



COUNTY OF EL DORADO, CALIFORNIA

BOARD OF SUPERVISORS POLICY

Subject: INCIDENT RESPONSE POLICY	Policy Number: A-14	Page Number: 1 of 4
	Originally Adopted: 11/14/2023	Last Revised Date: 11/14/2023

I. PURPOSE

The purpose of this policy is to ensure El Dorado County properly identifies, contains, investigates, remediates, reports, and rapidly responds to security incidents to minimize impact on the organization, thus ensuring that the best possible levels of service quality and availability are maintained.

The procedure establishes the response process in instances where there is a potential or actual breach of privacy and confidentiality of protected information.

II. DEFINITIONS

Breach – The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for unauthorized purpose.

Data Owner – Individuals who have direct responsibility for the data that resides and/or is primarily used within their department. The owner is accountable for classifying the data and reviewing the classification.

Incident Response Plan (IRP) – The County’s internal security procedures guide for managing all stages of incident response.

Protected Data - Applies to data that County is required to keep private under State, Federal, County, Tribal, and Local regulations, including but not limited to:

- PI - Personal Information as defined in the California Information Practices Act in Civil Code section 1798.29, or as may be amended, for data breach notification
- HIPAA - Health Insurance Portability and Accountability Act
- CJIS - Criminal Justice Information Systems
- PHI - Protected Health Information
- PCI - Payment Card Information

III. POLICY

- A. This policy mandates that any individual who suspects that a theft, breach or exposure of El Dorado County Protected Data has occurred must immediately provide a description of what occurred via e-



COUNTY OF EL DORADO, CALIFORNIA

BOARD OF SUPERVISORS POLICY

Subject: INCIDENT RESPONSE POLICY	Policy Number: A-14	Page Number: 2 of 4
	Originally Adopted: 11/14/2023	Last Revised Date: 11/14/2023

mail to security.support@edcgov.us or report through the use of the help desk reporting web page at <http://helpdesk>. This e-mail address and web page is monitored by the El Dorado County's Chief Information Security Officer.

- B. This policy applies to all individuals who collect, access, maintain, distribute, process, store, use, transmit, dispose of, or otherwise handle Protected Data for El Dorado County departments. Any agreements with vendors will contain language similar that protects data for the County of El Dorado.
- C. An Incident Response Plan will support this policy for all organizational information systems that house or access County of El Dorado controlled information. The Incident Response Plan will address the seven stages of incident response:
 - 1. Preparation
 - 2. Detection
 - 3. Analysis
 - 4. Containment
 - 5. Eradication
 - 6. Recovery
 - 7. Post-Incident Activity
- D. The Chief Information Security Officer will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach, or exposure has occurred. If a theft, breach, or exposure has occurred, the Chief Information Security Officer will follow the EDC Incident Response Plan.
- E. The Incident Response Plan will be tested annually using tabletop exercises. Where appropriate, tests will be integrated with testing of related plans (Business Continuity Plan, Disaster Recovery Plan, etc.) where such plans exist. The results of these tests will be documented and shared with key stakeholders.
- F. The Incident Response Plan will be reviewed by the Chief Information Security Officer on an annual basis and revised as needed based on the documented results of previously conducted tests or live executions of the Incident Response Plan. Upon completion of plan revision, the updated IRP will be distributed to key stakeholders.



COUNTY OF EL DORADO, CALIFORNIA

BOARD OF SUPERVISORS POLICY

Subject: INCIDENT RESPONSE POLICY	Policy Number: A-14	Page Number: 3 of 4
	Originally Adopted: 11/14/2023	Last Revised Date: 11/14/2023

III. PROCEDURE

A. Incident Response Plan

1. The Information Technologies Director and Chief Information Security Officer shall be responsible for the delivery of detailed Incident Response Plan. This plan will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards, reporting, remediation, and feedback mechanisms. The plan shall be available to all personnel whose duties involve data privacy and security protection.
2. The plan is subject to changes as required and may be updated and re-published as necessary under the authority of the Director, Information Technologies (IT). Where changes are substantive, notifications of changes will be distributed to the affected EDC governmental communities.

B. Confirmed Theft, Data Breach, or Exposure of El Dorado County Protected Data

1. As soon as a theft, data breach or exposure containing Protected Data is reported or identified, the execution of the documented Incident Response Plan and Procedures will begin.
2. The Chief Information Security Officer will document the incident report and in collaboration with the data owner will chair an incident response team to coordinate the handling, investigation, and reporting of the breach or exposure.
3. The Chief Information Security Officer will contact County Counsel to review if the information disclosed meets the criteria for Protected Data for purposes of the breach notification requirements.
4. Incidents reported will be tracked, documented, and reported to appropriate officials and/or authorities, both internal and external to the organization.

C. Enforcement

1. Any El Dorado County personnel found in violation of this procedure described in Section III.B may be subject to disciplinary action, up to and including termination of employment.
2. Any third-party partner company found in violation may have their network connection terminated.

IV. REFERENCES

Incident Response Plan



COUNTY OF EL DORADO, CALIFORNIA

BOARD OF SUPERVISORS POLICY

Subject: INCIDENT RESPONSE POLICY	Policy Number: A-14	Page Number: 4 of 4
	Originally Adopted: 11/14/2023	Last Revised Date: 11/14/2023

V. RESPONSIBLE DEPARTMENT

Information Technologies

VI. DATES (ADOPTED, REVISED, NEXT REVIEW)

Originally Adopted:	11/14/2023		
Last Revision:	11/14/2023	Next Review:	11/14/2027