EXHIBIT C
Section 31A: Napa County Information Technology Use & Security Policy
(as amended to include Payment Card Industry Addendum) (Redline)

Approved March 25, 1997
Revised ~~Effective~~ April 17, 2001
Revised January 27, 2026

NAPA COUNTY INFORMATION TECHNOLOGY USE & SECURITY POLICY

I. STATEMENT OF POLICY

Napa County has a significant investment in networked and on-line personal computer technology in order to assist employees in performing their jobs as efficiently as possible. In addition, advancements are being made to integrate voice and facsimile communications capabilities into the County's personal computer and network technology. As a result County employees are expected to ensure that computers, software, electronically stored data, facsimile, voice-mail equipment and other telecommunications systems are secure and used appropriately. This Policy is intended to apply to all County Information Systems equipment and devices, such as, personal computers, laptops, telephones, cellular phones, facsimile machines, hand-held devices and personal data assistants ("PDAs"). For further guidance, please refer to the Information Technology Use & Security Guidelines.

A. Purpose of Policy

1. To Establish Appropriate Use and Security Guidelines

The County makes every effort to provide employees with the best technology available to conduct the County's official business. Therefore, this policy has been created to advise all users regarding the appropriate use of, access to, and the disclosure of information created, transmitted, received and stored via the use of County computing and telecommunications networks, systems and equipment (collectively referred to as Napa County's Information Systems) and is intended to guide employees in the performance of duties as related to the use of these Information Systems. All employees and other users are required to adhere to this Policy. Certain departments may have unique requirements and are encouraged to develop separate policies and guidelines to address those issues.

2. To Provide Notice Regarding Expectation of Privacy

This Policy is also intended to notice employees that all County Information Systems, and their contents, are not confidential or private. That is, all data, including any that is stored electronically or printed as a document, is subject to audit, review, disclosure and discovery. **Such data may be subject to disclosure pursuant to the Public Records Act (California Government Code Section 6250 et. seq.).** ***Therefore, there is no expectation of privacy in the use of the County's Information Systems.***

Accordingly, the County reserves the right to access and monitor employee use of the County's Information Systems as well as any stored information, created or

received by County employees, with the County's Information Systems. The reservation of this right is to ensure that the County's Information Systems are used securely and appropriately in an ethical and lawful manner.

3. Applicability of This Policy to Other County Information Systems Users

Persons providing services to the County pursuant to a contract, vendors, or others who use the County's Information Systems during the course of performing their duties, will be held accountable for abiding by this Policy.

II. USE OF COUNTY INFORMATION SYSTEMS

A. General Use Statement

As improvements in County technology provide increased connectivity, the actions of one employee can impact the integrity and security of a telecommunications network used by many. A County employee, or any other user granted use of the County's Information Systems is expected to use those systems in a responsible manner by complying with all policies, relevant laws and contractual agreements.

All County Information Systems furnished to employees as well as to any other users, are Napa County property, intended for County business use. Use of County Information Systems for personal or commercial gain is prohibited. As a condition of employment, all employees will be required to sign a Standard of Conduct Agreement to acknowledge that they have read and understand this Policy, and, by so signing, consent to the County's accessing, reviewing and disclosing data or messages stored in the County's Information Systems. Department Heads are responsible for taking appropriate action for any violations of this policy.

These same Policy provisions, as well as other applicable County policies, apply to employees and any other users who access the County's Information Systems from remote sites.

B. Prohibited Use

The use of the County's Information Systems is restricted to "official County business", therefore, certain conduct is considered to be in violation of the County's Information Technology Use & Security Policy. In addition, such prohibited use may be in violation of other applicable County policies. Examples of prohibited use include, but are not limited, to the following:

- Personal use of or time spent for personal gain which exceeds incidental use.

- Using the County network to gain unauthorized access to other areas of the County system or other systems to which the County is connected. Such an action is a violation of this Policy as well as the Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C. § 2510.

- Attempting to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secured data.

- Knowingly or carelessly running or installing on any computer system or network, programs known as computer viruses.

- Violating terms of applicable software licensing agreement or copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images etc.

- Using County resources for private commercial activity such as creating products or reports for sale.

- Using electronic mail to harass or threaten others. This includes sending repeated, unwanted e-mail to another user.

- Using the Computer or Internet for political campaigns.

- Transmitting or reproducing materials that are vulgar, lewd, disturbing or sexually explicit or that otherwise violate existing County policy.

- Transmitting or reproducing materials that are slanderous or defamatory in nature or that otherwise violate existing County policy.

- Representing yourself as someone else, real or fictional, or sending a message anonymously.

- Downloading files from the Internet without first scanning them with the County's standard virus prevention software.

- Sending, posting or providing access to any sensitive or confidential County material or information unless for official County business purposes.

- Any violation of this Policy may result in disciplinary action up to and including termination as well as civil and/or criminal prosecution.

III. COUNTY INFORMATION SYSTEMS DATA ACCESS

A. Right of Access

1. The County has an unrestricted right of access to, inspection of, and disclosure of all voice and electronic data and software on any County equipment or media, at the request of appropriate County management. Such access and disclosure shall be in accordance with, and subject to any controls or restrictions imposed by applicable statutes or licenses, and in a manner consistent with preservation of evidentiary privileges.

2. Access to and review of voice and electronic data and Internet files on County Information Systems or media will follow supervisory lines. The supervisor and higher authorities under whom each staff member, other user, or official, works has the authority to access, inspect and disclose information, in accordance with the policies contained in this section, and consistent with applicable statutes or licenses. Peers and subordinates have no authority to access or disclose except as specifically granted by Department manager.

B. Obligation to Provide Access

Individual County employees, officials, or other users of County Information Systems or media are required to immediately provide access, decrypt and disclose any passwords, files or data to appropriate County management upon request. (All County employees, officials and other users shall be informed of this requirement and required to sign and acknowledge the Information Technology Use Standard of Conduct Agreement)

IV. SOFTWARE AND DATA OWNERSHIP

A. County of Napa Ownership Rights

1. Ownership rights for all software owned or controlled by the Napa County are vested in the "County of Napa" and are subject to the controls, policies, and procedures established by the Board of Supervisors, except where otherwise provided by software license or consultants under a contract. All software and documentation developed by or under the supervision (direct or indirect) of County programming personnel during work hours or using County Information Systems is the property of the County, until such time that the County abandons or transfers ownership except where such ownership or work is governed by an existing contract or agreement.

2. Data files are public records under the control of the appointed Custodians of Records for the respective County Departments, appointed or elective offices.

Ownership and control of such information shall be consistent with the California Public Records Act. The fact that individual items or collections of data or software are public in nature, or actually are public records, does not diminish the "property" aspects of County ownership.

3. The County may, in its sole discretion, assert, establish and exercise property rights in any and all data, files and software stored, maintained, created or placed on any County Information Systems including transferable media such as diskettes and tapes, unless that file or software is the licensed property of another entity. The assertion, establishment, and exercise of such rights may occur at any level along lines of supervisory authority. Such action shall be in a manner consistent with state and federal laws. Request for review of such action shall be to the applicable Department Head, whose decision is final.

4. The Department of Information Technology Services (ITS) has custodial responsibility for software licensing and data security administration. This includes all data and programs supporting network systems including the processing and storage of data for County Departments.

V. STATUS OF OTHER POLICIES

This policy supercedes and replaces all other policies on the same subject, especially that policy entitled, "NAPA COUNTY COMPUTER INFORMATION & SECURITY POLICY" adopted by the Board of Supervisors effective on or about March 25, 1997. The County reserves the right to amend or append this policy to include necessary guidelines for new developments in computer information use, such as storage of e-mail and stored data and integrated telecommunications systems with computer and electronic data systems, or whenever it is appropriate to conform to state and federal laws, rules and regulations.

NAPA COUNTY
Information Technology Use & Security Policy
STANDARD OF CONDUCT AGREEMENT

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

This is to certify that I have read and understand and agree to abide by the Napa County Information Technology Use and Security Policy.

I understand that as a County employee or person who provides services to the County, I have access rights only to the information with which I have been assigned to work and that accessing confidential information in files or other stored communications data other than those to which I am assigned to work, or using County equipment or on-line services to access and/or distribute to other County employees, contractors or members of the public, any unacceptable information obtained from any source, is expressly prohibited.

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 and/or telecommunications system in accordance with applicable laws and policies in order to ensure the proper use and maintenance of these systems.

I further 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.

I also agree to periodically review the associated Information & Technology Use & Security Guidelines. 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 is required. I understand that updates to this Policy and associated Guidelines will be made available to me when changes or modifications to these occur.

This acknowledgement form will be filed in my personnel file and with the Department of ITS.

EMPLOYEE ACKNOWLEDGMENT:

_____ _____
Employee Name (print) Signature

_____ _____
Employee's Department Date

Payment Card Industry (PCI) Addendum

Contents

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 requits 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 Information Security, Privacy, & Acceptable Use Acknowledgement and PCI addendum.

K. Retention Policy.

Napa County shall retain the completed Information Security, Privacy, & Acceptable Use Acknowledgement 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.

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