# COUNTY OF SAN MATEO

## Software Policy

**Overview**
The installation and running of unlicensed software on the County network and/or County devices is strictly prohibited. With few exceptions, software is protected pursuant to relevant copyright laws and licensing agreement for its use, distribution, and reproduction. Any installation of unlicensed software is likely in violation of copyright protections. Furthermore, installation of unlicensed software could introduce malware to the County's network, making it vulnerable to outside attack.

**Policy Purpose**
The purpose of this policy is to ensure that all software purchased for and installed on County computers and servers is appropriately evaluated, licensed, installed, and used in accordance with its license agreement, County policies, and applicable laws.

**Scope**
This policy applies to all software, whether purchased, leased, or obtained as shareware or freeware, or cloud-hosted software solutions and applies to all employees, contractors, vendors, and agents, collectively known as workforce members, using the County of San Mateo's computing devices. This policy also covers all computers, servers, smartphones, tablets, and other computing devices operating within the County including all personal and home computers used for County business.

**Policy**
All software purchased or developed for or on behalf of the County of San Mateo shall be deemed the property of the County and shall be used in compliance with the license and/or contract agreement.

**A. Installation**

1. Only County-owned software shall be installed on County computing devices by authorized personnel.

2. Commercial software that has not been acquired through the County's procurement process is prohibited and shall not be installed on any County system.

3. Each software instance is required to have a license.

4. Software that requires installation on or that is distributed via the County's servers and networks must not be purchased or acquired without technical review by and agreement from the Information Services Department (ISD).

5. Workforce members may not install or distribute personally-owned software on any County-owned computing devices or network without the written permission of the Chief Information Officer (CIO) or designee.

6. Workforce members shall not attempt to disable or reconfigure the Personal Firewall software.

7. Should the software license permit, the CIO or designee may authorize certain employees to provide a copy of County licensed software for home use only when a business need can be demonstrated.

8. Software that is free and/or open-source and shareware, including limited use, such as academic version or restricted non-retail versions, shall not be installed on any County-owned devices.

9. Exceeding the permitted number of users for servers shall be considered an overuse of a software license and therefore an unauthorized use.

Installing non-County equipment, programs, or services that provide ongoing communications with the Internet is prohibited.

**B. Upgrades**

All software must be maintained within two software release or versions.

1. A legal copy of the software to be upgraded must already be installed on the computing device receiving the upgrade.

**C. Duplication**

1. Software shall not be duplicated except for backup and archival purposes by designated employees.

2. Workforce members who illegally reproduce or distribute software may be subject to civil damages and criminal penalties.

**D. Software as a Service**

1. Accounts for cloud-based software, e.g., Dropbox, Google Docs**,** shall not be set up with a County email and/or used for County business without the written approval of the CIO or designee.

2. All software, subscription-based or otherwise shall be approved by the CIO or designee prior to PROCUREMENT, per the B-1 policy of the County.

**E. Software Acquisition**

1. Workforce members requiring software other than that provided directly by the County must submit a request, stating the business need. For departments that subscribe to ISD's PC/Laptop service, requests should be made through ISD's Service Desk Ticketing System (ServiceNow). For non-subscription departments that support their own workstations, requests should follow the appropriate process as defined by the department's IT group. Each request shall be considered on a case-by-case basis.

**F. Audit**

1. The County may conduct periodic audits to ensure software compliance. County departments that manage IT for their workforce will conduct such audits in partnership with ISD.

**G. Software Destruction**

1. Software that has been deemed obsolete shall be destroyed by designated employees.
2. Workforce members who leave the County and who have County software (and/or data) installed on personal/non-County owned computers, must remove all such software and data prior to their departure from the County.

**H. Asset Management System**

1. ISD shall maintain a master IT Asset Management (ITAM) system for software licenses including user information. A department can leverage ISD's ITAM or operate its own software recordkeeping system, and will provide ISD with either real-time updates via a live feed or monthly bulk updates.

2. License and user information must be maintained in a secure place and updated annually.

**Responsibilities**

The CIO or designee will review this policy annually and recommend any necessary changes to the County Manager. Department Heads shall be responsible for advising the CIO or designee of all situations that require deviation from or exception to this policy. Exceptions must be granted by the CIO or designee in writing. It is also the responsibility of all County departments to ensure that their workforce members are familiar with this policy and for every workforce member to conduct their activities accordingly.

**Policy Enforcement**

The CIO or designee is the policy administrator for information technology resources and will ensure this process is followed. Additionally, Division Directors, managers and Department Heads are responsible for compliance with County policy within their respective administrative areas.

Any violations of this policy shall be reported to the CIO or designee. Violations will be investigated and may result in disciplinary action up to and including dismissal from County employment. Violators of this policy may also be subject to contract termination, denial of service, and/or legal penalties, both criminal and civil.

**Revision History**

| Effective Date | Changes Made |
|---|---|
| 8/30/2017 | Policy proposed |
| 7/31/2018 | Policy proposal updated |
| 6/22/2020 | Policy updated |