

# 9400-P190: Reporting Security Events and Vulnerabilities

## I. PURPOSE

This policy establishes requirements for reporting and responding to information security events and vulnerabilities.

Note: This policy deals with cyber (information technology) security and does not address the physical security of facilities or assets. Response to a breach of physical security shall be governed by other policies/procedures as appropriate. If unauthorized physical access to a technology resource leads to unauthorized logical access to state information, multiple reporting policies, including this policy, are applicable.

## II. SCOPE

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to as “agencies”) of the State of Wyoming.

## III. POLICY

As a condition of access to state information resources, all members of the workforce shall report events, suspected incidents, or system vulnerabilities to a supervisor and/or appropriate agency IT staff in a timely manner. Supervisors shall ensure that IT is informed.

Note: This requirement shall NOT be construed in any manner to encourage, authorize, or condone an intentional search for system weaknesses and/or malfunctions. Intentional acts of exploring state information resources to discover weaknesses or malfunctions in security controls by personnel who are not authorized to do so shall be deemed to be malicious and unauthorized hacking.

An event shall be declared a security incident by an agency-identified security and/or technical professional when there is sufficient evidence to indicate that it is adverse to the interests of the agency’s information stewardship and/or meet pre-established criteria for security incident declaration.

Agencies shall respond to all reported events that have the potential to become security incidents.

Agencies shall have a working plan for reporting on, responding to, recovering from, and preventing recurrence of information security incidents. The plan shall be kept up to date and continually improved upon with lessons learned. Procedures to execute the plan shall be repeatable and thorough, yet flexible enough to handle an ever-changing threat environment.

Detailed procedures and contingencies for the implementation of incident response shall be labeled confidential and distributed on a need-to-know basis.

## **9400-P190: Reporting Security Events and Vulnerabilities**

Executives responsible for the impacted agency shall participate in the incident response process.

Personnel tasked with incident response shall be proficient in their specific responsibilities (see Pending Policy 9400-P191: Security Incident Management).

System administrators of state information resources are empowered and expected to terminate communications with internal or external entities operating in a manner injurious to the security and operations of the agency or the state's wide area network (WAN). Administrators shall take measures to stop the threat then perform the required notifications. The appropriate notifications shall be made when time permits on the events and actions taken during the emergency.

**CIO Approved Date: 03/18/2009**