



CALIFORNIA OFFICE OF INFORMATION SECURITY & PRIVACY PROTECTION



(916) 445-5239
WWW.INFOSECURITY.CA.GOV

ACCESS CONTROL
INFORMATION SHEET No. 7
DECEMBER 11, 2008

Does Your Agency Implement Forced Password Changes?

If your department has a policy of a 30 to 90 day password expiration then it would fall within the current standards, policies, and practices adopted by the state.

The state has adopted the American National Standards Institute/Federal Information Processing Standards (ANSI/FIPS) standards (see State Administrative Manual [SAM] Section 5100). The ANSI/FIPS standards and many others, such as the International Organization of Standards (ISO) 27002 recommend a forced change frequency of at least every 90-days. Passwords should consist of a minimum of 8 characters comprised of a combination of numbers, letters and special characters. There should also be some form of limitation on password reuse to avoid reusing or cycling old passwords.

National Standards of Standards and Technology (NIST) Special Publication (SP) 800-12 *An Introduction to Computer Security: The NIST Handbook* states, "Periodic changing of passwords can reduce the damage done by stolen passwords and can make brute-force attempts to break into systems more difficult."

Internal Revenue Service (IRS) PUB 1075 *Tax Information Security Guidelines for Federal, State, and Local Agencies and Entities* states, "Passwords shall be changed every 90 days, at a minimum, for standard user accounts to reduce the risk of compromise through guessing, password cracking or other attack & penetration methods. Passwords shall be changed every 60 days, at a minimum, for privileged user accounts to reduce the risk of compromise through guessing, password cracking or other attack and penetration methods."

SAM 5305.2 (formally SAM Section 4842.1) states, in part, "...each agency that employs information technology must establish a risk analysis process to identify and assess risks associated with its information assets and define a cost-effective approach to managing such risks." Our office recommends that each Agency identify their business need and the risks associated with the frequency of implementing a forced password change.

We also recommend that you consult with your management regarding this issue. SAM 5315.1 (formally SAM Section 4841.1) states, "Agency information technology management is responsible for (1) implementing the necessary technical means to preserve the security, privacy, and integrity of the agency's information assets and manage the risks associated with those assets and (2) acting as a custodian of information per SAM Section 5320.3" (formally SAM Section 4841.6).

Another component to consider is whether or not access into a system(s) can be gained by an intruder through a desktop via a compromised password or weak password. An agency should look at the Federal audit and accountability requirements. The FIPS-200 requires that organizations 1) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and 2) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. System controls should prohibit the use of weak passwords.

Other state policy sections that can be pointed to in support of these requirements include:

- SAM Section 5305 (formally SAM Section 4840) states in part, "State agencies need to ensure the integrity of computerized information resources by protecting them from unauthorized access, modification, destruction, or disclosure and to ensure the physical security of these resources."
- SAM 5310, states among other things, "Each agency must provide for the integrity and security of its information assets by establishing appropriate internal policies and procedures for preserving the integrity and security of each automated, paper file, or data base including : 1. Establishes and maintains management and staff accountability for protection of agency information assets."
- SAM Section 5315.1 states, State agency heads are accountable for the computerized information resources held by their agencies. They are responsible for the integrity of computerized information resources, and the authorization of access to those resources. All agency employees share in this responsibility as well.
- SAM 5320.2 states "The responsibilities of an agency unit that is the designated owner of an automated file or database consist of: Classifying each file or database for which it has ownership responsibility in accordance with the need for precautions in controlling access to and preserving the security and integrity of the file or data base. Defining precautions for controlling access to and preserving the security and integrity of files and data bases that have been classified as requiring such precautions. Authorizing access to the information in accordance with the classification of the information and the need for access to the information. Monitoring and ensuring compliance with agency and state security policies and procedures affecting the information. Identifying for each file or data base the level of acceptable risk. Filing Information Security Incident Reports with the Office. See SAM Section 5360. The ownership responsibilities

must be performed throughout the life cycle of the file or database, until its proper disposal. Program units that have been designated owners of automated files and data bases must coordinate these responsibilities with the agency Information Security Officer.

- SAM 5335.2 states “Information maintained in a personal computer system, including laptop computers and mobile devices, must be subjected to the same degree of management control and verification of accuracy that is provided for information that is maintained in other automated files. Files containing confidential or sensitive data (as defined in SAM Section 5320.5) should not be stored in personal computer systems unless the agency can demonstrate that doing so is in the best interest of the state and that security measures have been implemented to provide adequate protection. Proposals to use desktop or laptop computers to maintain or access files containing confidential or sensitive data as defined in SAM Section 5320.5, must be approved by the agency's Information Security Officer (SAM Section 5315.1) before implementation. The Information Security Officer will determine that the proposal complies with all applicable provisions of the SAM dealing with information security and risk management (SAM Sections 5300 through 5399).”
- SAM 20000 also speaks to internal controls and accountability requirements for state agencies. Implementing forced password change policies, practices, and procedures are a component of strong internal controls and accountability.

Below is a list of additional resources on the topic which you may find helpful.

- The SAM Chapter 5300 can be located at <http://www.oispp.ca.gov/government/policy.asp#sam>
- FIPS-200, Minimum Security Requirements for Federal Information Systems <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>
- NIST SP 800-12 An Introduction to Computer Security: The NIST Handbook <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>
- NIST Special Publication 800-63, E-Authentication Requirements http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
- NIST SP 800-100, Information Security Handbook for Managers <http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf>
- ISO/IEC 27002:2005 - Section 11.5.3 Password Management System (The State has adopted this standard as a framework for its security program. This information is copyrighted and must be purchased by the applicable state agency. If necessary, we can share with you the intent of the standard if you would find that information useful.)
- IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies and Entities <http://www.irs.ustreas.gov/pub/irs-pdf/p1075.pdf>