

**SAM – INFORMATION SECURITY
(Office of Information Security)**

INFORMATION SECURITY INCIDENT MANAGEMENT
(Revised 6/14)

5340

Policy: Each state entity must promptly investigate incidents involving loss, theft, damage, misuse of information assets, or improper dissemination of information. All state entities are required to report information security incidents consistent with the security reporting requirements in this policy and manage information security incidents to determine the cause, scope, and impact of incidents to stop unwanted activity, limit loss and damage, and prevent recurrence. Additionally, each state entity shall develop, disseminate, and maintain a formal, documented incident response plan that provides for the timely assembly of appropriate staff that is capable of developing a response to, appropriate reporting about, and successful recovery from a variety of incidents.

Each state entity shall develop documented procedures to facilitate the implementation of the incident response plan and associated incident response controls including, but are not limited to:

1. Immediately reporting suspected and actual security incidents in accordance with the criteria and procedures set forth in [SIMM 5340-A](#) and other applicable laws and regulations;
2. Managing security incident case assignments and the security investigation process in a timely and effective manner;
3. Managing security incidents involving a breach of personal information in accordance with the criteria and procedures set forth in SIMM 5340-C.
4. Mobilizing emergency and third party investigation and response processes if necessary;
5. Consulting with system owners to help quarantine incidents and limit damage;
6. Consulting with Personnel Management if there is a violation of appropriate use policy; and
7. Communicating with law enforcement when actual or suspected criminal activity is involved.

Implementation Controls: NIST SP 800-53: [Incident Response \(IR\)](#); [SIMM 5340-A](#); SIMM 5340-C