Approved by Chris Urbina, Executive Director and Chief Medical Officer, February 2012

SUMMARY

Colorado Department of Public Health and Environment information systems constantly are under attack from a wide range of threats that include both internal and external sources. To prevent, detect and respond to security incidents, the department requires user guidelines for reporting and responding to attacks. This policy sets forth the requirements for maintaining guidelines to ensure all incident response reporting is processed in a timely and effective manner.

POLICY

The department shall maintain incident response procedures and guidance to enable users to identify, report and respond to information security incidents in a timely and coordinated manner.

A security incident is defined as an adverse event caused by either a failure of a security mechanism or an attempted or threatened breach of those mechanisms (e.g., computer hacker system penetrations, shared user IDs, computer viruses, stolen papers, stolen equipment or disks, etc).

Incidents are categorized according to their seriousness. A Level 1 incident may include mitigation for known problems for which the cause and the remedy are well-understood by PC technicians and no sensitive information has been compromised. Removing a known virus from an infected machine would be a Level 1 incident. A Level 2 incident is one in which there is any one of the following:

- a real or potential compromise of a server, PC, laptop, database or papers containing sensitive information
- uncertainty as to the best way to mitigate the potential damage
- suspicion of internal malfeasance
- system reports or logs that indicate an unusual occurrence or possible intrusion

Project managers will ensure their employees understand what to do when presented with a security incident, including reporting procedures.

PROCEDURE

1. **Incident Reporting**
    a. All employees should report immediately to the Office of Information Technology (OIT) Help Desk any viruses or other malicious software found on a workstation. Any **suspected**

virus or suspected malicious software should be reported as well. Do not use email to send a message if you suspect your computer is infected. Call the Help Desk to report the problem.

b. All employees should immediately report any suspected security incident to the Help Desk and to their supervisor. This is required of all employees, regardless of division or program, network or server involved. If the Help Desk line is busy or unmanned during work hours, employees should contact one of the members of the Incident Response Team directly. If it is after hours, the employee should follow any emergency procedure for his/her section, and leave a message on the Help Desk line. See Incident Response Team.

c. OIT technicians should report to the Help Desk any Level 1 incidents. This reporting will enable the department to meet state reporting requirements and estimate the level of malicious software problems at the department.

2. **Incident Response**

a. The Help Desk shall notify the Incident Response Team lead (normally the privacy officer) of a suspected Level 2 incident **immediately**. If the privacy officer is not available, other members of the Incident Response Team will be contacted, starting with the security officer. Then the Help Desk can call any remaining Incident Response Team members.

b. Likewise, if a team member hears about a suspected incident directly, the team member should alert the privacy officer, as team lead, first. Then the team member should notify others in the order above.

c. The Team Lead shall begin to complete an Incident Reporting Form with all known information and give the form to the team lead to complete as the incident is investigated and resolved.

d. The team lead shall call together the members of the Incident Response Team, and direct their efforts to resolve the incident.

e. The team lead shall communicate the status of any Level 2 incidents to the security officer as soon as time permits. The final Incident Response Form shall be submitted to the security officer.

f. The team lead shall communicate back to the person who reported the Level 2 incident with whatever information is appropriate for general dissemination about the incident.

g. The team lead shall recommend what changes should be made to limit similar incidents in the future.

h. Program managers shall ensure all employees report and respond to incidents according to department guidance. Refer to Incident Response Plan to Level 2 Incidents.

i. All employees shall immediately comply with directives from the Incident Response Team regarding steps to control or end the incident. This may include instructions to disconnect the computer from the network, but leave the computer on, or follow through with a particular procedure.

3. Plan Maintenance and Testing

a. The security officer shall maintain and test department incident response procedures and guidance on a periodic basis to ensure the guidance remains effective.

b. The security officer shall amend and maintain the procedures and guidance to address the following critical elements for effective incident response:

i. Incident identification and analysis, including the establishment of normal operations baselines and mechanisms to notify appropriate personnel of deviations from the baseline.

ii. Incident escalation and reporting, including a "calling tree" list of individuals to be contacted and escalation conditions and time frames.

iii. Selecting individuals for and forming an Incident Response Team that will be responsible for the investigation and resolution of the incident, including sufficient communications to all interested parties during and after the investigation. This team should include technical, business, management and, if necessary, legal personnel.

iv. Determining whether a security incident is severe enough to warrant the initiation of the Disaster Recovery Plan.

v. Ensuring steps are taken during the course of the investigation to properly document the incident, process any evidence collected and document all steps taken during the investigation.

vi. Making recommendations based on the results of the investigation to prevent future occurrences of similar incidents.

vii. Performing post-incident analysis, including follow-ups on the implementation of recommendations and determining the effectiveness and efficiency of the incident response process.

4. Compliance

Any employee not complying with this policy and these procedures may be subject to state personnel system progressive disciplinary action. Other non-employees will be disciplined with appropriate action, up to and including termination.

TOOLS/GUIDANCE/STANDARDS

Incident Response Team
Incident Response Plan to Level 2 Incidents
Department Policy 15.6 Reporting Potential Problems
Security Incident Reporting Form

REFERENCE

HIPAA Security Rule, §164.508 (a) (6)(i), Administrative Safeguards, Security Incident Procedures and (ii)(A) Response and Reporting