

STATE of ARIZONA – Government Information Technology Agency

Statewide
Information
Security and
Privacy
Office

**SISPO
POLICY**

P900

**TITLE: Information
Security Incident
Management**

Effective Date: May 31, 2011

1. AUTHORITY

Under the authority of A.R.S. § 41-3507 and Executive Order 2008-10, The Statewide Information Security and Privacy Office (SISPO) is responsible for ensuring development and implementation of risk mitigation strategies by each budget unit to identify threats and vulnerabilities to the confidentiality, integrity and availability of state information and the information technology infrastructure.

2. PURPOSE

This policy requires a budget unit to implement and maintain an effective budget unit enterprise plan for prompt identification, reporting, response, resolution and, as may be required, data breach notification to affected individuals related to an information security incident as defined by this policy.

3. SCOPE

This policy applies to all budget units whose workforce or contractors are authorized to access or use the state information technology infrastructure or who access, use or disclose state information at any location where the activity is performed. State information includes any format or on any medium (e.g. electronic, hardcopy, and records generally as defined by A.R.S. § 41-1350) including oral communications.

4. POLICY

The budget unit shall develop and implement a written incident response framework including governance, policy and procedures approved by the budget unit's Chief Executive Officer (CEO) for the identification, reporting and response to an information security incident by workforce and contractors. The information security incident management framework shall be consistent with SISPO policies, standards and procedures.

4.1. DEFINITIONS

4.1.1. "AZNet" means the contractor for the State of Arizona telecommunications and network.

4.1.2. "Budget unit" means a department, commission, board, institution or other budget unit of the state organization receiving, expending, or disbursing state funds or incurring obligations of the state including the Arizona Board of Regents but excluding the universities under the jurisdiction of the Arizona

Board of Regents, the community college districts and the legislative or judicial branches. A.R.S. § 41-3501(2).

4.1.3. “Chief Executive Officer” (CEO) means the chief executive officer of a budget unit (See also GITA Administrative Rule. R2-18-101(2)).

4.1.4. “Confidential Information” (CI) means information other than Restricted Personal Identifying Information (RPII) that may only be disclosed as permitted or required by state or federal law or administrative rule. Confidential information includes critical business infrastructure information as defined by ARS 41-1801 and critical infrastructure information as defined by the U.S. Department of Homeland Security (6 USC 131; 49 CFR 1520).

4.1.5. “Contractor” means an individual, government entity or non-government business entity providing products or services for a budget unit or on behalf of a budget unit. The term “contractor” includes a “business associate” as defined by HIPAA at 45 CFR 160-103 [insert hyperlink], temporary personnel or other third parties, including subcontractors or other agents utilized by a contractor, that are not part of the budget unit workforce but have access Restricted Personal Identifying Information (RPII), confidential or sensitive information or to the state information technology infrastructure.

4.1.6. “Data Breach” means an information security incident involving (1) unauthorized access of Restricted Personal Identifying Information (RPII) and (2) the unauthorized access poses a substantial risk of financial, reputational or other harm to individuals affected by the incident. (See the Notification of Breach of Security System, the Arizona data breach notification law, ARS 44-7501 and the Health Insurance Portability and Accountability Act (HIPAA) data breach notification standard, 45 CFR Part 164, Subpart D).

4.1.7. “Discovery” means the date and/or time a budget unit or contractor becomes aware of or reasonably believes an information security incident has occurred.

4.1.8. “Information Privacy Incident” means an information security incident resulting in unauthorized access of personal identifying information defined by this policy as Restricted Personal Identifiable Information (RPII), Confidential Information (CI) or Sensitive Information (SI).

4.1.9. “Information Security Incident” or “Incident” means an event, as referenced in ARS 41-3507(E), that a budget unit, a budget unit’s or contractor, or the state reasonably believes has the potential to compromise the confidentiality, integrity, or availability of a RPII, CI or SI or the state information technology infrastructure.

4.1.10. “Restricted Personal Identifying Information” (RPII) means data elements that are a subset of confidential information and create a high severity risk information security incident from unauthorized access. The RPII also may be subject to the Arizona data breach notification law (ARS 44-7501) or HIPAA data breach notification standard (45 CFR Part 164, Subpart D). The data elements defined as RPII by this policy are:

- (a) An individual's first name or first initial and last name in combination with any one or more of the following data elements for the individual, when the data element is not encrypted, redacted or secured by any other method rendering the information unreadable, unusable or undecipherable:
 - Social security number
 - Driver license number
 - Non-operating identification license number
 - Financial account number, credit card number, debit card number, or charge card account number
 - Financial account number, credit, debit, or charge card account number in combination with computer access information as defined by ARS 13-2301(E)(2), including any security code, access code, biometric identifier or record, password or user ID for access to any electronic file or account

- (b) “Protected Health Information” (PHI) as defined by the Privacy Rule of the Health Insurance Portability and Accountability Act or 19961 (HIPAA) as maintained by a budget unit that must comply with HIPAA.ⁱ

4.1.11. “Sensitive Information” (SI) means personal identifying information or other categories of information that if disclosed are reasonably likely to adversely affect the best interest of the state or the best interest of an individual. SI may include personal identifying information as discussed in the Arizona statute Government Anti-Identification Procedures (ARS 41-4171 and 41-4172) when such information is not otherwise defined as “restricted personal identifying information” or “confidential information.

4.1.12. ”Unauthorized Access” means to access, acquire, use, disclose, view, exchange, transmit, maintain, retain, modify, store, record, dispose of or destroy RPII, CI or SI without authority, in excess of authority or with the intent to compromise the confidentiality of the information. Unauthorized Access includes the loss or other unauthorized access of a device, technology component or record containing RPII, CI or SI or the destruction/disposal of records that does not comply with the Arizona Record Destruction law, ARS 44-7601.

4.2. INFORMATION SECURITY INCIDENT FRAMEWORK

4.2.1. Each budget unit Chief Executive Officer (CEO), in compliance with Executive Order 2008-10, will appoint an Information Security Officer (ISO) and an Agency Privacy Officer (APO) with qualifications to coordinate and facilitate implementation of the budget unit's information security incident management framework.

- (a) If the budget unit must comply with the Health Insurance Portability and Accountability Act (HIPAA), the CEO shall also appoint a HIPAA Compliance Officer (HCO) with qualifications to facilitate and coordinate management of an information security incident that involves the privacy and security of "protected health information" as defined by the HIPAA Privacy Rule at 45 CFR 164.501 (see also 45 CFR 160.103).
- (b) The ISO, APO and HCO shall also collaborate with the Statewide Information Security and Privacy Office (SISPO), the State Information Protection Center (SIPC) and the state telecommunications/network contractor for incident identification and management (AzNet).
- (c) The CEO will signify implementation of this policy and its standards by completion of the Executive Checklist (Exhibit 2).

4.2.2. Each budget unit shall promptly report incidents and participate in the SISPO online incident report and response (IRR) system as required by the SISPO Incident Submission and Response Standard, P900-S905.

4.2.3. Workforce shall receive training at or near time of hire and periodically thereafter on incident management requirements consistent with this policy and standards for the safeguard of RPII, CI and SI and the protection of the information technology infrastructure. It is recommended that annual training be provided on safeguarding of RPII. Individuals other than employees (e.g. interns, students, temporary workers, should receive training at or near the first assignment of duties for the budget unit.

4.2.4. A data exchange/use agreement following GITA Classification and Categorization of Data Standard, P740-S741, shall be used for all contracts and agreements, including purchase orders that involve the exchange/use of RPII, CI or SI. The data exchange/use agreement shall identify what data elements of RPII, CI or SI will be exchanged/used and the safeguards employed to protect the information from unauthorized access. The data exchange/use agreement will also address the contractor's responsibility to:

- (a) Promptly identify an information security incident and fully collaborate with the budget unit until closure of the incident by the budget unit and SISPO.
- (b) Provide the budget unit with the specific contact information for communication between the budget unit and the third party related to an information security incident.

4.2.5. A budget unit shall develop and implement an information security framework using methodologies consistent with this policy, the Incident Submission and Response Standard, P900-S905, and the Data Breach Notification Standard, P900-S910, which provide for tracking and trending of incidents by type of incident, severity category, root cause and success of remediation to prevent further similar incidents.

- (a) Executive leadership shall review budget unit incident trends and effectiveness of risk reduction methodologies at least once a year and as part of its strategic plan process. Incident trends will be reviewed more frequently depending on the severity of the incidents (e.g. data breach) and similar types of incident that re-occur.
- (b) There shall be written evidence of incident-trend review and changes of information security and privacy risk strategies by the budget unit.

4.3. INCIDENT SUBMISSION AND RESPONSE

4.3.1. A budget unit shall establish a written process for the prompt identification, reporting, investigation and mitigation of an information security incident consistent with the GITA SISPO Incident Submission and Response Standard, P900-S905.

4.3.2. The severity of information security incidents, including privacy incidents, shall be categorized using the severity levels of “high”, “medium” and “low” as defined by the Incident Submission and Response Standard, P900-S905, section 4.3.

4.3.3. An information security incident shall be reported in a timely manner by a budget unit according to the risk severity of the incident consistent with the Incident Submission and Response Standard, P900-S905, section 4.3.

4.3.4. A budget unit that receives a high severity alert from AZNet, SIPC or SISPO will maintain direct collaboration (i.e. email or telephone) with AZNet, SIPC and SISPO until the immediate threat or vulnerability is

mitigated when the incident has the potential to require a temporary suspension of the budget unit's network operating infrastructure.ⁱⁱ

4.3.5. The budget unit shall establish an incident response team for response and resolution of a high severity incident. To the extent the resources are available, it is recommended that the team include:

- (a) Representatives from the affected program(s),
- (b) Agency Public Information Officer,
- (c) Legal counsel,
- (d) Human Resources (as applicable to the incident),
- (e) Law enforcement if a crime is indicated by the nature of the incident (e.g. theft of RPII, CI or SI or a device that contains such information),
- (f) Agency procurement officer and/or State Procurement Office if incident involves a contractor,
- (g) Agency risk management officer and/or State Risk Management Office if high severity incidents including incidents that involve a crime,
- (h) Others as may be identified by the budget unit on a need to know basis for resolution of the incident.

4.3.6. The status of incident resolution will be updated as required by the Incident Submission and Response Standard, P900-S905.

4.3.7. Incidents will be resolved as soon as possible and **within 60 days** after incident discovery unless a delay is required because of a criminal investigation or other complicating factors (see Incident Submission and Response Standard, section 4.10).

4.3.8. The budget unit shall promptly notify contractors who are not involved with the incident but whose business operations or technology infrastructure may be impacted by the information security incident.

4.4. DATA BREACH NOTIFICATION

4.4.1. The information security incident framework will include written process for prompt identification of an incident that involves unauthorized access to RPII and the potential for that incident to become a data breach.

- (a) A risk assessment will be used to determine if a data breach is reasonably likely to have occurred and if the budget unit must notify affected individuals (see SISPO Data Breach Notification Standard, P900-S910).

- (b) At its option for the best interest of the state, a budget unit may conduct a risk assessment when a high severity incident involves Confidential Information (CI) or Sensitive Information (SI). The risk assessment will guide the budget unit on response to the incident when significant risk of harm exists to individuals whose information confidentiality has been compromised as a result of the incident.

4.4.2. A budget unit defined as a “covered entity” by HIPAA will incorporate data breach notification requirements for the Health Insurance Portability and Accountability Act (HIPAA) into its incident management framework. (45 CFR Part 164, Subpart D). See the SISPO Data Breach Notification Standard, P900-S910, Appendix A.

4.4.3. Information security incidents that involve a data breach will be updated and closed consistent with the Incident Submission and Response Standard, section 4.10.

4.4.4. The incident management framework will include compliance with data breach notification requirements of other federal law, regulations or industry standards, as may be applicable to the budget unit.iii

5. CORRECTIVE ACTION AND ENFORCEMENT

5.1. Corrective Action. For high and medium severity incidents, the budget unit shall conduct and document a root-cause analysis or comparable method of analysis to identify the seminal cause of the information security incident or a data breach. The cause of low severity incidents shall also be identified. A root-cause analysis shall be conducted on low severity incidents that show a trend of re-occurrence or change to a higher severity.

5.2. Enforcement. A budget unit will develop methods for ensuring that workforce and contractors understand and meet their responsibility to safeguard RPII, CI or SI and the state information infrastructure consistent with this policy, related standards and exhibits.

6. RETENTION OF RECORDS

The budget unit shall retain records related to non-HIPAA information security and/or privacy incidents for a period of three (3) years after incident closure. For HIPAA related incidents, records shall be retained after closure for a period of six (6) years and consistent with the Arizona State Library, Archives and Public Records “*General Retention Schedule for State Agencies, Management Records*”, Item #15, Schedule Number 000-09-154 (<http://www.lib.az.us/records/pdf/State%20-%20management.pdf>).

7. AUTHORITIES

- ARS 41-3507 – Duties, Statewide Information Security and Privacy Office
- EO 2008-10 – Executive Order, Mitigating Cyber Threats
- ARS 41-3504 – Powers and Duties of the Agency
- ARS 13-2301(E)(2) – Computer Tampering
- ARS 41-770 – Causes for Dismissal or Discipline
- ARS 41-1350 – Definition of Records
- ARS 44-7501 – Notification of Breach of Security System (AZ Data Breach Law)
- Arizona Administrative Code, Title 2, Chapter 5, Department of Administration, Personnel Administration
- 45 CFR Parts 160, 162 and 164 – Rules for the Health Insurance Portability and Accountability Act of 1996
- GITA Statewide Policy P740-S741, Classification and Categorization of Data Standard

ⁱ References to HIPAA mean the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) as amended by the American Recovery and Reinvestment Act of 2009 (Pub. L No. 111-5) (the “HITECH Act”) any associated regulations and the federal regulations published at 45 CFR Parts 160 and 164 (collectively referred to as “HIPAA”).

ⁱⁱ Delegation of authority by GITA/SISPO to AZNet for implementation of ARS 41-3507(D) is pursuant to GITA – ADOA Memorandum of Understanding: AZNet Critical Incident – Temporary Shutdown of State Network Infrastructure Services Criteria, dated October 27, 2009.

ⁱⁱⁱ Examples of such laws, regulations or industry standards include but are not limited to the Federal Trade Commission Health Breach Notification Rules (a breach of unsecured Personal Health Records, as required by 16 CFR 318), the Payment Card Industry (PCI) Data Standards (protection of payment card information) and the Financial Services Modernization Act of 1999 (also known as the “Gramm Leach Bliley Act” which safeguards financial information held by “financial institutions” as defined by Act).