Attachment 10

Identification and Authentication Policy - ITAM-0616

COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	IDENTIFICATION AND AUTHENTICATION POLICY	ITEM NUMBER:	ITAM-0616
OWNER:	DEPARTMENT OF GENERAL SERVICES	ADOPTION DATE:	MM/DD/20YY
APPROVER(S):	COUNTY BOARD OF SUPERVISORS	REVIEW DATE:	MM/DD/20YY
VERSION:	1.0	PAGE:	PAGE **1** OF **7**

I. Purpose

To ensure that only properly identified and authenticated users and devices are granted access to County Information Technology (IT) resources in compliance with County IT security policies, standards, and procedures, along with applicable State and Federal requirements.

II. Audience

The primary audience for this policy is Information Technology Professionals (County executives, managers, employees, contractors, vendors, and third parties) whose responsibilities include managing, administering, and operating County networks or systems.

III. Scope

This policy applies to any Information System that electronically generates, receives, stores, processes, or transmits County-owned data, whether the system is hosted on the county network or by a third-party provider. Additionally, these provisions apply to anyone doing business as the County and/or in support of the County that is provisioned access to County Networks or systems. This includes employees, contractors, consultants, temporaries, and other workers at the County, including all personnel affiliated with third parties, collectively referred to hereafter as “agents”.

IV. Definitions

See ITAM-0602, Glossary of Definitions

V. Policy

It is the policy of the County Board of Supervisors that:

Identification and authentication is a technical measure that prevents unauthorized users (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate users. All County IT systems must have a means to enforce user accountability when using state IT systems, so that system activity (both authorized and unauthorized) can be traced to specific users. To ensure user accountability, requires that all County IT systems implement a method of user identification and authentication. The user identification tells the system who the users are; the authentication mechanism provides an added level of assurance that the users really are who they say they are. Authentication consists of something a user knows (such as a password), something the user has (such as a token or smart card), or something the user is (such as a fingerprint). User identification and authentication also can enforce separation of duties. The following outlines the minimum security control requirements which all County information systems must adhere to in order to operate in

a production environment.

1. IDENTIFICATION AND AUTHENTICATION (County Users)

   County IT or Departmental IT shall:

   a. Ensure that information systems uniquely identify and authenticate County users or processes acting on behalf of County users.

   b. Ensure that information systems implement multifactor authentication for network access to privileged accounts as required by state and Federal rules and regulations.

   c. Ensure that information systems implement multifactor authentication for network access to non-privileged accounts.

   d. Ensure that information systems implement multifactor authentication for local access to privileged accounts.

   e. Ensure that information systems implement replay-resistant authentication mechanisms for network access to privileged accounts.

   f. Ensure that information systems implement multifactor authentication for remote access to systems as required by state and Federal rules and regulations such that one of the factors is provided by a device separate from the system gaining access and the device utilizes a cryptographic strength mechanisms that protects the primary authentication token (secret key, private key or one-time password) against compromise by protocol threats including: eavesdropper, replay, online guessing, verifier impersonation, and man-in-the-middle attacks.

   g. Ensure that information systems accept and electronically verify Personal Identity Verification (PIV) credentials.

2. DEVICE IDENTIFICATION AND AUTHENTICATION

   County IT or Departmental IT shall:

   a. Minimize the ability of non-authenticated or non-identified devices establishing a network connection.

3. IDENTIFIER MANAGEMENT

   County IT or Departmental IT, through department information systems owners, shall:

a. Ensure that the County manages information system identifiers by receiving authorization from departmental business systems owners and County IT or Departmental IT to assign an individual, group, role, or device identifier.

b. Select an identifier that identifies an individual, group, role, or device.

c. Assign the identifier to the intended individual, group, role, or device.

d. Disable the identifier after 60 days of inactivity.

4. AUTHENTICATOR MANAGEMENT

County IT or Departmental IT shall:

a. Manage information system authenticators (as established by County IT) by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.

b. Establish initial authenticator content for authenticators defined by the organization.

c. Ensure that authenticators have sufficient strength of mechanism for their intended use.

d. Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.

e. Change default content of authenticators prior to information system installation.

f. Establish minimum and maximum lifetime restrictions and reuse conditions for authenticators.

g. Authenticators should be changed/refreshed every 90 days on elevated permissions if other password schemas are not deployed (MFA, One Time Use, ‘Machine’ generated, or other more secure methods are deployed).

h. Protect authenticator content from unauthorized disclosure and modification.

i. Require individuals and devices to implement specific security safeguards to protect authenticators.

j. Change authenticators for group/role accounts when membership to those accounts changes.

k. Ensure that information systems for password-based authentication enforce minimum password complexity that must not contain the user's entire Account Name value or entire Full Name value.

l. Create passwords no less than 8 characters on platforms that have restrictions around lengths, especially maximum lengths, such as legacy platforms. If legacy system doesn't allow for minimum password protections, accelerate retirement of legacy system.

m. Create passwords between 15 to 20 characters utilizing self-imposed password complexity when passwords are human derived.

n. Create passwords of no less than 20 characters when an authorized County password manager is being leveraged.

o. Enable 'Show Password While Typing' function.

p. Allow Password 'Paste In'.

q. Do not use any 'password hints' processes or, as an example, Knowledge-based authentication (KBA) questions like "What street did you grow up on?" (these are not permitted).

r. Base User Passwords may be utilized (no reset needed) indefinitely unless there is a suspected or real breach of authentication security or other indicators of risk to require immediate password resets of all users.

s. Elevated user (Admins) passwords should be at least 20 characters and contain numerous symbols/emojis. Admin passwords will expire a maximum of 90 days.

t. Administrators MUST only use their ADMIN (elevated) authentications during administrative work and MUST log out to return to any 'normal user' activity.

u. Elevated permission users must utilize individual and specific password authentication for each enterprise device being managed. Each Enterprise device must have a separate and distinct set of credentials per each administrator. Administrators should be limited to only what is needed to manage and to have appropriate backup.

v. Utilize system generated dynamically assigned passwords for 'Managed Accounts'.

w. Utilize Dynamic Access Control to force user permission changes dynamically

without additional administrator intervention if the user's job or role changes (resulting in changes to the user's account attributes in AD DS).

x. The use of machine generated single use passwords on Enterprise systems is highly recommended.

y. Shared passwords shall not be used unless there is a documented approval by Central IT or County CISO with an 'exception request'. If a shared password is permitted for a specific instance then the 'business owner' MUST deploy additional 'defenses in depth' protections to offset the lack of security presented by shared password risks.

z. Store and transmit only cryptographically protected passwords.

aa. Allow the use of a temporary password for system logons with an immediate change to a permanent password.

bb. Ensure that information system, <u>for PKI-based authentication,</u> validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

cc. Enforce authorized access to the corresponding private key.

dd. Map the authenticated identity to the account of the individual or group.

ee. Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

ff. Require that the registration process to receive appropriately applied County defined types of and/or specific authenticators be conducted by IT Staff and/or departmental business systems owner before applying appropriate role-based access.

gg. Ensure that the information system, for hardware token-based authentication, employs mechanisms that satisfy existing State and Federal rules and regulations.

5. AUTHENTICATOR FEEDBACK

County IT or Departmental IT shall:

a. Ensure that information systems obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

6. CRYPTOGRAPHIC MODULE AUTHENTICATION

   County IT or Departmental IT shall:

   a. Ensure that information systems implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable state and federal laws, directives, policies, regulations, standards, and guidance for such authentication.

7. IDENTIFICATION AND AUTHENTICATION (NON-COUNTY USERS)

   County IT or Departmental IT shall:

   a. Ensure that information systems uniquely identify and authenticate non-County users or processes acting on behalf of non-County users.

   b. Ensure that information systems accept and electronically verify Personal Identity Verification (PIV) credentials from other government agencies.

   c. Ensure that information systems accept only Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative approved third-party credentials.

   d. Ensure that the organization employs only FICAM-approved information system components in those systems deemed to require appropriate levels of security to protect sensitive technology assets and protected and confidential data and information to accept third-party credentials.

VI. Exceptions

See ITAM-0600, IT Security Program

VII. Non-Compliance

See ITAM-0600, IT Security Program

VIII. References and Sources

1. Applicable Rules, Laws, and Regulations:

   a. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53a – Identification and Authentication (IA), NIST SP 800-12, NIST SP 800-63, NIST SP 800-73, NIST SP 800-76, NIST SP 800-78, NIST SP 800-100,

NIST SP 800-116.

b. Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors.

c. Federal Information Processing Standards (FIPS): FIPS 201, FIPS 140.

d. State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

2. Related Policies:

3. Referenced Documents:

4. Revision History:

VERSION	CHANGE	AUTHOR	DATE OF CHANGE
1.0	Initial Release	CISO/Policy Committee	08/25/2021