California
DEPARTMENT OF TECHNOLOGY
Office of Information Security

(916) 445-5239
HTTPS://CDT.CA.GOV/SECURITY/

ACCESS CONTROL
INFORMATION SHEET NO. 7
MAY 2017 (REVISED)

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 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, "Each state entity must provide for the protection of its information assets by establishing appropriate administrative, operational and technical policies, standards, and procedures to ensure its operations conform with business requirements, laws, and administrative policies, and personnel maintain a standard of due care to prevent misuse, loss, disruption or compromise of state entity information assets. Each state entity shall adopt, maintain and enforce internal administrative, operational and technical policies, standards and procedures in accordance with SIMM 5305-A to support information security program plan goals and

objectives." 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, " Each state entity shall determine the information security requirements (confidentiality, integrity, and availability) for its information assets in mission/business process planning; determine, document and allocate the resources required to protect the information assets as part of its capital planning and investment control process; and, establish organizational programming and budgeting documentation." SAM 5320.3 (formally SAM Section 4841.6) states, "Each state entity shall document and monitor individual information security and privacy training activities including basic security and privacy awareness training and specific information system security training; and retain individual training records to support corrective action, audit and assessment processes. The ISO will be responsible for ensuring that training content is maintained and updated as necessary to address the latest security challenges that may impact users."

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, "Each state entity is responsible for establishing an information security program. The program shall include planning, oversight, and coordination of its information security program activities to effectively manage risk, provide for the protection of information assets, and prevent illegal activity, fraud, waste, and abuse in the use of information assets."
- SAM 5310, states among other things, "State entity heads shall direct the establishment of an entity-specific Privacy Program. The Privacy Program shall ensure, and privacy coordinators shall confirm, that the requirements contained in the California Information Practices Act, this policy and the associated standards are adhered to by the state entity and its personnel."
- SAM Section 5315.1 states, "Each state entity shall determine the information security requirements (confidentiality, integrity, and availability) for its information assets in mission/business process planning; determine, document and allocate the resources required to protect the information assets as part of its capital

planning and investment control process; and, establish organizational programming and budgeting documentation".

- SAM 5320.2 states, "Each state entity shall determine the appropriate content of security and privacy training based on the assigned roles and responsibilities of individuals and the specific security requirements of the state entity and the information assets to which personnel have access. Privacy training content will ensure personnel understand their responsibility for compliance with the Information Practices Act of 1977 and the penalties for non-compliance". 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, "Each state entity shall ensure that information systems are capable of being audited and the events necessary to reconstruct transactions and support after-the-fact investigations are maintained. This includes the auditing necessary to cover related events, such as the various steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions in service-oriented architectures."
- 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://sam.dgs.ca.gov/TOC/5300.aspx
- FIPS-200, Minimum Security Requirements for Federal Information and Information Systems http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf
- NIST SP 800-12 An Introduction to Computer Security: The NIST Handbook http://csrc.nist.gov/publications/drafts/800-12r1/sp800_12_r1_draft.pdf
- NIST Special Publication 800-63, E-Authentication Requirements http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf
- NIST SP 800-100, Information Security Handbook: A Guide for Managers http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.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 https://www.irs.gov/pub/irs-pdf/p1075.pdf