Office of Systems Integration "SERVING CALIFORNIA"	**SECURITY POLICY** **Control Number: OSI-AP-07-03**
PASSWORD STANDARD	**Effective Date: November 7, 2007**

Purpose

The purpose of this policy is to establish a password protection standard for the employees of the Office of Systems Integration (OSI).

Scope

The standard applies to all OSI staff and all prime contractors and non-prime contractors who access OSI information systems and assets.

Policy

A username and password are typically the minimum requirement to access all systems within OSI. This password policy mandates that users are to create passwords with rules that ensure strong passwords and enforce controls that limit a password's vulnerability to guessing, brute force attacks, and password-cracking tools. All OSI computing devices, including workstations, laptops, and PDA's (e.g. Blackberry's) are to be, at a minimum, protected by a username if applicable and a strong password.

Additionally, when a device is not in use, a user is required to lock the screen in a manner requiring that the username and password be entered in order to unlock the device. The expectation is that when logged on to an OSI device, staff and contractors will not leave their computer terminal or workstation unattended unless the screen is locked.

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 adhere to the following requirements:

Standard Requirements (continued)

1. Passwords must be at least eight characters long.

2. Passwords may not contain your user name or any part of the user's full name.

3. User default passwords must be changed upon first login.

4. Default device passwords must be changed before the device is placed on the network or upon first login.

5. Passwords must be changed immediately if compromised.

6. Dictionary words may not be a word in any language, slang, dialect, jargon, etc.

7. Passwords may not be based on a user's personal information, such as names of family members, pets, etc.

8. 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:

1. Password History – The number of preceding passwords that cannot be reused. Six unique iterations are required prior to re-using a password.

2. Maximum Password Age – The number of days before a user is allowed to change their password. At a minimum, a user is required to reset a password every 90 days.

3. Minimum Password Age – The number of days before a user is allowed to change his or her password. This value is set to one day. If a user feels that the password has been compromised before the one day has passed, then the user should contact the project-specific Help Desk for resolution.

Standard Requirements (continued)

4. Lockout Count – The number of unsuccessful login attempts before an account is locked out. If locked out, the user must contact the project-specific Help Desk to request that the password be reset. The number is determined by each project within OSI. If a user wishes to know the number set by his or her department, the user will need to check with the project-specific Help Desk.

5. Reset Lockout – The length of time before the number of unsuccessful logon attempts is reset to zero. This number is determined by each project within OSI.

Password Protection Requirements:

1. A user must not disclose his or her password to anyone at any time for any reason.

2. If any person demands your password, the user should refer him or her to this document or have him or her call the Information Security Officer (ISO) at OSI. If a situation arises wherein a user requires temporary access to another user's computer, a Systems Administrator would be able to change the login credentials to allow for temporary access.

3. When a device is not in user, the user is required to lock the screen in a manner requiring that the username and password be entered in order to unlock the device.

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

5. Passwords should not be inserted into unencrypted e-mail messages or other non-secure forms of electronic communication. When distributing new account information to The requestor, the username and password should be sent in separate e-mail messages.

6. Passwords should not be distributed via unencrypted e-mail messages or other non-secure forms of electronic communication. When distributing new account information to a user, the username and password should be sent in separate e-mail messages.

7. Do not use the same username and password created for access to OSI devices for non-OSI related website accounts (e.g. personal internet service provider account, personal bank account, etc.).

Standard Requirements (continued)

8. Accounts that have system-level privileges granted through group memberships or programs, such as “sudo”, must have a unique password from all other accounts held by users in that group. When the user of one of these types of accounts leaves, the password of this account should be changed to prevent unauthorized use.

9. Desktop administrators must disable the account of any staff that leaves a project in a timely manner.

Applicability and Exclusions

1. This standard applies to anyone accessing OSI IT resources that require authentication and applies to all applicable OSI IT resources.

2. Any questions regarding the applicability of this standard should be directed to the Information Security Officer at OSI for clarification.

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

Auditing and Reporting

1. Auditing may be performed on a periodic or random basis by the Information Security Officer or his/her designees.

2. In the event that an audit determines that password standard is not being applied, notification will be sent to the appropriate person for remediation.

3. Any known violations of this standard must be reported to the OSI Information Security Officer and the reporting employee’s immediate supervisor.

Approval

Original signed on November 7, 2007 and on file

PAUL BENEDETTO **Date**
Chief Deputy Director
Office of Systems Integration