
Information Technology Use

324.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the proper use of department information technology resources and data stored as the result of such.

324.2 APPLICABILITY

This policy shall be applicable to all Department employees and unpaid staff (e.g. VIPs & interns).

324.2.1 TERMINATION, ABSENCE AND LAYOFF

Employees who are terminated, laid off or placed on administrative leave have no right to the contents of their e-mail, or voice mail messages and are not allowed access to the e-mail, computer file or voice mail system.

Supervisors may access an employee's e-mail, voice mail, and computer files at any time for County/departmental business purposes.

324.3 POLICY

It is the policy of the San Diego County Probation Department that employees shall use information technology resources, including telephones and voice mail, teleconferencing facilities, computers, software and systems, and other technological applications (e.g. fax machines) that are issued or maintained by the Department or personally owned in a professional manner and in accordance with the County of San Diego Administrative Manual Information Technology policies. These policies may be found at the County of San Diego Intranet Site. The information Technology policies contain a 0400 item (policy) number.

0400-01 County Information Systems – Management and Use

0400-02 Internet Use

0400-03 Computer Accounts – Management and Use

0400-04 Passwords – Management and Use

0400-05 Workstation – Use and Security

0400-06 Remote Access to County Network

0400-07 Telecommunications Systems – Management and Use

0400-08 County Information Systems – Solutions Planning and Development of Requirements

0400-09 Employee Bring Your Own Device (BYOD) Acceptable Use Policy

0400-09A Employee Owned Device User Consent and Waiver Agreement

0400-11 County Information – Classification, Protection Level, and Proper Security

Employees shall complete and sign the Telecommunications Policy Employee Acknowledgement form, which confirms the understanding of this policy.

Information Technology Use

324.4 RESTRICTED USE

Use of County-owned or County-purchased software by staff must be for tasks or assignments (e.g. telecommuting) authorized by the Department and is to be returned to the Department upon completion of tasks or assignments for which they have been used.

County computer databases can be accessed for professional and training purposes by all probation staff that has completed the California Offender Record Information (CORI) and California Law Enforcement Telecommunications System (CLETS) training. County computer databases are not to be accessed for personal purposes.

324.4.1 SOFTWARE

Employees shall not copy or duplicate any copyrighted or licensed software except for a single copy for backup purposes in accordance with the software company's copyright and license agreement.

To reduce the risk of a computer virus or malicious software, employees shall not install any unlicensed or unauthorized software on any department computer. Employees shall not install personal copies of any software onto any department computer.

When related to a criminal investigation, software program files may be downloaded only with the approval of the Information Systems Technology (IT) staff and with the authorization of the Chief Probation Officer or designee.

No employee shall knowingly make, acquire or use unauthorized copies of computer software that is not licensed to the Department while on department premises, computer systems or electronic devices. Such unauthorized use of software exposes the Department and involved employees to severe civil and criminal penalties.

Introduction of software by employees should only occur as part of the automated maintenance or update process of department- or County-approved or installed programs by the original manufacturer, producer or developer of the software.

Any other introduction of software requires prior authorization from IT staff and a full scan for malicious attachments.

324.4.2 HARDWARE

Access to technology resources provided by or through the Department shall be strictly limited to department-related activities. Data stored on or available through department computer systems shall only be accessed by authorized employees who are engaged in an active investigation or assisting in an active investigation, or who otherwise have a legitimate law enforcement or department-related purpose to access such data. Any exceptions to this policy must be approved by a Supervisor.

Information Technology Use

324.5 INSPECTION OR REVIEW

A Supervisor or the authorized designee has the express authority to inspect or review the computer system, all temporary or permanent files, related electronic systems or devices, and any contents thereof, whether such inspection or review is in the ordinary course of his/her supervisory duties or based on cause.

Reasons for inspection or review may include, but are not limited to, computer system malfunctions, problems or general computer system failure, a lawsuit against the Department involving one of its employees or an employee's duties, an alleged or suspected violation of any department policy, a request for disclosure of data, or a need to perform or provide a service.

The IT staff may extract, download or otherwise obtain any and all temporary or permanent files residing or located in or on the department computer system when requested by a Supervisor or during the course of regular duties that require such information. This includes, but is not limited to e-mails, phone records, electronic files, and internet history.