

1. **AUTHORITY**

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) (A.R.S. § 41-3504(A (1))) including the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a)))). The Statewide Information Security and Privacy Office shall serve as the strategic planning, facilitation and coordination office for information technology security in the state (A.R.S. § 41-3507(A)).

2. **PURPOSE**

This standard defines budget unit responsibilities for responding to and reporting cyber attacks and for sharing information related to potential incidents or threats with the State's Information Protection Center (SIPC).

3. **SCOPE**

This applies to all budget units. Budget unit is defined as a department, commission, board, institution or other agency of the state 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).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each budget unit.

4. **STANDARD**

To secure and protect the State of Arizona's critical IT business processes and assets from cyber-crime or cyber-terrorism, budget units shall report all cyber intrusions to the Statewide Information Protection Center (SIPC).

4.1. **CYBER INTRUSIONS**: Budget units shall report any of the following acts by any person who, **without authority** or **acting in excess of authority**:

- Accesses an IT device (server, storage, or client) or network with the intent to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or network.
- Accesses, alters, damages, or destroys any IT device, network, or any physically or logically connected IT devices.
- Accesses, alters, damages, or destroys any computer application systems, programs, or data.

- Recklessly disrupts or causes the disruption of any services provided through the use of any IT device or network.
 - Denies or causes the denial of IT-related services to any authorized user of those services.
 - Recklessly uses an IT device or network to engage in a scheme or course of conduct that is directed toward another person and that seriously alarms, torments, threatens, or terrorizes the person.
 - Prevents a computer user from exiting an Internet, Intranet, or internal host site, computer system, or network-connected location in order to compel the user's computer to continue communicating with, connecting to, or displaying the content of the service, site, or system.
 - Knowingly obtains any information that is required by law to be kept confidential or any records that are not classified as public records by accessing an IT device or network that is operated by the State, a political subdivision of the State, or a medical institution.
 - Introduces a computer-related contaminant (e.g., malicious code, virus, worm, etc.) into any IT device or network.
 - Makes multiple attempts to access an IT device or network system within a brief period of time.
- 4.2. CYBER INTRUSION REPORTING – The budget unit shall notify SIPC within one hour of a penetrated intrusion that has either created a cyber-crime of identity theft, compromised data/information, destruction of system files, and/or denial of services.
- The following information, at a minimum, is required when reporting intrusions to SIPC:
 - a. Budget unit name;
 - b. The budget unit SIPC Coordinator's name and phone number; and
 - c. Brief description of intrusion and damages (real or anticipated).
 - Whenever possible, the budget unit should capture and maintain log entries for a minimum of one week following the detection of intrusion (or longer at the discretion of the application or system owner). Log entries provide significant detail that can be used for investigation and prosecution of the intruder.
- 4.3. SIPC INCIDENT REPORT – After notifying SIPC of the intrusion, the budget unit shall complete a SIPC Incident Report (see Attachment A) available from <http://www.azdoa.gov/isd/ais/state-infrastructure-protection-center>. The budget unit representative completing the report should provide as much detail as possible in the comments fields and annotate the description of the intrusion with explanatory remarks. As more information becomes available or the situation changes, the budget unit shall revise and re-submit the incident report to SIPC with a clear date-time stamp.
- 4.4. SIPC ACTIVITY – Depending on the reported damage from the intrusion, SIPC will be in constant contact with the SIPC Coordinator or designee at the affected

budget unit, GITA, the Department of Public Safety, the Attorney General's Office, and other organizations, as necessary, until resolution and recovery efforts have been completed.

4.5. SIPC ALERT NOTIFICATIONS

4.5.1. **SIPC Responsibilities** – As SIPC creates or receives computer security alerts, it shall forward them to all budget unit CIOs or designees. Each alert shall state, as a minimum, the identity of the risk, level of risk, and any available patches or inoculants to mitigate the risk.

4.5.2. **Budget Unit Responsibilities** -- Upon receiving a SIPC Alert, budget unit CIOs or designees shall notify budget unit personnel about the alert. The CIO shall send alert notifications by email and determine whether to send it to "Agency All," or specific divisions within the budget unit, or only to specific individuals, depending on the content.

4.6. SIPC MEMBERSHIP – Each budget unit shall be a member of SIPC. The budget unit CIO or designee shall complete a SIPC Membership Application (see Attachment B) and deliver it to ADOA SIPC. The budget unit CIO or designee shall ensure that the contact information on the form remains current and apprise SIPC of any changes.

5. **DEFINITIONS AND ABBREVIATIONS**

Refer to the PSP Glossary of Terms located on the GITA website at http://www.azgita.gov/policies_standards/ for definitions and abbreviations.

6. **REFERENCES**

- 6.1. A. R. S. § 41-621 et seq., "Purchase of Insurance; coverage; limitations, exclusions; definitions."
- 6.2. A. R. S. § 41-1335 ((A (6 & 7))), "State Agency Information."
- 6.3. A. R. S. § 41-1339 (A), "Depository of State Archives."
- 6.4. A. R. S. § 41-1461, "Definitions."
- 6.5. A. R. S. § 41-1463, "Discrimination; unlawful practices; definition."
- 6.6. A. R. S. § 41-1492 et seq., "Prohibition of Discrimination by Public Entities."
- 6.7. A. R. S. § 41-2501 et seq., "Arizona Procurement Codes, Applicability."
- 6.8. A. R. S. § 41-3501, "Definitions."
- 6.9. A. R. S. § 41-3504, "Powers and Duties of the Agency."
- 6.10. A. R. S. § 41-3507, "Statewide Information Security and Privacy Office: Duties".
- 6.11. A. R. S. § 41-3521, "Information Technology Authorization Committee; members; terms; duties; compensation; definition."
- 6.12. A. R. S. § 44-7041, "Governmental Electronic Records."
- 6.13. Arizona Administrative Code, Title 2, Chapter 7, "Department of Administration Finance Division, Purchasing Office."
- 6.14. Arizona Administrative Code, Title 2, Chapter 10, "Department of Administration Risk Management Section."

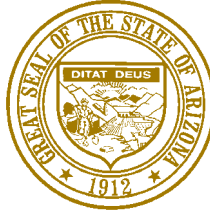
- 6.15. Arizona Administrative Code, Title 2, Chapter 18, “Government Information Technology Agency.”
- 6.16. [Statewide Policy P100, Information Technology.](#)
- 6.17. [Statewide Policy P800, IT Security.](#)
- 6.18. State of Arizona Target Security Architecture,
http://www.azgita.gov/enterprise_architecture.

7. ATTACHMENTS

Attachment A – Arizona Statewide Infrastructure Protection Center (SIPC) Incident Report

Attachment B – ADOA SIPC Membership Application

Attachment A – Sample of Arizona Statewide Information Protection Center (SIPC) Incident Report



SIPC Incident #

Governor Jan Brewer

Arizona Statewide Infrastructure Protection Center (SIPC) Incident Report

Contact Information

First Name:		Last Name:	
Title:		Department and/or Business Unit:	
Phone:		Alt Phone:	
Mobile:		Pager:	
Email:		Fax:	

Incident General Information

Suspected Source of Incident:	<input type="checkbox"/> External <input type="checkbox"/> Internal	Type of Incident:	Selection
Estimated Date/Time Incident occurred:		Date/Time Incident detected:	
Impact on Business:	Selection	Current Risk Level to Business:	Selection
Systems and/or Services Impacted:			
Source IP, Port, Protocol:		Destination IP, Port, Protocol:	
Operating System and Version, patch:			

Incident Detection Information

Comments:	
-----------	--

Incident Mitigation Information

Comments:	
-----------	--

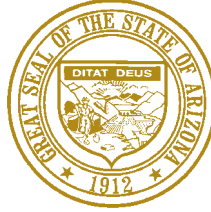
Additional Incident Status Information

Comments:

Email completed form to SIPC@AZDOA.GOV
For any questions or inquires please contact 602 542-2252
Form Revised 05-01-2007

CONFIDENTIAL

Attachment B – Sample of ADOA SIPC Membership Application



Janice K. Brewer
Governor

WILLIAM BELL
Director

ARIZONA DEPARTMENT OF ADMINISTRATION
Information Services Division
100 N 15TH AVE, SUITE 400
PHOENIX, ARIZONA 85007
(602) 542-2250

To: Darrell Mills, ADOA Security Manager
ADOA Information Security

Subject: Membership to the Statewide Infrastructure Protection Center (SIPC) Alert Group

Membership requires a person's contact information in the event of an incident or alert.

ADD UPDATE REMOVE

DATE
: _____

LAST NAME: _____ FIRST NAME: _____

AGENCY: _____

AGENCY ADDRESS: _____

CITY: _____ STATE: _____ ZIP CODE: _____

TELEPHONE NUMBER: _____ PAGER NUMBER: _____

BLACK BERRY NUMBER: _____ CELL PHONE NUMBER: _____

EMAIL ADDRESS: _____

SIGNATURE: _____ DATE: _____

Please complete and FAX or E-Mail to:
FAX Number: 602.542.0095 E-Mail: SIPC@AZDOA.GOV

For ADOA Administrative Use Only

Request Received: _____ Date	Request Completed: _____ Date	Received By: _____ AIS Analyst
---------------------------------	----------------------------------	-----------------------------------

Form Updated: 02/04/09