"APO" means the Agency Privacy Officer who is generally designated by the budget unit CEO to facilitate adoption of privacy safeguards and compliance for all personal identifying information acquired, used, disclosed or maintained by the agency. The APO works collaboratively with the HIPAA Compliance Officer (as applicable), the ISO and the SISPO to adopt and carry out the provisions of the SISPO Information Security Incident Management Policy (P900) and its standards (S905 and S910). The APO will generally oversee the response to information security incident that poses a risk of a data breach.

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

"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).

"Chief Executive Officer" (CEO) means the chief executive officer of a budget unit (See also GITA Administrative Rule. R2-18-101(2)). "Critical Business Infrastructure Information" (CBII) that relates to systems or technology infrastructure which enables a budget unit to provide vital services, exercise civil authority, maintain the safety and well being of citizens, or sustains the industrial or economic base of the State or the nation during an emergency. CBII includes critical information infrastructure as defined by A.R.S. § 41-1801.

"CISO" means Chief Information Security Officer for the State of Arizona appointed by authority of A.R.S. § 41-3507(B) to manage the statewide information security and privacy office, or the CISO's designee to act on behalf of the CISO.

"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. Confidential information includes critical business infrastructure information as defined by ARS 41-1801 [insert hyperlink] and critical infrastructure information as defined by the U.S. Department of Homeland Security (6 USC 131; 49 CFR 1520).

"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 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.

"CPO" means the Chief Privacy Officer and HIPAA Coordinator for the State of Arizona established by the CISO under the authority of A.R.S. § 41-3507(B) to support the CISO to develop, implement and maintain a statewide privacy plan for SISPO and act as the designee for the CISO.

"Covered Entity" means a heath care provider who transmits any PHI in electronic form in connection with a HIPAA defined transaction, a health plan or health care clearing house as defined by HIPAA (45 CFR 160.103), including a budget unit or a component of a budget unit that performs functions defined by HIPAA as a covered entity or covered component.

"Critical Alert Notification" means an information security incident identified by AzNET that poses a high probability of risk to the technology infrastructure of a budget unit and/or the State involving the following types of events: (a) cyber-crime, evidence of identity theft and/or unauthorized destruction of system files, data content, format and/or information; (b) compromised data/information such as a data breach of Restricted Personal Identifying Information (RPII), (c) a denial of services attack; or (d) an event that impacts the sustainable use of critical business technology infrastructure or information.

"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).

"Discovery" means the date and/or time an agency or contractor becomes aware of or reasonably believes an information security incident has occurred.

"DHHS" means the federal Department of Health and Human Services which oversees implementation of the HIPAA regulations applicable to health care providers that conduct electronic health care transactions, health plans and health care clearinghouses (i.e. also called "covered entities"). The department enforces the HIPAA regulations applicable to covered entities.

"HCO" means a HIPAA Compliance Officer designated by the budget unit CEO to develop, implement and maintain privacy and/or security compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Provisions, its amendments and regulations. The HCO works collaboratively with the budget unit ISO, APO and SISPO for incident identification, reporting and resolution.

"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).

"IRR System" means the electronic Incident Reporting and Response System and data base administered by the State Information Security and Privacy Office (SISPO) for the submission, management and trending of state information security incidents.

"Information Security Incident" or "Incident" means an event as referenced in ARS 41-3507(E) which a budget unit, a budget unit's business partner 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.

"ISO" means the Information Security Officer generally designated by the budget unit CEO to facilitate information security technology compliance and adoption of the Information Security Incident Management Policy (P900) and its standards (S905 and S910). The ISO works collaboratively with the Agency Privacy Officer and/or the HIPAA Compliance Officer (as applicable), the Statewide Information Security and Privacy Office (SISPO), the Arizona Department of Administration State Information Protection Center (SIPC) and AZNet for incident management and prevention.

"Non-critical Incident" means an incident identified by AzNET that requires investigation and response to AzNET by the budget unit as soon as possible confirming whether suspicious cyber activity identified by AzNET is an actual or potential reportable incident and not a false positive activity occurring at the budget unit.

"Possible Non-essential Network Traffic" means an AzNET identified cyber activity that is referred to SIPC for email notification to an involved agency or agencies to determine if it is a non-incident or an activity that after investigation is determined to be a non-critical reportable incident.

"Protected Health Information" or "PHI" means individually identifiable health information (45 CFR 160.103) including demographic information that is created or received from an individual by a HIPAA covered entity or component that is:

(a) Transmitted or maintained in electronic media or in any other form or media;
(b) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
(c) Identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.

"Restricted Personal Identifying Information" (RPII) means data elements that are a subset of confidential information and create a high 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 SISPO Information Security Incident Management Policy (P900) 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's 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 an agency that must comply with HIPAA.

"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.

"SIPC" means State Information Protection Center.

"SISPO" means Statewide Information Security and Privacy Office as enacted by A.R.S. § 41-3507(A) and a unit of the Arizona Government Information Technology Agency.

"Temporary Suspension of State Information Infrastructure" means steps taken by AzNET under a delegated statutory authority granted by SISPO under ARS 41-3507(D) [insert hyperlink][1] in response to a critical incident to shut down any part of the state information technology system that is owned, leased, outsourced or shared in order to isolate the source of, or stop the spread of, an information security/privacy data breach or other similar incident. A budget unit shall comply with directives to temporarily discontinue or suspend operations of information infrastructure within time frames required by SISPO policy.

"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.

"Workforce" or “workforce member” means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. Workforce does not include individuals who are “business associates” as defined by HIPAA, contractors or business partners.