

SOCIAL SERVICES AGENCY

ADMINISTRATIVE POLICIES AND PROCEDURES MANUAL

Subject: Information Technology Security and Usage Number: I 6
Approved: Signature on file Date: 03-20-15

POLICY

SSA workforce members shall adhere to applicable SSA, County of Orange (including [the ITSP](#), County of Orange-Attachment A), State (including the State of California Welfare and Institutions Code 10850), and Federal regulations relating to information technology security, privacy, and confidentiality of information as each may now exist or be herein after amended.

Unless within the scope of job responsibility, any violation of this policy is subject to immediate revocation of user's access to SSA network and associated applications. SSA workforce members may be subject to disciplinary action including suspension, termination, civil, and/or criminal prosecution. Causes for disciplinary action may include, but are not limited, to the following activities:

1. Use of E-mail and all other forms of electronic communication, Internet browsing, or computers, tablets, smart phone and all other electronic devices for any of the following:
 - a. Harassing others using offensive, obscene and/or vulgar language; or threatening others, including creating messages containing sexual or racial overtones or slurs, and/or messages disparaging of others based on race, sex, age, national origin, sexual orientation, marital status, and/or other personal characteristics protected under federal, state or local laws.
 - b. Disrupting or interfering with County operations or job responsibilities.
 - c. Misrepresenting facts to the detriment of SSA.
2. Unauthorized access to County or other non-County computer networks and/or applications.
3. Failure to protect Confidential Information from unauthorized disclosure.
4. Unauthorized disclosure of Confidential Information.
5. Unauthorized software installation(s) on SSA computer systems.
6. Unauthorized access, attempt to access or to encourage others to access County, State, Federal or other computer systems and networks that are not directly within the current scope of employee's job responsibilities.

All SSA workforce members shall do the following:

1. Keep their user IDs and passwords confidential and secured at all times. Should a password be compromised, it shall be changed immediately, and the supervisor shall be notified.
2. Restrict user ID usage only for currently assigned SSA job duties and responsibilities.
3. Use County resources, such as data and information, for County business objectives only. Use of these resources for private or personal gain is prohibited and may be subject to administrative, civil, and criminal penalties (California Penal Code Section 502).
4. Protect Confidential Information of clients to prevent unauthorized disclosure. Only the minimum amount of Confidential Information necessary for business operations should be

copied, downloaded, exported or stored on any electronic device or in paper format. Any compromise of Confidential and/or Personally Identifiable Information shall be immediately reported to the supervisor.

5. Request software installations on SSA computers, laptops, tablets and other devices from an authorized agent of the SSA Information Technology team. **DO NOT INSTALL ANY software/application into County SSA devices.**
 6. Seek permission from SSA Information Technology team prior to copying a County-owned software/application.
 7. Use of any County electronic communication systems is for business use only; any personal use shall not disrupt or interfere with County operations or job responsibilities.
-