| SUBJECT: | INFORMATION SECURITY INCIDENT MANAGEMENT POLICY | ITEM NUMBER: | ITAM-0530 |
|---|---|---|---|
| OWNER: | DEPARTMENT OF GENERAL SERVICES | ADOPTION DATE: | MM/DD/2019 |
| APPROVER(S): | COUNTY BOARD OF SUPERVISORS | REVIEW DATE: | MM/DD/2022 |
| VERSION: | 1.1 | PAGE: | PAGE **1** OF **6** |

## I. Purpose

This document establishes the policy requirements for responding to information security incidents at the County of Santa Barbara. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies, procedures and reporting requirements.

## II. Audience

The audience for this policy is all County of Santa Barbara Departments.

## III. Scope

This policy applies to the information systems, data, and networks of the County of Santa Barbara and any person or device who gains access to these systems or data.

## IV. Definitions

1. Cybersecurity Awareness Training: A formal process for educating employees about computer security.

2. Event: Any observable occurrence in a network or system.

3. Health Insurance Portability and Accountability Act (HIPAA): Established in 1996, HIPAA is United States legislation that provides data privacy and security provisions for safeguarding medical information.

4. Information Technology (IT): The technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data.

5. LAN Administrators: Local Area Network (LAN) administrators are IT personnel assigned to provide technical support within specific departments.

6. Security Breach: Any incident that results in unauthorized access of data, applications, services, networks, and/or devices by bypassing their underlying security mechanisms.

7. Security Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

8. Security Incident Handling Procedures: The set of repeatable documented operational activities undertaken to identify, contain, report and remediate a security incident.

9. Security Incident Response: The mitigation of violations of security policies and recommended practices.

## V. Policy

The following elements provide the overall direction to support the County of Santa Barbara in mitigating the risks from computer security incidents through guidance on identifying and responding to incidents effectively and efficiently. Specific operational aspects of incident management such as response time will be handled by processes and procedures at the departmental level.

### A. Roles and Responsibilities

- Central IT – The Computer Security Emergency Response Team (CSERT) within the General Services, Information Communications & Infrastructure (ICT) division, will provide assistance to remediate security incidents and provide any needed coordination with law enforcement and other external incident response partners. CSERT will maintain standard processes and procedures for the handling of security incidents.

- Chief Information Security Officer (CISO) – The CISO will coordinate with the office of the Chief Executive Officer (CEO) and other senior management during security incidents with a moderate to high impact to the County that may include but are not limited to data breaches, theft and damage to County assets.

- County Counsel – Guidance by County Counsel should be sought if there is reason to believe that a security incident may have legal ramifications, including evidence collection, prosecution of a suspect, or a lawsuit, or if there may be a need for a memorandum of understanding (MOU) or other binding agreements involving liability limitations for information sharing.

- Cybersecurity Management Communications Team (CMCT) – The CMCT will act as liaison to the CISO, providing communication to the general public, senior leadership and other stakeholders so that the CISO may focus on cybersecurity response coordination activities.

- Department System Owners – Department system owners and related personnel will work in concert with CSERT to ensure appropriate reporting procedures are documented and followed in the event that a security incident rises to the level of a security breach such as the loss of sensitive information to any appropriate regulating agency such as the State of California.

- HIPAA Privacy Officer – The County HIPAA Privacy Officer investigates incidents in which a breach of PHI may have occurred, report breaches as necessary, and ensure patients´ rights in accordance with state and federal laws.

- Information Security Officers (ISOs) – Department resources with the assigned role as ISO may be needed to provide specialized assistance with identifying, containing, reporting and remediating security incidents.

- IT Technical Support – Department IT resources such as LAN Administrators may be engaged to provide skills and expertise to assist in security incident response such as whether to disconnect a compromised system.

B. Common Security Incident Types

- Compromised Asset – A security incident that results in a compromised asset such as a network device, application, user account, etc.
- Data Exposure – The result of intentionally or accidentally exposing sensitive information to an unauthorized party.
- Denial of Service (DoS) – A security incident that causes a disruption to County operations that results in a degradation or loss of capability to deliver County services.
- Hacking – Reconnaissance or suspicious activity originating externally or internally to the County network.
- Malware Infection – A virus or other destructive software that infects County devices and causes performance degradation, inaccessibility of data, sensitive data disclosure or data loss.
- Policy Violations – Deliberate violations to County Policy such as inappropriate use of County assets, unauthorized information or system access, sharing offensive material and other items identified in the County Acceptable Use Policy and other applicable policies.
- Suspicious Email – Unsolicited or malicious email messages and other security-related events.
- Unlawful Activity – A security incident of a criminal nature such as fraud, theft, software license violation, illegal pornography, etc.

  The degree of impact will vary depending on the incident circumstances.

C. Security Incident Documentation and Reporting

- Security Incident Handling
  - Isolated Incidents – Security incidents may occur within an individual department where the impact is localized such as an individual phishing email or lost mobile device. These incidents must be reported to Central IT, although they may be resolved by the local department ISO if assistance is not needed. Local department incident handling procedures must be documented and followed.

- Complex Incidents – Larger more complex security incidents, such as malware outbreaks or the loss of sensitive information, will require immediate notification to Central IT. Internal Information related to the incident reporter or handler will be captured by CSERT such as name, role, department, location and other contact information. Details related to the incident will be captured including dates/timestamps, root cause, response activities and other items identified in CSERT incident handling procedures. CSERT incident handling procedures will be followed.

- Security Incident Communication – Security incidents must be immediately communicated to quickly contain and remediate negative effects. While departments may have unique reporting requirements such as to the State of California, the following communication must also occur.

  - End users – End users should notify their LAN Administrator and ISO of any suspected security issues.

  - LAN Administrators and ISOs – Notify Central IT if a suspected incident has occurred, regardless of incident type. This notification should be made via connected ticketing system or email. Document relevant information such as: indicators of compromise, time, affected user(s) and machine(s), and any pertinent artifacts such as screenshots, event logs, etc. Complex incidents must be followed-up with a phone call to Central IT to ensure expedited attention.

  - Central IT – Complex incidents should be communicated to the CISO. If health records are involved, the County HIPAA Privacy Officer will be notified as well. Central IT will provide a mass email message and website posting if appropriate. In a complex incident, the County's mass notification system will be used to disseminate critical security incident information. This communication will include data pertinent to the incident as well as affected users and services.

- Legal Requirements – If the security incident results in a breach of sensitive information such as health records, the CISO and/or County Council will be notified. Applicable legal and regulatory reporting requirements will be followed depending on the type of information. For example, the loss of criminal justice information requires a specific reporting procedure found within the FBI Criminal Justice Information Services (CJIS) policy. Similarly, the breach of HIPAA data is a legally reportable event with specific guidelines in terms of the number of records, reporting times, etc.

- Theft, Fraud and Related Abuses – Should the security incident involve the theft of County assets, fraudulent activities such as financial manipulation or related abuses, the incident that is detected or suspected must be reported immediately and simultaneously to a direct supervisor and the Internal Audit Division of the Auditor-Controller's Office. If the immediate supervisor is suspected as being a party to the improprieties or irregularities, the next higher supervisor should be

informed. County-issued devices that are considered reportable include, but are not limited to the following:

- Laptops / tablets
- Mobile phones
- Removable data storage devices containing sensitive information

Further details on reporting theft and fraud may be found in the "County of Santa Barbara Fraud, Theft, and Loss Policy."

D. Sharing Security Incident Information with Outside Parties

- Affiliated Partners – CSERT and other County entities may need to communicate with affiliated partners regarding a security incident. This may include sharing information with law enforcement, federal/state agencies and other organizations with which the County has an existing affiliation.

- Media – Any interaction with the media will follow media communications procedures that comply with the County's policies on media interaction and information disclosure.

1. Applicable Rules, Laws, and Regulations:

   Please note that this list is not intended to be exhaustive as other rules, laws and regulations may apply.

   i. California Data Breach Notice - California Civil Code sections 1798.29 and 1798.82

   ii. California Health Facilities Data Breach - California Health & Safety Code section 1280.15

   iii. FBI Criminal Justice Information Services Security Policy

   iv. Health Insurance Portability and Accountability Act of 1996

   v. IRS Publication 1075

   vi. Payment Card Industry Data Security Standard

   vii. Contractual obligations with service providers, vendors and other parties

2. Exceptions: N/A

3. Non-Compliance: Employees who intentionally cause a security incident, or fail to report one, may be subject to disciplinary action. Failure to report information security incidents may place the County at further risk through the lack of remediation response as well as for non-compliance with mandatory legal and regulatory reporting requirements.

4. Related Policies:

   i. County Auditor-Controller Policy L1.1, "County of Santa Barbara Fraud, Theft, and Loss Policy"

   ii. County Acceptable Use Policy, Use of County Computing Resources (includes e-mail and internet policies)

5. Referenced Documents: N/A

6. Revision History:

| VERSION | CHANGE | AUTHOR | DATE OF CHANGE |
|---|---|---|---|
| 1.0 | Initial Release | Thomas Gresham | 08/18/2018 |
| 1.1 | Policy Committee Approved Changes | Thomas Gresham | 04/29/2019 |