

SAM – INFORMATION SECURITY
(Office of Information Security)

INCIDENT HANDLING
(Revised 8/2015)

5340.3

Policy: Each state entity shall implement incident handling for information security and privacy incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Incident handling shall coordinate with business continuity planning activities (SAM section 5325). Incident handling capability shall include procedures for coordination among many groups within a state entity, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and executive management.

If during the recovery and lessons learned phase of an incident, the state entity uncovers a deficiency in their program, the state entity shall take action to prevent reoccurrence and report their action plan through the Plan of Action and Milestone (POAM) process. State entities shall use the standardized POAM reporting instructions and tool ([SIMM 5305-B and SIMM 5305-C, respectively](#))

Implementation Controls: NIST SP 800-53: [Incident Response \(IR\); Plan of Action and Milestones \(SIMM 5305-B and SIMM 5305-C\)](#).