Office of Technology & Solutions Integration CALIFORNIA HEALTH & HUMAN SERVICES AGENCY	**SECURITY POLICY** **CONTROL NUMBER: OSI-2021-03**
Acceptable Use Policy	**Revised: September 27, 2023**

Purpose

Information Assets owned by the Office Technology & Solutions Integration (OTSI) are strategic assets intended for official business use and are entrusted to state Personnel in the performance of their job-related duties.

Inappropriate use of OTSI Information Assets may negatively affect the confidentiality, integrity, or availability of the information, information systems, or other Information Assets of the OTSI and/or the State of California. Consequently, it is important for all users to access and use Information Assets in a responsible, ethical, and legal manner that safeguards OTSI data and other assets.

Additionally, the appropriate use of Information Assets benefits the State and the OTSI by strengthening the protection of the OTSI and its Personnel and business partners from illegal and/or potentially damaging activities.

This policy defines and establishes the requirements for the appropriate use and safeguarding of the OTSI's Information Assets. All Personnel must read and sign the OTSI Acknowledgement of Policies, attesting that he/she understands and agrees to comply with the policy prior to accessing any OTSI Information Assets.

Authority

Pursuant to California Government Code Section 7929.210 and 11549.3, the OTSI is required to ensure the security and confidentiality of the information it processes on behalf of its clients and employees. This security policy complies with California Government Code Section 11549.3.

This policy may be updated at any time to ensure changes to the OTSI's organization structure and/or business practices are properly reflected in the policy.

To view all published Information Security policies, visit the Information Security Office Intranet Page and click on ISO Policies.

Ownership of Information

Data and information in hard copy format and/or data and information that is electronically created, sent, received, processed, or stored on Information Assets owned, leased, administered, or otherwise under the custody and control of the OTSI are the property of the OTSI. Any information not specifically identified as the property of other parties, and that is transmitted, processed, or stored on the OTSI's and business partner IT facilities and resources (including e-mail, messages, and files) is the property of the OTSI.

Individual access and use of OTSI Information Assets are neither personal nor private. As such, OTSI management reserves the right to monitor and/or log all employee use of OTSI Information Assets with or without prior notice.

Scope and Applicability

The scope of this policy extends to all OTSI, and agency Information Assets owned or operated by the OTSI, Information Assets managed by third parties on behalf of the OTSI, and all Information Assets that process or store OTSI information in support of OTSI mission and business functions. This policy applies to all OTSI Personnel.

Policy Directives

General Use and Ownership

1. Personnel shall use and protect OTSI Information Assets in accordance with this policy and applicable information security and privacy policies.
2. Personnel shall not share their work-related account(s), passwords, Personal Identification Numbers (PIN), security questions/answers, security tokens (e.g., smartcard, key fob), or similar information or devices used for authentication and authorization purposes.
3. Personnel shall not attempt to access any data, documents, email correspondence, and programs contained on OTSI systems for which they do not have authorization.
4. Personnel shall not access copyrighted information in any way that violates the copyright.
5. Personnel shall not make unauthorized copies of copyrighted or OTSI-owned software.
6. Personnel shall only download, procure, and/or use software, including, but not limited to, free trials, shareware, and freeware, which has been approved/reviewed by the OTSI Privacy Officer, the OTSI Information Security Officer (ISO), the OTSI

Chief Technology Officer (CTO), and OTSI Legal, as required by established OTSI procedure.

Unacceptable Use

7. Personnel shall not use OTSI Information Assets to engage in or solicit the performance of any activity that violates laws, regulations, rules, policies, standards, and/or other applicable requirements issued by the federal government, the State of California, and/or the OTSI.
8. Personnel shall not forward OTSI confidential messages or material to external locations.
9. Personnel shall not use OTSI Information Assets for personal use or benefit, political activity, unsolicited advertising, unauthorized fundraising, or an outside endeavor not related to state business such as an employee's side-business.
10. Personnel shall not use OTSI Information Assets to distribute, disseminate or store emails and/or intentionally access websites that contain pornographic, racist or offensive material, chain letters, unauthorized mass mailings.
11. Personnel shall not intentionally introduce any form of computer virus, malware, or malicious code into the OTSI network.
12. Personnel shall not purposely engage in activity that may harass, threaten, or abuse others or intentionally access, create, store, or transmit material that the OTSI may deem to be offensive, indecent, or obscene.
13. Personnel shall not purposely engage in activity that is illegal pursuant to local, state, or federal laws.
14. Personnel shall not connect any non-OTSI issued: desktop, laptop, smart phone, tablet, or other devices to the OTSI wired or wireless network, unless written approval is obtained from a manager.
15. Personnel shall not connect any non-OTSI issued USB devices, flash drives, or any other multimedia devices unless written approval is obtained from a manager.
16. Personnel shall not undertake any deliberate activities that waste staff effort or networked resources.

Security and Propriety Information

17. Personnel shall report any security concerns pertaining to OTSI Information Asset security of which they become aware to the OTSI ISO, designee or appropriate security staff. Security concerns in Information Asset security include unexpected software or system behavior, which could result in unintentional disclosure of information or exposure to security threats.
18. Personnel shall not engage in any activity that attempts to circumvent the OTSI's security controls (e.g., spoofing email, anonymous proxies, or unauthorized encryption), or other activities that may degrade the performance of information resources or may deprive an authorized user access to OTSI assets.
19. Access to the Internet from OTSI owned or leased, home based, computers must adhere to all pertinent policies. Personnel shall not allow family members

or other non-employees to access OTSI computer systems.

20. Personnel shall report any suspected or actual activities and/or events indicating misuse or any violation of this Acceptable Use Policy to their management, the OTSI ISO, designee or appropriate security staff.

Minimal and Incidental Use

Government Code section 8314 permits minimal and incidental personal use of state resources. At the OTSI, this means as follows:

1. Minimal and incidental personal use of electronic mail, Internet access, fax machines, printers, phones, and copiers are restricted to OTSI approved Personnel only and does not include family members or others not affiliated with the OTSI.
2. Minimal and incidental use must not result in direct costs to the OTSI, cause legal action against, or cause embarrassment to the OTSI.
3. Minimal and incidental use must not interfere with the normal performance of an employee's work duties.
4. Storage of personal electronic mail messages, voice messages, files, and documents within the OTSI's computer resources must be minimal.

OTSI management will resolve minimal and incidental use questions and issues in collaboration with the OTSI's ISO, OTSI Human Resources, and OTSI Legal.

Roles and Responsibilities

OTSI Director or Information Security Office

The OTSI Director has the ultimate responsibility to establish and maintain this policy and delegates responsibility for the OTSI policy program to the ISO.

The OTSI ISO shall:

1. Ensure that all OTSI Personnel are aware of this policy and acknowledge their individual responsibilities.
2. Review this policy annually and update it accordingly.
3. Ensure that procedures are reviewed annually and updated accordingly.
4. Periodically audit and assess compliance with this policy.

OTSI Users

1. All Personnel are required to follow the directives in this policy.
2. All Personnel are required to report any incidents of possible misuse or violation of this policy to the OTSI ISO.
3. All Personnel are required to read and acknowledge they have read and understand this policy.

Violations/Enforcement

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries, contract termination for contractors, and dismissal of interns and volunteers.

   Personnel are also subject to loss of OTSI information resources access privileges. Additionally, Personnel may be subject to civil penalties and/or criminal prosecution.

2. The OTSI ISO is responsible for the periodic auditing and reporting of compliance with this policy. The OTSI ISO is responsible for defining the format and frequency of the reporting requirements and communicating those requirements, in writing, to OTSI management.

Auditing

The OTSI has the right to audit any activities related to the use of state Information Assets.

Reporting

Any violations of security policies must be immediately reported to the direct manager and the OTSI ISO.

Exception Request Process

If compliance is not feasible or is technically impossible, if existing policy currently in place already meets these requirements, or if deviation from this policy is necessary to support a business function, the respective manager must formally request a policy exception as defined below.

1. Any request for security exceptions shall be requested through Service Now.
2. Exceptions to this policy must be approved by the requestor's manager, ISO, and the CTO.
3. The term of an approved security exception may not exceed twelve (12) months.

Approval

DocuSigned by:
Brian Wong
981846AEE780497...

1/12/2021

Approved by the Office of the Directorate by the Chief Information Officer **Date**

Related Policies, Procedures and Standards

To view all published Information Security policies, visit the Information Security Office Intranet Page and click on ISO Policies.

Reference #	Article
SAM 5320.4	Personnel Security
SIMM 5305-A	Information Security Program Management Standard
ISO Processes and Procedures	Removable Media Acceptable Use Procedures

Revision History

Date	Description of Change	By
01/12/2021	Revised policy to align with State of California and Federal NIST 800-53 v5 control standards; Assigned new control number (previously #OSI-SP-08-08)	ISO
01/10/2023	Update Government Code to include 7929.210 Pursuant to California Government Code Section 7929.210 and 11549.3	ISO
9/27/2023	Review and Update OSI to OTSI, logo change and header change.	ISO

Definitions of Key Terms

The OTSI uses the information security and privacy definitions issued by the California Department of Technology Office of Information Security in implementing information security and privacy policy. Terms and definitions are defined here and on the California Department of Technology website at https://cdt.ca.gov/security/technical-definitions/.

Information Assets	Information Assets include (a) all categories of paper and automated information, including (but not limited to) records, files, and databases; and (b) information technology facilities and equipment (including telecommunications networks, personal computer systems, laptops, tablets, and mobile devices), and software owned or leased by state entities.
NIST	National Institute of Standards and Technology https://www.nist.gov/
Personnel	OTSI employees, retired annuitants, student assistants, volunteers, contractors, and/or sub-contractors, and interns.

Office of Systems Integration "SERVING CALIFORNIA"	**ADMINISTRATIVE POLICY** **Control Number: OSI-2019-02**
Equal Employment Opportunity (EEO) Discrimination/Harassment Prevention Policy and Complaint Filing Procedures	**Revised: July 1, 2008** **Revised: August 1, 2020**

PURPOSE

The Office of Systems Integration (OSI) is committed to providing an equal employment opportunity work environment to all employees, applicants, vendors, contractors, clients, customers, and members of the public and creating a work atmosphere in which all individuals are treated with respect and professionalism. Consistent with this commitment, it is the policy of the OSI to provide a workplace free from discrimination, harassment, and retaliation and ensure nondiscrimination and equal access to State jobs, work assignments, training, and other employment-related opportunities for all OSI employees and job applicants. This policy applies to all aspects of employment within the OSI including recruitment, hiring, promotion, transfer, training, corrective and/or disciplinary action, adverse action, and other terms, conditions, and benefits of employment.

All employees are prohibited from discriminating against or harassing anyone on the basis of their protected status with regard to age, ancestry, citizenship, color, disability, domestic violence victim status, gender, gender expression, gender identity, genetic information, marital status, medical condition, medical leave (requesting or approved for leave under the Family and Medical Leave Act or the California Family Rights Act), mental disability, military and/or veteran status, national origin, physical disability, political affiliation, race; (including hairstyle or hair texture traits historically associated with race), religion, reasonable accommodation process (request for or participating), retaliation/reprisal, sex or sexual harassment (including pregnancy, childbirth, lactation, and medical conditions related to pregnancy, childbirth or lactation), sexual orientation, and/or any other status protected by State or federal law.

POLICY

All employees are prohibited from retaliating against any person because the person has opposed any practices forbidden under this policy or because the person has filed a complaint, testified, or assisted in any proceeding related to this policy. All employees are prohibited from aiding or coercing the doing of any acts forbidden under this policy. Disciplinary action, up to and including dismissal, may be taken against any employee who violates this policy.

The process set forth for reporting allegations of discrimination, harassment, including sexual harassment, and retaliation is found in this document under the OSI *Discrimination and Harassment Complainant/Respondent Filing Procedures*. Every OSI employee, whether a

witness, complainant, or alleged harasser, is expected to cooperate fully with every investigation.

DEFINITIONS

Discrimination: Any employment practice or behavior that treats one person unfairly over another, according to factors unrelated to their ability or potential. Discriminatory behavior or practice can result in employees being denied fair and equal consideration for employment, retention, evaluation, or advancement. Discrimination occurs when individuals are treated unfairly or differently based upon any protected status identified in the "Purpose" section of this policy.

Sexual Harassment: Federal and State regulations have defined sexual harassment as a form of sex discrimination. It can consist of, but is not limited to, unwelcome sexual advances, requests for sexual favors, the display of sexually derogatory posters, cartoons, drawings, or other physical or verbal conduct of a sexual nature by supervisors or others in the workplace.

The law categorizes sexual harassment into two types:

1. *Quid Pro Quo* (Latin for "something for something"). This form of sexual harassment occurs when an employee exercising authority over another employee makes submission to sexual conduct either an explicit or implicit term or condition of employment (including hiring, compensation, promotion, retention, work assignment, etc.), or when submission to or rejection of sexual conduct by an employee is used as a basis for employment decisions affecting the employee. Quid pro quo occurs when a supervisor or manager:
    - Demands, as an explicit or implied term or condition of employment decisions, a subordinate submit to sexual advances (this may include situations which began as reciprocal relationships but later cease to be reciprocal), and/or
    - Makes requests for sexual favors or other verbal, visual, or physical conduct of a sexual nature that is an explicit or implied term or condition of employment decisions.

    Examples of quid pro quo harassment include:

    - Request(s) for sexual favors in exchange for a promotion or raise.
    - Expressed or implied statement(s) that a person will be demoted or fired if she/he does not submit to a sexual request and/or carries out the threat.

2. *Hostile Environment Sexual Harassment* is a form of discrimination which occurs when an individual is subjected to unwelcome sexual advances or other gender-based conduct that is sufficiently severe or pervasive to interfere with the individual's work environment. The work environment must be both subjectively and objectively perceived as abusive. The courts look at the totality of the circumstances surrounding the alleged incidents of harassment to determine whether unlawful conduct has occurred. Generally, there must be a pattern of unlawful conduct, although a single serious incident in some cases, such as sexual battery, might be enough to constitute unreasonable interference with an

employee's work performance and/or create an intimidating, or otherwise offensive work environment. The harasser can be a manager, supervisor, co-worker or a non-employee, such as a supplier/vendor or customer. Examples include:

- Submission to such conduct is made either explicitly or implicitly as a term or condition of employment.
- Leering, making or sending sexual jokes or sexually suggestive remarks, or making sexual gestures.
- Making offensive, negative or demeaning remarks about a person's gender or physical appearance.
- Deliberate and unwelcome touching, hugging, patting, and/or blocking a person's movement.
- Displaying offensive sexual illustrations or pictures in the workplace.
- Unwelcome pressure for dates or sex (this may include situations which began as reciprocal relationships, but later ceased to be reciprocal).

EXAMPLES OF PROHIBITED CONDUCT

Discrimination and harassment (including sexual harassment and retaliation) refers to behavior that is unwanted and unwelcome and which is imposed on a person who reasonably regards it as offensive or undesirable. Such behavior fails to respect the rights and dignity of others and/or may interfere with an individual's effective work performance. The type of prohibited discriminatory or harassing behavior/conduct which may be found to constitute a violation of EEO policy includes, but is not limited to:

- Making employment decisions based on an individual's protected characteristics.
- Changing the terms, conditions, or privileges of employment of an employee in retaliation for filing an EEO complaint or participating in the discrimination complaint process.
- Denying or failing to provide reasonable accommodation for a disability or a bona fide religious practice.
- Denying a leave request for which an employee is eligible under the Family Medical Leave Act (FMLA) or the California Family Rights Act (CFRA).
- Using discriminatory/derogatory terms or telling discriminatory jokes based on an individual's protected status.
- Treating an individual more and/or less favorably than other individuals based on their protected status.
- Displaying offensive, derogatory, or discriminatory objects, pictures (including cartoons), or posters that are inappropriate and/or negatively reference an individual's protected status.
- Posting, sending, uploading/downloading messages with discriminatory, harassing, or retaliatory content in any form via electronic mail, the intranet/internet websites, cell phone, texting, facsimile (fax), and mail (inter-office, public, or private).
- Reprisals or threats after an individual complains about others making derogatory comments or jokes concerning an individual's protected status, or after he/she complains about being treated less favorably than other individuals because of his/her protected status.

- Discriminating against any employee in violation of this policy which may create a hostile work environment.
- Engaging in any unwelcomed verbal or physical contact such as leering (staring in a sexual manner), blocking the path of a person, or whistling at another individual.
- Communication of a sexual nature, sexually explicit or obscene jokes, profanity, sexual gestures, sexually suggestive correspondence, notes, invitations, e-mail, voicemail, or gifts.
- Employment benefits affected in exchange for sexual favors (may include situations where a third party is treated less favorably because others have acquiesced to sexual advances).
- Sexual advances which are unsolicited or unwelcome. This may include situations that began as welcome or reciprocated but later ceased to be welcome or reciprocated.

In some cases, a person's actions may not be intended as discriminatory or harassment but may be so perceived by either the recipient of such behavior or a third-party observer. If a reasonable person would find the actions(s) offensive or intimidating, it will be held that discrimination or harassment has occurred, even if such is not the intention of the person exhibiting the behavior.

CONFIDENTIALITY

The OSI will respect the privacy rights of individuals who either report or are accused of harassment, discrimination, or retaliation. Consistent with State and federal law, the OSI will attempt to maintain the confidentiality of personal information. The OSI will not, however, be able to maintain information as confidential if disclosure is necessary for the OSI to investigate a complaint or to take appropriate action, or if disclosure is otherwise required by law (for example, the OSI is required to respond to a subpoena or other legal process).

ROLES AND RESPONSIBILITIES

Equal Employment Opportunity (EEO) Officer

The EEO Officer enforces the OSI's EEO policies and will take appropriate action, including investigating, facilitating the mediation program, and providing information in response to discrimination/harassment complaints. This includes ensuring that all employees are informed of their rights (*Complainant's Statement of Rights)*. The EEO Officer strives to complete an investigation within ninety (90) days of the filing of a formal complaint. If the EEO Officer is unable to complete the investigation within the 90-day period, the EEO Officer will inform the complainant in writing as to the reason(s) they are unable to issue a decision in the allotted time.

Manager/Supervisor

Managers and supervisors provide equal opportunity in employment to the OSI employees and job applicants and are responsible for maintaining standards that promote a work environment that is free from discrimination, harassment, retaliation, and unprofessional or disrespectful conduct and assures employees that the OSI does not tolerate such behavior or conduct. A manager/supervisor:

- Adheres to and enforces the OSI *Discrimination/Harassment Policy*.
- Ensures employees under their supervision/management attend mandated training.
- Advises their employees of their rights (*Complainant's Statement of Rights*) and the process for filing a discrimination complaint as described in this document.
- **Immediately** notifies the EEO Officer upon becoming aware of conduct that may be in violation of the policy and
- Submits documentation, within 3 working days of the complaint, to the EEO Officer, of the discussions or other facts from the employee (complainant) of a potential policy violation.
- Takes proactive, direct, immediate, corrective, and effective action to prevent and stop inappropriate conduct and/or violations of the policy of which they become aware, regardless of how the information is acquired and regardless of the complainant's desire to keep the complaint confidential. It is the obligation of the OSI managers and supervisors to stop prohibited conduct; therefore, complete confidentiality cannot be guaranteed. However, we ensure strict discretion and information will be shared only with those who need to know.
- Provides a response, in coordination with the EEO Officer, to the employee (complainant) within fifteen (15) calendar days of being informed of the complaint.
- Protects the individual (complainant) alleging discrimination or harassment from reprisal/retaliation.

Managers and supervisors will be subject to appropriate corrective and/or disciplinary action, up to and including termination, for failing to carry out their duties to enforce the policy, even if they have not personally engaged in the discrimination/harassment. As provided by law, managers and supervisors may be held personally responsible in a civil suit if they personally engage in discriminatory or harassing conduct, or if action taken by them was ineffective in stopping the discrimination or harassment. Their actions taken must be reasonably calculated to effectively stop the discrimination or harassment.

A manager or supervisor who engages in a sexual or personal relationship with a subordinate shall immediately report that relationship to his/her immediate manager or supervisor. The immediate manager or supervisor will contact the EEO Officer or Personnel Officer to coordinate action(s) that the OSI may deem appropriate under the circumstances, including modifying reporting relationships.

Employee

Every employee has the right to work in an environment free from harassment, discrimination, and retaliation. (See *Complainant Statement of Rights*). All employees must avoid offensive or inappropriate behavior or conduct, and all have a shared responsibility for ensuring the workplace and job-related functions are free from discrimination and/or harassment.

An employee who is the recipient of harassing, discriminatory, or retaliatory behavior as described in the OSI EEO *Discrimination/Harassment Policy*; or perceives comments, gestures, or actions of another to be offensive or unwelcome is strongly encouraged to communicate to that person their behavior is not welcome or acceptable. However, failure to do so does not preclude the employee from complaining to a supervisor or filing a complaint with the EEO

Office. If an employee feels threatened or otherwise prefers to not communicate directly with the harasser, the employee should immediately seek assistance from the employee's manager, supervisor, or EEO Officer and:

- Understand and adhere to the OSI EEO Discrimination/Harassment Policy.
- Sign the *Acknowledgement of Receipt of Equal Employment Opportunity Policy* form, and provide a copy to the EEO Office.
- Attend related mandated training.
- Refrain from engaging in, condoning, and/or tolerating discrimination, harassment, and/or retaliation.
- Immediately report witnessed violations of the Policy by an informal or formal complaint. In the case where the alleged harasser is the manager/supervisor or where the employee feels uncomfortable talking with the manager/supervisor, the employee should report the incident directly to the EEO Officer.
- Fully cooperate in the inquiry and/or investigation processes and resolution of a complaint.

An employee who is found to have violated this policy will be subject to appropriate corrective and/or disciplinary action, up to and including termination, regardless of job level/classification. Additionally, as provided by law, individuals found to have engaged in prohibited conduct may be held personally liable for their actions, regardless of whether a manager or supervisor fails to take appropriate action.

AUTHORITY

The following authorities prohibit discrimination, harassment (including sexual harassment) in employment, and retaliation and requires employers take all reasonable steps to prevent discrimination, harassment, and/or retaliation from occurring at the workplace. All employees are prohibited from engaging in behavior that rises to the level of discrimination, harassment, or retaliation in violation of the following:

- Title VII, Civil Rights Act of 1964
- California Government Code Section 12940-12951
- California Government Code Section 18500
- California Government Code Section 19700-19706
- California Fair Employment and Housing Act (FEHA) of 1959 (including amendments)
- Age Discrimination in Employment Act (ADEA) of 1967
- Rehabilitation Act of 1973
- Americans with Disabilities Act of 1990 (including amendments)
- California Genetic Information Non-discrimination Act (GINA)
- Governor's Executive Order S-6-04
- SPB Rules 64.1 - 64.6 (California Code of Regulations, Title 2 Section 64.1-64.6)

DISCRIMINATION/HARASSMENT COMPLAINT FILING PROCEDURES

INTRODUCTION

Employees have different options for raising and/or resolving complaints with the OSI. While the procedures that follow pertain to discrimination and harassment complaints, it should be noted that general complaints of rude/discourteous behavior or workplace bullying, which are not based on a protected status, may be submitted to the OSI Equal Employment Opportunity Office.

Complaints that an individual has been a subject of discrimination or harassment based on one or more protected status may be resolved through the mediation program, informal process, formal complaint process, or the filing of an external complaint as described below:

MEDIATION

Mediation is a voluntary and confidential alternative dispute resolution (ADR) process available within the OSI that promotes a better understanding in the workplace and assists employees, supervisors, and managers in reaching mutually satisfying solutions in workplace disputes. Mediators are certified professionals from the Public Employment Relations Board (PERB); there is no charge to the employee(s) participating in the Mediation Program.

Mediation can be used to resolve disputes arising out of claims of discrimination or harassment. It is a voluntary and confidential process in which all parties must agree to participate. If involved in a dispute, an employee can request mediation by contacting the Equal Employment Opportunity (EEO) Officer. The EEO Officer serves as the liaison for the mediation program and will contact the other parties involved in the dispute to ask if they agree to mediation. If the case is determined to be appropriate for mediation, a date will be set by the PERB case coordinator. A certified mediator from the PERB will be assigned to help the disputing parties resolve their differences. Note: Not all cases are appropriate for mediation.

INFORMAL PROCESS

Employees are not required to utilize the informal process but are encouraged to do so as the first step to resolution. An employee (complainant) who believes that he/she has been harassed or discriminated against is strongly encouraged to inform the offending employee that their behavior is unwelcome, offensive, and/or inappropriate. If after informing the offending employee, and the behavior, actions, or comments do not stop; or if the complainant is uncomfortable going directly to the offending party, he/she is strongly encouraged to report the behavior to his/her manager/supervisor.

The manager/supervisor will contact the EEO Officer to coordinate an in-take interview with the complainant and witnesses and provide a response to the complainant within fifteen (15) calendar days of being informed of the complaint. Alternatively, the complainant may go directly to the EEO Officer who will conduct the in-take interview and provide a response to the complainant within fifteen (15) calendar days. The response will indicate if the complaint can be resolved by the manager/supervisor and EEO Officer without further investigation or if the complaint is within the OSI's jurisdiction and a formal investigation is required.

The complainant shall be given the *Complainant's Statement of Rights* form by the EEO Officer and provided an overview of their rights in the formal process.

FORMAL COMPLAINT PROCESS

If the employee is not satisfied with the results of the informal process or decides to bypass the informal process, a formal complaint of discrimination or harassment may be filed with the EEO Officer by completing the *Discrimination/Harassment Complaint Form*. The EEO Officer shall give the employee the *Complainant's Statement of Rights* form and provide an overview of their rights in the formal process.

Upon completion of the in-take process and the EEO officer determining the complaint is within the OSI's jurisdiction, a formal investigation may begin within seven (7) calendar days of receipt of the complaint. The EEO Office strives to complete an investigation within ninety (90) calendar days of the filing of the formal complaint. The final response by the EEO Officer will be rendered in writing to the employee (complainant).

Basis of Discrimination: An individual filing a complaint (complainant) must allege that he/she was discriminated or harassed on the basis of age, ancestry, citizenship, color, disability, domestic violence victim status, gender, gender expression, gender identity, genetic information, marital status, medical condition, medical leave (requesting or approved for leave under the Family and Medical Leave Act or the California Family Rights Act), mental disability, military and/or veteran status, national origin, physical disability, political affiliation, race, religion, reasonable accommodation process (request for or participating), retaliation/reprisal, sex or sexual harassment (includes pregnancy, childbirth, lactation, and medical conditions related to pregnancy, childbirth or lactation), sexual orientation, and/or any other status protected by State or federal law. (*See Basis of Discrimination Protected Group Categories and Examples of Prohibited Conduct.)*

Timeframe: A complaint of discrimination, including harassment, must be filed within 365 calendar days of the date of the discriminatory action. If the employee or applicant just obtained knowledge of the facts of the unlawful discrimination or harassment, an additional 90 calendar days may be granted following the one-year expiration date per California Government Code section 12960.

EXTERNAL FILING OPTIONS

State Personnel Board

If the complainant is not satisfied with the OSI's decision, and the complaint involves discrimination, harassment, retaliation, or denial of a reasonable accommodation for a known physical or mental disability, he/she may file a complaint to the State Personnel Board (SPB) Appeals Division within thirty (30) calendar days after the receipt of the EEO Officer's decision. If the OSI has failed to provide a decision within ninety (90) days of the complaint being filed, the complainant may file a complaint with the Appeals Division within one-hundred and fifty (150) days of the date the complainant filed the complaint with the OSI.

Complaints must be filed in compliance with the requirements and timeframes specified by civil service laws and regulations. See the SPB Appeals Resource Guide available online at www.spb.ca.gov for specific information.

State Personnel Board Appeals Division
801 Capitol Mall
Sacramento, CA 95814-4806

Phone: (916) 653-0799
Fax: (916) 654-6055
Email: appeals@spb.ca.gov

Department of Fair Employment and Housing (DFEH)

Individuals may file a complaint either separately or concurrently to the DFEH at any time during the informal/formal complaint processes within three years of the incident.

Department of Fair Employment & Housing
(DFEH) Headquarters
2218 Kausen Drive, Suite 100
Elk Grove, CA 95758
www.dfeh.ca.gov

Toll free: 1- 800-884-1684 (voice); 1-800-700-2320 (TTY); or California's Relay Service at 711

United States Equal Employment Opportunity Commission (EEOC)

Individuals may file a complaint either separately or concurrently to the EEOC at any time during the informal/formal complaint process within one-hundred and eighty (180) calendar days from the date of the incident. See the U.S. EEOC webpage for their timeframe extension criteria.

United States Equal Employment Opportunity Commission (EEOC)

For complaint filing instructions and/or to locate the nearest EEOC office go to: www.eeoc.gov

Or call: Toll free: 1-800-669-4000 (voice);

1-800-669-6820 (TTY Deaf/Hard of Hearing callers only); or 1-844-234-5122 (ASL Video Phone for Deaf/Hard of Hearing callers only)

NOTE: Employees in certain Bargaining Units have an additional option of filing through the grievance process. However, it should be noted that the same complaint cannot be filed through both the OSI EEO Office and the OSI Labor Relations Office grievance processes. Please refer to the appropriate Memoranda of Understanding (MOU) for specific grievance filing guidelines.

Additional Information:

- Acknowledgement of Receipt of the EEO Policy and Discrimination Complaint Process
- Complainant's Statement of Rights
- Basis of Discrimination Protected Group Categories (DFEH 2017)
- Discrimination/Harassment Complaint Form
- Complainant's Guide Pamphlet
- Respondent's Guide Pamphlet
- Mediation Program Pamphlet

Issued by the Office of the Directorate

Office of Systems Integration "SERVING CALIFORNIA"	**ADMINISTRATIVE POLICY** **Control Number: OSI-AP-07-05**
INCOMPATIBLE ACTIVITIES	**Revised: October 15, 2009**

Authority

Section 19990 of the Government Code requires in part that: "A state officer or employee shall not engage in any employment, activity, or enterprise which is clearly inconsistent, incompatible, in conflict with, or inimical to his or her duties as a state officer or employee." Each state agency is directed to determine, as specifically as possible, the kinds of activities that are deemed inappropriate. Pursuant to this mandate, the California Health and Human Service Agency (hereinafter referred to as "the Agency") has developed this Incompatible Activities Policy.

Policy

It is the policy of the Agency to comply with all provisions of Government Code section 19990. Therefore, no Agency officer or employee shall engage in any employment, activity, or enterprise which is clearly inconsistent, incompatible, or in conflict with his or her duties as an Agency employee.

All management is responsible for ensuring that subordinate staff are informed of this policy and all prospective employees should be made aware that in accepting employment they must abide by these policies. **EACH EMPLOYEE SHALL BE GIVEN A COPY OF THIS POLICY.**

The following statements, examples, and guidelines do not attempt to specify every activity that may be incompatible, nor should they be taken as the only rules that must be observed by an employee. The items included below are illustrations of principles and are not all-inclusive. Interpretation of policy will be made on a case-by-case basis.

Penalty for Violation of Incompatible Activities Policy

An employee may be subject to disciplinary action for a violation of Government Code section 19990. The severity of any adverse action taken will depend upon all circumstances of the particular violation (e.g., any adverse consequences to the Agency caused by the seriousness of the particular activity).

Definitions

"Employee" includes all employees of the Agency. The term encompasses any attempt by an employee to circumvent the following policies by the use of a friend, relative, dependent, outside employment, or other entity to accomplish indirectly what the following policy prohibits. This definition of "employee" applies throughout this policy.

"Person" includes individuals, spouses and/or registered domestic partners of individuals, firms, corporations, partnerships, associations, other governmental bodies, or agents and representatives of these entities. This definition of "person" applies throughout this policy.

"Outside Employment" is defined as any partnership, ownership, or services performed by an Agency employee on his/her own time, during other than normal working hours, for which he/she may or may not receive any form of compensation. This includes business/employment of spouses and/or registered domestic partners which the employee would have a financial interest in by operation of law. This definition of "outside employment" applies throughout this policy.

"Outside Activity" is defined as any employment, enterprise, or service performed by an Agency employee on his/her own time, during other than normal working hours, for which he/she may or may not receive any form of compensation, including volunteer work. This definition of "outside activity" applies throughout this policy.

Outside Employment and/or Activity

An employee **MAY** engage in an outside employment and/or activity that is not directly or indirectly related to the employee's functions or responsibilities of his/her Agency duties. Examples of employment and/or activities that typically do not deal with Agency are:

- Cashiering and/or retail sales
- Crafts/handiwork
- Ranching
- Usher at community events

An employee **SHALL NOT** engage in outside employment and/or activities that are directly or indirectly related to the functions and responsibilities of his/her Agency duties or that is subject directly or indirectly to the review, control, inspection, audit, or enforcement by that employee. Examples of employment and/or activities that may be related to Agency are:

- Counseling
- Day care
- Foster care
- Group care homes
- Skilled nursing care

Outside Employment and/or Activity (continued)

- Involvement in any employment/activity that is subject to the review, control, inspection, audit, or enforcement by the employee
- Medical exam/reviews
- Real estate agent/broker

Employees are responsible for submitting in writing, a description of any and all outside employment and/or activities that may be related to the Agency. In some instances, an individual incompatible activity determination will need to be prepared by the Agency.

An employee is **PROHIBITED** from engaging in the following outside activities or employment:

1. An employee shall not counsel, advise, or assist, other than as part of regular performance of Agency duties, any person in the preparation, presentation, or defense of any appeal, application, claim, notice, petition, record, report, statements, or other writing or matter that is before, or may be presented to Agency in any administrative hearing or court proceeding or action arising under the laws administered by Agency or department within the Agency.

2. An employee shall not serve, either directly or indirectly, as the representative for any person who is either an applicant for, or a recipient of, any type of public service or assistance from any Agency program. An employee shall not serve, either directly or indirectly, as the representative for any person that is either applying for, or has obtained, any license issued by an Agency program, or which is subject to audit by an Agency program.

3. An employee shall not serve, either directly or indirectly, as the representative of any person in any state hearing, administrative hearing, or trial in which Agency is a party or adjudicator, unless required as part of his/her duties as an employee of the Agency.

4. An employee shall not contract on his/her own behalf as an independent contractor with any state agency to provide services or goods. (See Public Contract Code section 10410.)

No outside employment and/or activity should create a situation in which the employee fails to devote full-time attention and efforts to his/her Agency duties during regular hours of employment. In all outside activities and/or employment situations, the employee must abide by the restrictions listed below.

Misuse of Position and/or Resources

Misuse of position and/or resources include using state time, facilities, equipment, or supplies for private gain and/or for the advantage of another person. Any activity

Misuse of Position and/or Resources (continued)

pursued during or outside of regular work hours that may impede an employee's ability to comply with this obligation is incompatible.

Examples of prohibited activities and/or activities that constitute misuse of position and/or resources include but are not limited to:

1. No employee shall use, either during or outside of office hours, any Agency symbol, badge, uniform, identification card, record, information, facility, staff time, equipment, supplies, training material, vehicle, telephone, address, postage, mailing list, or influence of a state position for personal gain and/or advantaged, or lend or give such items to clients, contractors, providers, or other persons, unless otherwise authorized by law.

2. No employee shall use copy machines or computer equipment and software for home or personal use.

3. No employee shall accept, take, or convert to one's own use, products of any kind in the course of or result of inspections of products or facilities.

4. No employee shall arrange for employment outside state service while on duty.

5. No employee shall use the status of Agency to solicit directly or indirectly business of any kind or to purchase goods or services for private use at discounts from a person who does business with the State.

6. No employee shall use confidential or non-confidential information available to an employee by virtue solely of the employee's state employment for personal gain and/or advantage, or for the personal gain and/or advantage of another person. Supervisors should make reasonable efforts to ensure employees are aware of what information is confidential.

7. No employee shall provide confidential information to persons who have not been authorized to receive such information.

8. No employee shall provide services or information to prospective bidders on any contract which are not available to all bidders on the contract.

9. No employee shall provide or use the names of persons or records of the Agency for a mailing list that has not been authorized.

10. No employee shall prepare, present, or publish any speech, article, or other writing relating to the operation of the Agency for compensation from a source other than the State without prior approval of the Agency.

Misuse of Position and/or Resources (continued)

11. No employee shall use the authority of his/her position with the Agency to violate or circumvent, or assist another to violate or circumvent, any state or federal laws, regulations, and policies relating to programs administered by the Agency.

12. No employee who has been given authority to make outside purchases for materials or services for the Agency shall make such purchases from any business entity in which they have a financial interest

Gifts

1. No employee shall accept, solicit, or pass on to other persons any gift, including money, or any service, gratuity, favor, entertainment, hospitality, loan, or any other thing of value from any current, former, or prospective OSI consultant or contractor.

2. If an employee receives an offer of a valuable favor, expensive gift, or cash, the employee's direct supervisor must be notified immediately, even when the offer has been refused. The supervisor will elevate the issue as appropriate.

3. For all other situations, the Political Reform Act (Government Code section 81000 et. seq.) imposes limits on gifts and prohibits honoraria payments received by designated state employees. In addition, the Act establishes filing requirements for the Statement of Economic Interests (Form 700) on an annual basis.

Use of State Time to Market Products

State and Agency policies prohibit the use of state time and resources by employees to market products. In addition, the Incompatible Activities Policy requires that during hours of duty, employees are to devote their full time, attention and efforts to their state office and/or assigned duties. The term product includes, but is not limited to, cosmetics, food products, housewares, mail orders, jewelry, and other sundry products. Employees involved in the marketing of products must confine such activities to non-work time during the workday.

Political Activities

Political activities for state employees and officers are covered under the Federal "Hatch Act" and applicable state statutes. For information regarding specific political activities, please contact your supervisor or Department of Social Services Legal Office.

Consultants

All full-time and part-time consultants to Agency are subject to the provisions of Agency's Incompatible Activities Policy.

Former Employees

Once an employee leaves state service, he/she is no longer subject to the provisions of Government Code section 19990. However, former employees are governed by the Political Reform Act, which restricts post-government employment under the provisions of Government Code sections 81000-91015. For information regarding these restrictions, please contact your supervisor or Departmental of Social Services Legal Office.

Procedures

All employees shall complete the attached certification. Those employees who are engaged in, or wish to engage in, any employment or activity that falls into "Category B or C" as indicated on the certification page, must complete the Incompatible Activities Certification and submit a written description of the specifics addressed to his/her immediate supervisor for review. This written description should include the name of the employer or activity, the function to be performed, the number of hours per week that the activity and/or employment will involve, if paid or volunteer, and the basis on which the employee believes that the employment and/or activity may/may not be compatible. This notification shall be made prior to engaging in the outside employment and/or activity so that a determination can be made with review by legal counsel as to the permissibility of the employment and/or activity.

Appeal Procedures

Employees have the right to appeal the application of this policy to their individual situation. Represented employees should follow the appeal process stated in their Memorandum of Understanding (MOU). If there is no process in the MOU, the employee may file a written appeal with the Agency. All non-represented employees may file a written appeal with the Agency. The written appeal should include the reason(s) the employee disagrees with the decision.

Certification

The certification shall be signed and submitted by all Agency employees.

Questions

Questions regarding this policy should be directed to your supervisor or the Administrative Operations Branch Manager.

Approval

Crystal Cooper Date
CHIEF DEPUTY DIRECTOR
Office of Systems Integration

Office of Technology & Solutions Integration CALIFORNIA HEALTH & HUMAN SERVICES AGENCY	**SECURITY POLICY** **CONTROL NUMBER: OSI-2021-37**
Password Policy	**Revision Date: October 12, 2021**

Purpose

This policy defines the requirements for the use of strong passwords to protect Information Assets owned by the Office of Technology & Solutions Integration (OTSI).

Information Assets owned by the OTSI are strategic assets intended for official business use and are entrusted to state Personnel and business partners in the performance of their job-related duties. Insufficient access controls or unmanaged access to information could lead to intentional and/or inadvertent unauthorized disclosure or theft of this information, resulting in potential harm to individuals, loss of public trust, litigation and/orsanctions. By accessing any OTSI Information Technology (IT) resources, all Personnel agree to abide by the terms of this policy.

Authority

Pursuant to California Government Code Section 7929.210 and 11549.3, the OTSI is required to ensure the security and confidentiality of the information it processes on behalf of its clients and employees. This security policy complies with California Government Code Section 11549.3.

This policy may be updated at any time to ensure changes to the OTSI's organization structure and/or business practices are properly reflected in the policy.

To view all published Information Security policies, visit the Information Security Office Intranet Page and click on ISO Policies.

Scope and Applicability

The scope of this policy extends to all Information Assets owned or operated by OTSI, Information Assets managed by third parties on behalf of OTSI, and all Information

Assets that process or store OTSI information in support of the OTSI mission and business functions. This policy applies to all Personnel and governs all forms of access to OTSIInformation Assets.

Policy Directives

1. A User shall not disclose their password to anyone, at any time, for any reason.

2. If any person requests that a User disclose a password, the User shall refer them to this document or have them contact the Information Security Office (ISO). If a situation arises wherein a User requires temporary access to another User's computer, they shall contact the help desk for temporary access with their own login credentials.

3. When a device is left unattended, the User shall lock the screen in a manner requiring that the password be entered to unlock the device.

4. If a User is prompted by an application or website with the option to "Remember Password", the User shall not use this feature.

5. Passwords shall only be distributed to Personnel verbally or through e-mail. If a password is sent using e-mail to a non-OTSI User, encryption shall be used. Other methods of distributing a password shall be approved by the ISO.

6. The same password shall not be used in more than one account or system.

7. Desktop administrators shall immediately disable the account of any staff that leaves the OTSI.

8. When a User changes a password, the User shall not use a predictable pattern, such as incrementing a number or using the current month.

9. All Personnel shall comply with the OTSI Password Standard.

Roles and Responsibilities

OTSI Director or Information Security Office

The OTSI Director is ultimately responsible for this policy and delegates responsibility forthe OTSI policy program to the ISO.

The OTSI ISO shall:

Ensure that all OTSI Personnel are aware of this policy and acknowledge theirindividual responsibilities.

1. Review this policy annually and update it accordingly.
2. Ensure that password standards are reviewed annually and updated accordingly.
3. Periodically audit and assess compliance with this policy.

OTSI Users

1. All Personnel are required to follow the directives in this policy.
2. All Personnel are required to report any incidents of possible misuse or violation of this policy to the OTSI ISO.
3. All Personnel are required to read and acknowledge they have read and understand this policy.

Violations/Enforcement

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries, contract termination for contractors, and dismissal of interns and volunteers. Personnel are also subject to loss of OTSI information resources access privileges. Additionally, Personnel may be subject to civil penalties and/or criminal prosecution.
2. The OTSI ISO is responsible for the periodic auditing and reporting of compliance withthis policy. The OTSI ISO is responsible for defining the format and frequency of the reporting requirements and communicating those requirements, in writing, to OTSI management.

Auditing

OTSI has the right to audit any activities related to the use of state Information Assets.

Reporting

Any violations of security policies must be immediately reported to the OTSI ISO.

Exception Request Process

If compliance is not feasible or is technically impossible, if existing policy currently in place already meets these requirements, or if deviation from this policy is necessary to support a business function, the respective manager must formally request a policy exception as defined below.

1. Any request for security exceptions shall be requested through Service Now.
2. Exceptions to this policy must be approved by the requestor's manager, ISO and the Chief Technology Officer.
3. The term of an approved security exception may not exceed twelve (12) months.

Approval

DocuSigned by:
7E78A029D2DF44D...

10/12/2021

Approved by the Office of the Directorate by the Chief Information Officer **Date**

NIST 800-53 References

Family	Control
Identification and Authentication (IA)	IA-1 Authenticator Policies and Procedures IA-5 Authenticator Management

Related Policies, Procedures and Standards

To view all published Information Security policies and standards, visit the Information Security Office Intranet Page and click on ISO Policies. See below for related state policies, procedures, and standards.

Reference #	Article
SAM 5360	Identity and Access Management
SIMM 5305-A	Information Security Management Program Standard
ISO Standards	OTSI Password Standard

Revision History

Date	Description of Change	By
10/12/2021	Revised policy to align with CDT standards and move the specific password control settings into a separate Password Standards document.	ISO
01/10/2023	Update Government Code to include 7929.210 Pursuant to California Government Code Section 7929.210 and 11549.3	ISO
09/27/2023	Review and updated items related to the OTSI name change including logo and headings.	ISO

Definitions of Key Terms

The OTSI uses the information security and privacy definitions issued by the California Department of Technology Office of Information Security in implementing information security and privacy policy. Terms and definitions are defined here and also, on the California Department of Technology website at https://cdt.ca.gov/security/technical-definitions/.

Information Assets	Information Assets include (a) all categories of paper and automated information, including (but not limited to) records, files, and databases; and (b) information technology facilities and equipment (including telecommunications networks, personal computer systems, laptops, tablets, and mobile devices), and software owned or leased by state entities.
NIST	National Institute of Standards and Technology https://www.nist.gov/
Personnel	OTSI employees, retired annuitants, student/graduate assistants,volunteers, contractors, sub-contractors, and interns.
User	A person who is specifically authorized to access and use information or another information asset, such operating a computer.

Office of Systems Integration "SERVING CALIFORNIA"	**OSI Password Standard** **Effective Date: December 8, 2021**

Purpose

The purpose of this standard is to establish password requirements for Office of Systems Integration (OSI) Personnel, and to comply with California State Administrative Manual (SAM) Section 5360.

Standard Requirements

Password Attributes used at OSI must exhibit “strong” password characteristics. A strong password is of sufficient length and complexity that it is producible only by the user who chose it, such that any attempt at successfully guessing it would necessarily require more time than a password cracker would be reasonably willing to invest in guessing it.

To satisfy this requirement, passwords shall adhere to the following general requirements:

1. Passwords must be at least 15 (fifteen) characters long.
2. Passwords must not contain the username or any part of the user’s full name.
3. User default passwords must require a change upon first login.
4. Default device and software passwords must be changed before placed on the network or upon first login.
5. Passwords must be changed immediately if compromised.
6. Passwords must not be a dictionary word in any language, slang, dialect, jargon, etc., unless the words are combined as a passphrase. Choose a password that is easy for you to remember but would be hard for another to guess. One useful approach is to use a sentence or saying to create a “passphrase” by using the first letters, capitalization, and special characters as substitutes.

7. Passwords must not be based on a user's personal information, such as names of family members, pets, etc.
8. All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 6 months.
9. Passwords must contain characters from at least three of the following four classes:

Description	Example
Upper Case Letters	A, B, C, … Z
Lower Case Letters	a, b, c, … z
Numerals	0, 1, 2, …
Non-alpha-numeric "special characters"	Punctuation marks and other symbols

The following password attributes are required at OSI, and apply to all user, system, and service accounts:

1. Password History: Six unique iterations are required prior to re-using a password.
2. Maximum Password Age: At a minimum, a user must be required to reset a password every 365 days.
3. Minimum Password Age: This value must be set to one day. If a user feels that the password has been compromised before the one day has passed, then the user should report the incident to the Information Security Office.
4. Lockout Count: Users will be temporarily locked out of their accounts after the 5th failed login attempt within a 15-minute time period. The temporary lockout duration will last for 30 minutes. If users need assistance with their passwords, they should contact the ITO Help Desk.

Exceptions

Exceptions to this standard will be considered on a case-by-case basis and only when requested using appropriate documentation.

Approval

DocuSigned by:
Daniel Pure
44D8E33F1F604DC...

12/8/2021

Signature of Information Security Officer **Date**

Related Policies, Procedures and Standards

Reference #	Article
OSI-2021-37	Password Policy

REVISION HISTORY			
Revision #	**Date of Release**	**Author**	**Summary of Changes**
Original	12/8/2021	ISO	Original document

Definitions of Key Terms

The OSI uses the information security and privacy definitions issued by the California Department of Technology Office of Information Security in implementing information security and privacy policy. Terms and definitions are defined here and also on the California Department of Technology website at https://cdt.ca.gov/security/technical-definitions/.

Personnel	OSI employees, retired annuitants, student assistants, volunteers, contractors, sub-contractors, and interns.
Password History	The number of preceding passwords that cannot be reused.
Maximum Password Age	The number of days before a user is allowed to change their password
Minimum Password Age	The number of days before a user is allowed to change his or her password.
Lockout Count	The number of unsuccessful login attempts before an account is locked out.
Reset Lockout	The length of time before the number of unsuccessful logon attempts is reset to zero.

Office of Technology & Solutions Integration CALIFORNIA HEALTH & HUMAN SERVICES AGENCY	**SECURITY POLICY** **CONTROL NUMBER: OSI-2022-15**
Peer-to-Peer Policy	**Effective Date: April 7th, 2023**

Purpose

Peer-to-Peer (P2P) file sharing involves using technology that allows internet users to share files that are housed on their individual computers. P2P applications, such as those used to share music files are some of the most common forms of file sharing technology. However, P2P applications introduce security risks that may put the Office of Technology & Solutions Integration's (OTSI) information or computers in jeopardy. The following risks may be realized if P2P is used on the OTSI's network:

- Installation of malicious code
- Exposure of sensitive or personal data
- Susceptibility of attack
- Denial of Service (DOS)
- Unwanted access to network services or devices
- Prosecution if copyrighted files or pirated software are illegally downloaded and used

Examples of P2P applications include, but are not limited to, BitTorrent, uTorrent, DC++:DC++, RetroShare, Shareaza, Soulseek, Vuze, Freecast, eMule, FrostWire, Limeware, and Grokster.

The objectives of this policy are to establish OTSI requirements for the systematic approach to the availability of technology infrastructure resources, and to ensure related services are identified, formally planned for, and maintained. The goal of this policy is to support the state and OTSI's business services and critical infrastructure by mitigating risks and maintaining the level of availability as determined by the organizations' senior management.

Authority

Pursuant to California Government Code Section 7929.210 and 11549.3, the OTSI is required to ensure the security and confidentiality of the information it processes on behalf of its clients and employees. This security policy complies with California Government Code Section 11549.3.

This policy may be updated at any time to ensure changes to the OTSI's organization structure and/or business practices are properly reflected in the policy.

To view all published Information Security policies, visit the Information Security Office Intranet Page and click on ISO Policies.

Scope and Applicability

The scope of this policy extends to all Information Assets owned or operated by the OTSI, Information Assets managed by third parties on behalf of the OTSI, and all Information Assets that process or store OTSI information in support of the OTSI mission and business functions. This policy applies to all Personnel and governs all forms of access to OTSI Information Assets.

Policy Directives

The OTSI shall:

1. Prohibit the use of peer-to-peer technology for any non-business purpose. This includes, but is not limited to, transfer of music, movies, software, and other intellectual property.

2. Ensure business use of peer-to-peer technologies is approved by the OTSI Chief Information Officer (CIO) and Information Security Office (ISO).

3. Remove unauthorized P2P file sharing applications upon discovery on the OTSI network.

4. Ensure authorized peer-to-peer traffic is segregated and bandwidth is throttled by the network administrator at the direction of the CIO and ISO, based on utilization and effect on overall network traffic.

5. Ensure that if an artist, author, publisher, or law enforcement agency contacts the OTSI regarding intellectual property violations or related matters, OTSI Legal is notified.

6. Block all well-known P2P ports unless a business case can be made and approved by the OTSI ISO.

7. Ensure no files containing Personally Identifiable Information (PII) or other sensitive, proprietary, or protected information are shared using P2P applications.

8. Not permit Personnel to engage in P2P activities while using OTSI Virtual Private Network (VPN) services unless a business case can be made and is approved by the ISO.

9. Use technology-based deterrents to combat the unauthorized distribution, downloading, uploading, streaming, scanning, storage or sharing of material not related to business purposes on the OTSI's network. These deterrents may include traffic monitoring, bandwidth shaping, and next-generation firewalls.

Roles and Responsibilities

OTSI Director or Information Security Office

The OTSI Director is ultimately responsible for this policy and delegates responsibility for the OTSI policy program to the ISO.

The OTSI ISO shall:

1. Ensure that all Personnel are aware of this policy and acknowledge their individual responsibilities.

2. Review this policy annually and update it accordingly.

3. Periodically audit and assess compliance with this policy.

4. Investigate, with OTSI Legal, all reported copyright law violations.

5. Maintain oversight of OTSI security policies and procedures.

6. Ensure all P2P applications and software that are active on the OTSI network have a valid business reason and have been approved by the direct manager, the ISO, and the CIO.

7. Assist Information Asset Owners and Information Asset Custodians in the identification of P2P controls and processes.

8. Ensure that data security controls, methods and processes meet OTSI and applicable regulatory requirements for security and privacy.

OTSI Information Asset Owners and/or Program Management

Information Asset Owners shall:

1. Support the delivery of OTSI mission, state essential functions, or critical infrastructure.

2. Ensure that a business case for P2P applications is valid.

3. Work with the ISO to ensure all safeguards and network controls are in place to prevent unauthorized access to OTSI Information Assets.

OTSI Information Asset Custodians

Information Asset Custodians shall:

1. Implement access technology and process controls as approved by Information Asset Owners.

2. Implement user access and associated rights and privileges as requested and approved by Information Asset Owners.

3. Revoke or modify individual user access rights and privileges upon notification from Information Asset Owners.

4. Maintain access records as defined by Information Asset Owners.

5. Notify the OTSI ISO and Information Asset Owner should a security incident occur.

OTSI Users

1. All Personnel are required to follow the directives in this policy.

2. All Personnel are required to report any incidents of possible misuse or violation of this policy to the OTSI ISO.

3. All Personnel are required to read and acknowledge they have read and understand this policy and applicable OTSI information security and privacy policies.

Violations/Enforcement

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries, contract termination for contractors, and dismissal of interns and volunteers. Personnel are also subject to loss of OTSI information resources access privileges. Additionally, Personnel may be subject to civil penalties and/or criminal prosecution.

2. The OTSI ISO is responsible for the periodic auditing and reporting of compliance with this policy. The OTSI ISO is responsible for defining the format and frequency of the reporting requirements and communicating those requirements, in writing, to OTSI management.

Auditing

The OTSI has the right to audit any activities related to the use of state Information Assets.

Reporting

Any violations of security policies must be immediately reported to the OTSI ISO.

Exception Request Process

If compliance is not feasible or is technically impossible, if existing policy currently in place already meets these requirements, or if deviation from this policy is necessary to support a business function, the respective manager must formally request a policy exception as defined below.

1. Any request for security exceptions shall be requested through Service Now.
2. Exceptions to this policy must be approved by the requestor’s manager, ISO, and the Chief Technology Officer.
3. The term of an approved security exception may not exceed twelve (12) months.

Approval

DocuSigned by:
James Duckens
4837DA2CCB3C46F...

4/7/2023

Approved by the Office of the Directorate by the Chief Information Officer **Date**

NIST 800-53 References

Family	Control
Configuration Management	CM-1, CM-2, CM-3, CM-4, CM-6, CM-7, CM-10, CM-11
Systems and Communication Protection	SC-1, SC-5, SC-6, SC-7

Related Policies, Procedures and Standards

To view all published Information Security policies, visit the Information Security Office Intranet Page and click on ISO Policies. See below for related state policies, procedures, and standards.

Reference #	Article
SAM 5315.6	Activate Only Essential Functionality
SAM 5315.7	Software Usage Restrictions
SAM 5345	Vulnerability and Threat Management
SAM 5350	Operational Security
SIMM 5305-A	Information Security Management Program Standard

Revision History

Date	Description of Change	By
2022	Revised policy to align with State of California and Federal NIST 800-53 v5 control standards; Assigned new control number (previously OTSI-IT-08-16)	ISO
01/09/2023	Update Government Code to include 7929.210 Pursuant to California Government Code Section 7929.210 and 11549.3	ISO
04/07/2023	New	ISO
09/29/2023	Review and updated items related to the OTSI name change including logo and headings.	ISO

Definitions of Key Terms

The OTSI uses the information security and privacy definitions issued by the California Department of Technology Office of Information Security in implementing information security and privacy policy. Terms and definitions are defined here and on the California Department of Technology website at https://cdt.ca.gov/security/technical-definitions/.

Information Assets	Information Assets include (a) all categories of paper and automated information, including (but not limited to) records, files, and databases; and (b) information technology facilities and equipment (including telecommunications networks, personal computer systems, laptops, tablets, and mobile devices), and software owned or leased by state entities.
Information Asset Custodians or Custodians	Personnel responsible as caretaker for the proper use and protection of Information Assets on behalf of the Information Asset Owner.
Information Asset Owners or Owners	The person(s) having responsibility for making classification, categorization, and control decisions regarding Information Assets. Owners are often management affiliated with a particular project or division.
NIST	National Institute of Standards and Technology https://www.nist.gov/

Personnel	OTSI employees, retired annuitants, student/graduate assistants, volunteers, contractors, sub-contractors, and interns.

Office of Systems Integration "SERVING CALIFORNIA"	**ADMINISTRATIVE POLICY** **Control Number: OSI-AP-08-10**
Reasonable Accommodation Policy and Request Process	**Effective Date: September 1, 2008**

Purpose

The Reasonable Accommodation Policy and Request Process communicates the Office of Systems Integration's (OSI) commitment to, providing equal opportunity in the job application process; enabling individuals with disabilities to perform the essential functions of his/her job; ensuring equal enjoyment of the terms, conditions, and privileges of employment to persons with disabilities; and complying with federal and state reasonable accommodation federal requirements.

Authority

Rehabilitation Act of 1973: Federal Act prohibits discrimination on the basis of a disability and promotes the rehabilitation and employment of individuals with disabilities.

Americans with Disabilities Act of 1990: Federal Act prohibits state employment agencies from discriminating against qualified individuals with disabilities in job application procedures, hiring, firing, advancement, compensation, job training, and other terms, conditions, and privileges of employment.

Pregnancy Discrimination Act of 1978: Discrimination on the basis of pregnancy, childbirth, or related medical conditions is unlawful.

California Fair Employment and Housing Act (Government Code 12926): State Act provides protection to employees and applicants with disabilities from employment discrimination and offers greater protection than the Americans with Disabilities Act.

Government Code Section 19230/California Code of Regulations (Section 7293.5): Requires employers to make reasonable accommodation to the physical or mental limitations of an otherwise qualified applicant or employee who is an individual with a disability, unless the accommodation would impose an undue hardship on the employer.

Executive Order D-48-85: Requires employers to make every effort, including provision of reasonable accommodation, to enable employees with disabilities to return to work.

Policy

OSI will engage in a timely, good faith, interactive process with its employee or applicant to determine reasonable accommodation and will make reasonable accommodation for the known physical or mental disability, or medical condition of a qualified employee or applicant, unless to do so would cause an undue hardship. In addition, OSI will ensure that its employees and applicants are protected from discrimation, harassment, or retaliation on the basis of an actual or perceived disability, and/or for exercising their right to request reasonable accommodation on account of a physical or mental disability, or medical condition.

Definition

Disability: A physical or mental condition that limits major life activity.

Essential Functions: The fundamental job duties of the employment position. A function may be essential if (1) the position exists to perform the function; (2) there are a limited number of employees available to perform the function; or (3) the function is highly specialized and the person was hired for his/her expertise.

Individual with a Disability: An individual with a disability is one who (1) has a physical or mental impairment or medical condition that limits one or more major life activities; (2) has a record or history of such an impairment or condition; or (3) is regarded as having such a impairment or condition.

Interactive Process: Whereby both the employee and his/her manager/supervisor make a good-faith effort to explore alternatives that will enable an employee to perform the essential functions of the job. Process requires an ongoing dialogue to keep employee informed about the request.

Major Life Activity: Includes functions such as caring for one's self, performing manual task, walking, seeing, hearing, speaking, breathing, learning, and working.

Medical Condition: Any health impairment related to or associated with a diagnosis of cancer or a record or history of cancer, or genetic characteristics.

Physical or Mental Disability: Any physiological disease, disorder, condition, cosmetic disfigurement, or anatomical loss that affects one or more of the following body systems: neurological, immunological, musculoskeletal, special sense organs, respiratory, including speech organs, cardiovascular, reproductive, digestive, genitourinary, hemic and lymphatic, skin and endocrine; or any mental or psychological disorder or condition, such as mental retardation, organic brain syndrome, emotional or mental illness, or specific learning disabilities.

Definition (continued)

Reasonable Accommodation: A modification or adjustment to the application process, work environment, or the circumstances under which the job is customarily performed which enables qualified individuals with disabilities to enjoy benefits and privileges of employment.

Qualified Individual with a Disability: An individual with a physical or mental disability or medical condition who (1) possesses the requisite job qualifications; and (2) can perform the essential functions of the job with or without reasonable accommodation.

Undue Hardship: An action requiring significant difficulty or expense when considered in light of factors such as an employer's size, financial resources, and the nature and structure of its operation.

Reasonable Accommodation

A request for reasonable accommodation is a statement that a qualified individual needs an adjustment or change, at work; in the application process; or in a benefit or privilege of employment for a reason related to a disability or medical condition. All qualified employees with a disability or medical condition are eligible for a reasonable accommodation.

An employee may request a reasonable accommodation verbally or in writing to his/her supervisor/manager or the Reasonable Accommodation Coordinator. Once a request for an accommodation is made, the reasonable accommodation process begins. An important step in this process is the *"interactive process."* The interactive process represents a good-faith effort to explore alternatives that will enable an employee to perform the essential functions of the job. The employee requesting the accommodation, his/her manager/supervisor, and the Reasonable Accommodation Coordinator must engage in discussions with each other regarding the request, the process for determining whether an accommodation will be provided, and potential accommodations. Communication is a key component throughout the entire process.

Examples of Reasonable Accommodation

Any form of accommodation is reasonable if it enables an employee or applicant with a disability or medical condition to perform the essential functions of his/her job and ensures equal employment opportunities. Examples of potential reasonable accommodations include, but are not limited to:

- Making existing facilities used by employees readily accessible to and usable by individuals with disabilities
- Job restructuring
- Reassignment to a vacant position
- Part-time or modified work schedules

Examples of Reasonable Accommodation (continued)

- Acquisition of tools, equipment, devices, furnishings, etc.
- Modification of tools, equipment, devices, furnishings, etc.
- Adjustment or modification of examinations
- Adjustment or modification of training materials
- Adjustment or modification of workplace policies
- Provision of a qualified reader
- Provision of a qualified interpreter

The number of potential reasonable accommodation(s) is infinite because the appropriate accommodation is based upon the needs of both the employee or applicant and OSI.

An employer is not required to lower quality or production standards to make an accommodation; nor is an employer obligated to provide personal use items such as glasses or hearing aids.

The law provides that, under certain circumstances, an employer is not required to provide an accommodation.

Those circumstances are:

- Even with the accommodation, the employee or applicant cannot perform the essential functions of the job because of his/her disability or medical condition.
- Even with the accommodation, the employee or applicant cannot perform the essential functions of the job in a manner which would not endanger his/her health or safety because the job imposes an imminent and substantial degree of risk to the employee or applicant.
- Even with the accommodation, the employee or applicant cannot perform the essential functions of the job in a manner which would not endanger the health or safety of others to a greater extent than if an individual without a disability performed the job.
- Granting the accommodation would impose an undue hardship upon the employer.

Criteria for Evaluating Undue Hardship

Providing a reasonable accommodation may impose an undue hardship upon an employer if it requires significant difficulty or expense. There are a number of factors considered when evaluating whether granting an accommodation would result in an undue hardship, including, but not limited to:

- The nature and cost of the accommodation needed.
- The overall financial resources of the office involved in providing the accommodation, the number of persons employed at the office, and the effect on expenses and resources or impact of the accommodation upon the operation of the office.

Criteria for Evaluating Undue Hardship (continued)

- The type of operations, including the composition, structure, and functions of the employer's workforce.

Responsibility

Reasonable Accommodation Coordinator

- Ensure that all employees are informed of the Reasonable Accommodation Policy and Request Process.
- Ensure OSI managers and supervisors receive a copy of this policy, sign the Manager/Supervisor Acknowledgement of Receipt of Reasonable Accommodation Policy and Request Process form and forward a copy to the Equal Employment Opportunity Office.
- Coordinate and oversee the interactive process with the employee and the manager/supervisor.
- Consult with the manager/supervisor and/or employee regarding what accommodations would best allow the employee to perform the essential functions of the position.
- Provide a response within twenty (20) working days from the date of the employee's request for reasonable accommodation.
- Evaluate if a request for accommodation will cause an undue hardship, or violates other laws or employment practices.
- Provide training to managers/supervisors on the reasonable accommodation program and processes.

Managers and Supervisors

- Review the Reasonable Accommodation Policy and Request Process and sign the Manager/Supervisor Acknowledgement of Receipt of Reasonable Accommodation Policy and Request Process form and forward a copy to the Equal Employment Opportunity Office.
- Inform employees or applicants of the Reasonable Accommodation Policy and Request Process.
- Identify situations that may require reasonable accommodation and discuss them with the employee or applicant even if the employee or applicant has not yet identified the need for an accommodation.

Responsibility (continued)

- Provide a current Essential Functions Duty Statement to employees in positions under his/her supervision.

- Advise and coordinate requests for reasonable accommodation with the Reasonable Accommodation Coordinator.

- Participate in the “interactive process.”

Employee

- Identify the need for requesting reasonable accommodation and notify his/her manager/supervisor.

- Review the Reasonable Accommodation Policy and Request Process and complete the Request for Reasonable Accommodation form.

- Provide the department with all relevant medical information.

- Participate in the “interactive process.”

- Cooperate with department staff in determining the most appropriate accommodation.

Confidentiality Regarding Medical Information

Medical information obtained in connection with the reasonable accommodation process must be kept confidential. All medical information, including information about functional limitations and reasonable accommodation needs, that OSI obtains in connection with a request for reasonable accommodation must be kept in files separate from the individual’s official personnel file. Any OSI employee who obtains or receives such information is strictly bound by these confidentiality requirements to the extent possible.

The Reasonable Accommodation Coordinator will maintain custody of all records obtained or created during the processing of a request for reasonable accommodation, including medical records, and will respond to all requests for disclosure of the records. Whenever medical information is disclosed, the individual disclosing the information must inform the recipients of the information about the confidentiality requirements.

Process for Requesting Reasonable Accommodation

Applicants for Examination or Employment: Applicants who are in need of special arrangements for either a written or an oral test, or hiring interview, must indicate so on their State of California Examination and/or Employment Application (STD. 678). Request for reasonable accommodation involving delegated or decentralized examinations or

Process for Requesting Reasonable Accommodation (continued)

hiring interviews should be submitted to OSI's Human Resources Section. Requests concerning centralized examinations administered by the State Personnel Board (SPB) should be submitted directly to the SPB. The examination announcement or job bulletin will identify the responsible state department. Mark the appropriate box in Part 2 of the state application. The completed application should be submitted to the appropriate state department by the final filing date indicated on the examination announcement or job bulletin. You will be contacted to make specific arrangements. State departments are required to respond to the request within ten (10) working days after the application has been approved for admittance to the examination. If you have not been contacted by the time you receive a notice to appear at a test or hiring interview, call the appropriate testing office or Human Resources Office as noted on the examination announcement or job bulletin.

Job Accommodation: Current OSI employees or applicants offered employment with OSI may request reasonable accommodation as follows:

1. An OSI employee with a disability or medical condition who needs a reasonable accommodation to perform the essential functions of his/her position should make OSI aware of his/her need for accommodation by (1) notifying their immediate manager/supervisor; or (2) contacting the Reasonable Accommodation Coordinator.

2. The Reasonable Accommodation Coordinator will provide the employee with a copy of OSI's Reasonable Accommodation Request Packet containing:

    - Reasonable Accommodation Policy and Request Process
    - Request for Reasonable Accommodation form
    - A copy of the employee's essential functions duty statement

3. The employee must complete and sign Section I of the Request for Reasonable Accommodation form, and have his/her physician/health care provider complete and sign Section III. The completed Request for Reasonable Accommodation form must be returned to the Reasonable Accommodation Coordinator, who will confirm with the employee that the completed form and medical information has been received.

4. The Reasonable Accommodation Coordinator will review the request to ensure Sections I and III are complete. If additional information is needed from the employee's physician/health care provider in order to determine whether or not a reasonable accommodation can be provided (per Section II), the Reasonable Accommodation Coordinator will send a letter to the physician/health care provider requesting the additional information. The employee will receive a copy of the letter.

Process for Requesting Reasonable Accommodation (continued)

5. Within five (5) working days of receiving the completed Request for Reasonable Accommodation form, the Reasonable Accommodation Coordinator will forward the form to the employee's supervisor to provide input in Section IV. The supervisor shall complete Section IV within five (5) working days of receiving the form and return it to the Reasonable Accommodation Coordinator.

   Note: The employee's supervisor shall receive only the Request for Reasonable Accommodation form. The supervisor shall not have access to or review any supporting medical verification provided by the employee's physician/health care provider.

6. After the Reasonable Accommodation Coordinator receives all necessary information, the employee, manager/supervisor, and the Reasonable Accommodation Coordinator will use the interactive process to explore available options for a reasonable accommodation.

7. The Reasonable Accommodation Coordinator will respond in writing to the employee's request within twenty (20) working days of receiving the documents discussed above. If the employee does not receive a response within twenty (20) working days, he/she should contact the Reasonable Accommodation Coordinator to inquire about the status of his/her pending request.

   The notification provided to the employee will state that:

   - The requested accommodation or an alternate reasonable accommodation has been granted; or
   - The requested accommodation has been denied; or
   - Additional information is needed from the employee and/or his/her physician health care/provider and a decision will be forthcoming after the necessary information has been provided.

   The employee's supervisor will also receive a copy of the notification.

Appeal Process

If the employee is not satisfied with the department's response for Reasonable Accommodation, the employee may file a formal appeal with the State Personnel Board's Appeals Division, within thirty (30) calendar days after receiving the response.

Appeal Process (continued)

The employee may also concurrently appeal the denial of reasonable accommodation on the basis of discrimination due to a disability/medical condition with the following:

Department of Fair Employment and Housing (DFEH)
Sacramento District Office
2000 0 Street, Suite 120
Sacramento, CA 95814
Telephone: (916) 445-5523; Toll-free: (800) 884-1684
FAX: (916) 323-6092; TTY: (800) 700-2320
Timeframe: Within 365 calendar days of the incident

United States Equal Employment Opportunity Commission (EEOC)
350 The Embarcadero, Suite 500
San Francisco, CA 94105-1260
(415) 625-5600
Timeframe: Within 180 calendar days from the date of the incident

Questions or Assistance

The Reasonable Accommodation Coordinator is responsible for overseeing the coordination and implementation of an accommodation. The employee should contact the Reasonable Accommodation Coordinator any time he/she has questions or concerns about the status of a pending accommodation.

Approval

Original signed by Paul Benedetto on September 18, 2008

PAUL BENEDETTO **DATE**
Acting Director, Office of Systems Integration

Office of Systems Integration "SERVING CALIFORNIA"	**ADMINISTRATIVE GUIDELINES** **CONTROL NUMBER: OSI 2019-10**
Security Badge and Access Card	**Revised Date: August 15, 2019**

Purpose
Define and set guidelines for the use of security badges (photograph identification) and access cards for Office of Systems Integration (OSI) employees in designated work areas.

Definitions
Security badges include the OSI logo, employee's name, and photograph. Security badges provide identification and ensure employees' rights to occupy the building and are also used as identification when visiting other state agencies.

Access cards are coded according to specific access needs of employees. Access cards allow OSI to protect employees and ensure the integrity of data files and equipment.

Visitor passes are to be visibly worn at all times by those who are not OSI employees or contractors. The visitor pass will have the OSI logo, "Visitor Pass", name of visitor, date, and suite number.

Business Services Office (BSO) provides guidance to OSI projects on the day to day business operations and non-IT purchasing. Business Services oversees business operations support such as: badge access, facility requests, space planning, moving services, records retention, surplus, and interagency mail.

Temporary badges ("Temp badges") are access cards available for short term use by either state staff that have misplaced their badge for any *one* business day and/or visitors that will be onsite for an extended amount of time.

Guidelines
All OSI employees and contractors are required to display their security badge or visitor pass within all OSI occupied office spaces and use the access cards to enter or leave their work areas. This guideline is intended to provide OSI employees, contractors, and visitors assurance that physical security is in effect and the integrity of data files and equipment are protected. Visitors must check in and out with the front desk staff or designated area for the suite. All visitors will be given a visitor pass that must be kept visible at all times.

Guidelines and Responsibilities

- Supervisors and managers or their designees are responsible for initiating requests for access cards and any additions/deletions to employee access. This can be done by completing an Onboarding/Offboarding or Badge Request through the ServiceNow Portal. BSO will receive the request and work the ticket directly through ServiceNow. Security badges and access cards may be picked up by contacting BSO via email at BusinessServices@osi.ca.gov or during BSO walk in hours. The BSO walk in hours are Monday, Wednesday, and Friday from 9:00 am to 11:00 am.

- Security badges and access cards must be in possession and visible at all times while in OSI office areas. OSI employees and contractors are required to sign out temporary access cards if they are not in possession of their own. Temporary access cards are obtained from the BSO and must be returned by close of business that same day. Staff are not authorized to grant access into OSI offices without a clearly displayed picture ID.

- If an OSI employee or contractor misplaces, loses, or has their security badge stolen, it must be reported to the BSO immediately by inputting a Badge Request on ServiceNow. The security badge will be deactivated and a new one will be issued.

- Visitors must be escorted to their destinations. All visitors are required to sign in at the reception area or designated suite access check in and receive their visitor pass. If no reception staff is available, visitors are to check in with the OSI employee or contractor they are meeting. The OSI employee or contractor will issue a visitor pass. At the conclusion of their business, visitors are escorted to the reception area and are required to sign out prior to departure and must return their temporary visitor pass to the receptionist.

- Temporary badges can be obtained through the designated BSO Liaison or via a ServiceNow Badge Request. When requesting a temporary badge, the requestor will be required to verify his or her identity through a form of official identification. Official identification can include, but is not limited to, state issued driver's license, state issued identification card, or passport. Temporary badges shall only be active for one business day, unless otherwise specified. The temporary badge shall be returned to the BSO Liaison by close of business (COB) that same day.

- Supervisors and managers are responsible for submitting Onboarding/Offboarding Requests through ServiceNow at least ten days in advance of new or transferring employee arrivals. Advanced notice enables staff adequate time to prepare for new (or transferring) employees, including activating access cards, security badges, telephones, and IT requirements.

- When submitting a ServiceNow Request, it will be disbursed to several units including BSO, whom issues security badges. New badge requests only apply to security badges that only need access during business hours. 24/7 Badge access

requires approval from the Project manager and typically takes longer to process as it involves property management to grant access to exterior doors and stairwells. For changes in security badge access, place a Badge Request through ServiceNow detailing the changes in access. The following is a timetable for access badge requests:

Type of Request	Timeline to Process
New badge request	1-2 Business days
Badge Deactivation	2-3 Business days
Badge access updates	2-3 Business days
24/7 Badge access	3 Business days
Replacement Badges	3 Business Days

Note: For requests related to personnel actions or emergency disablement of badge access, coordination and approval from Human Resources and/or Legal is required.

- Students and consultants are given access Monday through Friday from 7:00 a.m. to 6:00 p.m. to their assigned suites. Approval for access outside these guidelines must be submitted in writing to the BSO by supervisors and managers. Access to any suite other than the employee's home suite must be approved in writing by the manager of that suite and sent to the Business Services Office before access can be authorized.

- Employees are responsible for ascertaining the identity of anyone in the office areas that is unknown and does not have a visible security badge or visitor pass.

If there are any questions regarding this policy, please contact the BSO at 263-0746 or email at BusinessServices@osi.ca.gov.

8/13/19

Robert Huskison Date
DEPUTY DIRECTOR OF ADMINISTRATION

Office of Systems Integration "SERVING CALIFORNIA"	**Security Policy** **Control Number: OSP-AP-14-01**
Social Media Policy	**Effective Date: July 8, 2014**

Purpose

This policy documents the expectations and responsibilities when using state resources or conducting state business to exchange information with, and utilizing social media technologies. Many state entities, including the Governor's Office, use social media communication with great success, but as with most technologies, there is a measure of risk to address and mitigate.

Background

The Office of Systems Integration (OSI) Social Media Policy covers the use of social media for sharing or posting official agency information and the internal two-way flow of information. The use of social media subjects the OSI to possible exposure of confidential data and information and is both a cyber security and business communications issue.

Scope

This policy applies to all OSI full-time or part-time employees, contractors, consultants, other governmental entities and volunteers who are authorized to use state government-owned or leased equipment or facilities or access OSI information systems and assets.

Policy

The OSI Social Media Policy establishes the following:

1. Users shall not post or release information exempt from disclosure under the California Public Records Act (PRA) to social media websites and applications. This includes but is not limited to a public agency, if, on the facts of the particular case, disclosure of that record would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency. (Government Code 6254.19)
2. Users shall not post or release information exempt or prohibited from disclosure under any law or other OSI policy.

3. Users shall not, unless expressly authorized, express opinions on behalf of the OSI and shall clearly designate any such publicly posted opinions as personal and not expressive of the opinions or positions of the OSI.
4. Users' activities related to social media use must not interfere with any performance of a user's job.
5. Users should be aware that social media communications are considered public records and, consequently, may be kept for a certain period of time in compliance with the OSI Records Management Policy.
6. Users should engage in productive interactions that add organizational value. Social web participation should be aligned with OSI's social media vision and strategy.
7. The audience should be respected and users should avoid negative personal comments or inflammatory subjects.
8. Content that is deemed not suitable by the OSI, including comments containing any of the following content, shall not be allowed for posting:
    a. Profane language or content;
    b. Content that promotes, fosters or perpetuates discrimination on the basis of race, creed, color, age, religion, sex, gender, marital status, status with regard to public assistance, national origin, physical or mental disability or sexual orientation;
    c. Comments that support or oppose political campaigns or ballot measures;
    d. Sexual content, sexual harassment, or links to sexual content;
    e. Solicitations of commerce;
    f. Illegal conduct or encouragement of illegal activity;
    g. Information that may tend to compromise the safety or security of the public or public systems; or
    h. Content that violates a legal ownership interest of any other party.
9. OSI employees delegated as blog moderators shall only allow blog comments that are topically related to the particular blog subject being commented and thus within the purpose of the forum, with the exception of the prohibited content list in number 8.
10. Use sound judgment and think about the audience's reaction to a post before you engage. A blog post may live for many years in the web even after it has been deleted, so protect the OSI's privacy and reputation.
11. Present OSI in a positive light and avoid making derogatory comments about OSI and OSI's products, services, management, employees, or systems.
12. Know and follow all OSI policies, including the Acceptable Use Security Policy and the confidentiality and non-disclosure agreement policy.
13. If in doubt about whether a post or comment response is appropriate, the OSI employee shall seek advice from his or her manager or email osiinfosecurity@osi.ca.gov.

Chat and Email

Chat- History shall not be saved and usage includes non-essential business communications. Chats may include but are not limited to quick messages, social

planning communications, questions, and notifications. Examples of communication include: “Are you at your desk?”, “Do you have time to meet today?” and “Please call me when you are available.”

Email- History is backed up on the server for extended periods of time and usage includes essential business communications. Email may include but it is not limited to longer detailed questions and responses, communications about issues or decisions, questions/answers, sending files, external communications, personnel communications, legal communications, confidential communications, attorney-client privileged communications, and longer messages that cannot be communicated in limited text.

Recording

Recording Group Presentations- Meeting notifications indicating that a presentation is being recorded shall be posted in several areas of the presentation room.

Recorded Meetings- Prior to start of a meeting, the facilitator shall notify participants that the meeting is being recorded. The meeting facilitator shall ensure the notification of audio visual recording is included in the recorded meeting.

Definitions

Social Media- Also referred to as social networking and Web 2.0 technologies are those which allow users to collaborate, chat, video call, face time, record communications, post pictures, post videos, and share information over the Internet with a network of other social users, or the community as a whole (e.g., Facebook, YouTube, Twitter, Instagram, BlogSpot, LinkedIn, Digg, Flicker, etc.).

OSI Authorized Social Media User – A person delegated by the OSI Directorate, who communicates officially on behalf of the OSI.

OSI Blog Moderator– A person delegated by the OSI Directorate, who reviews, authorizes and allows content to be posted to the OSI blog site.

Roles and Responsibilities

1. The OSI Information Security Office (ISO) will establish a periodic reporting requirement to measure the compliance with and effectiveness of this policy.
2. The OSI ISO will establish formal standards and processes to support the intent of this policy and to address requirements imposed on the OSI as established by other governmental entities.
3. All employees shall adhere to the Social Media Standards SIMM 66B All OSI employees are required to protect confidential information. Information the OSI would not otherwise publicly disclose due to confidentiality laws, contractual duty

and other restrictions shall not be disclosed or discussed on the social media websites or applications.

4. All OSI employees are required to read, acknowledge and sign this policy. Any questions should be directed to the employee's manager or to the OSI ISO at osiinfosecurity@osi.ca.gov.
5. Only OSI Authorized Social Media Users may express opinions on, or post OSI related business information to, public social media on behalf of the OSI (Refer back to Policy Section - #3 for personal opinion postings).

Disclaimer

Access to Internet services is made available by the OSI to users as a privilege. The Internet has the ability to provide access to sites and information which is not under the control of the OSI. The OSI makes no representation concerning the content of these sites nor should the fact that the employer has provided access be construed or interpreted as an endorsement by the OSI.

Liability

Users of electronic mail and the Internet accept responsibility for any and all actions, and consequences of those actions, while using the electronic mail and the Internet.

Exceptions

Exceptions to this policy will be considered only when the requested exemption is documented with a business justification and presented to the OSI Information Technology Office and ISO.

The following are the links to the Exemption Procedure and Exemption Form:

Exemption Request Procedures
Exemption Request Form

Violations/Enforcement

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporary employees, termination of employment relations in the case of contractors or consultants, and dismissal for interns and volunteers. Additionally, individuals are subject to loss of the OSI information resources access privileges, civil, and criminal prosecution.
2. The OSI ISO is responsible for the periodic auditing and reporting of compliance with this policy. The OSI ISO will be responsible for defining the format and frequency of the reporting requirements and communicating those requirements, in writing, to OSI management.

The following are incorporated by reference:

Government Code Section 8314
OCIO Social Media ITPL 10-02
SAM 5310
OSI Acceptable Use Security Policy OSI-SP-08-08
OSI Information Security Incident Response Policy OSI-ITS-07-08
OSI Privacy and Security Awareness Training Policy OSI-SP-08-01
OSI Exemption Request
OSI Web Filtering Standards
Confidentiality and Non-Disclosure Agreement Policy
Records Management Policy
Social Media Standards (SIMM 66B)

Approval

APPROVED 7/21/2014

_____

John Boule Date
Director

SOCIAL MEDIA POLICY

SECURITY RESPONSIBILITIES AND ACKNOWLEDGEMENT

The Office of Systems Integration (OSI) makes its social media resources available to employees, authorized contractors, and volunteers as a necessary tool. The OSI Social Media Policy, also referred to as social networking and Web 2.0 technologies are those which allow users to collaborate, chat, video call, face time, record communications, post pictures, post videos, and share information over the Internet with a network of other social users, or the community as a whole (e.g., Facebook, YouTube, Twitter, Instagram, BlogSpot, LinkedIn, Digg, Flicker, etc.), are provided to employees, authorized contractors, and volunteers for the purpose of conducting OSI-approved activities. All users are responsible for using these resources in an effective, ethical, and lawful manner. As a condition of using social media every user is required to understand and comply with the Social Media Policy and all relevant laws, regulations, policies and practices governing the use of social media.

ACKNOWLEDGEMENT

I have read and understand the OSI Social Media Policy. I have read and understand the above policy statement. I understand that my failure to adhere to the OSI Social Media Policy could result in violation of this policy and may result in disciplinary action that may include termination for employees and temporary employees; termination of employment relations in the case of contractors or consultants; and dismissal for interns and volunteers. Additionally, individuals are subject to loss of the OSI information resources access privileges, and may be subject to civil and or criminal prosecution.

I understand this signed acknowledgment form shall be kept in my official personnel file.

Employee's Name (Printed)	Employee's Office
Employee's Work Telephone Number	Employee's Work Address

Employee's Signature	Date

Office of Systems Integration "SERVING CALIFORNIA"	**ADMINISTRATIVE POLICY** **CONTROL NUMBER: OSI-AP-17-02**
VENDOR REFERENCE POLICY	**Effective Date: 12/2/2017**

Purpose

The purpose of this policy is to provide guidelines for when an Office of Systems Integration (OSI) employee may provide vendor references.

Scope

This policy applies to all instances where an OSI employee or an OSI consultant, as specified in this policy, is asked to provide a reference for a vendor, regardless of whether the reference is oral or written, signed or unsigned. It applies to client or customer references, key staff references, and non-key staff references.

Definitions

Non-Evaluative Vendor Reference: This type of reference would only require the OSI employee to confirm otherwise public information regarding the work performed by the vendor, such as the type of work performed, length of performance, key personnel who performed the work, and other similar information. This type of reference does not in any way provide an evaluation of the vendor's performance.

Evaluative Vendor Reference: This type of reference would require the OSI employee to evaluate the vendor's performance. Such an evaluation would include rating the vendor's performance on a point or other scale (e.g., 1-5, average, above-average, poor, etc.).

OSI Solicitations: Any solicitation where the OSI will be a signatory to the resulting contract. This includes solicitations conducted within and outside of the OSI's delegated authority.

Non-OSI Solicitations: Any solicitation where the OSI will not be a signatory to the resulting contract.

Policy

General Standard:

All OSI employees providing vendor references should do so only if they are the employees most knowledgeable regarding the vendor's performance who are willing and able to provide references.

Non-Evaluative Vendor Reference:

An OSI employee with appropriate personal knowledge may provide a Non-Evaluative Vendor Reference.

Evaluative Vendor Reference:

1. *OSI Solicitations*

Executives at the highest level in the OSI possess the apparent weight and authority of the California Health and Human Services Agency (CHHSA) and, as such, must avoid the appearance that the CHHSA, and thus the state, is endorsing any particular vendor in a solicitation under the CHHSA's authority. The OSI Director, Chief Deputy Director, division Deputy Directors and the Agency Information Officer shall not provide Evaluative Vendor References for OSI Solicitations.

In addition, the following OSI employees shall not be permitted to provide an Evaluative Vendor Reference for an OSI Solicitation:

- An employee who had any substantive input into the procurement strategy or document formation, or who will be evaluating the bids received.
- An employee who has an actual or perceived personal interest, financial or otherwise, in the vendor. An actual or perceived personal interest may occur when an OSI employee has a financial interest in the vendor (e.g., stock ownership) or has some other personal relationship with the vendor that could reasonably give rise to the appearance of bias or impropriety if he or she served as a reference for that vendor (e.g., former employee of the vendor). Financial interests need not necessarily rise to the level of a disqualifying interest under the Political Reform Act of 1974. Questions about whether an employee has an actual or perceived personal interest should be directed to the OSI Legal Division.
- An employee who is otherwise prohibited by the language of the procurement documents from providing an Evaluative Vendor Reference.

The division Deputy Director may assign an OSI employee to provide an Evaluative Vendor Reference if that employee:

a. Is not prohibited by this policy from providing an Evaluative Vendor Reference;

b. Is not in direct control of the project (e.g. project manager, contract manager, or procurement manager); and
c. Has the appropriate personal knowledge to provide the reference.

2. *Non-OSI Solicitations*

For solicitations of other departments within the CHHSA, the OSI Director, Chief Deputy Director and the Agency Information Officer shall not provide an Evaluative Vendor Reference.

For solicitations of departments outside of the CHHSA, at the county level, in other states, or at the federal government, an OSI employee with appropriate personal knowledge may provide an Evaluative Vendor Reference. However, in situations where the OSI has collaborated with one of these entities on the solicitation or has had an oversight relationship that would bring the OSI into the procurement process, the employee shall contact the OSI Legal Division before providing an Evaluative Vendor Reference.

Endorsements:

No OSI employee shall grant any vendor permission to use the OSI logo in the vendor's promotional materials without reasonable compensation and the approval of the OSI Director, Chief Deputy, or his or her designee.

Consultants:

All full-time and part-time consultants to the OSI who are required to file Statements of Economic Interest at Disclosure Category 1 under the CHHSA Conflict of Interest Code are subject to the provisions of this policy.

Exceptions:

In instances where there are no parties willing and able to provide a vendor reference other than OSI employees who may be prohibited from providing references pursuant to this policy (e.g., a vendor that has performed work exclusively for the OSI), the project shall contact the OSI Legal Division, which will, in coordination with the OSI Acquisitions and Contracting Services Division, determine whether an exception to this policy may be warranted.

Authority

- Government Code sections 19990 and 87450 prohibit state officers and employees from engaging in any employment, activity, or enterprise which is clearly inconsistent, incompatible, in conflict with, or inimical to their duties as state officers or employees.

- The Political Reform Act of 1974 (Gov. Code, § 81000 et seq.) prevents public officials from making, participating in making, or influencing governmental decisions in which they have a financial interest.
- The Fair Political Practices Commission (FPPC) regulations (Cal. Code Regs., tit. 2, § 18110 et seq.) implement the Political Reform Act of 1974.

Office of Systems Integration "SERVING CALIFORNIA"	**SECURITY POLICY** **Control Number: OSI-SP-09-01**
WIRELESS SECURITY	**Effective Date: January 16, 2009**

Purpose

Computing devices equipped with wireless capability can provide users with improved communication and enhanced productivity. These improvements come at the cost of increased security risk. Such risks include possible unauthorized access, and the introduction of malicious code.

Scope

This policy applies to all devices with wireless capability including, but not limited to; laptops, handheld computing devices, smartphones, and personal digital assistants (PDAs).

This policy must be adhered to by State of California employees, volunteers, contractors, vendors or researchers who access the network through wireless devices.

Policy

Standard Requirements

1. Protect all wireless devices by enabling the password protection feature. Passwords should adhere to the OSI Password Standard to the extent the device is technologically capable.

2. Guard against loss, theft, or unauthorized use by physically securing the wireless device when not in use. Report any loss or theft immediately to the OSI Information Security Office.

3. Protect the data stored on the wireless device by enabling the encryption feature. Store only necessary information on the wireless device to reduce the risk of confidential, sensitive, or personal information being compromised.

4. Defend against unauthorized connection to the wireless device by disabling wireless interfaces when not in use, not connecting to anything identified as an "unsecured wireless network," enabling firewall software when connecting to the Internet, and disabling file sharing when not in use.

5. Ensure secure communications through a Virtual Private Network (VPN).

6. Avoid introducing malware by disabling wireless functionality before connecting through a docking station and by keeping anti-virus software and definition files as well as system software and security patches current.

7. State-issued laptops must connect periodically to the Local Area Network (LAN) or VPN for maintenance and updates. Alternatively, quarterly maintenance may be scheduled with the local Helpdesk. Standard laptop images will include endpoint security.

Wireless LANS (WLAN)

Wireless technology is rapidly becoming a significant participant in network deployment strategies. Along with its obvious advantages in speed and ease of use, there are serious security concerns:

1. WLAN security must include Wi-Fi Protected Access (WPA2) with Advanced Encryption Standard (AES) 256-bit.

2. Two-factor authentication mechanism (SecurID, TACACS+, RADIUS) must be used.

3. Service Set Identifier (SSID) must not be broadcasted.

4. MAC Address filtering must be used.

5. The wireless signal must not exceed the boundaries of the intended usage perimeter.

6. A centralized architecture must be used. Access points must be "thin" with no state or other information stored on the device.

7. Intrusion detection/prevention systems (IDS/IPS) must be deployed to detect and respond to potential suspicious, unauthorized, or malicious activities.

Hotspots

Hotspots are venues allowing wireless communication devices to connect to a wireless network using Wi-Fi, Bluetooth and related standards. Most hotspots are unsecured.

User data is shared as clear text as all users access the internet via the hotspot. This is very dangerous as users may thus “sniff the network” easily and retrieve potentially sensitive information. Abuse can be avoided by the use of VPN.

All wireless devices connected to a hotspot must connect back to OSI via a VPN connection before use.

Wireless Modems

Wireless modems connect to a wireless network instead of a telephone system from PCMCIA, ExpressCard or Compact Flash hardware. Wireless modems are sometimes called aircards or data cards. When you connect with a wireless modem you are attached directly to your wireless Internet Service Provider (ISP) and you can then access the Internet:

1. Only state-issued wireless modems are allowed.

2. Wireless modems may only be attached to state-issued equipment.

3. Wireless communication must be performed at a minimum128-bit encryption.

Smartphones

Smartphones are high-end phones providing voice, messaging, and multimedia communication with additional capabilities found in PDAs. A smartphone can be defined as either a phone that runs complete operating system software providing a standardized interface and platform for application developers, or simply a phone with advanced features like email and Internet capabilities, and/or a full keyboard. Some popular operating systems found on smart phones include iPhone OS, RIM BlackBerry, Windows Mobile/CE. The following applies to all smartphones:

1. State-issued BlackBerry smartphones with tethered modem capabilities can be used as an external modem to connect a computer to the Internet. State-issued BlackBerry smartphones may only be tethered to state-issued equipment.

2. State-issued BlackBerry smartphones shall enable content protection. Although BlackBerries transmit data securely, it does not store data securely unless enabled. This prevents someone with physical access to your handheld from connecting it to a personal computer (PC) and extracting sensitive data.

3. State-issued BlackBerry smartphones shall enable Wireless Transport Layer Security (WTLS) encryption to encrypt data that the device sends or receives over the Internet through the BlackBerry Enterprise Server (BES) and Wireless Application Protocol (WAP) gateway.

4. State-issued BlackBerry smartphones reported lost or stolen will be immediately wiped remotely from the BES.

Bluetooth

Bluetooth is a wireless protocol utilizing short-range communications technology facilitating data transmissions over short distances from fixed and/or mobile devices, creating wireless personal area networks (PANs). The design principle was to create a protocol that would allow a number of devices to be connected together seamlessly without an overly complex configuration procedure. The following applies to all Bluetooth devices:

1. Disable Bluetooth if Bluetooth technology is not used.

2. Bluetooth devices must be turned off when not in use.

3. Only Bluetooth v1.2 or later is allowed.

4. Only Bluetooth Class 2 or Class 3 radios are allowed. Class 1 radios provide an approximate range of 100 meters and are prohibited.

5. Bluetooth devices are to be paired to the BlackBerry device in a secure area (i.e., office or in the home) and not in public. Pairing establishes a wireless communication method between the BlackBerry device and the Bluetooth device.

6. When technology supports it, Bluetooth pairing passkeys should be at least eight decimal digits in length and generated randomly for each pairing.

7. By default the discoverable option on the BlackBerry device is to be disabled other than for the initial pairing process. This will ensure that the mobile device cannot be detected by another Bluetooth enabled device. The Bluetooth discovery option is enabled / disabled on the BlackBerry device under the Bluetooth options.

8. By default the address book transfer option on the BlackBerry device is to be disabled. This will prevent the possibility that the address book can be copied to another device via Bluetooth.

9. Transmissions (including messages, files, and images) from unknown or suspicious devices shall never be accepted.

References

OSI Password Standard OSI-AP-07-03
OSI Encryption on Portable Computing Devices Policy OSI-AP-06-09
OSI Information Security Incident Response Policy OSI-ITS-07-01

Guidelines on Cell Phone and PDA Security NIST SP 800-124
OSI Bluetooth Security Whitepaper
Guide to Bluetooth Security NIST SP 800-121
Establishing Wireless Robust Security Networks NIST SP 800-97

Exceptions

Exceptions to this policy will be considered only when the requested exception is documented and presented to the OSI Information Security Office.

Approval

ORIGINAL SIGNED BY PAUL BENEDETTO

PAUL BENEDETTO Date
ACTIING CHIEF DIRECTOR
Office of Systems Integration

Office of Systems Integration "SERVING CALIFORNIA"	**ADMINISTRATIVE POLICY** **CONTROL NUMBER: OSI-2021-01**
WORKPLACE VIOLENCE and BULLYING PREVENTION PROGRAM	**Effective Date: April 01, 2006** **Revision Date: July 01, 2010** **Revision Date: May 01, 2019**

Purpose

The Office of Systems Integration (OSI) Workplace Violence and Bullying Prevention Program (WVBPP) is to ensure the OSI provides a workplace free from recognized hazards and/or behaviors that are likely to cause serious physical harm or death to employees, vendors, contractors, customers, or members of the public. It also ensures the OSI provides employees with a place to conduct its business free from threats, intimidation, harassment, abusive conduct, and acts of violence in a safe, healthy, and productive work environment. Intimidation, threats, assaults, and acts of violence in the workplace or affecting the work situation are unacceptable and shall not be tolerated. Prompt, effective action shall be taken when such incidents occur. Disciplinary actions include, but may not be limited to, informal or formal measures, corrective action memorandums, letters of reprimand, suspension, reduction in salary, demotion, or dismissal from State service.

Compliance

The OSI is committed to ensuring all health and safety policies and procedures involving workplace violence and bullying prevention are clearly communicated and understood by all employees. Employees are responsible for using safe work practices by following all policies and procedures and shall comply with work practices that are designed to make the workplace a secure, safe, and healthy work environment. Employees shall not engage in threats or physical actions which create a security hazard for others in the workplace. Employees who fail to comply with the WVBPP policy and procedures will be disciplined appropriately.

All employees shall receive training on general and job-specific workplace security practices. Workplace violence prevention training and instruction are provided no less than once every other year; additional training may be provided when warranted. All employees must complete and sign the Workplace Violence Prevention

Acknowledgement Form which will be placed in the employee's Official Personnel File (OPF).

The OSI adheres to California Penal Code section 171 which states that any person who brings or possesses a firearm (or other weapon as specified) within a State or local building or any meeting required to be open to the public is guilty of an offense punishable by imprisonment. A State workplace shall be anywhere a State employee is conducting authorized State business or en route to and from (excluding normal commute) a location where State business is, will be, or has been conducted. (See Penal Code section 171 for additional information regarding weapons prohibited within any State or local public building.)

In addition, the California Department of General Services (DGS) Administrative Order #01-05a further specifies the prohibition of firearms or other dangerous weapons in all DGS-owned buildings or leased spaces, garages, and parking facilities, including space within buildings shared with other departments or agencies. This prohibition shall apply even if a person has a permit for a concealed carry weapon (CCW).

Law enforcement officers are exempt from this policy.

In the event there is credible information that a person is in violation of this policy, contact and notify a supervisor/manager, the Human Resources Office, the Equal Employment Opportunity Officer, and/or security personnel as appropriate.

Responsibilities

- **Equal Employment Opportunity (EEO) Officer** – The EEO Office is responsible for maintaining the WVBPP policy and procedures in conformance with State and federal laws. The EEO Officer shall take all reports of workplace violence seriously and will conduct a thorough inquiry and recommend appropriate actions.

- **Manager/Supervisor** - All managers/supervisors are responsible for ensuring compliance with the provisions of WVBPP and its implementation for their area of responsibility. Managers/supervisors shall immediately report all incidents of workplace violence and provide documentation to the OSI EEO Officer.

- **Employee –** All OSI employees shall act professionally, courteously, and responsibly which ensures compliance with the State of California's workplace violence and bullying prevention policy requirement (Government Code sections 12950.1 and 19572) and the OSI policy and procedures. Employees shall report all acts of violence in the workplace to their manager/supervisor and the OSI EEO Officer.

Incident Reporting Procedures

If there is an imminent risk of harm (*i.e.*, an immediate real threat) and/or someone is seriously injured or ill:

a. Dial 9-1-1 for Law Enforcement and/or medical assistance.
b. Notify a supervisor/manager and the EEO Officer.

For further reporting information, responsibilities, procedures, and the investigation process see the WVBPP Procedures guide.

Workplace Violence and Bullying Prevention Program Training

Contact the Training Coordinator, in the OSI Human Resources Office, for information about scheduled or additional training at (916) 263-3976.

Legal Authority

California Labor Code section 6400 et seq. and Title 8, California Code of Regulations section 3203: Requires that every employer shall furnish a place of employment that is safe and healthful for employees.

California Government Code section 12950.1: Requires that employers shall include prevention of abusive conduct (also known as bullying) as a component of specified training/education; further defines “abusive conduct”; and states that a single act shall not constitute abusive conduct, unless especially severe and egregious.

California Government Code section 19572: Prohibits discourteous treatment, negligence, and/or recklessness in the workplace and constitutes cause for discipline.

California Penal Code section 71:

Prohibits any person from threatening or inflicting unlawful injury upon any public officer or employee, which would cause the public officer, or employee to refrain from doing any act in the performance of his/her duties.

California Penal Code section 171b: Prohibits any person from bringing or possessing within any state or local public building firearms and other weapons as described in this section. Any person who brings or possesses any of these items is guilty of a public offense, punishable by imprisonment.

California Penal Code section 16000 *et seq.* Unlawful carrying and possession of weapons.

Memorandum of Understanding(s) Bargaining Units 1, 3, 4, 11, 14, 15, 17, 20, and 21: Requires that each department shall maintain a WVBPP which shall be in writing and distributed and/or made available to all employees.

Issued by the Office of the Directorate