

Statewide  
Information  
Security and  
Privacy  
Office

**SISPO**  
**Incident Management Policy and  
Standards**

**TITLE: Data Classification  
Matrix<sup>i</sup>**

**Exhibit 1**

**Effective Date: May 31, 2011**

**RESTRICTED PERSONAL IDENTIFYING INFORMATION**

“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 types of information listed in the table as RPII is a minimum standard. Agencies may classify other types of hardcopy or electronic information as RPII. Agencies will maintain a data classification system to identify and safeguard RPII acquired, used, disclosed, or retained by the agency. Please refer to the GITA Classification and Categorization of Data Standard, P740, S741 for additional information.

For public records requests of this information, seek advice from legal counsel on how to protect the information and respond to the request.

<b>RPII--Types of Information</b>	<b>Expected Access Control</b>	<b>Disclosure and Legal Considerations</b>
<p><b>First Name or Initial and Last Name</b> when combined with any one or more of the following for that individual:</p> <ul style="list-style-type: none"> <li>• Social Security Number</li> <li>• Driver’s License Number</li> <li>• Non-operating identification license number</li> <li>• Financial account number, credit card number, debit card number, charge card number or other transaction account number</li> <li>• Financial, credit, debit, or charge card account number in combination with computer access</li> </ul>	<p><u>Digital Records:</u></p> <ul style="list-style-type: none"> <li>• Encrypt in transit</li> <li>• Encrypt on mobile devices</li> <li>• Defense in Depth or Encryption at rest</li> <li>• Access through a secure portal</li> </ul> <p><u>Hardcopy Records:</u></p>	<p>Meets the definition of “personal information” from the Arizona Notification of Breach of Security System law (aka: Arizona Data Breach Law) ARS 44-7501 and definition for ARS 44-7601, required destruction for hardcopy records.</p> <p>Financial accounts take many forms. They include but are not limited to: retirement accounts, accounts for securities, security entitlement account, depository account, online banking</p>

RPII--Types of Information	Expected Access Control	Disclosure and Legal Considerations
<p>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</p>	<ul style="list-style-type: none"> <li>• “Need to know/ minimum necessary access” only as approved by management and policy</li> <li>• Maintain in a locked, restricted file area at any work location</li> <li>• Redact or destroy information prior to disclosure unless legal counsel advises to disclose the information</li> <li>• Not recommended for virtual office or telework</li> </ul>	<p>accounts and transaction accounts.</p> <p>Computer access information also includes but is not limited to: electronic serial number, personal identification number (PIN), an access device to an account; information used by an individual to establish access to an account if such information is retained for authentication purposes or password resets (e.g. date of birth or mother’s maiden name in combination with response to a security question, or similar information)</p>
<b>Protected Health Information<sup>ii</sup>:</b>		
<p>The following is the list of identifiers which together or individually must be safeguarded from unauthorized access (See the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rules (45 CFR 164.514(a)(2)(i) and (ii))</p> <ol style="list-style-type: none"> <li>1. Names (e.g. family, friends or other individuals involved with the care or payment of care regarding the individual)</li> <li>2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent</li> </ol>	<p><u>Digital Records:</u></p> <ul style="list-style-type: none"> <li>• Encrypt in transit</li> <li>• Encrypt on mobile devices</li> <li>• Defense in Depth or Encryption at rest</li> <li>• Access through a secure portal</li> </ul> <p><u>Hardcopy Records:</u></p> <ul style="list-style-type: none"> <li>• “Need to know/</li> </ul>	<p><b>Protected Health Information</b> is individually identifiable health information related to the past, present and future health care or payment of health care of an individual as defined by the HIPAA Privacy Rule 45 CFR 164.501; see also 45 CFR 160.103. Categories of individually identifiable health information are listed in items 1-18, below.</p> <p>The data elements in items 1-18 individually or in combination must be safeguarded by agencies (i.e. called “covered entities”) that comply with the HIPAA privacy and security regulations. If the</p>

<b>RPII--Types of Information</b>	<b>Expected Access Control</b>	<b>Disclosure and Legal Considerations</b>
<p>geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census</p> <ol style="list-style-type: none"> <li>3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older</li> <li>4. Telephone Numbers</li> <li>5. Fax Numbers</li> <li>6. Electronic Mail Addresses</li> <li>7. Social Security Numbers</li> <li>8. Medical Record Numbers</li> <li>9. Health Plan Beneficiary Numbers</li> <li>10. Account Numbers</li> <li>11. Certificate/License Numbers</li> <li>12. Vehicle Identifiers and Serial Numbers, including License Plate Numbers</li> <li>13. Device Identifiers and Serial Numbers</li> <li>14. Web Universal Resource Locators (URLs)</li> <li>15. Internet Protocol (IP) Address Numbers</li> <li>16. Biometric Identifiers, including Finger and Voice Prints</li> <li>17. Full Face Photographic Images and any Comparable Images</li> <li>18. Any other unique identifying number, characteristic, or code that could reasonably be used to identify the individual</li> </ol>	<p>minimum necessary access” only as approved by management and policy</p> <ul style="list-style-type: none"> <li>• Maintain in a locked, restricted file area at any work location</li> <li>• Redact or destroy information prior to disclosure unless legal counsel advises to disclose the information</li> <li>• Not recommended for virtual office or telework</li> </ul>	<p>data element(s) is(are) not encrypted, de-identified, destroyed or otherwise rendered unreadable, unusable or undecipherable an unauthorized access occurs, the agency may need to notify individuals and DHHS of the breach.</p>

**CONFIDENTIAL INFORMATION**

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). Unauthorized access to CI creates an information security incident that must be reported to SISPO.

The types of information listed in the table below are examples of CI made confidential by Arizona statute. For additional guidance, please refer to the Arizona Attorney General, *Arizona Agency Handbook, Chapter 6: Public Records, Appendices 6.1 and 6.1.2: Records Made Confidential/Non-Disclosable by Arizona Statute*, 2001. Agencies will maintain a data classification system to identify and safeguard CI as may be acquired, used, disclosed, used or retained by the agency. Please refer to the GITA Classification and Categorization of Data Standard, P740, S741 for additional information.

For public records requests of this information, seek advice from legal counsel on how to protect the information and respond to the request.

CI - Types of Information	Recommended Access Control	Disclosure and Legal Considerations
<p>Computer Access Information: Includes a card, token, code, account number, electronic serial number, mobile or personal identification number, password, encryption key, biometric identifier, remote identification codes, other electronic identifier or other means of account access, including a canceled or revoked access device information</p>	<p><u>Digital Records:</u></p> <ul style="list-style-type: none"> <li>• Encrypt at rest and in transit</li> <li>• Access through a secure portal</li> <li>• No ability to download or print on <u>personal</u> devices at any designated worksite (e.g. agency location or telework/virtual office site)</li> </ul> <p><u>Hardcopy Records:</u></p>	<p>See also the Arizona Computer Tampering Law, ARS 13-2301(E)(2)</p>

CI - Types of Information	Recommended Access Control	Disclosure and Legal Considerations
	<ul style="list-style-type: none"> <li>• “Need to know/ minimum necessary access” only as approved by management and policy</li> <li>• Maintain in a locked, restricted file area at any work location</li> <li>• Redact or destroy information prior to disclosure unless legal counsel advises to disclose the information</li> <li>• Not recommended for virtual office or telework</li> </ul>	
<p>Proprietary or Confidential Computer Security Information:</p> <p>Includes access devices, security practices, methods and systems; architecture; communications facilities; encryption methods; and system vulnerabilities for a specific computer, computer system or computer network.</p> <p>Applies to information technology network or pathway diagrams, network asset information related to computer or network security, IP addresses or other information that can be used to identify a system or to enter an access point</p>	<p>As above</p>	<p>See the Arizona Computer Tampering Law, ARS 13-2301(E)(13).</p> <p>Does <u>not</u> include information made available to the public by an owner or operator of the computer, computer system or computer network.</p>

CI - Types of Information	Recommended Access Control	Disclosure and Legal Considerations
without authority or in excess of authority		
<p>Critical Infrastructure Information: Includes infrastructure diagrams and related information for systems and assets, virtual or physical, which are vital to the state or the nation for security, economic security, public health, welfare or safety.</p>	As above	See also ARS 41-1801, Critical Infrastructure Information System. Applies primarily to the Department of Public Safety (DPS) but other agencies may also be have related information. 6 USC 131. Includes information not usually public and related to the security of critical infrastructure or protected systems.
Information security assessments or risk audits		See ARS 13-2301(E) and ARS 39-129, Federal Risk Assessment for Critical Infrastructure
Investigations of privacy and security incidents		Best interest of the state. Contact SISPO if disclosure occurs or a request for information occurs. Contact agency counsel for public records request of this information.
GITA records containing confidential information obtained from budget units		See ARS 41-3504(A)(9).
<p>Behavioral/health/medical Information: Includes communicable disease, genetic information, blood type, public health information confidential by law, employee health information, occupational health information, Family Medical Leave Act (FMLA) information, and health care payment records</p>		<p>Access to this information is controlled by law.</p> <p>See ARS 12-2291 et seq, Medical Record Confidentiality; ARS 36-509, Mental Health Records Confidentiality; ARS 36-664 – 36-667, Communicable Disease Information; and ARS 12-2802, Genetic Testing Results. Please refer to the Arizona Attorney General’s Office Agency Handbook, Chapter 6, Appendices 6.1 &amp; 6.2 for additional laws that apply. Federal laws also control access to this information (e.g. Alcohol and Drug Abuse information confidentiality, 42 CFR Part 2). See also the AGO Agency Handbook</p>
Vital Records Certificates (e.g. birth and death)		ARS 36-342 prohibits disclosure except as permitted by the State Registrar
Eligible Person Information – home address, home		ARS 39-123 and 39-124 -- “Eligible Persons” are

CI - Types of Information	Recommended Access Control	Disclosure and Legal Considerations
telephone number and, for law enforcement, photographs in certain circumstances		law enforcement, criminal justice and individuals who are victims of domestic violence or protected by a court order against harassment or other violent acts. Information is not a public record.
Attorney-client and other privileged communications	As above	See the AGO Agency Handbook
Auditor General special research request working papers and audit files		See ARS 41-1279.05, Confidential Records of Auditor General.  Recipients of record copies may not redisclose. These records are not a public record.
Requests for Attorney General Opinions		See ARS 38-507
Personnel Records access except as permitted by R-2-5-501 (1) Employee name (2) Date of employment (3) Current and previous class titles and dates received (4) Name and location of current and previous agencies to which employee is/was assigned (5) Current and previous salaries and dates of each change (6) Name of employee's current or last supervisor (7) Disciplinary records as required by Arizona law		See ARS 39-128 for disclosure of employee disciplinary records for a public body.  See also behavioral/health/medical information.
Personal Information obtained for state use (e.g. personnel applications or other purposes of identification): Includes full date of birth, physical description, ethnic origin, information protected by the Arizona		See ARS Title 41, Chapter 9, Articles 3 and 4 (ARS 41-1441, et seq; ARS 41-1461) and the federal Privacy Act. See also the AGO Agency Handbook

CI - Types of Information	Recommended Access Control	Disclosure and Legal Considerations
and federal disability laws, marital status, religion, sexual orientation/gender, employee home address and telephone number, personal history information, mother's maiden name		
Photograph of Individual (usually facial)	As above	May be SI if the individual did not receive assurances from the agency at time of collection by the agency that the information was confidential
Criminal History Information		See ARS 41-1750 and the AGO Agency Handbook.
Finger print records and images		Multiple laws. See AGO Agency Handbook. Includes workforce and customers
Immigration information (Visa, passport, refugee travel documents, including photographs)		U.S. and other countries
Employment authorization documents		Includes: I-9 status, Visas, Permanent Resident card (e.g. green card)
Citizenship records such as U.S. naturalization forms		
Procurement Information such as bids or solicitations prior to public issuance		See the AGO Agency Handbook. Contact the State Procurement Office or your agency procurement office for additional guidance on confidential information related to procurement activities.
Family Educational Rights and Privacy Act (FERPA) information is CI <u>except "directory information"</u> : name, address, telephone number, university email address, campus card photo, data and place of birth, major fields of study, participation in official activities and sports, dates of attendance/enrollment verification, degrees and awards received and institution most recently/previously attended.		See 20 USC 1232(g) and 34 CFR Part 99. An individual may request that the excepted information <u>not</u> be disclosed
Taxpayer Information, including tax identification number (Other than SSN)		See the AGO Agency Handbook  If an SSN is used for any identification number,

<b>CI - Types of Information</b>	<b>Recommended Access Control</b>	<b>Disclosure and Legal Considerations</b>
		the number is classified as CI. If the SSN is combined with the individual's name, the number is classified as RPII
Trade Secrets and other Intellectual Property	As above	See the AGO Agency Handbook
Other Information classified as confidential information by statute or rule or as designated by the agency		See the AGO Agency Handbook

### SENSITIVE INFORMATION

“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. Unauthorized access to information defined by an agency as SI creates an information security incident that must be reported to SISPO.

The types of information listed in the table below are examples of SI. The definition of what information is sensitive information is generally agency specific. The category of “sensitive information” should be included in the agency’s data classification system. Please refer to the GITA Classification and Categorization of Data Standard, P740, S741 for additional information.

For public records requests of this information, seek advice from legal counsel on how to safeguard the information but respond to the request.

SI--Types of Information	Recommended Access Control	Disclosure and Legal Considerations
Signatures: any copy of likeness of the original “wet” signature	<p><u>Digital Records:</u></p> <ul style="list-style-type: none"> <li>• Encrypt at rest and in transit</li> <li>• Access through a secure portal</li> <li>• No ability to download or print on <u>personal</u> devices at any designated worksite (e.g. agency location or telework/virtual office site)</li> </ul> <p><u>Hardcopy Records:</u></p> <ul style="list-style-type: none"> <li>• “Need to know/ minimum necessary</li> </ul>	See ARS 41-4171, 41-4172, ARS 13-2001. Best interest of the state or an individual should be considered. Is the signature, if access without authorization, be used for an unauthorized or illegal purpose.

SI--Types of Information	Recommended Access Control	Disclosure and Legal Considerations
	<p>access” only as approved by management and policy</p> <ul style="list-style-type: none"> <li>• Maintain in a locked, restricted file area at any work location</li> <li>• Redact or destroy information prior to disclosure unless legal counsel advises to disclose the information</li> <li>• Not recommended for virtual office or telework</li> </ul>	
<p>Identification Numbers (other than SSN, DL or NOL): Professional License Number Employee Identification Number (EIN) Student Identification Number (FERPA) Military Identification Number</p>	<p>As above</p>	<p>See ARS 41-4171, 41-4172, ARS 13-2001. If an SSN is used for any identification number, the number is classified as CI. If the SSN is combined with the individual’s name, the number is classified as RPII.</p>
<p>Tax Identification Number (other than SSN)</p>		<p>May also be CI depending on the agency and purpose of use.</p>
<p>Photograph of Individual (usually facial)</p>		<p>May also be CI if acquired from the individual and the individual received assurances that the photograph would be treated as confidential information</p>
<p>Business Entity Information combined in the following manner: The entity's name, address, telephone number, employer identification number, account number</p>		<p>As defined by ARS 41-4171, 41-4172 and 13-2001(4)</p>

SI--Types of Information	Recommended Access Control	Disclosure and Legal Considerations
or electronic serial number, the identifying number of the entity's depository account or any other information or data that is unique to, assigned to or belongs to the entity <b>and</b> that is intended to be used to access services, funds or benefits of any kind that the entity owns or to which the entity is entitled		
Other information classified as sensitive information by the agency	As above	See GITA Classification and Categorization of Data Standard, P740, S741

**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 39-123 – Information Identifying Eligible Individuals (Protection of certain information for law enforcement officers and victims of harassment/domestic violence)
- ARS 44-7501 – Notification of Breach of Security System (AZ Data Breach Law)
- ARS 44-1373, 44-1373.01 and 44-1373.02 – Restricted Use of Personal Identifying Information (Restricted Use of Social Security Numbers)
- ARS 44-1698 – Security Freeze on Credit Reports and Credit Scores
- ARS 44-4171 and 44-4172 (ARS 13-2001) – Government Anti-Identification Procedures (Protection of certain personal identifying information)
- Arizona Administrative Code, Title 2, Chapter 5, Department of Administration, Personnel Administration

Arizona Attorney General, *Arizona Agency Handbook, Chapter 6: Public Records, Appendices 6.1 and 6.1.2: Records Made Confidential/Non-Disclosable by Arizona Statute*, 2001.

---

<sup>1</sup> The Data Classification Matrix is a guide for an Arizona state agency to identify the types of information that pose varying levels of harm to individuals and risk of resources or credibility to the state when unauthorized access occurs to the information. The Statewide Information Security and Privacy Office developed the term Restricted Personal Identifying Information (RPII) to emphasize what information requires the highest level of safeguards by an agency against unauthorized access and a data breach. The Data

---

Classification Matrix, however, does not limit or otherwise restrict access to information as permitted by Title 39 of the Arizona Revised Statutes (e.g. public record disclosure laws).

<sup>ii</sup> PHI must be safeguarded by a HIPAA “covered entity” from unauthorized disclosure unless encrypted, deidentified or destroyed or otherwise rendered unreadable, unusable or undecipherable as defined by the HIPAA Privacy Rule at [insert citation from breach notification rule]. See also 45 CFR 164.514(a)(2)(i) and (ii) for further information on de-identification of PHI or the use of a limited data set 45 CFR 164.514.