reporting of payment card information breaches. Although the primary focus of the PCI-DSS is on web-based sales and processing payment card information via the internet, other services have the potential to expose cardholder information. Therefore, all County credit card merchants, including merchants transmitting via a terminal on a dedicated phone or Ethernet line, must comply. This acceptable use policy is established and implemented regarding PCI system use, system security, and determining an acceptable level of risk as well as clearly defining security responsibilities and the expected behavior of all individuals with access to the system.

Unauthorized or improper use of Payment card data may compromise the confidentiality, integrity, or availability of sensitive data, information systems, or other critical County resources.

Additionally, the appropriate use of information assets benefits the County by strengthening the protection of the County and its personnel and business partners from illegal or potentially damaging activities.

### ***B. Purpose***

This policy defines and establishes the requirements for the appropriate use and safeguarding of payment card information in compliance with PCI-DSS.

## **II. Scope & Applicability**

This policy is applicable to all County departments/locations that process, transmit or store cardholder information in a physical or electronic format. This pertains to ALL transactions including those initiated via the telephone, over the counter, via the internet, etc. All computers and electronic devices are governed by PCI-DSS. This includes, but is not limited to, servers that store payment card numbers, workstations that are used to enter payment card information into a central system, and any computers or credit/debit card swipe devices through which payment card information is transmitted. Furthermore, this policy applies to all personnel with

access to payment card information, including employees, consultants and temporary workers, as well as any third-party vendors that may process payment cards on behalf of Napa County.

The policy statements contained herein are a supplemental set of controls meant to complement the existing Napa County Acceptable Use Policy covering all Napa County information assets.

### **III. Custody of PCI Data**

Employees, contractors, and third-party service providers are custodians of PCI data, not owners. Access to PCI data is granted solely for official County business and must adhere to all applicable County policies, the PCI Data Security Standard (PCI DSS), and relevant state and federal laws.

Individual access and use of payment card data is neither personal nor private. As such, Napa County management reserves the right to monitor and/or log all personnel use of county information assets.

### **IV. Policy Directives**

#### ***A. Compliance Required.***

Compliance with PCI-DSS is required of all County personnel and departments that accept, process, transit, or store payment cardholder information.

This includes any County employee or contractor who, in the course of doing business on behalf of Napa County, is involved in the acceptance of payment card and e-commerce payments for the County.

#### ***B. System Requirements.***

Only PCI-DSS compliant equipment, systems, and methods (as approved by the Coordinator) may be utilized to process, transmit, and/or store cardholder information.

#### ***C. Training Requirements.***

County personnel and contractors who, in the course of doing business on behalf of Napa County, are involved in the acceptance of payment card and e-commerce payments for the County must attend training specific to PCI-DSS standards at least annually.

#### ***D. Capture Device Protection Measures.***

Protect devices that capture payment card data via direct physical interaction with the card from tampering and/or substitution.

#### ***E. Regular Inspection of Capture Devices.***

Inspect the card-reading devices at least monthly to look for tampering or substitution.

***F. Prohibition on Transmission of Data.***

Transmitting payment card information by email or fax is forbidden. Never send unprotected PANs by end-user messaging technologies (i.e. email, instant messaging, SMS, chat, etc.)

***G. Custodian Responsibilities.***

County personnel and contractors who, in the course of doing business on behalf of Napa County, are involved in the acceptance of payment card and e-commerce payments for the County are responsible for protecting cardholder information in accordance with PCI-DSS and Napa County policy and therefore may not acquire or disclose cardholder data, nor use said data for any unauthorized or improper purpose

***H. Prohibition on Sale or Purchase of Payment Card-Related Information.***

County personnel and contractors who, in the course of doing business on behalf of Napa County, are involved in the acceptance of payment card and e-commerce payments for the County may not sell, purchase, provide, or exchange said information in any form including but not limited to imprinted sales slips, carbon copies of imprinted sales slips, mailing lists, tapes, or other media obtained by reason of a card transaction to any third party. All requests to provide information to any party outside of your department must be coordinated with the Coordinator in the Treasurer-Tax Collector's Office. This applies also to contractors or agents who obtain access to payment card or other personal payment information in the course of conducting business on behalf of the County.

***I. Pre-Hire Background Check.***

County personnel and contractors who, in the course of doing business on behalf of Napa County, are involved in the acceptance of payment card and e-commerce payments for the County will be subject to background screening prior to hire to minimize the risk of attacks from internal sources.

***J. Acknowledgment.***

County personnel and contractors who, in the course of doing business on behalf of Napa County, are involved in the acceptance of payment card and e-commerce payments for the County must acknowledge they have read and understood this policy and applicable information security and privacy policies immediately upon gaining access to Payment card data and annually thereafter via the PCI Governance Policy Acknowledgment.

***K. Retention Policy.***

Napa County shall retain the completed PCI Governance Policy Acknowledgment for each employee or contractor involved in the acceptance of payment card and e-commerce payments for the County for the applicable period.

## **V. Prohibition on Incidental Use**

Incidental personal use of County PCI information assets is strictly forbidden.

PCI information assets must only be used in conjunction with authorized County business.

## **VI. Roles and Responsibilities**

### ***A. Appointment of PCI-DSS Compliance Officer as Central Coordinator***

The PCI-DSS Compliance Officer will serve as the Coordinator of PCI activities, with assistance from the Chief Information Security Officer.

### ***B. Responsibilities of Central Coordinator***

The Coordinator must approve each merchant bank or processing contact of any third-party vendors, include processors, software providers, payment gateways, or other service providers on behalf of Napa County.

### ***C. Department Compliance Responsibilities***

All County credit card departments must prove compliance to the Coordinator by completing an annual PCI-DSS self-assessment questionnaire and, if applicable, allow for remote external scans by a PCI approved quality assessor.

### ***D. Approval of Payment Card Processing Software and Equipment***

All contracts or purchases of software and/or equipment related to payment card processing will be originated and/or approved by the Coordinator and the Chief Information Security Officer. This applies regardless of the transactions method or technology used.

## **VII. Enforcement**

### ***A. Policy Statement***

Security breaches or lack of adherence to the requirements surrounding proper handling of credit/debit card information could result in serious consequences for Napa County.

### ***B. Enforcement Action***

County personnel who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County personnel, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County information assets, and other actions as well as both civil and criminal penalties.

## **VIII. Auditing**

### ***A. Systems Monitoring***

Individual activities on Napa County computer systems are subject to authorized monitoring to ensure system functionality, verify the application of prescribed security countermeasures, and protect against unauthorized use.

### ***B. Reporting***

Activity in violation of this agreement discovered in the course of authorized systems monitoring will be reported to the appropriate managerial staff.

### ***C. Provision of Systems Monitoring Information to Law Enforcement***

If authorized systems monitoring reveals possible evidence of criminal activity, such information may be provided to law enforcement personnel.

## **IX. Reporting**

All personnel must report actual or perceived policy violations or security incidents to the ITS Service Desk by telephone at (707) 253-4160, or by emailing [itsservicedesk@countyofnapa.org](mailto:itsservicedesk@countyofnapa.org).

For more information about reporting security incidents or policy violations to the Napa County CISO, go to <https://countyofnapa.sharepoint.com/sites/InformationSecurity>.

## **X. Security Exemption Process**

If compliance is not feasible or is technically impossible, if existing policy currently in place already meets these requirements, or if deviation from this policy is necessary to support a business function, the respective manager must formally request a security variance by submitting the IT Standards Exemption Request to the CISO.

## **XI. Reference**

PCI-DSS 4.0  
NIST SP 800-53

**County of Napa, California  
PCI Governance Policy Acknowledgment**

**BY SIGNING THIS FORM, I UNDERSTAND AND AGREE TO THE FOLLOWING:**

- I. I certify that I have read, understand, and agree to abide by the Napa County Payment Card Industry Governance Policy.

**Access & Use of PCI Assets is Limited to Official County Business**

- II. I understand that as a County employee or person who provides services to the County and who has access to Payment Card Industry (PCI) information assets and payment card information as part of the scope of my job duties, my right of access extends only to the information and information assets with which I have been assigned to work.
- III. I understand that accessing confidential information in files or other stored communications data other than that with which I am assigned to work, or using County equipment or online services to access and/or distribute such information is expressly prohibited.
- IV. I understand that incidental personal use of County PCI assets is strictly prohibited, and that PCI information assets must only be used in conjunction with authorized County business.

**Monitoring of County Systems**

- V. I understand that the County maintains the right to monitor, access, examine and disclose all data and information stored and transmitted by a County computer, telecommunications system, or other PCI asset in accordance with applicable laws and policies in order to ensure the proper use and maintenance of these systems.

**Enforcement**

- VI. I understand that failure to comply with any of the guidelines and requirements of the Napa County Information Technology Use and Security Policy, as well as other related County Policies and state and/or federal law could result in disciplinary action, up to and including termination of my employment.

**Periodic Review & Agreement to Complete Assigned Training**

- VII. I agree to periodically review the PCI Governance Policy and complete required training(s) as assigned by the County.
  
- VIII. In addition, changes or modifications may be made to this Policy and I understand that the law, this Policy and associated Guidelines regarding the use of the County’s information systems are continually evolving. Therefore, I understand that my regular review of this Policy and completion of assigned training is an ongoing obligation. I understand that updates to this Policy and associated Guidelines will be made available to me when changes or modifications to these occur.

**Retention of Acknowledgment in Personnel File**

- IX. I understand that this acknowledgement form will be filed in my personnel file and with Napa County Information Technology Services.

**EMPLOYEE ACKNOWLEDGMENT:**

Employee Name (print)	Signature
Employee’s Department	Date