Approved March 25, 1997
Revised April 17, 2001
Revised xxxxx xx, 2026

NAPA COUNTY INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

Contents

I. Background & Purpose

A. Background

Napa County owns or controls significant information assets to assist employees in performing their jobs. Napa County's information assets include but are not limited to hardware devices (e.g. laptops, cell phones), software (e.g., Microsoft Office), cloud-based resources (e.g., Sharepoint and Microsoft OneDrive), and data, as they are strategic assets intended for official business use and are entrusted to personnel in the performance of their job-related duties.

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.

County employees have an ongoing obligation to ensure that these assets are secure and used appropriately. Unauthorized or improper use of County information assets may compromise the confidentiality, integrity, or availability of sensitive data, systems, or other critical County resources.

B. 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 Napa County's information assets and is intended to guide employees in the performance of duties as related to the use of these assets. All employees and other users are required to adhere to this Policy. Security policies supporting the effective execution of the principles detailed herein are the sole responsibility of the Information Technology Services department under the direction of the Chief Technology Officer. Certain departments may have enhanced requirements and are encouraged to develop separate policies and guidelines to address those issues.

2. To Provide Notice That There is No Expectation of Privacy When Using County Information Assets

This Policy is also intended to provide notice to employees and vendors that all County information assets, and their contents, are not confidential or private. 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 7920.000 et. seq.).** ***Therefore, there is no expectation of privacy in the use of the County's information assets.***

Accordingly, the County reserves the right to access and monitor employee use of the County's information assets as well as any stored information, created or received by County employees, with the County's information assets. The reservation of this right is to ensure that the County's information assets are used securely and appropriately in an ethical and lawful manner.

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

Persons providing services to the County pursuant to a contract, vendors, or others who use the County's information assets while performing their duties are subject to the provisions of this Policy.

II. Authority & Applicability

A. Authority

The Board of Supervisors adopts this policy pursuant to the County's legal authority to manage and protect County property and operations, and to supervise the conduct of County officers and the use of County resources (e.g., California Government Code §§ 25003, 25005). This policy provides users with notice regarding expectations of privacy and supports lawful, secure, and accountable use of County information assets and data, consistent with:

- Privacy rights (California Constitution, Article I, Section 1).
- Public records duties (California, Government Code § 7920.000 et seq.).
- Prohibitions on unauthorized access to computer data and systems (California Penal Code § 502).
- Prohibitions against misuse of public resources for personal purposes (California Government Code § 8314).

B. Applicability

The scope of this policy extends to all information assets owned or operated by Napa County, including but not limited to hardware devices (e.g. laptops, cell phones), software (e.g., Microsoft Office), cloud-based resources (e.g., Sharepoint and Microsoft OneDrive), and data, and to all personnel and entities authorized to use these assets.

III. Policy

A. Directives

1. Personnel must report any security concerns pertaining to County information asset security of which they become aware to their Napa County supervisor or contract manager and the Napa County Chief Information Security Officer (CISO), designee or appropriate Napa County Information Security staff. Security concerns include unexpected software or system behavior, which could result in unintentional disclosure of information or exposure to security threats, as well as potential threats or vulnerabilities.

2. Personnel must report any suspected or actual activities and/or events indicating misuse or violation of this Acceptable Use Policy to their Napa County supervisor or contract manager and to the Napa County CISO, designee, or appropriate security staff.

3. Personnel must acknowledge they have read and understood this policy and applicable information security and privacy policies immediately upon gaining access to County information assets and annually thereafter via the Information Security, Privacy, & Acceptable Use Acknowledgement.
4. Napa County shall retain the completed Information Security, Privacy, & Acceptable Use Acknowledgement.
5. Personnel must access only the information for which they have both (1) authorized access and (2) a need-to-know, meaning that the information is necessary to the performance of their job.
6. Personnel must protect County information assets from unauthorized access.
7. Personnel must inform the Napa County ITS Service Desk the date when access is no longer required (e.g., completion of a project, transfer, graduation, retirement, resignation).
8. Personnel must utilize their assigned County account credentials when accessing or registering for approved third-party applications or services that support this functionality. Personnel must use their assigned County account credentials to authenticate these services, rather than creating separate usernames and passwords.
9. The County considers certain County-approved tools, including but not limited to those used for collaboration, messaging, conferencing, file-sharing, text, and meeting recording, to be County information assets. Content created, transmitted, recorded, or stored using these tools is subject to monitoring, retention, disclosure, and public records requirements, and may not be externally shared or recorded unless authorized and conducted in accordance with County policy.

B. Prohibited Use

1. The use of personal accounts for work-related access is prohibited unless explicitly authorized by the County's Information Technology Department.
2. Personnel must not assume the privileges of others and attempt to gain access to information for which they have no authorization.
3. Personnel must not engage in any activity that attempts to circumvent County security controls, including but not limited to spoofing email, anonymous proxies or unauthorized encryption, or other activities that may degrade the performance of County information assets or may deprive an authorized user of access to county information assets.

4. Personnel must not use County information assets to store, send or arrange to send emails or access content that contains chain letters, unauthorized mass mailings, malicious code, or pornographic, racist or offensive material. This directive shall not be read to prohibit authorized personnel from storing or accessing material which violates this policy if doing so is necessary for the conduct of County business (e.g., Human Resources may store and access a record of an employee email which violates this policy for disciplinary purposes, Information Technology Services may store malicious code in a quarantine environment for the purposes of diagnosing and responding to the threats it poses, and the Sheriff, Child Welfare Services, County Counsel, District Attorney and Public Defender may preserve offensive materials in case files for the purposes of investigation, prosecution and defense).

5. Personnel must not use County information assets to engage in or solicit the performance of any activity that violates laws, regulations, rules, policies, standards and/or other applicable requirements issued by the federal government, the State of California, or Napa County.

6. Personnel must not use County information assets for personal enjoyment, private gain or advantage, personal gain, campaign activity, unsolicited advertising, unauthorized fundraising, or an outside endeavor not related to County business that exceeds permitted incidental use (See subparagraph III.C. for Incidental Use).

7. Personnel must not share their work-related account(s), passwords, Personal Identification Numbers (PIN), security questions/answers, security tokens (e.g., smartcard, key fob), or similar information or devices used for authentication and authorization purposes.

8. The use of personal or non-County–owned devices to access County information assets is prohibited unless expressly authorized by the County's Division of Information Technology Services. Authorized use is limited to approved remote access or mobile device solutions and must comply with all applicable County security, monitoring, and data protection requirements. Personnel must not connect or otherwise attach personal or unauthorized devices or equipment to county information assets.

9. Personnel must not introduce or use unauthorized software, firmware, or hardware to or on any County information asset.

10. Personnel must not physically relocate information assets without proper authorization.

C. Incidental Use

Government Code Section 8314 permits incidental personal use of County resources.

At Napa County this means:

1. Incidental personal use of County information assets, such as electronic mail, internet access, and printers or copiers, is restricted to County personnel only and does not include family members or others not affiliated with Napa County.
2. Incidental use must not result in direct costs to the County, cause legal action against, or cause embarrassment to the County.
3. Incidental use must be infrequent and not interfere with the normal performance of personnel work duties.
4. Storage of personal email messages, voice messages, files and documents within Napa County computer resources must be nominal.
5. Napa County management will resolve incidental use questions and issues using these guidelines in collaboration with the CISO, Office of Human Resources management, and County Counsel.

IV. Exemptions from Policy Applicability

If a manager believes compliance with this policy 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 manager must, upon authorization by the applicable department head, formally request a security variance by submitting the IT Policy Exception Request to the CISO. The CISO has discretion to make a final determination as to feasibility of compliance, applicability of existing policy, or necessity of deviation to support a business function.

V. Violations of Policy

Any violation of this Policy may result in disciplinary action up to and including termination of employment or contractual relationship, as applicable, as well as civil penalties and referral to appropriate authorities for criminal prosecution.