

SAM – INFORMATION SECURITY
(Office of Information Security)

INCIDENT HANDLING
(Revised 12/13)

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.

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