

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)))).

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 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).

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.security.state.az.us/Security WEB Documents/CERT-WWW-IncidentReport.pdf](http://www.security.state.az.us/Security%20WEB%20Documents/CERT-WWW-IncidentReport.pdf). The budget unit representative completing the report should provide as much detail as possible in the remarks 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/](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. § 41-3521, "Information Technology Authorization Committee; members; terms; duties; compensation; definition."
- 6.11. A. R. S. § 44-7041, "Governmental Electronic Records."
- 6.12. Arizona Administrative Code, Title 2, Chapter 7, "Department of Administration Finance Division, Purchasing Office."
- 6.13. Arizona Administrative Code, Title 2, Chapter 10, "Department of Administration Risk Management Section."
- 6.14. Arizona Administrative Code, Title 2, Chapter 18, "Government Information Technology Agency."


- 6.15. [Statewide Policy P100, Information Technology.](#)
- 6.16. [Statewide Policy P800, IT Security.](#)
- 6.17. State of Arizona Target Security Architecture,  
[http://www.azgita.gov/enterprise\\_architecture](http://www.azgita.gov/enterprise_architecture).

## 7. ATTACHMENTS

Attachment A – Incident Response Report

Attachment B – ADOA SIPC Membership Application

**Attachment A – Incident Response Report**

		<h1 style="color: red; margin: 0;">Computer Emergency Response Team</h1> <h2 style="color: blue; margin: 0;">Incident Report</h2>			
<b>Agency:</b>		<b>Date:</b>			
<b>Contact Name:</b>		<b>Phone:</b>			
<b>Email:</b>		<b>Fax:</b>			
<b>Virus/Intrusion Name:</b>					
<b>Date of Incident:</b>		<b>Time of Incident:</b>			
1. Describe how the intrusion was discovered, its problems, systems affected, and damages:					
2. Describe possible solutions for resolving the problems:					
3. Describe recovery methods of system, information, data, networks, etc.:					
4. Estimated date and time system will be available to users/customers:					
5. Location of Computer System:					
6. Is the affected system/network critical to the mission of the agency? <input type="checkbox"/> Yes <input type="checkbox"/> No					
7. Is there evidence of spoofing? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown					
8. Who is the anti-virus provider for the agency?					
9. List the apparent source of the intrusion/attack (IP address), if known:					
10. The last time the operating system was updated?					
11. Please check type of problems and damages that apply:					
<input type="checkbox"/>	Trojan Horse	<input type="checkbox"/>	Unauthorized Root Access	<input type="checkbox"/>	Network Damages
<input type="checkbox"/>	Trapdoor	<input type="checkbox"/>	Web Site Defacement	<input type="checkbox"/>	Information/Data Damages
<input type="checkbox"/>	Bomb	<input type="checkbox"/>	Denial of Service	<input type="checkbox"/>	Theft of Information/Data
<input type="checkbox"/>	Worm	<input type="checkbox"/>	Distributed Denial of Service	<input type="checkbox"/>	Network Damages
<input type="checkbox"/>	Hoax	<input type="checkbox"/>	Operating System Damages	<input type="checkbox"/>	Other, please describe:
12. Suspected perpetrator or possible motivation of attack:					
<input type="checkbox"/>	Insider/Disgruntled Employee	<input type="checkbox"/>	Former Employee	<input type="checkbox"/>	Domestic Perpetrator
<input type="checkbox"/>	International perpetrator	<input type="checkbox"/>	Other, please describe:		

<b>13. What operating software systems were affected?</b>					
<input type="checkbox"/>	UNIX	<input type="checkbox"/>	Sun OS/Solaris	<input type="checkbox"/>	OS2
<input type="checkbox"/>	LINUX	<input type="checkbox"/>	MacOS	<input type="checkbox"/>	Windows
<input type="checkbox"/>	NT	<input type="checkbox"/>	Sun OS/Solaris	<input type="checkbox"/>	Other, Please describe:
<b>14. What Hardware systems were affected?</b>					
<input type="checkbox"/>	Compaq	<input type="checkbox"/>	Packard Bell	<input type="checkbox"/>	Toshiba
<input type="checkbox"/>	Dell	<input type="checkbox"/>	Apple	<input type="checkbox"/>	Micron
<input type="checkbox"/>	HP	<input type="checkbox"/>	Gateway	<input type="checkbox"/>	PC Clone
<input type="checkbox"/>	IBM	<input type="checkbox"/>	Fujitsu	<input type="checkbox"/>	Other, please describe:
<b>15. CPU/Speed:</b>					
<input type="checkbox"/>	Pentium/90	<input type="checkbox"/>	Pentium/233	<input type="checkbox"/>	Pentium/400
<input type="checkbox"/>	Pentium/100	<input type="checkbox"/>	Pentium/300	<input type="checkbox"/>	Pentium/450
<input type="checkbox"/>	Pentium/133	<input type="checkbox"/>	Pentium/333	<input type="checkbox"/>	Motorola
<input type="checkbox"/>	Pentium/200	<input type="checkbox"/>	Pentium/350	<input type="checkbox"/>	Other, please describe:
<b>16. Memory:</b>					
<input type="checkbox"/>	16 MB	<input type="checkbox"/>	32 MB	<input type="checkbox"/>	64 MB
<input type="checkbox"/>	128 MB	<input type="checkbox"/> Other, please describe:			
<b>17. Modem Speed:</b>					
<input type="checkbox"/>	28.8 baud	<input type="checkbox"/>	33.6 Baud	<input type="checkbox"/>	56 Baud
<input type="checkbox"/>	ISDN	<input type="checkbox"/> Other, please describe:			
<b>18. Internet Browser:</b>					
<input type="checkbox"/>	Microsoft Internet Explorer	<input type="checkbox"/>	Netscape Navigator/Communicator	<input type="checkbox"/> Other, please describe:	
<b>19. Agency Security Infrastructure (check all that apply):</b>					
<input type="checkbox"/>	CERT Team	<input type="checkbox"/>	Security Auditing Tool(s)	<input type="checkbox"/> Secure Remote Access Tools	
<input type="checkbox"/>	Firewall(s)	<input type="checkbox"/>	Packet Filtering	<input type="checkbox"/> Banners	
<input type="checkbox"/>	Intrusion Detection System(s)	<input type="checkbox"/>	Encryption	<input type="checkbox"/> Account/Access Control List	
<input type="checkbox"/>	Other, please describe:				
<b>20. What actions and technical mitigation have been taken?</b>					
<input type="checkbox"/>	System disconnected from network	<input type="checkbox"/>	System binaries checked	<input type="checkbox"/> No action taken	
<input type="checkbox"/>	Backup of affected system(s)	<input type="checkbox"/>	Log files examined	<input type="checkbox"/> Other, Please describe:	

<b>21. Critical State services affected (check all that apply):</b>					
<input type="checkbox"/>	Health	<input type="checkbox"/>	Transportation	<input type="checkbox"/>	Criminal Justice
<input type="checkbox"/>	Public Safety	<input type="checkbox"/>	Agriculture	<input type="checkbox"/>	Education/Higher Ed.
<input type="checkbox"/>	Corrections	<input type="checkbox"/>	Labor Employment	<input type="checkbox"/>	Revenue
<input type="checkbox"/>	Environmental	<input type="checkbox"/>	Human/Social Services	<input checked="" type="checkbox"/>	Administration
<b>22. Please list other agency/organization that been informed? (Please provide names and phone numbers)</b>					
<input type="checkbox"/>	DPS	<input type="checkbox"/>	State SIPC		
<input type="checkbox"/>	Attorney General	<input type="checkbox"/>	State CERT		
<input type="checkbox"/>	Other, please describe:				

**Attachment B – ADOA SIPC Membership Application**

JANET NAPOLITANO  
GOVERNOR



BETSEY BAYLESS  
DIRECTOR

**ARIZONA DEPARTMENT OF ADMINISTRATION  
INFORMATION SERVICES DIVISION**

100 N 15<sup>th</sup> AVE., SUITE 400  
PHOENIX, ARIZONA 85007

**M E M O R A N D U M**

**TO: Statewide Security Manager  
ADOA ISD Security Services**

**SUBJECT: Membership to the State Infrastructure Protection Center (SIPC) Alert Group**

This membership requires personal contact information in the event of an incident or alert on a vulnerability exists that may or may not directly affect your organization.

<b>Name:</b>	
<b>Agency Name:</b>	
<b>Address:</b>	
<b>City:</b>	
<b>Telephone Number:</b>	
<b>Pager Number:</b>	
<b>FAX Number:</b>	
<b>Email:</b>	

Send to ADOA/ISD Security Services, 100 N 15<sup>th</sup> Ave., Suite 400, Phoenix, AZ 85007 or FAX 602-542-0095