STATE of ARIZONA

Government **I**nformation **T**echnology **A**gency	**Statewide POLICY**	**TITLE: Social Networking**
	P505	**Effective Date: October 1st, 2009**

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 formulation of policies to effectuate the purposes of the agency (A.R.S. § 41-3504(A (13))).

2. PURPOSE

The purpose of this policy is to identify proper usage and behavior for Social Networking Applications for the State of Arizona to further protect the rights and privacy of its citizens and the integrity of state government.

3. SCOPE

This applies to all budget units. A 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. POLICY

Social networking services are online communication tools that focus on a community of interests or individuals who share in exploring the interests and activities of others including public and private organizations. This policy establishes that state personnel and/or contractors that use social networking applications through state resources shall perform the following:

4.1 PROPER USAGE FOR SOCIAL NETWORKING ON BEHALF OF THE STATE:

4.4.1 Administrative

A. State personnel and contractors in a budget unit who are responsible for content in social networking efforts shall first obtain approvals from the Budget unit CEO and CIO before registering and participating on behalf the State. State personnel, including but not limited to volunteers, students, interns and other representatives working with the state or an agency ("Personnel"), contractors, and vendors with a personal social networking registration or license shall not use a personal social network, web blog or blog system for conducting state business.

B. State personnel and contractors shall receive instruction and/or training by the agency before using social networking applications by the budget unit. In addition, the P501 Statewide Internet Use Policy and the P401 Statewide Email Use Policy shall be reviewed during training sessions.

C. When registering for social networking applications, all state personnel and contractors shall use their state email address when registering. If the application requires a USERNAME, the following syntax shall be used: http://twitter.com/<username><agency>azgov Example: http://twitter.com/jdoegitaazgov

Exceptions in the form of a different sanctioned e-mail will be governed by the internal policy of the agency depending on the functional and authorized role of the individual or group and subject to approval processes as applicable internally.

D. Budget unit CIO's shall develop and maintain a Social Networking Matrix that identifies state personnel and contractors participating in social networking activities which shall include the social networking application name (i.e., MySpace, Twitter, Facebook, Nixle.com, etc.), first and last name of the individual, username (if applicable), email address, and password. Password information may be maintained in any auditable and retrievable format depending on agency policy, standards and procedures.

E. Upon termination of personnel or contractors, the budget unit CIO shall be responsible for removing/deleting social networking registrations of such state personnel and contractors within 30 days or less of termination or contract expiration.(P800-S810 Rev 2.0 § 4.4.3)

F. GITA reserves the right to request a copy of a Budget units' Social Networking Matrix to address data/information risks, privacy issues, and security vulnerabilities/assurances for the state and for the Department of Homeland Security. TISA will be modified for agencies to electronically submit their Social Networking Matrix by FY2011 when submitting annual TISA compliance reports.

G. Jurisdiction and authority for the retention of public records remains with the State Library of Archives and Public Records (ASLAPR). The issue of public records for state programs and services should be addressed by each state agency with ASLAPR for compliance by the very nature of its content and whether it serves the state and/or the public.

4.4.2 Social Networking Activities

A. All social networking activities shall address programs and services of the business unit in support of its mission and delivery of services.

B. Before participating in any online activities, understand that anything posted online through social networking is available to anyone in the world. Any text or photo placed online is completely out of your control the moment it is placed online – even if you limit access to your site.

C. State personnel/contractors shall not post information, photos, links/URLs or other items online that would reflect negatively on any individual(s), its citizens, or the state, unless approved by agency policy.

D. State personnel/contactors shall not provide any confidential information pertaining to the State and home addresses, personnel phone number(s), birth date, or any other personal identifying information, as well as personal location or personal plans on a web blog or other social network system. By doing so, personal information could contribute to identity theft, personal harm and/or loss of property.

E. Budget unit web blogs/media shall have clear disclaimers that their views represent the best interest of state and its citizens. All web blogs shall be clear, direct, professional, honest, ethical, and written in the first person.

F. Be respectful and mindful of the state, in addition to state leadership, state employees, customers, partners, vendors, citizens, and the public when participating in social networks and web blogs.

G. A budget unit's online presence reflects a perception of the State. Be aware that images and comments reflect views and directions of the State, whether real or perceived.

H. State Personnel/contractors shall not reference, cite, or publish information, views or ideas of any third party without their written consent and only as permitted by the State for the purpose of conducting business on behalf of the State.

4.4.3 Markets Served

A. Budget units should develop a brief marketing plan addressing benefits of use of social networking applications by identifying markets and programs serving the public, information strategies and its use, proposed advertisements and promotion activities.

B. The plan should also identify management resources, internal teams, external management resources (contractors) and human resource needs to monitor usage, analyze information trends and prepare responses for the public or private individuals/organizations. Such information and trends can be an invaluable tool for gathering public and private information, identifying future training requirements or focus group information, or outreach programs and to improve public awareness.

4.4.4 Security and Privacy

A. State web blogs shall comply with the security and privacy policies/standards of the State (EO 2008-10). This applies to comments provided on other blogs, forums, and other social networking sites on behalf of the state. Information posted to the state web blog or external blogs or other social network sites is a public record. Personal identifying information, other confidential information or sensitive information is not permitted for posting to a blog or social network site.

B Each agency is responsible for reporting and responding to information security and privacy incidents, including breach notification requirements, if personal identifying information or other confidential or sensitive information is posted to a web blog or other social network system.

C Under no circumstance should State authorized business that involves the communication of personal identifying, confidential or sensitive information be conducted on a social network, web blog or blog system.

4.4.5 Legal

A. Comply with all applicable federal, state and local laws and regulations on Internet usage, including A.R.S. § 38-448 State Employees Access to Internet and Statewide Policy P252, Intellectual Property and Fair Use.

B. All State personnel, including but not limited to volunteers, students, interns and other representatives working with the state or an agency ("Personnel"), contractors, and vendors with a personal social networking registration or license shall receive a copy of A.R.S. § 38-448, and acknowledge by signing the Online Non-Disclosure Agreement form that any statements to media made through social networking resources while employed or contracted with the state that harms the reputation or credibility of the state and/or its citizens may be cause for discipline or dismissal (A.R.S. § 41-770). A user sign-on screen containing the contents of the Online Non-Disclosure Agreement form may be used in lieu of non-disclosure agreement document.

C. Respect copyright laws, intellectual property, and reference or cite sources appropriately.

D. Many social networking sites require that users agree to abide by a Terms of Service (ToS) policy. Business units are responsible for reading, knowing, and complying with the ToS policy of sites for which they register.

E. Logos, seals, URLs and trademarks, other than the State, may not be used without written consent from either the public or private organization.

4.4.6 Oversight

A. The State of Arizona reserves the right to monitor and log all web blog and blogging activity without notice.

B. The State of Arizona reserves the right to search social networking systems to further screen potential candidates for state employment.

4.4.7 Arizona Emergency Information Network (AzEIN Web 2.0) - Arizona Division of Emergency Management (ADEM)

A. Web 2.0 technologies such as YouTube, Twitter, and other social networking applications are used for disseminating emergency information to public and private organizations for the State. Such emergency notifications shall be submitted and administered through the Arizona Emergency Information Network (AzEIN) to reduce the impact of emergencies and disasters for personal property and life.

B. All government agencies and nongovernmental emergency relief organizations that provide emergency preparedness, response, recovery, protection of property, and life-safety emergency information shall obtain approval from ADEM to participate in the Arizona Emergency Information Network (AzEIN). Please contact azein@azdema.gov to participate or call (602) 689-6512 or fax (602) 464-6356. The AzEIN Emergency Bulletin Service (EBS) is available to all public and private organizations located at www.azein.gov.

5. DEFINITIONS AND ABBREVIATIONS

Social Networking Systems: A service that focuses on building online communities of people who share interests and/or activities, or who are interested in exploring the interests/activities of others. The main types of social networking services are those which contain category divisions, means to connect with the public and private individuals/organizations and a recommendation system linked to trust. Popular networking systems are Facebook, MySpace, Twitter, and LinkedIn.

Blog/Blogging: Providing commentary or news on a particular subject in an online interactive format. A typical blog can combine text, images, and links to other blogs and other media related to its topic.

Web blog: A type of website maintained by an individual or an organization for entry of blog (text) commentary, activities and events, or various types of media such as images, graphics, video and links to other blogs.

Please refer to the PSP Glossary of Terms located on the GITA website for additional definitions and abbreviations.

6. REFERENCES

6.1 A. R.S. § 38-421 Prohibits the theft or destruction of public records without lawful authority
6.2 A. R. S. § 38-448, "State employees; access to Internet pornography prohibited; cause for dismissal; definitions."
6.3 A. R. S. § 41-621 et seq., "Purchase of Insurance; coverage; limitations, exclusions; definitions."

6.4 A.R.S. § 39-101 – Permanent records must comply with media and storage standards established by ASLAPR;
6.5 A.R.S. § 39-121 – Public records shall be open to inspection by any person at all times during office hours
6.6 A. R. S. § 41-761 et seq., "Personnel Administration."
6.7 A. R. S. § 41-770, "Causes for dismissal or discipline."
6.8 A.R.S. § 41-1335 – Powers and duties of ASLAPR Director
6.9 A. R. S. § 41-1335 ((A (6 & 7))), "State Agency Information."
6.10 A. R. S. § 41-1339 Duties relating to historical values
6.11 A. R. S. § 41-1339 (A), "Depository of State Archives."
6.12 A. R. S. § 41-1345 – States that ASLAPR is responsible for preservation of public records
6.13 A.R.S. § 41-1346 – Each agency shall establish and maintain a records management program
6.14 A.R.S. § 41-1347 – Public records may not be destroyed or disposed of unless ASLAPR determines they have no further value
6.15 A.R.S. § 41-1348 – Agencies may reproduce records onto microfilm or electronic imaging with approval fro ASLAPR
6.16 A.R.S. § 41-1350 – Defines records as any documentary material regardless of physical form or characteristic
6.17 A.R.S. § 41-1351 – ASLAPR determines the value of records and prescribes the method of destruction
6.18 A. R. S. § 41-1461, "Definitions."
6.19 A. R. S. § 41-1463, "Discrimination; unlawful practices; definition."
6.20 A. R. S. § 41-1492 et seq., "Prohibition of Discrimination by Public Entities."
6.21 A. R. S. § 41-2501 et seq., "Arizona Procurement Codes, Applicability."
6.22 A. R. S. § 41-3501, "Definitions."
6.23 A. R. S. § 41-3504, "Powers and Duties of the Agency."
6.24 A. R. S. § 41-3521, "Information Technology Authorization Committee; members; terms; duties; compensation; definition."
6.25 A. R. S. § 44-7041, "Governmental Electronic Records."
6.26 Arizona Administrative Code, Title 2, Chapter 5, "Department of Administration, Personnel Administration.
6.27 Arizona Administrative Code, Title 2, Chapter 7, "Department of Administration Finance Division, Purchasing Office."
6.28 Arizona Administrative Code, Title 2, Chapter 10, "Department of Administration Risk Management Section."
6.29 Arizona Administrative Code, Title 2, Chapter 11, Article 3, "Solicitation" (A.A.C. R2-11-309).
6.30 Arizona Administrative Code, Title 2, Chapter 11, Article 4, "Special Events" (A.A.C. R2-11-401 to 409).
6.31 Arizona Administrative Code, Title 2, Chapter 18, "Government Information Technology Agency."
6.32 Statewide Policy P100, Information Technology.
6.33 Statewide Policy P252, Intellectual Property and Fair Use.
6.34 A.R.S. § 44-7041 – Creation; retention; conversion of written records;
6.35 EO 2008-10, Mitigating Cyber Security Threats
6.36 Statewide Policy P800, IT Security.

6.36.1 Statewide Standard P800-S830, Network Security.
6.36.2 Statewide Standard P800-S850, Encryption Technologies.
6.36.3 Statewide Standard P800-S860, Virus and Malicious Code Protection.
6.36.4 EO 2008-10, Mitigating Cyber Security Threats
6.37 Standard P800-S810 Rev 2.0, Account Management

7. ATTACHMENTS

None