

ARIZONA DEPARTMENT OF ADMINISTRATION	STATEWIDE POLICY	 State of Arizona
---	-----------------------------	--

P 5050 - SOCIAL MEDIA POLICY

DOCUMENT NUMBER:	P5050
EFFECTIVE DATE:	OCTOBER 11, 2016
REVISION:	1.0

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), the Agency shall establish a coordinated plan and program for information technology (IT) implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statute (A.R.S.)§18-104.

2. PURPOSE

The purpose of this policy is to define proper usage of social media for budget units (BUs) to conduct state business and behavior of individuals who have been authorized by the BU Director or his/her designee to develop, publish and maintain content on behalf of the BU or state government.

3. SCOPE

This policy applies to all BUs and IT integrations and/or data exchange with third parties that perform IT functions, activities or services for or on behalf of BUs or their Divisions. Applicability of this policy to third parties is governed by contractual agreements entered into between the BU and the third party/parties.

4. EXCEPTIONS

4.1 Policies, standards and procedures (PSPs) may be expanded or exceptions may be made by following the Statewide Policy Exception Procedure.

4.1.1 Existing IT Products and Services

- a. BU subject matter experts (SMEs) should inquire with the vendor and the state or agency procurement office to ascertain if the contract provides for additional products or services to attain compliance with PSPs prior to submitting a request for an exception in accordance with the Statewide Policy Exception Procedure.

4.1.2 IT Products and Services Procurement

- a. Prior to selecting and procuring information technology products and services, BU SMEs shall consider BU and Statewide IT PSPs when specifying, scoping, and evaluating solutions to meet current and planned requirements.

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:

- a. Be ultimately responsible for the correct and thorough completion of Statewide IT PSPs throughout all state BUs.

5.2 BU Director or his/her designee shall:

- a. Assign appropriate personnel to oversee the use of social media, evaluate and authorize BU requests for usage, and determine appropriateness of the content posted to social media sites; and
- b. Periodically review social media usage to ensure it continues to reflect the BU's communication strategy and priorities.
- c. Maintain and periodically verify the log of all user credentials, including effective dates.
- d. Ensure that credentials will comply with security policies in the event of user separation from the BU.

5.3 BU Supervisors shall:

- a. Ensure users are appropriately trained and educated on social media and IT policies;
- b. Monitor personnel activities to ensure compliance;
- c. Monitor and filter, as necessary, all social media content posted and/or viewed; and
- d. Respond to comments and inquiries received via social media, as appropriate.

5.4 Individual Users shall:

- a. Read, understand and follow this PSP, Statewide Policy P8280, Acceptable Use Policy, and related PSPs; and
- b. Ensure any social media usage is consistent with applicable laws, rules and Statewide and BU policies; inappropriate postings that include discriminatory remarks, harassment, threats of violence or similar inappropriate or unlawful conduct will not be tolerated.

6. STATEWIDE POLICY

This policy establishes and defines the guidelines and use of social media.

- 6.1** BUs that wish to use social media should develop a brief marketing plan addressing the following:
- a. Audience
 - b. Target Markets
 - c. Objective
 - d. Message
 - e. Sustainability strategy
 - f. Measurable metrics that will determine/measure success
 - g. Management Resources
 - h. Internal Teams
 - i. External Management Resources (i.e. contractors)
- 6.2** All BU authorized personnel and contractors who are responsible for content on behalf of the BU or the State or who speak officially on behalf of the BU or the State, in social media efforts, shall:
- 6.2.1** Receive proper instructions and training, as well as acknowledge their understanding of the Statewide Security Framework P8280, Acceptable Use Policy, BU specific policies, and standards and procedures, related to social media, before using any State social media communications;
 - 6.2.2** Share their login credentials with the administrator in the event that the social media site does not support an administrative role so that accounts may be disabled upon separation;
 - 6.2.3** Notify the account administrator of any changes, including separation, so that their account may be disabled timely;
 - 6.2.4** Obtain approvals from the BU Director or his designee before registering and participating in social media activity in an official capacity;
 - 6.2.5** Respect copyright laws, intellectual property, and reference/cite sources appropriately;
 - 6.2.6** Understand social media may not be used for personal gain, conducting private commercial transactions, or engaging in private business activities;
 - 6.2.7** Understand that postings to social media websites immediately become part of a public record.

- 6.2.8 Not post or release proprietary, confidential, sensitive, or other state government Intellectual Property;
 - 6.2.9 Identify themselves appropriately, using agency sanctioned identification, when posting or exchanging information;
 - 6.2.10 Address issues only within the scope of their specific authorization;
 - 6.2.11 Be respectful and mindful of the State, in addition to State leadership, State employees, customers, partners, vendors, citizens, and the public;
 - 6.2.12 Without prior approval from BU Director or his/her designee, not post information, photos, links or URLs or other items online that would reflect negatively on the State, its citizens or any individual;
 - 6.2.13 Not incite or promote violence or illegal activities;
 - 6.2.14 Not include information that reasonably could compromise public safety;
 - 6.2.15 Not promote or endorse political campaigns or candidates; and
 - 6.2.16 Use approved BU social media to post official BU information.
- 6.3 The BU reserves the right to monitor and log all web social media activity without notice.
- 6.4 **Personal use of social media outside of work:** Nothing in this policy prohibits the personal use of social media outside of work; however, such personal use shall be done in such a manner that it is not construed to be an official act of the State or the BU.
- 6.5 **Public Records/Records Retention** – social media sites contain communications sent to or received by BUs and are therefore public records subject to State retention schedules.

7. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the ADOA-ASET website.

8. REFERENCES

- 8.1 Policy P1000, Information Technology
- 8.2 A.R.S. § 18-104
- 8.3 Statewide Security Framework P8280, Acceptable Use Policy
- 8.4 A.R.S. § 38-448

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
6-15-2015	All comments from Budget Unit responses for request for comments	Draft	Raj Kollengode
10/11/2016	Updated all the Security Statutes	1.0	Morgan Reed, State CIO and Deputy Director