Attachment 11

Incident Response Policy - ITAM-0617

COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	INCIDENT RESPONSE POLICY	ITEM NUMBER:	ITAM-0617
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 **6**

I. Purpose

To ensure that County Information Technology (IT) and department IT properly identify, contain, investigate, remedy, report, and respond to computer security incidents.

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. 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 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:

Information Technology Incident Management refers to the processes and procedures agencies implement for identifying, responding to, and managing information security incidents. A computer incident within County is defined as a violation of computer security policies, acceptable use policies, or standard computer security practices. Refer to NIST SP 800-61 Revision 2 Computer Security Incident Handling Guide for guidance in creating an incident management policy and developing plans and procedures to support it. To clearly communicate incidents and events (any observable occurrence in a network or system), it is necessary for the agency incident response teams to adopt a common set of terms and relationships between those terms. All elements of the County should use a common taxonomy, per the definitions of terms, roles, and procedures contained in this document. System owners and the County CISO are kept informed of system vulnerability advisories from the US Computer Emergency Readiness Team (US-CERT), from software vendors, and other sources and should communicate this

information to relevant individuals and Departments. The process also must ensure tracking and implementation of corrective actions (e.g., developing filter rules and patching) and coordinates with responsible incident response capabilities regarding the handling and reporting of incidents involving systems under the program area's responsibility. Departments must report IT incidents to Central IT and the County CISO by completing an IT Incident Report (Appendix A) and provide as much information about the incident as possible including: the incident category, how the incident was discovered, affected IP addresses, port numbers, information about the affected agency system, impact to the agency, and the final resolution. The following table outlines the minimum security control requirements which all County information systems must adhere to in order to operate in a production environment:

1. INCIDENT RESPONSE TRAINING

The County shall:

a. Provide incident response training to information system users consistent with assigned roles and responsibilities:

i. Within 90 days of assuming an incident response role or responsibility.

ii. When required by information system changes, and annually thereafter.

b. Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.

c. Employ automated mechanisms to provide a more thorough and realistic incident response training environment.

2. INCIDENT RESPONSE TESTING

The County shall:

a. Test the incident response capability for the information system bi-annually using table top exercises to determine the incident response effectiveness and document all results.

3. INCIDENT HANDLING

The County shall:

a. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

b. Coordinate incident handling activities with contingency planning activities.

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

4. INCIDENT MONITORING

The County shall:

a. Employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

5. INCIDENT REPORTING

The County shall:

a. Require personnel to report suspected security incidents to the County incident response capability as soon as possible in order to allow for immediate mitigation of any on-going breach.

b. Report security incident information to the County CISO, Department SO, CIO, or any manager or supervisor.

6. INCIDENT RESPONSE ASSISTANCE

The County shall:

a. Provide an incident response support resource, integral to the County incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

7. INCIDENT RESPONSE PLAN

The County shall:

a. Develop an incident response plan that:

iii. Provides the County with a roadmap for implementing its incident response capability.

iv. Describes the structure and County of the incident response capability.

v. Provides a high-level approach for how the incident response capability fits into the overall County.

vi. Meets the unique requirements of the County, which relate to mission, size, structure, and functions.

vii. Defines reportable incidents.

viii. Provides metrics for measuring the incident response capability within the County.

ix. Defines the resources and management support needed to effectively maintain and mature an incident response capability.

x. Is reviewed and approved by the County CISO.

b. Distribute copies of the incident response plan to CSERT.

c. Review the incident response plan with CSERT.

d. Update the incident response plan to address system/County changes or problems encountered during plan implementation, execution, or testing.

e. Communicate incident response plan changes to CSERT.

f. Protect the incident response plan from unauthorized disclosure and modification.

County Computer Security Emergency Response Team

8. COUNTYWIDE COMPUTER SECURITY EMERGENCY RESPONSE

a. The County shall establish a Countywide Computer Emergency Response Team (CSERT). The CSERT shall be led by the Chief Information Security Officer (CISO) or the Chief Information Officer or their equivalent when the CISO is not available.

b. The CSERT shall consist of representatives from all County departments.

c. The CSERT shall communicate security information, guidelines for notification processes, identify potential security risks, and coordinate responses to thwart, mitigate, or eliminate security threats to County IT resources.

d. Upon the activation of CSERT by the CISO, all Departmental Information Security Officers (DISOs), Assistant DISOs, and other CSERT representatives shall report directly to the CISO for the duration of the CSERT activation.

9. DEPARTMENTAL COMPUTER EMERGENCY RESPONSE

a. Each County department shall establish a Departmental Computer Security Emergency Response liaison and has the responsibility for responding to and/or coordinating the response to security threats to County IT resources

within the County department as well the County CISO.

b. Representatives from each department shall also be active participants in CSERT as appropriate.

c. Each County department shall establish and implement Departmental Computer Security Emergency Response Procedures that consist of the following, at minimum:

i. Creating an incident response policy and plan.

ii. Developing procedures for performing incident handling and reporting.

iii. Setting guidelines for communicating with the CSERT and outside parties regarding incidents.

iv. Selecting a team structure and staffing mode.

v. Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies.

vi. Determining what services the incident response team should provide.

vii. Staffing and training the incident response team.

d. The Department shall inform the CSERT, as early as possible, of security threats to County IT resources.

e. Each County department shall develop a notification process, to ensure management notification within the County department and to the CSERT, in response to County IT security incidents.

f. The Department liaison and the CSERT have the responsibility to take necessary corrective action to remediate County IT security incidents. Such action shall include all necessary steps to preserve evidence in order to facilitate the discovery, investigation, and prosecution of crimes against County IT resources.

g. Each County department shall provide CSERT with contact information, including, without limitation, after-hours, for its primary and secondary CSERT representatives (e.g., DISO and Assistant DISO), and immediately notify CSERT of any changes to that information.

h. Each County department shall maintain current contact information for all personnel who are important for the response to security threats to County IT

resources and/or the remediation of County IT security incidents.

i. Each County department shall provide its primary and secondary CSERT representatives with adequate portable communication devices (e.g., cell phone and pager).

j. In instances where violation of any law may have occurred, proper notifications shall be made in accordance with County policies. All necessary action shall be taken to preserve evidence and facilitate the administration of justice.

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): NIST SP 800-53a – Incident Response (IR), NIST SP 800-16, NIST SP 800-50, NIST SP 800-61 – Computer Security Incident Handling Guide, NIST SP 800-84, NIST SP 800-115.

   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