

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

**INFORMATION SECURITY MONITORING**  
(Revised 6/14)

**5335**

**Policy:** Each state entity is responsible for continuous monitoring of its networks and other information assets for signs of attack, anomalies, and suspicious or inappropriate activities.

Each state entity shall ensure:

1. An event logging and monitoring strategy which provides for audit trails and auditability of events and appropriate segregation and separation of duties;
2. Event logging and log monitoring are performed with sufficient regularity that signs of attack, anomalies, and suspicious or inappropriate activities are identified and acted upon in a timely manner;
3. Sensors, agents, and security monitoring software are placed at strategic locations throughout the network;
4. Situational awareness information from security monitoring and event correlation tools are monitored to identify events that require investigation and response; and
5. Potential security events are reported immediately to the security incident response team.

**Implementation Controls:** NIST SP 800-53: [Audit and Accountability \(AU\)](#); [Physical and Environmental Protection \(PE\)](#); [Risk Assessment \(RA\)](#)