Attachment 20

System and Information Integrity Policy - ITAM-0628

COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	SYSTEM AND INFORMATION INTEGRITY POLICY	ITEM NUMBER:	ITAM-0628
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 County Information Technology (IT) resources and information systems are established with system integrity monitoring to include areas of concern such as malware, application and source code flaws, industry supplied alerts and remediation of detected or disclosed integrity issues.

II. Audience

The primary audience for this policy is Information Technology Professionals (County executives, managers, employees, contractors, vendors and third parties) whose responsibilities including 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:

Central IT and Departments must implement system and information integrity security controls including flaw remediation, information system monitoring, information input restrictions (such as validating input in all Web applications), and information output handling and retention. Integrity controls protect data from accidental or malicious alteration or destruction and ensure users that the quality and reliability of the information meets expectations.

It is expected that departments protect against malicious code (e. g. viruses, worms, Trojan horses, etc.) by implementing (anti-virus, anti-malware) solutions that, to the extent possible, includes a capability for automatic updates. Intrusion detection/prevention tools, techniques, and additional security protection mechanisms should be in place to be in compliance with requirements. 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. FLAW REMEDIATION

County IT or Departmental IT shall:

a. Identify, report, and correct information system flaws.

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

c. Install security-relevant software and firmware updates within industry standard recommendations and best practice intervals (generally weekly for end points and monthly for servers, switching and other devices) of the release of the updates.

d. Incorporate flaw remediation into the County configuration management process.

e. Employ automated mechanisms weekly to determine the state of information system components with regard to flaw remediation.

2. MALICIOUS CODE PROTECTION

County IT or Departmental IT shall:

a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.

b. Update malicious code protection mechanisms whenever new releases are available in accordance with County configuration management policy and procedures.

c. Configure malicious code protection mechanisms to:

i. Perform periodic scans of the information system minimally monthly and real-time scans of files from external sources at endpoint; network entry/exit points as the files are downloaded, opened, or executed in accordance with County security policy.

ii. Block malicious code; quarantine malicious code; send alert to administrator; IT Staff will take immediate mitigating actions in response to malicious code detection.

3. INFORMATION SYSTEM MONITORING

County IT or Departmental IT shall:

a. Monitor the information system to detect:

i. Attacks and indicators of potential attacks.

ii. Unauthorized local, network, and remote connections.

b. Identify unauthorized use of the information system through defined techniques and methods.

c. Deploy monitoring devices strategically within the information system to collect all appropriate data to determine any suspicious activity and at ad hoc locations within the system to track specific types of transactions of interest to the County.

d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

e. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to County operations and assets, individuals, other organizations, or based on law enforcement information, intelligence information, or other credible sources of information.

f. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable state and federal laws, directives, policies, or regulations.

g. Provide information system monitoring information to authorized personnel or business units as needed.

4. SYSTEM-GENERATED ALERTS

County IT or Departmental IT shall ensure that:

a. The information system that may be generated from a variety of sources (e.g. audit records or inputs from malicious code protection mechanisms; intrusion detection or prevention mechanisms; or boundary protection devices, such as firewalls, gateways, and routers) will be disseminated to authorized personnel or business units that shall take appropriate action on the alert(s).

b. Alerts be transmitted telephonically, electronic mail messages, or by text messaging as required. County personnel on the notification list can include system administrators, mission/business owners, system owners, or information system security officers.

5. SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

County IT or Departmental IT shall:

a. Receive information system security alerts, advisories, and directives from Multi State Information Sharing and Analysis Center, Microsoft, and other supporting/vendor entities on an ongoing basis.

b. Generate internal security alerts, advisories, and directives as deemed necessary throughout the County.

c. Disseminate security alerts, advisories, and directives to appropriate IT Staff as well supporting vendors and other supporting public agencies.

d. Implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

6. SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

County IT or Departmental IT shall:

a. Employ integrity verification tools or manual detection processes to detect unauthorized changes to any and all technology assets including systems containing protected data and information.

b. Ensure the information system performs an integrity check of technology assets at startup, and/or at intervals determined to be industry best practices.

c. Incorporate the detection of inappropriate events affecting County technology assets including unauthorized access of protected data and information into the County incident response capability.

7. SPAM PROTECTION

County IT or Departmental IT shall:

a. Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages.

b. Update spam protection mechanisms when new releases are available in accordance with County configuration management policy and procedures.

c. Manage spam protection mechanisms centrally.

d. Ensure information systems automatically update spam protection mechanisms.

8. INFORMATION INPUT VALIDATION

County IT or Departmental IT shall:

a. Ensure the information system:

i. Checks the validity of edits and new inputted data and fields of structured systems.

ii. Provides a manual override capability for input validation of structured applications and its data.

iii. Restricts the use of the manual override capability to only supporting roles as directed by the County CIO.

iv. Audits the use of the manual override capability.

v. Reviews and resolve within input validation errors.

vi. Behaves in a predictable and documented manner that reflects County and system objectives when invalid inputs are received.

9. ERROR HANDLING

County IT or Departmental IT shall:

a. Ensure the information system:

i. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.

ii. Reveals error messages only to appropriate administrators of those monitored systems.

10. INFORMATION HANDLING AND RETENTION

County IT or Departmental IT shall:

a. Handle and retain information within the information system and information output from the system in accordance with applicable state and federal laws, directives, policies, regulations, standards, and operational requirements.

11. MEMORY PROTECTION

County IT or Departmental IT shall:

a. Ensure the information system implements appropriate standards under guidance of industry best practices to protect its memory from unauthorized code execution.

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 – System and Information Integrity (SI)

ii. NIST SP 800-12

iii. NIST SP 800-40

iv. NIST SP 800-45

v. NIST SP 800-83

vi. NIST SP 800-61

vii. NIST SP800-83

viii. NIST SP 800-92

ix. NIST SP 800-100

x. NIST SP 800-128

xi. NIST SP 800-137

xii. NIST SP 800-147

xiii. NIST SP 800-155

b. State of California State Administrative Manual (SAM) 5300 et seq.

c. 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