### 3.08.010 Employees Subject to Standards

Employees of the County who are subject to the Local Agency Personnel Standards as contained in the California Administrative Code, shall have such rights and privileges as may from time to time be set forth in this title. (Prior code § 2-223(a)).

### 3.08.020 Rules and Regulations Compliance

All County employees shall hold their positions subject to such rules and regulations which may be established by Resolution of the Board of Supervisors. (Prior code § 2-223(b)).

### 3.08.250 Employment of Relatives—Nepotism

Except as to persons already employed on the effective date of this section, no person related to a full-time elected or appointed County officer, employee or contract employee by blood or marriage to the third degree of relationship shall be appointed or transferred into a department employing such relative in a direct conflict of interest position. For the purpose of this section, a direct conflict of interest shall mean a situation in which the employee of the relative would be in a position to affect the terms and conditions of one another's employment, including making decisions about work assignments, compensation, discipline, advancement or performance evaluation. (Ordinance NS 1021 § 1 (part), 1981: prior code § 2-180.13).

**Note: The above-referenced provision also applies to personal service contracts and extra-help employees.**

### 3.32.110 Failure to Perform Duties

Except when on authorized leave, any employee who fails to report for duty and work during the officially established work hours and days of his employment, and any employee who participates in a work stoppage against the County, shall be considered to have committed an act or acts which shall be grounds for dismissal from County service. (Prior code § 2-203(k)).

### 3.20.130 Other County Employment

A. No person employed in a full-time position shall be permitted to work for compensation for the County in any capacity other than his regular position. Exceptions hereto may be authorized by Resolution of the Board of Supervisors upon a finding that the public interest requires employment of a County employee for the rendering of a special service or services and the payment of compensation therefor.

B. A person employed in a part-time position may work for compensation for the County in another capacity provided the total time for such position does not require more time than required for full-time position established for such type of work.

C. Notwithstanding the provisions of Subsection A of this section, a person employed in a full-time position shall be permitted to receive compensation from the County for providing foster care to a child duly placed with such person by an agency of the County. (Prior code § 2-216).

**3.36.040 County Employment During Vacation**

No person shall be permitted to work for compensation for the County in any capacity during the time of his or her paid vacation from County service, provided however, that there shall be an exception for Election Day service as a poll worker or precinct inspector, as follows:

A County employee may work for compensation in the form of the applicable statutory stipend and mileage allowance from the Registrar of Voters whenever that employee voluntarily utilizes regular days off, department-approved vacation time or department-approved compensatory time off to serve as, or attend training to serve as, an Election Day poll worker or precinct inspector. (Ordinance 857, § 2003; Ordinance CS 598 § 5(part), 1995).

**3.08.030 Legal Services by County Employees**

A. The County Counsel, District Attorney, and Public Defender, and such other attorneys as may be employed full time in their respective offices, shall devote full time to their official duties and may not engage in the private practice of law, except that they may represent themselves, their relatives and members of their families in probate proceedings and other unprotected legal matters, without fee, with deduction of time devoted thereto from accrued vacation time.

B. The County Counsel shall act as attorney for the Public Administrator in all estates in which he is executor, administrator with the will annexed or administrator. In such matters the County Counsel shall collect the attorney's fees allowed by law and pay them into the County Treasury. (Prior code § 2-223(c)).

**Outside County Employment (Moonlighting)**—Personnel Policy

Employees should review any outside employment or business endeavors with his/her supervisor to ensure there are no conflicts with County employment. There are specific outside County employment policies for law enforcement and attorneys. Please refer to the Conflict of Interest Policy and Code of Ethics located in Tab 16 for guidance.

## SMOKING IN COUNTY FACILITIES

### 9.53.010 Responsibility of employers

It shall be the responsibility of employers to provide a smoke free workplace for all employees, but employers are not required to incur any expense to make structural or other physical modifications. (Ordinance CS 516 § 2 part), 1993).

## SMOKING IN COUNTY VEHICLES

Smoking will be prohibited in all County cars.

All County officials and personnel shall adhere to the following code to build public trust and ensure equitable treatment for all:

## Trustworthiness

- Demonstrate the highest standards of personal integrity, truthfulness, and honesty in all public activities.
- Protect confidential information from inappropriate use.

## Respect

- Treat all individuals in a respectful, courteous, and professional manner.
- Respect the County's responsibility to comply with State and Federal regulations.

## Responsibility

- Uphold the public trust.
- Conduct and perform job duties diligently and promptly.
- Make no promises of any kind which conflict with one's public duty and responsibilities.

## Fairness

- Treat others with impartiality and equity and provide or accept no special favors or privileges that may be perceived as influencing the performance of one's duties.
- Impartially apply applicable laws and regulations to everyone.

## Caring

- Create and maintain positive relationships.
- Consider the consequences of decisions on those affected by them.
- Strive to find solutions to our customer's issues or problems and offer suggestions for improvement to leadership when appropriate.

## Citizenship

- Make decisions that benefit the public interest.
- Engage only in activities that are consistent with the performance of one's duties.
- Comply with all laws and regulations applicable to the county.

## ACCEPTANCE OF GIFTS AND OTHER TOKENS OF APPRECIATION BY COUNTY EMPLOYEES

California Penal Code Section 70 makes it a misdemeanor for any public employee or officer to receive any gratuity or reward or promise thereof for doing an official act. California Government Code Section 87300 and the County Personnel Policies Manual set forth the provisions by which every County department establishes a conflict of interest code. **This code designates certain County employees occupying decision-making positions who must annually report gifts received if valued at $50 or more.** An important rule to keep in mind is, when there are questions, seek advice, and, when in doubt, do not accept the gift and/or provide full disclosure as appropriate.

The following guidelines describe Stanislaus County policy regarding acceptance of gifts and other tokens of appreciation by County employees or agents of the County not formally designated in their department's conflict of interest code. These guidelines set forth the acceptable courses of action to take when such gifts are received from members of the public. Gift giving between and/or among County employees is regarded as acceptable and not a topic of concern in this document.

"County Employee" is defined as a person officially occupying a position with the County. This includes all probationary, permanent, full-time, or part-time employees or extra-help employees and others who are considered "agents" of the County as defined by contract between the individual and the County.

### A. Basic Tenet:

**Avoid any appearance of impropriety and any act which appears improper even though it may not be illegal, i.e., neither seek nor accept directly or indirectly favor for performing duties as an employee.**

1. **Do not discriminate** in the provision of services to the public. This means not receiving gifts or other tokens of appreciation in connection with services rendered in the performance of duties for which they are already paid and not bestowing special favors upon any member of the public in return for gifts or gratuities.

2. **Do not solicit any gift or accept or receive any gift** whether it be money, services, loan, travel, entertainment, hospitality, promises, or any other form under circumstances where it can be reasonably inferred or expected that the gift was intended to influence in the performance of official duties or the gift is intended to serve as a reward for official action on the part of the employee.

3. **Do not receive economic advantage or discount** not available to all County employees. Examples of these occurrences include but are not limited to free or reduced admission to places of amusement or sporting events.

**B. Basic Tenet:**

**Recognize the problem in advance; intervene immediately.**

Recognizing that on some occasions, especially at Christmas or other holiday times, gifts such as candy, fruit, plants, or other tokens of appreciation are given to employees or departments, the purpose of this document is to standardize County employee behavior when such gifts are received. Responsibility for implementation of the guidelines herein lies at the department level.

**C. Basic tenet:**

**When the cumulative value of gifts received is $50 or more, reporting is required under the Fair Political Practices Commission's rules and regulations.**

Gifts of $50 or greater individual retail value (or, if several smaller gifts, $50 cumulative value) must be reported on an annual basis following the provisions set forth in the Conflict of Interest Code.

**D. Basic tenet:**

**Use the departmental chain of command to remove any appearance of impropriety.**

1. If, during the course of his/her official duties, a County employee receives a gift directed personally to him/her or to his/her department, he/she is obligated to report receipt of the gift to the immediate supervisor. When in doubt about the acceptability of a particular gift, the employee should advise his/her immediate supervisor of the situation and allow the supervisor to make the appropriate decision using a standard of reasonable care and judgment.

2. It is Stanislaus County policy that, with the exception of alcoholic beverages, if a gift such as candy is opened and made available for all department employees to share, the action is acceptable. If the same gift, however, is taken home for an employee's singular benefit, the action is unacceptable. If the item is alcoholic in nature, nonperishable, or impossible to divide among employees for some reason, the recommended course of action, at the discretion of the Department Head, is to donate the item to a local charity or return the gift to the donor with a note of thanks. In this manner, no one employee benefits from receipt of the gift.

**E. Basic tenet:**

**Be courteous; explain the gift policy in positive terms if asked.**

If members of the public bestow gifts upon County employees or inquire about the County's policy as to acceptance of such gifts, be courteous in your explanation of the policy. If a gift is deemed by a Department Head to be unacceptable and, therefore, returned to the giver, the accompanying note of thanks should be brief, concise, and polite so as not to offend the giver or create a negative impression of County employees.

## POLICY STATEMENT

In addition to any Federal or State conflict of interest requirements which may apply, no member of any board, commission, or committee shall make, participate in making, or in any way attempt to use their position to influence a decision in which he or she knows or has reason to know he or she has a financial interest. In all such cases, the affected member shall disclose their interest in the records of the board, commission, or committee and shall refrain from participating in all discussions and votes concerning the matter in which they have a financial interest.

The purpose of this policy is not only to avoid actual improprieties but also the appearance of possible improprieties. Therefore, it is the policy of the Board of Supervisors that any doubts as to whether a member should refrain from participating in a particular matter should be resolved in favor of nonparticipation.

## MANAGEMENT RESPONSIBILITY

The Clerk of the Board shall provide all appointees to the County commissions, committees, and boards with copies of the Board's Conflict of Interest Policy.

## PURPOSE

The purpose of the County's technology-based systems is to share information and computing resources, and improve the way service is provided to the public. As modern technology provides connectivity, the actions of one person can impact the integrity and security of a telecommunications network used by many. Any employee given the privilege of using Stanislaus County's computing and information resources is expected to act in a responsible manner by complying with all policies, relevant laws, and contractual agreements related to computers, networks, software, computer information and data to which an employee has access.

## COMPUTER INFORMATION

All computer information, including e-mail, created or received utilizing County computing resources is the property of the County. Subject to applicable legal privileges and confidentiality requirements, all computer information entered or received on County computers, including e-mail, is public and is subject to disclosure upon the demand of the County at any time. The physical location of the computer does not alter this policy. Unauthorized printing or tampering with computer information is not allowed. (i.e.: changing data in a central data base without authorization)

## CONFIDENTIALITY/PRIVACY

There is no right to privacy in any information created or received on any County computer or through any County computing resource. This includes any and all e-mails sent to and from an employee, any Internet Websites the employee has accessed, or any information created, sent to or stored on any County computer or system. The County has the right to monitor the computer use of its employees, to read or download any information or e-mails which any employee has accessed, created, stored or downloaded, and will take the appropriate disciplinary action for any misuse. This includes the County Network system as well as the employee's own personal drive at his/her own workstation, and any private e-mails which are accessed through the County's Internet system (AOL Mail, Yahoo Mail, etc.).

Since network access and use are to be used for County business, employees shall have no right or expectation of privacy in any Internet or e-mail activity using County equipment or networks. This includes Internet or e-mail activity that occurs after business hours. The County has software and systems that monitor and record all Internet and e-mail usage. Each World Wide Web site visit, newsgroup or e-mail message and each file transfer into and out of our internal networks is recorded. Department Heads, management, supervisors, Management Information Systems, the CEO's office and County Counsel have the right to review any Internet or e-mail activity of any employee at any time for any reason. The County reserves the right to inspect

any and all files stored in private areas of the network or a computer system in order to assure compliance with this policy.

## NETWORK USE POLICIES

"Network" refers to the connection of a computer workstation to a server or any other computer system through a local or wide area network. This policy applies to all Internet, Intranet, e-mail, file transfers (FTP), web browsers, word processors, spreadsheets or other software that can use networks to communicate.

## ACCEPTABLE USES OF NETWORKS/COMPUTER SYSTEMS

Stanislaus County network access and use of computers are intended to be used to conduct County business. Employees are encouraged to use technical resources as an efficient and effective business tool.

Networks and computers must be used in a manner that does not jeopardize security, confidentiality, or place the County in a litigious position as a result of breaking any local; state or federal law pursuant to privacy, public record, or copyright.

## UNACCEPTABLE USES OF THE NETWORK/COMPUTER SYSTEMS

County network access or individual computer usage may not be used for transmitting, retrieving, receiving or storing of any communications of a discriminatory or harassing nature or materials that are perceived as being obscene. Harassment of any kind is prohibited by County policy. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference shall be transmitted. No abusive, profane or offensive language will be transmitted through the County's network system. Electronic media may not be used for any other purpose that is illegal, against County policy, causes discredit to the employee's department or the County, or is contrary to the County's best interest.

Computers and computer networks shall be used only for authorized County business. It is unacceptable for employees to use networks for personal gain or profit, or for personal reasons that would result in depleting resources, impeding the organization's ability to conduct business, or cause any interruption or delay in service to the public.

## NETWORK/COMPUTER COMMUNICATION

Each employee is responsible for the content of all text, audio or images that they place or send over the County's network system, or which appear on their computer (including screensavers). No electronic communication may be sent which hides the identity of the sender or represents the sender as someone else, unless authorized by departmental directive. All messages communicated on the County's network system shall contain the employee's name. Any messages or information sent by an employee are statements that reflect on the County. All

communications sent by employees via the County's network system must comply with this and other County policies and may not disclose any confidential or proprietary County information.

## SOFTWARE DOWNLOADS

To protect the integrity of the network, downloading of software from anywhere on the network, including the Internet is limited to software that has been purchased by the County department or has been approved for downloading by the departmental network administrator. No employee may bring software from home or outside of authorized County purchases and install it on his/her computer even if only installed on the personal drive, without first having received permission from his/her manager or Department Head.

## COPYRIGHT ISSUES

All employees obtaining access to copyrighted materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except where expressly allowed by the copyright law or with expressed written permission from the right owner.

## SECURITY

County networks with access to the Internet must be protected by a firewall approved by County Management Information Services. Employees must abide County policies or any applicable local, State or Federal laws. Management Information Services routinely monitors usage patterns for its network communications for purposes of cost analysis, allocation, and managing the County's gateway to the Internet.

## DEPARTMENT HEAD RESPONSIBILITIES

Department heads have the responsibility for insuring that employees in their respective departments comply with County policies regarding Internet and e-mail.

## EMPLOYEE RESPONSIBILITIES

All employees have a responsibility to understand and comply with this policy. Employees and supervisors are to apply common sense and reasonable judgment in a consistent and non-discriminatory way when interpreting this policy.

## VIOLATION

An employee who violates this policy may be subject to the appropriate disciplinary action which may include suspension, demotion or termination from County employment. In addition, any employee found to have violated this policy may have his/her access to the Internet and e-mail limited or revoked completely.

## TELECOM POLICY

It is the policy of Stanislaus County that phones (desk phones and mobile phones) will be used to provide services to the County's customers and for internal efficiency. This policy applies to all staff, including contract employees, volunteers and all those working in any capacity for the County. Departments shall issue and manage all phones cost effectively and efficiently, ensuring that inventories, landlines and billing are aligned with staffing changes and usage. Staff are expected to adhere to departmental and County policies regarding phone use and shall acknowledge an understanding of these policies on the appropriate form prior to the actual assignment of any phone.

## PURPOSE

Phones may be assigned to designated staff to conduct County business and shall be utilized according to County policy. Phones are tools to increase effectiveness, efficiency and access for customers, reducing response time, as well as improving communications within the County. Contractors will only be assigned County phones as part of their contract, under the County telecom policy.

## TYPES OF PHONES AND PLANS

It is County policy that each employee should have access to a phone, whether a desk phone or a mobile phone, unless there is a specific reason, approved by the Department Head, to have both. Before selecting a mobile plan, it will be essential to establish actual usage based on experience and estimated job requirements for the individual employee. It is recommended that the least expensive plan (lowest amount of minutes) closest to the identified usage be selected. Care should be exercised when choosing a plan, to ensure it is not too low, as the extra additional minutes are costly. Usage can be monitored through review of the monthly bill or the mobile phone itself to determine if a higher cost/higher usage plan is needed.

The following guidelines have been created to assist in determining what option is the most efficient for each employee. Clearly, the most cost effective device and plan shall be selected, to meet individual staff requirements to communicate with customers (both internal and external).

## DESK PHONE

Cost effective when staff stays at their desk most of the time and has no need for a mobile phone due to their assignment. As contact with staff can only be made when they are at their desk, be aware of the business impact of not being able to reach them if they are away from their desk for long periods.

## MOBILE PHONE

Cost effective when staff is away from their desk working with clients, travelling, or their job function requires mobile access. If this option is selected, this should be their only phone. Various approved vendors offer options for either local coverage or for a wider roaming area. The Mobile Phone Requisition is designed to determine the most appropriate plan for the specific needs of the individual staff.

## GUIDELINES FOR THE SELECTION OF MOBILE PHONE AND PLANS

The County has worked diligently to select vendors that will provide the high level of customer service required by the County on a cost-effective basis. As a result of these efforts, the vendors on the "Vendor Selection Chart and Guidelines" have signed contracts with the County and now each department can select the plan most appropriate to their needs.

A number of the older plans currently in place are very cost effective and should be retained, unless the vendors increase the cost.

Before switching any plans, an assessment shall be made of any penalties or additional costs to determine if the switch is cost effective.

## PERSONAL USAGE

The County owns the phone, the rates and the contracts, which results in staff being liable for improper personal usage.

County policy does provide for limited brief personal calls by staff to their homes to check on minor children, notifying family of the need to work late and scheduling a doctor and dentist appointment. Use for family emergencies and security will be allowed, but if the emergency is ongoing, it is expected that staff make departmental leadership aware of the situation. Be aware that this also applies to incoming personal calls, regardless of billing. For staff that exceeds the brief personal calls outlined above, other arrangements must be made separate from the County.

For staff who expect to exceed this limited personal use, other arrangements must be made separate from the County. This personal usage policy applies to desk phones as well as mobile phones.

Phone plans must be selected based only on the County's needs. If the minutes on the plan are exceeded and there is unreasonable personal use identified, the employee assigned to the phone will be held responsible to reimburse the County for personal calls and the employee may be subject to disciplinary action.

If staff decide they want to have a second line on their County phone for personal use, billing on this line must be directed to their residence. Staff must ensure they do not accidentally use the County line for personal calls (and vice versa).

If the needs of the County require the unlimited minutes plan and if the staff member is required to be accessible after hours, staff may use the phone after hours for County business and for the limited personal use as defined in this policy. It will be important to ensure the County minutes plan is not exceeded.

Inappropriate use of County phones constitutes grounds for discipline under Stanislaus County Code Section 3.28.010. Inappropriate use includes unauthorized, non-business use of phones and misuse of County paid time in the conduct of such calls. It also includes unauthorized long-distance personal calls and/or loss of staff productivity because of ongoing, repeated incoming and outgoing personal telephone calls.

Department heads have the authority and the responsibility to identify inappropriate personal use of County phones in accordance with this policy and to take appropriate action if a violation occurs. This policy applies equally to County desk phones, mobile phones, two way radios and pagers and must be applied in a consistent manner. Staff should be free to use County phones for County business any time.

## USE ON VACATION

Unless specifically approved (on the Mobile Phone Requisition), staff shall not use the County mobile phone line while on vacation. The only use for carrying a County mobile phone while on vacation will be for the specific purpose of County business, or if staff have the separate personal line.

## MOBILE PHONE ETIQUETTE

Mobile phones should be turned off or set to vibrate mode during meetings, with rare exception, as it is not considerate of meeting attendees to take a call during a meeting. It is also an inefficient business practice. All interruptions should be kept to a minimum whenever possible. Unless staff duties require access at all times, phones should be answered during normal business hours, the exception being during breaks and lunches. Voice messages should be checked immediately upon return from a break, lunch or meeting.

The mobile phone ring should be set at an appropriate level, to avoid disturbing co-workers.

## USE IN A VEHICLE

If you are on County business and driving a vehicle, mobile phone usage must be limited and must not compromise your driving ability and safety, (including the safety of those around you). It is expected that staff will pull over and stop the vehicle if the phone call will compromise safety. All staff must comply with State law.

## USE OF MOBILE PHONES WHILE TRAVELING ON COUNTY BUSINESS

Refer to the Travel Policy, Tab 17, Page 24—Exception.

## REPLACEMENT POLICY

A County issued phone is considered to be County property and as such shall be treated with great care. It is understood that events may occur in which a phone becomes damaged. It is County policy that in the event that a County phone is damaged and must be replaced the individual may be held responsible for replacement cost if determined to be caused by negligent care or improper handling by staff. This will be a Department Head decision.

Some replacement costs have been built into the contracts and will be taken into consideration when applying the above policy.

## TYPE OF PHONE

A number of standard models of mobile phones will be made available as part of the contracts and at no cost to the County, for use by County staff. Business requirements may dictate additional options or phone specifications, to be approved by the Department Head. County sourced phones remain the property of the County.

## BUSINESS CARDS

It is recommended that all business cards list a phone number where calls can be routed for reception, but allow for an individual's mobile number if desired.

## FORWARDING CALLS

Reception staff receiving calls will, as always, need to use judgment when deciding what steps to take when a call is received. The following general process is suggested for both desk and mobile phones, at the staff member's discretion, unless it is an emergency:

1. Notify caller prior to transferring that he or she may reach a voicemail;
2. Transfer call if caller doesn't mind leaving a voicemail if recipient isn't available; and/or
3. If caller would prefer to leave a message with reception, e-mail message to recipient.

## MANAGEMENT RESPONSIBILITIES

Each department will identify a telecommunications coordinator, responsible to the Department Head, to act as liaison with the vendors as well as to ensure billing accuracy, that inventory is well managed and surplus lines are disconnected. This role may only require a few hours a month for a small department.

## PURPOSE

Stanislaus County is proud of its tradition of a collegial work environment in which all individuals are treated with respect and dignity. Each individual has the right to work in a professional atmosphere, which promotes equal opportunities and prohibits discriminatory practices. **AT STANISLAUS COUNTY, HARASSMENT, DISCRIMINATION AND RETALIATION WHETHER VERBAL, PHYSICAL OR ENVIRONMENTAL, IS UNACCEPTABLE AND WILL NOT BE TOLERATED.**

It is the intention of this Policy to prohibit, eliminate and prevent unlawful harassment, discrimination and retaliation and its effects in the workplace. To do this, the County, through this Policy, will define unlawful harassment, discrimination and retaliation and will set forth a procedure for filing, investigating and resolving internal complaints.

## POLICY

Harassment, discrimination and retaliation of an applicant or employee by an employee or non-employee on the basis of a protected classification is not acceptable and will not be tolerated. Protected classifications include, but are not limited to: race, color, religion, sex, national origin, ancestry, physical or mental disability, medical condition, marital status, age (over 40), sexual orientation, or genetic history. Annually, the Board of Supervisors reaffirms its commitment to non-discrimination by adopting the County's Equal Employment Opportunity Non-Discrimination Statement. Please review the annual Non-Discrimination Statement for updates to protected classifications. The Non-Discrimination statement is located in each department, in the Personnel Manual, and on-line on the County's Equal Rights website.

This Policy applies to all terms and conditions of employment, including, but not limited to: hiring, job assignments, promotion, disciplinary action, layoff, re-employment, transfer, leave of absence, compensation and training.

Disciplinary action up to, and including, termination will be instituted for employee's behavior which conflicts with expectations as described in the definition of harassment, discrimination, and retaliation set forth in this policy.

## HARASSMENT AND DISCRIMINATION

Discrimination and harassment behavior is a form of misconduct that violates this policy and in some cases may constitute discrimination that is in violation of federal and state law. When evaluating complaints of hostile, offensive or abusive conduct the County will consider both

current legal standards and County Policy Examples of harassment, discrimination, and prohibited unlawful behavior include, but are not limited to:

- Harassment behavior of any kind that is verbal, physical, visual, or electronically communicated based upon a protected classification. Examples of prohibited unlawful behavior include but is not limited to, the following:

    - Speech such as epithets, derogatory comments, offensive remarks or slurs and lewd propositioning on the basis of a protected classification. This includes inappropriate sex-oriented comments on appearance, including dress or physical features, or race-oriented stories and jokes.

    - Physical acts such as assault, impeding or blocking movement, offensive touching, or any physical interference with normal work or movement when directed at an individual on the basis of a protected classification. This includes pinching, grabbing, patting, propositioning, leering, or making explicit or implied on-the-job threats or promises in return for submission to physical acts.

    - Visual insults, such as derogatory posters, cartoons or drawings related to a protected classification.

    - Circulation or posting of written materials or electronic circulation of jokes, messages, cartoons, pictures.

    - Conduct that affects or interferes with an individual's job performance that creates a hostile, offensive, or abusive working environment.

- Sexual harassment is illegal and is a form of sex discrimination forbidden by federal and state law. The Equal Employment Opportunity Commission (EEOC) defines sexual harassment as:

    - Unwelcome sexual advances, requests for sexual favors, and other acts of a sexual nature when such conduct is made either explicitly or implicitly as a term or condition of an individual's employment; or

    - When rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual; or

    - When such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating hostile or offensive working environment.

- Other examples of types of conduct which may constitute sexual harassment include:

    - Explicit sexual propositions, preferential treatment in exchange for sexual favors, retaliating or getting back at someone who turns down sexual advances;

- Sexual innuendos, suggestive comments; Sexually oriented joking or teasing, jokes about gender specific traits; or
- Dissemination of printed visual material, display or electronic communication of offensive or obscene jokes, messages, or pictures.

- **It is no defense to a claim of harassment that the alleged harasser did not intend to harass.**

## RETALIATION

Any retaliation against a person for filing a harassment/discrimination charge or making a harassment/discrimination complaint is prohibited. Retaliation occurs when adverse action is taken against an individual who, reports a concern about potential illegal or unethical conduct or a violation of Stanislaus County's policies or procedures. Employees (supervisors, co-workers and management) found to be retaliating against another employee shall be subject to disciplinary action up to, and including, termination.

## COMPLAINT PROCEDURE

Employees are encouraged to resolve issues and concerns under this policy at the lowest supervisory level of the organization possible given the circumstances of the issues involved. While Stanislaus County encourages individuals who believe they are being harassed to firmly and promptly notify the offender that his or her behavior is unwelcome, Stanislaus County also recognizes that power and status disparities between the individuals involved in the situation may require an alternative resolution process. In the event that such informal, direct communication between individuals is either ineffective or impractical, the County's Equal Employment Opportunity (EEO) Complaint Procedures should be followed in reporting a complaint of harassment, discrimination or retaliation. The County's EEO Complaint Procedure is located in the County's Personnel Manual and on-line on the County's Equal Rights website. To initiate the EEO Complaint Procedure, any employee, job applicant, or person seeking County services who believes he or she has been subject to harassment, discrimination or retaliation in violation of this policy may make a complaint orally or in writing with any of the following:

1. Immediate supervisor;
2. Any supervisor or manager within or outside the department;
3. Department Head;
4. Departmental Equal Rights Officer;
5. Director of Personnel or Chief Executive Office designee; or
6. County Equal Rights Officer.

This procedure shall apply to allegations of harassment, discrimination and retaliation in any employment action or in the delivery of public services based upon a protected classification. County departments may develop separate policies and procedures related to processing complaints regarding the delivery of public services in compliance with all applicable federal and state laws and regulations. Applicants or employees may also file a complaint with a

government agency such as the Department of Fair Employment and Housing or the Equal Employment Opportunity Commission.

## APPLICATION

This Policy applies to all employees of Stanislaus County, including volunteers, contract employees, supervisory employees, department heads, and elected officials. All employees shall receive a copy of this Policy and shall sign a written acknowledgment that they have received and read a copy of the policy. A copy of this acknowledgment shall be placed in the employee's official personnel file.

## CONCLUSION

Stanislaus County has developed this Policy to ensure that all its employees can work in an environment free from harassment, discrimination and retaliation. Stanislaus County will make every effort to ensure that all personnel are familiar with the Policy and know that any complaint received will be thoroughly investigated and appropriately resolved. Employees are encouraged to contact their department's designated Human Resources Representative, or any member of the Chief Executive Office Human Resources Division at (209) 525-6333, with any questions related to the provisions of this policy.

## PURPOSE

Stanislaus County provides many health related services and is committed to safeguarding patients' privacy. The County is dedicated to raising the awareness of the importance of ensuring health privacy, in order to improve health care quality and access on both an individual and a community level.

## POLICY

Stanislaus County recognizes the responsibility to respect and protect the privacy rights of health information and will comply with all HIPAA provisions. These standards apply to all individuals and County employees who have access to, use, or disclose protected health information regardless of unit or division. Each covered component is responsible for developing and implementing policies and procedures specific to their department but consistent with County-wide policies. Each internal business associate as defined by the County is responsible for developing and implementing confidentiality policies and procedures specific to their department and the services they perform.

## PROVISIONS

1. Protect health insurance coverage for workers and their families when changing jobs, this is **"portability."**

2. Protect the **privacy** of Protected Health Information (PHI). The **Privacy Rule** sets standards for how protected health information should be controlled, by setting forth what uses and disclosures are authorized or required and what rights patients have with respect to their health information. The Privacy Rule prohibits the sharing of Individually Identifiable Health Information (IIHI) without a patient's permission unless the purpose of the disclosure is permitted by regulation—such as for treatment, payment or health care operations.

3. Establish **code sets**—national standards for the electronic transmission of health information. The health care industry will speak one common "language" when transmitting claim submissions and remittance advice.

4. Establish standards for the **security** of protected health information. The regulations require the adoption of administrative, physical and technical safeguards. The County will protect the integrity, confidentiality and availability of electronic protected health information from unauthorized access, alteration, deletion, or transmission. The compliance deadline for the Security Rule is April 21, 2005.

The County seeks to develop a workforce that reflects the cultural and ethnic make up of the community we serve. This is Board policy and is reflected in our hiring, promotions and retention of employees. It makes for good customer service and allows the County as an Institution to better understand all parts of our community.

Federal, State and County policy provides that employees shall not be prohibited from speaking languages other than English on the job unless it can clearly be shown that a "business necessity" exists for prohibiting language other than English. When a "business necessity" does exist, all affected employees will be immediately notified and expected to comply with the language requirements.

English is not the first language for many County employees. For some employees we seek your primary or secondary language skills and require you to use them in your job. However, the primary business language of Stanislaus County is English unless otherwise directed. This policy should be followed if you are subject to "business necessity" English only on the job.

**Government Code 12951**

(a) It is an unlawful employment practice for an employer, as defined in subdivision (d) of Section 12926, to adopt or enforce a **policy** that limits or prohibits the use of any **language** in any workplace, unless both of the following conditions exist: (1) The **language** restriction is justified by a business necessity. (2) The employer has notified its employees of the circumstances and the time when the **language** restriction is required to be observed and of the consequences for violating the **language** restriction. (b) For the purposes of this section, "business necessity" means an overriding legitimate business purpose such that the **language** restriction is necessary to the safe and efficient operation of the business, that the **language** restriction effectively fulfills the business purpose it is supposed to serve, and there is no alternative practice to the **language** restriction that would accomplish the business purpose equally well with a lesser discriminatory impact.

## COUNTY POLICY

The rights and legal constraints on political activities by public employees under State and Federal law are summarized below.

Restrictions which pertain to activities while on duty, to the use of department facilities, and to actions of employees in an official capacity all constitute the policy of the department. Additionally, for all employees, following are the prohibited activities and the permitted activities our legal counsel has interpreted as outlined in Government Code 3201 - 3204.5 and Section 3206 of the Code.

### A) PROHIBITED ACTIVITIES

Under the State law employees may **not** do any of the following:

1. Participate in political activities of any kind while in uniform (This includes official use of a County vehicle with official seal, even parked, that might imply official endorsement).

   Example: Sheriff deputies, security guards, and animal services officers may not participate in political activities of any kind while in uniform.

2. Knowingly solicit or receive political funds or contributions from OTHER OFFICERS OR EMPLOYEES OF THE COUNTY OR FROM PERSONS ON THE EMPLOYMENT LIST of the County, except:

   An officer or employee may solicit or receive political funds or contributions to promote the passage or defeat of a ballot measure that would affect the rate of pay, hours to work, retirement, civil service, or other working conditions of the officer or employee. Nothing in this section prohibits an officer or an employee of the County from communicating through the mail or by other means requests for political funds or contributions to a significant segment of the public which may include officers or employee of the County. (Officer or employee home addresses obtained through the regular course and scope of ones duties may not be used for this purpose.)

3. Make, demand or give notice of any political assessment, subscription or contribution within or upon County property, or within or upon premises used for governmental purposes by the County, at any time, unless;

The County property or premises is being used for the conduct of a public or political rally or similar event or the County property, such as a park, street or public land is not being used for the governmental purposes of the County.

4. Use, promise, threaten or attempt to use their County position or official authority to influence the political actions of other County officers or employees or those seeking County employment.

## B) PERMITTED ACTIVITIES

Generally employees **may**:

1. Express their opinions on political subjects and candidates.

2. Become a candidate for nomination or election in any partisan or nonpartisan campaign - national, state, or local.

3. Engage in partisan or nonpartisan political activities as an individual or as a member of a group.

4. Contribute to political campaign funds:

   a) IF THE CONTRIBUTION IS NOT MADE TO OR THROUGH ANOTHER COUNTY OFFICER OR EMPLOYEE, and

   b) If the contribution is not made on County property or County premises.

5. Join political organizations and vote on any questions presented.

6. Organize and manage political clubs; serve as officer, delegate or alternate, or as a member of any committee.

7. Participate actively in political conventions.

8. Attend political meetings, rallies, etc. and organize, prepare and conduct such gatherings.

9. Initiate, sign or circulate partisan or nonpartisan nominating petitions, distribute campaign literature, badges, etc.; provided THAT SUCH ACTIVITY DOES NOT TAKE PLACE DURING WORKING HOURS OR WHILE OTHERWISE ON DUTY.

10. Wear campaign badges, clothing, or buttons, provided THAT SUCH ACTIVITY DOES NOT TAKE PLACE DURING WORKING HOURS OR WHILE OTHERWISE ON DUTY. Employees may display bumper stickers, picture or posters on a private automobile or in the window of their home.

11. Speak publicly, or write letters or articles for or against any political candidates; endorse or oppose such candidate in the political advertisement.

12. Manage the campaign of a political candidate.

13. For employees whose primary job is in connection with federally funded activities (except revenue sharing) the following are prohibited and permitted activities as legal counsel has interpreted the Hatch Act.

    a) PROHIBITED ACTIVITIES / "HATCH ACT" COUNTY EMPLOYEE – These prohibitions apply to those employees whose primary job is in connection with federally funded activities (except revenue sharing) and employees whose primary job is funded with federal monies.

       YOU MAY NOT:

       1. Participate in political activities of any kind while in uniform.

       2. Knowingly solicit or receive political funds or contributions from other officers or employees of the County or from persons on the employment list of the County, except:

          An officer or employee may solicit or receive political funds or contributions to promote the passage or defeat of a ballot measure that would affect the rate of pay, hours of work, retirement, civil service, or other working conditions of the officer or employee. Nothing in this section prohibits an officer or an employee of the County from communicating through the mail or by other means requests for political funds or contributions to a significant segment of the public which may include officers or employee of the County. (Officer or employee home addresses obtained through the regular course and scope of ones duties may not be used for this purpose.)

       3. Directly or indirectly coerce, attempt to coerce, command, advise a local officer or employee to pay, lend, or contribute anything of value to a party, committee, organization, agency or person for political purposes.

          This section prohibits a County officer or employee from attempting to influence another County officer or employee to contribute anything of value for political purposes.

       4. Make, demand or give notice of any political assessment, subscription or contribution within or upon County property, or within or upon premises used for governmental purposes by the County, at any time, unless:

The County property or premises is being used for the conduct of a public or political rally or similar event or the County property, such as a park, street or public land is not being used for the governmental purposes of the County.

5. Use your official authority or influence for the purpose of interfering with or affecting the result of an election or a nomination for office.

   Among other possible restrictions, this would prohibit an officer or employee from using his County title or official stationery in connection with any political campaign, and from attempting to influence anyone's vote by such methods as promising employment or threatening dismissal.

b) PERMITTED ACTIVITIES/"HATCH ACT" COUNTY EMPLOYEE

**YOU MAY:**

1. Express your opinions on political subjects and candidates.

2. Become a candidate for nomination or election to any nonpartisan elective office.

3. Engage in partisan or nonpartisan political activities as an individual or as a member of a group.

4. Contribute to political campaign funds:

   A. IF THE CONTRIBUTION IS NOT MADE TO OR THROUGH ANOTHER COUNTY OFFICER OR EMPLOYEE, and

   B. If the contribution is not made on County property or County premises.

5. Join political organizations and vote on any questions presented.

6. Organize and manage political clubs; serve as officer, delegate or alternate, or as a member of any committee.

7. Participate actively in political conventions.

8. Attend political meetings, rallies, etc. and organize, prepare and conduct such gatherings.

9. Initiate, sign or circulate partisan or nonpartisan nominating petitions, distribute campaign literature, badges, etc.; provided THAT SUCH ACTIVITY DOES NOT TAKE PLACE DURING WORKING HOURS OR WHILE OTHERWISE ON DUTY.

10. Wear campaign badges, clothing, or buttons, provided THAT SUCH ACTIVITY DOES NOT TAKE PLACE DURING WORKING HOURS OR WHILE OTHERWISE ON DUTY. You may display bumper stickers, pictures or posters on a private automobile or in the window of your home.

11. Speak publicly, or write letters or articles for or against any political candidates; endorse or oppose such candidates in a political advertisement.

12. Manage the campaign of a political candidate.

## 1. PRECEDENCE

This document does not supersede or override any regulations promulgated by State or federal agencies, such as the requirements mandated by the Department of Justice, that are more stringent or impose additional requirements than this policy.

## 2. CONTENTS

Non-Compliance Policy
Implementation
Confidentiality/Privacy/Data
Ownership Information Systems
Communication Unacceptable Use
Portable Data
Mobile Users
User Passwords
Software Installation
Access Control
Assessment/Audit
Perimeter Security
Updates/Patch Management
Data Encryption Standards

## 3. NON-COMPLIANCE

An employee who violates this policy will be subject to the appropriate disciplinary action, which may include suspension, demotion or termination from County employment. Any criminal misuse of County computer resources will be investigated for possible legal prosecution. An employee found to have violated this policy may have his/her access to the County or departmental computer system, the Internet, the Intranet or the Email system limited or revoked completely. Any attempts to circumvent County IT Security measures shall themselves be viewed as violations of this policy.

Any employee aware of accidental non-compliance, misuse or suspicion of misuse, shall report the incident to a supervisor immediately.

Stanislaus County Departments that cannot, for whatever reason, comply with the requirements of this document**,** shall maintain a document describing the non-complying system or process. This document shall include a mitigation plan with specific budget and timetables identified, if applicable. It is understood that some current Stanislaus County information systems do not comply with certain requirements in this document. Departments shall undertake to correct/replace these systems to improve overall County IT security. Should a Stanislaus County Department need assistance in devising or implementing a mitigation plan for their non-complying system, that Department shall report it to the IT Security Manager and to request from the IT Security Manager such assistance.

Employees will not be held accountable for non-compliance when necessary items or actions to maintain compliance are within the Department's responsibility.

## 4. POLICY IMPLEMENTATION

Upon approval of this policy by the Board of Supervisors all County employees shall be expected to adhere to this policy as it is written. All employees have a responsibility to read, understand and comply with this policy.

The initial distribution of this policy, to all County employees, shall be through County payroll. It will be each Department's responsibility to ensure that each employee receives and signs the initial policy within thirty (30) days, absent a valid reason (e.g. vacation, leave of absence, etc.).

This policy shall apply to all County employees including, but not limited to, regular full-time, part-time, seasonal, temporary, supervisory, management, department heads, volunteers and Personal Service Contractors. This policy shall also apply to independent contractors who utilize any County computers or the County computer system.

As this policy may be frequently updated as technology and security threats change, a copy of the latest version of this policy shall be given to each employee annually by the Department. The supervisor should consider the employee's compliance with this Policy in evaluating the employee's performance. Any changes to this Policy that are of sufficiently significant nature, as determined by the Stanislaus County Security Special Interest Group and approved by the Stanislaus County Board of Supervisors and Department Heads, shall require all County employees to re-sign this Policy.

It is the Department's responsibility to ensure that all new Department hires have acknowledged receipt and reviewed this policy within 30 days of initial hire date. The Stanislaus County Security Special Interest Group, in conjunction with the CEO's office and SBT, will offer training sessions in regards to this policy. The training classes may be scheduled by contacting SBT and coordinating with the County IT Security Manager.

## 5. CONFIDENTIALITY/PRIVACY/DATA OWNERSHIP

a ) Any Internet-related activity, such as web site visits, downloads, chat sessions or web forum postings can and will be tracked and recorded.

b) The CEO's office and County Counsel, have the right to review any Internet or email activity of any employee at any time for any reason. The Department Heads or their designee have the right to review any Internet or email activity of any of their employees at any time for any reason. The County reserves the right to inspect any and all files stored in private areas of the County information systems in order to assure compliance with this policy.

c) All electronic data, including email, created or received utilizing County information systems is the property of the County. Subject to applicable legal privileges and confidentiality requirements, all electronic data entered or received on County information systems is public and is subject to disclosure upon the demand of the County at any time.

## 6. INFORMATION SYSTEMS COMMUNICATION

a) Each employee is responsible for the content of all text, audio or images that they place or send over the County's information systems, or which appear on their computer. No electronic communication shall be sent which hides the identity of the sender or represents the sender as someone else unless authorized by the Department Head.

b) All messages communicated on the County's information systems shall contain the employee's name unless authorized by the Department Head. Any messages or information sent by an employee are statements that reflect upon the County.

c) All communications sent by employees via the County's information systems shall comply with this and other County policies and shall not disclose any confidential or proprietary County information without proper authorization.

## 7. UNACCEPTABLE USE

a) County information systems access or individual computer usage shall not be used for transmitting, retrieving, receiving or storing of any communications of a discriminatory or harassing nature or materials that are perceived as being obscene. Harassment of any kind is prohibited by County policy.

b) No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference shall be transmitted. No abusive, profane or offensive language shall be transmitted through the County's information systems.

c) Electronic media shall not be used for any other purpose that is illegal, against County policy, causes discredit to the employee's department or the County, or is contrary to the County's best interest.

d) County computers and information systems shall be used only for authorized County business. It is unacceptable for employees to use County information systems for personal gain or profit, or for personal reasons that would result in depleting resources, impeding the organization's ability to conduct business, or cause any interruption or delay in service to the public. The occasional limited use by County employees to check home email, or access appropriate internet sites during lunch, break or after hours does not constitute inappropriate use in and of itself. Additionally, employees shall only access information systems with which they have authority to do so.

## 8. PORTABLE DATA

a) When an individual department has a business need for staff to utilize portable data, specific departmental procedures shall be used to insure the highest level of security is attained. When transporting or transmitting County information in portable format (i.e. a DVD or USB flash drive) the staff person shall be responsible for its security and shall take all reasonable precautions (keep in personal possession, in locked brief cases, encrypt when possible, et cetera) to insure that it does not fall into unauthorized hands.

b) Removing electronic data from the work-site is prohibited without proper written authorization. Staff is discouraged from creating or modifying County documents at home on personal computers.

## 9. MOBILE USERS

a) County shall not, as standard practice, purchase computers, software, software licenses, Internet or phone services or office equipment such as printers, fax machines, calculators, or furniture for staff who work from home (in-home telecommuters). Purchase of such items, as well as consumable supplies, must be at the direction and approval of a Department Head, and shall be in compliance with County budget, purchasing and management information services policies.

b) Software may in some instances be provided for use on non-County-owned systems when the Department Head approves purchase of the necessary licenses. County IT staff shall only install such software on an employee's personal computing device, when the Department Head provides prior written approval. In this case, the employee must bring the device to the County location. Virus protection software and Operating System patches shall be maintained and up-to-date on any computers or devices that will connect in any way to the County information systems.

c) In addition, the selection, installation, maintenance, repair or replacement of employee- owned equipment and software is the responsibility of the employee.

Computer equipment shall have a configuration that is compatible with County's Information Technology (IT) standards and infrastructure.

d) County-issued cell phones and or mobile devices, may contain privileged or confidential information such as contact information or even emails or documents. Some "smart phones" and similar mobile devices like Blackberry, iPhones or iPads may actually connect automatically to County email systems or other information technology systems owned or maintained by the County. Any such devices that store emails and/or connect to County IT systems shall be configured to automatically lock after a period of disuse and require a password to be unlocked. The "timeout" period, after which the phone or mobile device locks, shall not exceed thirty minutes and shall not exceed sixty minutes for sworn officers. Reasonable care should be taken to use a password that is not easily guessed. Lost or stolen phones/mobile devices in this category must be reported to the department telecom coordinator as soon as possible so that protective measures, such as disabling the device may be employed. Notification must take place within 24 hours. Phones or mobile devices previously used for storing email or other sensitive County information shall be completely purged of all information before being transferred to another employee, returned to the vendor or discarded. Non-County-owned smart phones or mobile devices may only be used to store emails or connect to County IT systems with the written approval of the Department Head or their designee and signed by the owner of the device. Those connecting non-County-owned devices must agree in writing that, should they leave County employment or otherwise have their access revoked by the County, their phone may be reset to factory condition by departmental IT staff. See 'Email Access Form' located on the last page of this policy.

e) In the event any County equipment is stolen, or needs replacement, repair or maintenance, County shall be responsible for its replacement, repair or maintenance if the equipment was approved by the Department Head and the telecommuter has provided the proper care and safety of the equipment. If County-owned equipment or property is stolen it is the responsibility of the telecommuter to call the police and obtain a police report number and provide the police report number to the department. If a telecommuter is moving to a new residence and has an existing business telephone line owned by County, the Department and County Telecommunications shall be notified of the move prior to the telecommuter vacating the residence, to ensure the telephone line is disconnected on a timely basis

f) In the event of equipment malfunction, the telecommuter shall notify his/her supervisor immediately. If repairs will take some time, the telecommuter shall be asked to report to a County facility until the equipment is usable.

## 10. USER ACCOUNTS

a) Business applications shall automatically enforce passwords that reflect this policy whenever possible. Passwords shall consist of at least 6 characters for internal systems and at least 8 characters for Internet accessible systems, mix of alpha (upper

and/or lower case), numeric and symbols (with at least 3 of the 4 categories satisfied). Passwords must change at least every 90 days and no sooner than every 10 days. Old passwords shall not be reused. A centralized method for password resets shall be deployed.

b) Accounts shall be disabled or deleted within 24 hours of staff termination, which includes resignation or retirement. In no event shall accounts remain accessible 72 hours after termination. When staff is reassigned within their department or transfer to another department their information systems privileges shall be modified to reflect their new duties or department. This account modification shall be performed within 24 hours of effective reassignment, and the account modification shall be performed within 72 hours of reassignment. It is recommended that any staff member on an approved leave greater than 30 days have their account disabled until they return.

c) Users shall not share accounts and passwords. As those who seek unauthorized access might attempt to mislead a workforce member into divulging their password by claiming that they are County Information Technology staff, passwords shall not be given out to any individual. (See exceptions to this rule in item e)

d) Users shall not use their account passwords that are currently in use on County systems with non-County systems (e.g. personal email accounts, banking accounts, etc.). The County recognizes that it is unable to track this on a normal basis. However, it is information that may become known through the course of a data or system breech investigation.

e) In cases where systems or devices are limited in their ability to provide more than 1 administrator or "privileged" account, that account may be shared with the appropriate staff if determined necessary by the Department Head or their designee. If a system or device that falls into this category is deemed important, necessary or critical to infrastructure, the account and all changes to the password shall be shared with the Department Head or their designee immediately after such change.

## 11. SOFTWARE/HARDWARE INSTALLATION

a) Only designated departmental technical support staff, appointed by the Department Head may install software. Departments may pre-authorize installation of software by other departmental employees for selected software, such as commonly used Internet browser plug-ins. Under no circumstances shall authorization be given to install unlicensed software on county equipment or allow multiple use of single-user software. Technical support staff shall have the authority to delete unauthorized software (including but not limited to screen savers, toolbars, animated programs, games) when detected. In such cases, supervisor(s) will be notified.

b) County staff working on and/or installing County licensed software on private P.C.s is an exceptional circumstance and shall require the prior written approval of the Department Head.

As there is some risk to the County with staff going to private homes, the P.C. (or laptop / tablet computer) shall be brought to the department's IT area.

If there are any security or virus issues, the latest copy of virus protection software shall be installed on the P.C. (or laptop) prior to it being connected to the County network. The owner of the private P.C. is responsible for the cost of this software.

Department Head authorization of software installation is not authorization for staff to work from home.

c) All software acquired by or on behalf of the County or developed by County employees or contract personnel on behalf of the County is and shall be deemed County property. All such software shall be used in compliance with applicable licenses, notices, contracts, and agreements. Employees shall not create, obtain, possess, execute, modify, or distribute any computer programs or material in violation of copyright laws.

d) Employees shall not connect any computer hardware, either personally owned or County- owned or network hardware (including, but not limited to, wireless networking hardware) to the Stanislaus County network without Department Head or their designees approval.

**12. ACCESS**

a) Access to Stanislaus County information systems, except for those devoted to public use, shall be authorized only for Stanislaus County workforce members, department approved partners and software programs having a need for specific information in order to accomplish a legitimate task. All such access shall be defined and documented.

b) Appropriate Stanislaus County information system owners, Department Heads or their chosen delegates shall define and authorize all access to Stanislaus County information systems. Such information system owners/stewards and delegates shall be formally designated and documented.

c) Appropriate Stanislaus County information system owners, Department Heads or their designated delegates shall review workforce member and software program access rights to Stanislaus County information systems to ensure that access is granted only to those having a need for specific information in order to accomplish a legitimate task. All access shall be regularly reviewed and revised as necessary.

d) As appropriate, Stanislaus information systems shall support one or more of the following types of access control to protect the confidentiality, integrity and availability of data contained on Stanislaus County information systems:

i. User based: each user is assigned specific privileges based on their individual status

ii. Role based: each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role

iii. Context based: rights are not assigned to users, but are assigned based on the particular circumstances of a transaction

e) As appropriate, security controls or methods that allow access to Stanislaus County information systems shall include, at a minimum:

i. unique user identifiers (user IDs) and a secret identifier (password) that enable persons and entities to be uniquely identified. User IDs shall not give any indication of the user's privilege level. Group identifiers shall not be used to gain access to Stanislaus County information systems,

ii. when unique user identifiers are insufficient or inappropriate, group identifiers shall be used to gain access to Stanislaus County information systems upon review by the appropriate owner/controller of the data being accessed,

iii. the prompt removal or disabling of access methods for persons and entities that no longer need access to Stanislaus County data and information systems,

iv. logging of changes to the configuration of a network using TACACS+ or similar technology for devices that support logging solutions of this type. The solution should uniquely identify who made the change, when the change was made, and "where possible" a reference number linked to documentation describing and authorizing the change by whatever party has oversight of the equipment in question.

f) Neither Stanislaus County workforce members nor software programs shall be granted access to Stanislaus County information systems until properly authorized. Only staff formally designated by the Department Head to work on information systems shall connect, move, tamper with or remove computer or network equipment from the Stanislaus County network.

g) Stanislaus County workforce members shall not provide unauthorized users access to Stanislaus County information systems.

h) Special system privileges, such as the ability to bypass normal resource access controls, shall be restricted to those directly responsible for system management and/or security. This access shall be authorized by the Department Head and documented.

i) Access to Stanislaus County information systems shall be managed in order to protect the confidentiality, integrity, and availability of all data. This pertains to any data, code or scripts stored or shared in any form on Stanislaus County owned resources. This includes: electronic information, information on paper and information shared orally or visually (such as telephone and video conferencing). County departments shall have a formal process for granting and reviewing appropriate access to Stanislaus County data and access to other information systems. The process shall include:

   i. capability for authorizing appropriate levels of access to Stanislaus County data and information systems,

   ii. procedure for tracking authorization of access to Stanislaus County data and information systems,

   iii. procedure for regularly reviewing and revising, as necessary, authorization of access to Stanislaus County data and information systems,

   iv. procedure for the Department Head or designee to authorize access to information systems based on both the right and the need to know basis,

j) The type and extent of access authorized to Stanislaus County information systems shall be based on risk analysis. At a minimum, the risk analysis shall consider the following factors:

   i. the importance of the applications running on the information system,

   ii. the value or sensitivity of the data on the information system,

   iii. the extent to which the information system is connected to other information systems

k) Where risk analysis shows it is necessary, appropriate encryption shall be used to protect the confidentiality, integrity and availability of data contained on Stanislaus County information systems. See Data Encryption Standards page 14.

l) The Department Head may determine there is a legitimate business need to provide Independent Contractors with access to County data or services. This shall be permitted only if the following requirements are met:

   i. Independent Contractors shall enter into an agreement with Stanislaus County prior to accessing any information on the Stanislaus County information systems,

   ii. Independent Contractors shall have the minimum access required to complete the tasks assigned,

iii. Independent Contractors access shall be enabled only for the time period required. Whenever possible, access should be configured to automatically expire,

iv. Independent Contractors shall be given a copy of, and comply with, all applicable Stanislaus County IT policies related to information systems,

v. accounts shall be terminated within 8 hours of the last day the Independent Contractor has worked,

vi. the standard work contract with any Independent Contractors who will be given network access shall include a copy of the Department and/or County IT Security policy and it shall include specific language about penalties that will be assessed if the policy is violated.

m) The Department shall maintain documentation on Independent Contractors who have been given network access, with appropriate detail (IP/MAC address being used, duration and terms of their access). Appropriate background investigations will be conducted on contractors who have access to sensitive information such as the Criminal Justice information systems.

n) Departments may have a legitimate business need for department employees and/or Independent Contractors to perform work from their homes or a remote site and may use the Internet as the network medium for providing said access. Remote access shall be permitted only if all of the Access requirements are met as well as the following requirements:

i. Stanislaus County Human Resources Policies regarding employees working from home shall be observed,

ii. encryption standards for Internet communications shall be employed. See Data Encryption Standards page 14

iii. remote access implementations shall include suitable encryption and logging of authentication attempts, both success and failures. Such logs shall be stored centrally and reviewed regularly by system administrators,

iv. analog access shall be used with Department Head approval only,

v. two-factor authentication shall be implemented for all remote access activity when possible. This frequently takes the form of smart card or biometrics systems,

vi. Remote access implementations using VPN's shall prohibit "Split-Tunnels" when connecting from non County owned devices or when County owned

devices are connected to non-County owned networks. The Department Head or their designee, may authorize "Split-Tunnels on a case by case basis if a critical need for such is determined."

o) The Department Head shall determine that there is a legitimate business need to allow remote control access of County systems from the Internet, either for Departmental IT staff or for Independent Contractors. This shall be permitted only if the following requirements are met:

i. any remote control mechanism shall have logging capabilities, logs shall be stored external from the device being remotely controlled

ii. in the situation where a Department has a legitimate business need to allow remote control to be performed by someone other than the local logged in user, that Department shall have a documented procedure for permitting this activity. The procedure, at a minimum, will address who may perform such remote control and under what circumstances. It is understood that there may be legitimate business needs for allowing such remote control, e.g. for system maintenance. However, as allowing such remote control provides significant opportunity for abuse and circumvention of sound security procedures, its use is discouraged

iii. when remote control is being performed by someone other than the local logged in user, the session shall be of limited duration, with a County employee monitoring the access and ensuring that it is properly terminated. Auto logins or user account caching for remote access systems is prohibited.

**13. ASSESSMENT/AUDIT**

a) An annual risk assessment report shall be created for every department and must be stored in a secure manner. The risk assessment shall contain defined categories of risk such as:

i. highly sensitive: areas where large amounts of confidential data is stored and maintained

ii. sensitive: areas where terminals are located which can access highly sensitive data,

iii. public access: areas where the general public has direct physical access to devices connected to the County data network.

b) Self-administered audits shall be performed at least once annually. Self- administered audits will also be performed when events trigger such actions. Events that trigger such actions would include such things as changes in network topology, changes in server software or hardware configurations, or changes in operational procedures.

c) Peer and External audits shall be performed at a minimum, biennially. A core peer group made up of internal County personnel will perform peer audits with Department Head approval, knowledge and coordination. External audits shall be performed by an independent non- biased third party vendor external from the County with Department Head approval, knowledge and coordination.

d) Stanislaus County shall provide a standard automated assessment tool to facilitate the auditing process and provide consistency. The Information Technology Security SIG will determine the requirements for such a system and the processes and procedures for its use.

e) A County-wide IT Assessment team shall be formed and shall perform penetration testing on a regular basis to determine if existing security controls are effectively protecting the County's information technology systems. No penetration testing shall be performed without Department Head approval, knowledge and coordination. Each member of the team conducting penetration testing shall have previously passed a background check appropriate for the Department and information system being tested.

f) All audit results shall be reported to the specific Department. Any results that identify County security issues shall be shared with the IT Security Manager and the Security SIG.

g) Departments shall be able to identify departmental expenses related to ongoing security needs, in accordance with guidelines to be developed by the Security SIG.

h) Stanislaus County departments shall identify and audit all access controls used to protect information technology systems annually. The audit shall be provided to the Stanislaus County Security Special Interest Group where appropriate. The annual report shall be stored in a secure manner (e.g. appropriate file access permissions are employed).

## 14. PERIMETER SECURITY

The County-Wide Area Network encompasses the data networks of Stanislaus County agencies. Any potential weakness at any County agency, has the ability of compromising every other County data system. There is a recognized need for some County agencies to have external network connections with partners, with the State of California, with the Federal Government and to the Internet. These links create weaknesses that shall be addressed. All perimeter security shall be protected by access controls.

a) All network security mechanisms shall at a minimum provide the following safeguards:

i) permit only the traffic required,

ii) must be hardened to deter compromise,

iii) default configurations, especially in regard to system authentication shall be replaced with reasonable alternatives,

iv) logs of all pertinent traffic permitted through the access controls shall be kept and stored separate from the access controls,

v) a current detailed network diagram of the connection to the County network, describing its purpose and defining security measures taken shall be provided to the County IT Security Manager unless an exception is approved by the CEO.

b) Wireless data networking solutions connected to the Stanislaus County Wide Area Network extend the WAN, sometimes beyond the confines of Stanislaus County properties. Therefore, more stringent security measures shall be employed. At a minimum, wireless data network implementations will:

i) use appropriate encryption, *See Data Encryption Standards page 14*

ii) require authentication, such as the IEEE 802.1x specification which deals with enhanced security,

iii) use non-default configurations for Admin account password and Service Set Identifier (SSID). The SSID should be non-descriptive so that a casual user could not identify to whom the network belongs,

iv) not allow administration from the wireless interface. Administration may only be permitted through the wired interface of the device,

v) adjust power levels such that the radio signal does not extend further than necessary,

vi) log all access, preferably to a device on the wired network.

c) Wireless data network components should also:

i) filter traffic such that only required services are supported,

ii) suppress SSID advertisements,

iii) filter devices based on pre-determined MAC addresses.

## 15. UPDATES/PATCH MANAGEMENT

a) Operating Systems and mission-critical applications shall be updated on a regular basis. There are several components to Updating/Patch Management:

   i) determining when updates are available,

   ii) testing updates to determine what benefit/risk is associated with them,

   iii) deploying updates in a timely fashion once it has been determined that it is safe to do so,

   iv) track which systems the update has been delivered to.

b) Each Department shall have a documented procedure for how updates/patch management is to be performed and monitored.

## 16. DATA ENCRYPTION STANDARDS

a) For local traffic that does not leave the Stanislaus County Wide Area network encryption mechanisms that are deemed acceptable include 3DES, AES, and SSL.

b) For wireless data networking components such as wireless access points, wireless bridges and wireless peer-to-peer networking, the strongest supported encryption method should be employed. At a minimum Wi-Fi Protected Access 2 (WPA2) shall be used. *See also Perimeter Security page 12*.

c) Where Stanislaus County data does or might reasonably traverse a non-Stanislaus County-owned network, such as the Internet, American Encryption Standards (AES) or 256-bit Secure Socket Layer shall be employed.

d) Stronger encryption methods shall be employed, but all encryption methods that vary from these Standards must be documented and reported to the Department Head and may be provided to the IT Security Manager and the Security SIG upon request.

The use of County "vehicles" shall be restricted to official County business and work activities. County "vehicles" include, but are not limited to: vehicles, autos, boats, trucks, aircraft (both fixed and non-fixed wing), motorcycles, all-terrain vehicles and any other equipment capable of transporting people or equipment.

Use of County vehicles for personal business or for any purpose other than County business is prohibited. County vehicles shall not be used for any private or business purpose. County departments with "on-call" employees shall develop regulations governing the use of County vehicles by on-call employees.

Transportation in a County-owned vehicle of any non-County person not engaged in official County business is prohibited unless otherwise expressly permitted by applicable law or department policy, or unless prior specific authorization is given by the Chief Executive Officer or his/her designee.

When County-owned aircraft are utilized for transportation purposes, departments should consider using the most economical means of travel.

The County's aircraft operated by the Sheriff's Office shall only be utilized for law enforcement or emergency-related purposes or County governmental purposes with the prior approval from the Chief Executive Officer or his/her designee. County aircraft shall not be used for commercial purposes or the benefit of a private business. Accurate flight records shall be maintained and shall identify passengers by name and shall include the purpose of the flight and the destination unless such information would compromise or interfere with a criminal investigation.

Each County Department Head and Elected Official is responsible for the implementation and enforcement of the provisions of this policy.

The following personnel regulation is a statement of County policy concerning the promotion of particular religious beliefs by County employees and volunteers to their fellow employees, other volunteers, clients of the department, or the general public. This policy may be augmented by departmental policies relating to specific issues or operations.

It is the policy of the County that employees and volunteers are to maintain a position of "separation of church and state" and neutral non-involvement in matters of individual religious beliefs.

The promotion of particular religious beliefs, concepts, organizations, practices or the dissemination of religious material or information on County time or using County resources is prohibited. Religious items such as bibles, crosses, posters, drawings, pictures, or similar items with religious writings should not be displayed on County property.

This policy is necessary if public employees are to apply the laws and provide the services paid for by the taxpayers to everyone without regard to matters such as religion or creed.

This policy is not intended to abridge in any way an employee's right to practice or maintain his or her own religious beliefs. However, proselytizing employees or promoting one's religion in the workplace is not appropriate.

Notwithstanding the above, please note that through the course and scope of an employee or volunteer's assigned duties, particularly in the custodial facilities or inpatient settings, they may be required to display and distribute religious materials and information as requested by patients or inmates, and/or in accordance with applicable State standards.