Tier 1 Control Standards (State-Wide)

Social Media Applications

Standard ID
IOT-CS-SEC-130

Published Date
12/11/2009

Effective Date
12/11/2009

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
09.0 Information Protection Processes and Procedures (PR.IP)
09.1 PR.IP-1
09.1.1 Configuration Management

Purpose
The state seeks to communicate information with convenience and efficiency. Social media applications (Facebook, Twitter, YouTube, etc.) offer opportunities to broaden or enhance communications on government matters. This standard is established to ensure that state agencies consider the costs, benefits and risks with implementing a social media application.

Scope
IOT Supported Entities

Statement
Below are the requirements and process related to approval for social media applications:

Internal to the Agency

- Evaluate their citizen or business communication needs, the effectiveness of current communications, and the value new social media tools might provide. The use of social media tools by similar business functions in the public and private sectors should be evaluated.
- Assign a primary and backup employee to manage each social media application.
- Ensure all users with access to the social media must strictly abide by the Stipulations section of this practice.
- Present a business case identifying the costs and benefits, as well as the success criteria for the project.
- Assess the risks associated with the social media application. A brief summary of the risks and the risk mitigation measures put into place should be incorporated into the business justification documentation (the form found in Practice 3.1.1 – Risk Assessment Process may be helpful).
- Educate targeted audiences by providing appropriate security and privacy tips as they relate to the agency’s social media application.

External Review and Approval

- IOT Security will review the social media tool to be used and other security issues. If approved, IOT Security will add their comments to the form for subsequent approver’s review in addition to the agency information. If not approved, IOT Security will return the request to the agency with comments.
- IN.gov Governance Board will review the request ensuring the implementation and maintenance plans are sound and the tool identified is capable of meeting the objectives of the project. If approved, the request will be forwarded to the Governor’s
Office. If not approved, it will be returned to the agency with comments.

- The Governor’s Office will conduct a final review ensuring that the overall project appropriately represents the objectives of the administration. If approved, the agency can begin the implementation.

Stipulations

- State owned social media sites never store, display, or request personal or confidential information from citizens (e.g. social security numbers, health information).
- Forum and chat interfaces/capabilities are prohibited (A Facebook wall does not qualify as a forum or chat but is considered an area for comments).
- Comments left by visitors, when permitted, are continuously monitored for appropriateness.
- Agency responses to comments are made only by authorized individuals.
- Social media applications should not be developed for the state workforce. There are more appropriate technologies available for such purposes. Social media continues to be blocked from most of the state workforce.
- State email addresses are to be used for account setup on a state owned social media site. Administration of the site should only be conducted with a work based account ID.
- Accounts and IDs established to support social media sites and applications are to be used solely for the support of state business. Such accounts and IDs are not to be used to access personal accounts.
- Ensure that all graphics, video, written materials and other intellectual property used on the site are owned by the state or adhere to applicable laws regarding use.
- State workforce members are not to comment on other non-state social media outlets in their work capacity without express authorization from agency leadership.
- State workforce members are not to install non-approved 3rd party applications to the Facebook pages or interface.

Roles

All Personnel

Responsibilities

Agencies shall pursue, implement and manage social media tools for the furtherance of their business mission. IOT shall review and approve for security concerns. IN.gov Governance Board shall review and approve for soundness in approach, and the Governor’s Office shall have final review and approval.

Management Commitment

Management shall exercise due diligence in relation to this Standard and make a valid business decision that considers risk.

Coordination Among Organizational Entities

Agencies shall work with IOT, IN.gov Governance Board and the Governor's Office in the vetting of social media applications.

Compliance

Agencies must provide follow-up information after implementation on a quarterly basis to ensure that the tool is being properly maintained and that success criteria are met. All agencies currently using a social media application must fill out the social media request form as well. All existing use is subject to modification.

Exceptions

No exceptions.