COUNTY OF SAN LUIS OBISPO

Countywide Information Security Program

Administrative Policy

Title: Information Security Program Acceptable Use Policy

Effective Date: November 5, 2004
Reviewed: April 2025
Revised: April 30, 2025
Approved by: Countywide Information Security Committee

PURPOSE

County computing assets, whether they are connected to the County network or not, are provided to County workforce members to be used for the purpose of conducting County business.

The purpose of this policy is to inform County of San Luis Obispo workforce members how to comply with County standards for the acceptable use of all County computing assets.

SCOPE and APPLICABILITY

The scope of this policy is the use of any County computing asset by any County workforce member regardless of location or access methodology.

ACCEPTABLE USE

Workforce members shall:

- Use County computing assets and information in compliance with County and department policies and procedures as well as all other pertaining laws and regulations.
- Ensure that software is properly licensed, free of malicious code and authorized before installation and use on County issued computing assets.
- Prevent unauthorized access, disclosure, modification, or misuse of sensitive information, including Personally Identifiable Information (PII), Criminal Justice Information (CJI), Protected Health Information (PHI), Federal Tax Information (FTI) and Payment Card Information (PCI).
- Report known or suspected security incidents such as the actual or potential loss of control or compromise of authenticators (hardware token, mobile phone used for authentication, etc.), passwords or sensitive information, including PII, CJI, PHI, FTI, or PCI, maintained by or in possession of the workforce member.

- Immediately report all lost or stolen equipment, known or suspected security incidents, account compromises, security policy violations, or suspicious activity.
- Secure sensitive information (on paper and in electronic formats) including logging off or locking systems when left unattended or when visitors are present.
- Permit only authorized workforce members to use County issued computing assets and to access sensitive information necessary to perform job functions.
- Sanitize or destroy electronic media and papers that contain sensitive information when no longer needed, in accordance with department records management and sanitization policies or as otherwise directed by your department head.
- Complete security awareness training within 30 days of employment and on an annual basis thereafter.
- Understand and comply with any additional department specific policies, standards, or procedures.

PROHIBITED USE

Workforce members shall not:

- Direct or encourage others to violate County or department policies, procedures, standards, or guidelines.
- Circumvent security safeguards or reconfigure systems except as authorized.
- Use another workforce member's account, identity, or password.
- Share their personal passwords or authentication tokens.
- Share sensitive information with third parties except as authorized through formal agreements to ensure data protection.
- Abuse authorized access to sensitive information.
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for personal use for self or others.
- Use County issued computing assets or County provided network resources as part of an effort to gain unauthorized access to other systems.
- Remove County issued computing assets or County provided network resources from County property without prior authorization and in accordance with County or department policies and procedures.
- Modify software without approval.
- Create, download, view, store, copy or transmit materials related to sexually explicit content, gambling, terrorism, computer hacking, or activities otherwise prohibited unless explicitly authorized.
- Transport, transfer, email, remotely access or download sensitive information, including PII, CJI, PHI, FTI, or PCI, unless such action is explicitly permitted as part of normal job duties.
- Store or transmit County information, unless legally acceptable, using unsanctioned storage media or internet services such as personal email or personal cloud storage solutions.
- Store sensitive information on devices or services not managed by the County such as unmanaged laptops, smartphones, USB flash drives or on remote systems or

cloud services without authorization or appropriate safeguards, as stipulated by County and department policies.

- Use County issued computing assets or County provided network resources for activities that are inappropriate or offensive to fellow employees or the public. Such activities include, but are not limited to hate speech, harassment, bullying, intimidation, or other abusive conduct that ridicules others based on race, creed, religion, color, age, sex, disability, national origin, or sexual orientation.
- Use County issued resources for regular personal use (such as using County email to create personal accounts like Netflix, reddit, or twitter), commercial use, non-profit use, political use, or personal profit (e.g. crypto-mining) unless expressly allowed with written approval from your department head and the Chief Information Security Officer or Chief Information Officer. **Exception – see Exception for Personal Use of County Provided Network Resources below.**
- Be provided access to information produced or maintained on County computing assets upon separation from the County. For example, upon retirement, workforce members will not be given access to County email accounts or data contained within.
- Create, copy, transmit or retransmit chain letters or other unauthorized mass mailings regardless of the subject matter.
- Connect personal or unauthorized information technology applications or systems to existing County network resources without the appropriate management authorization, including the installation of unauthorized network equipment.
- Intentionally acquire, use, reproduce, transmit or distribute any controlled information including computer software and information that includes information subject to the Privacy Act, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary information or export-controlled software or information.

Other Guidance on the Use of County-Owned Technology

- Any use of County issued computing assets or County provided network resources, including e-mail, Internet, or application usage, is made with the understanding that such use is not private, is not anonymous, and may be subject to monitoring.
- Workforce members do not have a right to, nor shall they have an expectation of privacy while using County issued computing assets or County provided network resources at any time.
- Workforce members have no inherent right to utilize County issued computing assets or County provided network resources for personal use. All information in County issued computing equipment, even personal information, is subject to discovery.
- Unauthorized or inappropriate use of County issued computing assets or County provided network resources could result in loss of use or limitations on use of equipment, disciplinary or adverse actions, and / or criminal penalties.
- Law enforcement and or/other County employees in situations where they are engaged in the performance of their job duties are authorized to use County

provided assets to perform their job duties without restriction unless doing so creates an unreasonable risk to the County Enterprise Network.
- Departments may adopt policies that are more restrictive than these guidelines.

Exception for Personal Use of County Provided Network Resources

- The County may provide a best effort wireless network for personal use, from personal devices, with the expectation that the behaviors described in this policy (Information Security Program Acceptable Use Policy) apply to its use and use of this network may be subject to monitoring.

Additional Rules for Workforce Members with Privileged Access

Staff who have elevated privileges have significant access to processes and information in systems. In addition, some non-technical roles have physical access to critical systems. As such, workforce members with privileged access have added responsibilities to ensure the secure operation of any County system.

Personnel with elevated privileges are to:

- Advise the asset owner on matters concerning cybersecurity.
- Assist the asset owner in developing security plans, risk assessments, and supporting documentation for the certification and accreditation process.
- Ensure that any changes to any system that affect contingency and disaster recovery plans are conveyed to the asset custodian responsible for maintaining continuity of operations plans for that system.
- Ensure that adequate physical and technical safeguards are operational within their areas of responsibility and that access to information is restricted to authorized personnel on a need-to-know basis.
- Verify that workforce members have received appropriate security training before allowing access to any system.
- Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing and review audit logs.
- Document and investigate known or suspected security incidents or violations and report them to the Chief Information Security Officer (CISO).

DEFINITIONS

Workforce Member:

Employees, and other persons whose conduct, in the performance of work for the County of San Luis Obispo, is under the direct control of the County of San Luis Obispo, whether they are paid by the County of San Luis Obispo or not. This includes full and part time employees, contractors, affiliates, associates, students, volunteers, interns, political positions, and staff from third party entities who provide services to the County of San Luis Obispo.

Network:

A network where:

(i) Establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or
(ii) Cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (at least concerning confidentiality and integrity).

An internal network is typically organization-owned yet may be organization-controlled while not being organization-owned.

Computing Asset:

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Note: Computing Assets also include specialized systems such as industrial/process control systems, telephone switching, and private branch exchange (PBX) systems, and environmental control systems.

Sensitive Information:

Any information that is required by Local, State, and/or Federal law that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization.

This includes business and operational information that is generated by County workforce members in the performance of their jobs.

SANCTIONS

Violations of this policy may result in disciplinary measures for the involved workforce members, up to and including dismissal. At a minimum, violations may result in the removal of access to the County Network, either temporarily or permanently.

REVIEW

This policy is to be reviewed annually to determine if it complies with current recommendations, guidelines, mandates, statutes, practices, and County of San Luis Obispo operations. If changes are required, the policy will be updated as needed.

Acceptable Use Policy Acknowledgement Form

I acknowledge receipt of this policy and understand that I am bound by its contents:

SIGNATURE	
NAME	
TITLE	
DEPARTMENT	
DATE	