State of Nevada

Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.3.04.03	Social Media for Business Use	B	3/31/2017	1 of 4

1.0 PURPOSE

Agencies and departments are encouraged to use Social Media technologies for business use to engage their customers and employees where appropriate. There is a measure of risk to address and mitigate any issues with the use of Social Media. The following requirements will assist in risk mitigation.

This standard is not to be misinterpreted as requiring any state agency to allow the use of Social Media technologies in its environment. Further, this standard does not supersede any existing state agency Social Media policy which exceeds the requirements of this standard.

2.0 SCOPE

This standard applies to all state agencies using Social Media technologies within or for the Executive Branch of Nevada State Government.

3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Officer (CIO).

4.0 RESPONSIBILITIES

The agency head and appointed Information Security Officer (ISO) have the responsibility to ensure the implementation of and compliance with this standard. The agency ISO and unit managers are responsible for disseminating this standard and implementation within their units.

5.0 RELATED DOCUMENTS

State Information Security Program Policy 100, Section 5.4.5 Internet Security

6.0 STANDARD

6.1 General Agency Management Requirements

A. Prior to authorizing and enabling Internet access to Social Media web sites, agency management shall conduct a formal risk assessment of the proposed connections utilizing agency Risk Management processes. The assessment shall, at a minimum, include the analysis of the risks (including risk mitigation strategies) involved in providing Users access to Social Media web sites including:

1. Employee productivity;
2. The Network bandwidth requirements and impacts;
3. Reputational risk to personnel, the agency, and the State;
4. Potential avenue for exposure or leakage of sensitive or protected information such as copyrighted material, intellectual property, personally identifying information, etc.;

5. Potential avenue for malware introduction into the organization's IT environment; and,

6. The potential use of "other than government" sections of Social Media web sites.

B. State agencies shall document this risk analysis and retain it for a minimum of two years.

6.2 Agency IT Administrator Requirements

A. Limit Internet access Social Media web sites according to the agency's acceptable use policy, while allowing authorized Users to reach content necessary to fulfill the business requirements. Limitations may include:

1. Opening Internet access only to the government sub-domains on the Social Media web sites;

2. Allowing Internet access to Users who are specifically authorized;

3. Preventing unnecessary functionality within Social Media web sites, such as instant messaging (IM) or file exchange;

4. Agency IT staff must implement processes to minimize any risks associated with social media activities while allowing employees to use best practices in maximizing the effectiveness of social media activities.

B. Enable technical risk mitigation controls to the extent possible. These controls may include:

1. Filtering and monitoring of all Social Media web site content posted and/or viewed;

2. Scanning any and all files exchanged with the Social Media web sites.

6.3 Agency Requirements

A. Users shall not speak in Social Media web sites or other on-line forums on behalf of an agency, unless specifically authorized by the agency head or the agency's Public Information Office. Users may not speak on behalf of the State unless specifically authorized by the Governor.

B. Users shall connect to, and exchange information with, only those Social Media web sites that have been authorized by agency management in accordance with the requirements within this and other agency and State policies.

C. Users shall minimize their use of "other than government" sections of the Social Media web sites.

D. Users shall not post or release proprietary, confidential, sensitive, personally identifiable information (PII), or other state government Intellectual Property on Social Media web sites.

E. Users who connect to Social Media web sites through State information assets, who speak officially on behalf of the state agency or the State, or who may be perceived as speaking on behalf of an agency or the State, are subject to all agency and State

requirements addressing prohibited or inappropriate behavior in the workplace, including acceptable use policies, user agreements, sexual harassment policies, etc.

F. Users who are authorized to speak on behalf of the agency or State shall identify themselves by: 1) Full Name; 2) title; 3) Agency; and 4) Contact Information, when posting or exchanging information on Social Media forums, and shall address issues only within the scope of their specific authorization.

G. Users who are not authorized to speak on behalf of the agency or State shall clarify that the information is being presented on their own behalf and that it does not represent the position of the State or an agency.

H. Users shall not utilize tools or techniques to spoof, masquerade, or assume any identity or credentials except for legitimate law enforcement purposes, or for other legitimate State purposes as defined in agency policy.

I. Users shall avoid mixing their professional information with their personal information.

J. Users shall not use their work password on Social Media web sites.

For individual use, refer to your agency acceptable use policy.

7.0 DEFINITIONS

None

8.0 RESOURCES

Nevada Public Records Act: A Manual for State Agencies, Bulletin No. 3

To assist in implementing this standard, additional information and resources are available at the following links.

CIO Councils' Guidance for Secure Use of Social Media by Federal Departments and Agencies – http://www.cio.gov/Documents/Guidelines_for_Secure_Use_Social_Media_v01-0.pdf

Intel Social Media Guidelines – http://www.intel.com/sites/sitewide/en_US/social-media.htm

IBM Social Computing Guidelines – https://www-950.ibm.com/blogs/09100912-b777-4fcf-b726-f28424d9dc44/resource/IBMSocialComputingGuidelines.pdf?lang-en us

Best Practices for Social Media Usage in North Carolina – http://www.records.ncdcr.gov/guides/best_practices_socialmedia_usage_20091217.pdf

New Media and the Air Force, Air Force Public Affairs Agency, Emerging Technology Division – https://www.af.mil/shared/media/document/AFD-090406-036.pdf

9.0 EXCEPTIONS

Requests for exception to the requirements of this Information Security Standard must be documented, provided to the Office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).

Approved By

Title	Signature	Approval Date
State Information Security Committee	Approved by Committee	11/17/2016
State Chief Information Security Officer (CISO)	Signature on File	
State Chief Information Officer (CIO)	Signature on File	3/31/2017

Document History

Revision	Effective Date	Change
A	3/31/2017	Initial release
B	12/26/2018	Renumbering (136 to S.3.04.03) and compliance to ADA standards.