

STATE of ARIZONA – Government Information Technology Agency

Statewide Information Security and Privacy Office	SISPO Incident Management Policy and Standards P900-E902	TITLE: Executive Checklist Exhibit 2 Effective Date: May 31 , 2011
--	---	---

AUTHORITY

ARS 41-3507 created the Statewide Information Security and Privacy Office (SISPO) and the requirements for the state information security and privacy assurance plan. The assurance plan requires each budget unit to immediately report information security incidents to SISPO and deploy mitigation strategies (ARS 41-3507(E)). Contractor agreements require incident notification to the budget unit. Contractors must collaborate with the budget unit to deploy mitigation strategies until incident closure.

The budget unit chief executive officer (CEO) will ensure development and implementation of agency procedures that address the following components consistent with the SISPO policy and standards:

Policy/Standard Component	Date Implemented	Agency Procedure No.
The CEO designates an information security officer (ISO), privacy officer (APO) and HIPAA privacy officer (HCO), as applicable, the point persons for incident response and coordination. They collaborate together, with management and personnel to safeguard the information technology network/devices and provide for the appropriate use and disclosure of information classified as restricted personal identifying information (RPII), confidential information (CI) and sensitive information (SI) in electronic and non-electronic format or media.		
The budget unit formally adopts the SISPO Policy 900 and its standards for its information security incident management program or the budget unit confirms its existing policies, standards and procedures are consistent with the SISPO 900 policy and standards.		
The budget unit has specific written procedures for prompt identification and response to a data breach by workforce, contractors or other individuals who access the technology network/devices or restricted personal identifying information.		
Workforce receives documented, periodic training consistent with the SISPO Policy 900 and standards. Contractors are trained or verify knowledge consistent with the policy. Workforce and contractors are accountable for compliance with Policy 900 and its standards.		
Contractor agreements provide for incident/breach reporting and response consistent with SISPO Policy (P900) and its standards.		
The CEO and executive leadership receive periodic reports that track and trend incident risk severity and frequency and the success of incident remediation or corrective action.		

Approved by: _____
 Signature of Budget Unit Chief Executive Officer

Date: _____

Printed Name: _____