Attachment 4

Access Control Policy - ITAM-0610

COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	ACCESS CONTROL	ITEM NUMBER:	ITAM-0610
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 **9**

I. Purpose

To ensure that access to County systems, data, and other resources is limited to only those authorized persons and things and that the level of such access granted is in accordance 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:

Logical access controls are the system-based mechanisms used to designate whom or what is to have access to a specific system resource and the type of transactions and functions that are permitted. They include controls that:

- Manage user accounts, including activation, deactivation, changes and audits.
- Restrict users to authorized transactions and functions.
- Limit network access and public access to the system.
- Enforce assigned authorizations that control system access and the flow of information within the system and between interconnected systems.
- Identify, document and approve specific user actions that can be performed without identification or authentication.
- Enforce separation of duties.
- Enforce technical limitations which can prevent unauthorized access to system resources, etc.

County IT and Department IT shall be responsible for Access Controls over the IT Systems under their respective jurisdiction of responsibility and control. 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. ACCOUNT MANAGEMENT

a. Identify and select the following types of information system accounts to support organizational missions and business functions: individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.

b. Assign account managers for information system accounts.

c. Establish conditions for group and role membership.

d. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.

e. Require approvals by system owners for requests to create information system accounts.

f. Create, enable, modify, disable, and remove information system accounts in accordance with approved procedures and regulations.

g. Monitor the use of information system accounts.

h. Notify account managers within 24 hours when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes. In situations of hostile terminations, notify account managers as soon as possible. The notification should be prior to or at the time of termination.

i. Authorize access to the information system based on a valid access authorization or intended system usage.

j. Review accounts for compliance with account management requirements annually.

k. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

l. Ensure the use of shared group credentials is kept to a minimum.

m. Employ automated technology tools and utilities to support the management of information system accounts.

n. Ensure that the information system automatically disables temporary and emergency accounts after usage.

o. Ensure that the information system automatically disables inactive accounts no later than 6 months but preferably less than 60 days.

p. Ensure that the information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate IT personnel.

2. ACCESS ENFORCEMENT

a. Ensure that the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

3. INFORMATION FLOW ENFORCEMENT

a. Ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on applicable policy.

4. SEPARATION OF DUTIES

a. Minimize access by unique authentication and duties as possible to prevent malevolent activity without collusion.

b. Document access by individuals and/or groups having access to critical systems.

c. Define information system access authorizations to support minimal access schemas.

5. LEAST PRIVILEGE

a. Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

b. Authorize explicitly access to hardware and software controlling access to systems and filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.

c. Require that users of information system accounts, or roles, with access to systems containing protected or confidential information, use non-privileged accounts or roles, when accessing non-security functions.

d. Restrict privileged accounts on the information system to least privileged users of those systems that are sensitive technology assets and those systems containing protected and confidential information.

e. Ensure that the information system audits the execution of privileged functions.

f. Ensure that the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

6. UNSUCCESSFUL LOGON ATTEMPTS
Information systems shall:

a. Enforce a limit of consecutive invalid logon attempts by a user during 15 incorrect log-in attempts if system or application allows for this limit.

b. Lock the account/node automatically for a limited period or until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

7. SYSTEM USE NOTIFICATION
Information Systems should:

a. Display to users an approved system of use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable state and federal laws, directives, policies, regulations, standards, and guidance and states informing that:

i. Users are accessing a County information system.

ii. Information system usage may be monitored, recorded, and subject to audit.

iii. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties.

iv. Use of the information system indicates consent to monitoring and recording.

v. There are not rights to privacy.

b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.

c. Publicly accessible systems should:

i. Display system use information designated during log-on screen, before granting further access.

ii. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

iii. Include a description of the authorized uses of the system.

8. SESSION LOCK
Information systems should:

a. Prevent further access to the system by initiating a session lock after sixty days of inactivity or upon receiving a request from a user.

b. Retain the session lock until the user reestablishes access using established identification and authentication procedures.

c. Conceal, via the session lock, information previously visible on the display with a publicly viewable image.

9. SESSION TERMINATION

a. Ensure that the information system automatically terminates a user session after twenty minutes of inactivity.

10. PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

a. Identify user actions that can be performed on the information system without identification or authentication consistent with organizational missions and business functions.

b. Document and provide supporting rationale in the security plan for the information system, user actions not requiring identification or authentication. Use best security practices such as a developed DMZ and appropriate firewalling to prevent non-credentialed access to internal systems.

11. REMOTE ACCESS

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

b. Authorize remote access to the information system prior to allowing such connections.

c. Ensure that the information system monitors and controls remote access methods.

d. Ensure that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

e. Ensure that the information system routes all remote accesses through all appropriate managed network access control points to reduce the risk for external attacks.

f. Authorize the execution of privileged commands and access to security-relevant information via remote access only for approved business needs.

g. Document the rationale for such access in the security plan for the information system.

12. WIRELESS ACCESS

a. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.

b. Authorize wireless access to the information system prior to allowing such connections.

c. Ensure that the information system protects wireless access to the system using authentication of users and devices and encryption.

13. ACCESS CONTROL FOR MOBILE DEVICES

a. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.

b. Authorize the connection of mobile devices to organizational information systems.

c. Employ full-device encryption or container encryption to protect the confidentiality and integrity of information on approved devices. Such encryption can be minimally accomplished by password protected device schemas included within the device OS.

14. USE OF EXTERNAL INFORMATION SYSTEMS

a. Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

i. Access the information system from external information systems.

ii. Process, store, or transmit organization-controlled information using external information systems.

b. Permit authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

i. Verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan.

ii. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

15. INFORMATION SHARING

   a. Facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for determined requirements set forth by the IT Management Team or Departmental IT Management.

   b. If needed, employ the use of the Central IT to assist users in making information sharing/collaboration decisions.

16. PUBLICLY ACCESSIBLE CONTENT

   a. Designate individuals authorized to post information onto a publicly accessible information system.

   b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.

   c. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.

   d. Review the content on the publicly accessible information system for nonpublic information weekly and removes such information, if discovered.

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 Publications (SP):

      i. NIST SP 800-53a – Access Control (AC)

      ii. NIST SP 800-12

iii. NIST 800-46

iv. NIST SP 800-48

v. NIST SP 800-77

vi. NIST SP 800-94

vii. NIST SP 800-97

viii. NIST SP 800-100

ix. NIST SP 800-113

x. NIST SP 800-114

xi. NIST SP 800-121

xii. NIST SP 800-124

xiii. NIST SP 800-164

b. NIST Federal Information Processing Standards (FIPS) 199

c. 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