

SAM – INFORMATION SECURITY
(Office of Information Security)

INCIDENT RESPONSE TRAINING
(Revised 12/13)

5340.1

Policy: Each state entity shall provide incident response training to information system users consistent with assigned roles and responsibilities.

Incident response training shall be at an appropriate level for the assigned roles and responsibilities of state entity personnel. For example, regular users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle/remediate incidents; and incident responders may need more specific training on chain of custody, forensics, reporting, system recovery, and restoration. Incident response training shall include, at a minimum, user training in the identification and reporting of suspicious activities, both from external and internal sources.

Implementation Controls: NIST SP 800-53: [Incident Response \(IR\)](#)