Privacy and Security

As with any type of communication, there is a certain degree of risk associated with participation on social media platforms. In general, agency communications directors should approach social media engagement with common sense. Just as privacy and security are carefully accounted for and monitored on state agency Web sites and personally identifiable information is not shared through traditional communication mediums, such as press releases, the same approach applies to social media engagement.

When sharing content on social media platforms, make sure it is public content and not confidential, critical, or personally identifiable information. Ohio IT Policy ITP-B.11, "Data Classification," outlines the various data classification labels that each agency already has in place. Ohio Revised Code Chapter 1347 also provides guidance on what is considered personally identifiable information. Agencies need to be mindful of these requirements when deciding what content is appropriate. In order to ensure that content managers adhere to these requirements, formal training or guidance to agency employees should be sought out. Failure to protect confidential, critical or personally identifiable information exposes not only the state but individual state employees to significant legal liability and could potentially have a negative impact on Ohio's citizens.

Examples of personally identifiable information are outlined in Ohio IT Bulletin ITB-2008.02, "Privacy Impact Assessments." This bulletin also addresses privacy impact assessments and will help agencies determine whether they need to conduct such an assessment prior to launching social media efforts.

If state agencies are participating on third party social media platforms, they should include a disclaimer on their pages that advises users that they are no longer on a State of Ohio site and that the privacy policy of the social media platform applies. A link to the platform's privacy policy should be included. In addition, agency communications directors must work with agency legal counsels to review the privacy statement of the third party platform and ensure that it is not in direct conflict with any federal or Ohio laws or policies regarding privacy protection.

Social media platforms are easily accessible and, typically, new accounts are quick and simple to establish and utilize. However, communications directors should discuss the utilization of social media platforms with their agency information technology department to addressing any security concerns prior to launching initiatives.

Agencies should conduct a risk assessment prior to making a final determination as to whether or not to participate in social media. Ohio IT Policy ITP-B.1, "Information Security Framework," provides guidance to agencies on how to conduct a risk assessment.

A multi-layered security strategy is required to provide sufficient protection to individuals, the agency and the IT infrastructure.

Individual Security Risks: Social media platforms all collect some type of personal profile information, including name, gender, location, employer, photographs, and names of friends, personal interests, and affiliations. If someone is able to gain access to this information, it could enable identity fraud and personal attacks. It could also result in the posting of fraudulent profile pages and messages, defamation, and theft of artwork or intellectual property.

Organizational Security Risks: Since organizational profile pages are only protected with a user ID and password, the organizational profile page can also become an object for attack. Organizations can also be subject to defamation and identity fraud, which can lead to damage to organizational image and reputation.

IT Infrastructure Risks: Social media platforms provide an opportunity to spread malicious code, such as viruses and worms. The ability to use mobile devices that allow the exchange of rich-media content, as well as text messages to engage in social networks, intensifies this issue.

In order to mitigate these risks, it is important that agency communications directors work with their IT representatives to ensure that Ohio IT security policies are reviewed and implemented where appropriate. Since agencies may be leveraging third party platforms, it becomes even more important that IT security personnel are involved to ensure that the controls in place on third party platforms satisfy state and federal IT requirements. Agencies should check the security of third party platforms to ensure that it complies with state and agency IT security policy.

Some of the standard security practices that should be implemented are as follows:

- Using strong passwords (letters, numbers, and characters) on all accounts
- Scanning uploaded and downloaded content for viruses and other inappropriate code.
- Filtering all content obtained from social networks for malware
- Monitoring content on a regular basis to detect unauthorized alterations
- Monitoring staff behavior and content, and gauging the success of security controls

- Allowing IT security personnel to have full access to read all content uploaded to or through a profile
- Reviewing the organizational profile regularly to identify visual and other performance problems
- If involved on multiple social media platforms, ensure that the security controls for each type of media have been analyzed and determine if varying controls need to be implemented for each type of platform

Ohio agencies need to make their internal and external users aware that social media platforms can often be prime targets for phishing and social engineering attacks.

Phishing, or "spear fishing," is an attack targeting a specific user or group of users and it attempts to deceive the user into performing an action that launches an attack (e.g., opening a document or clicking a link.) Spear fishers leverage the personal information they uncover on social media platforms to build trust with their targets. The practice of whaling, which is spear fishing a high-value individual, may involve sending customized documents that actually look like internal documents to spread malicious code. Spear fishers may use URL shortening technologies to obscure the actual Web site name. Attackers collect personal information about a target from social media platforms and may pose as a "friend" to elicit information, action, or support. Providing security awareness training to social media platform users is an important way to mitigate the risk of spear fishing or social engineering attacks being successful.

Due to the open nature of social media platforms, the opportunity for incidents to occur is significant. These incidents can take many forms, such as the implementation of fraudulent sites, false and disparaging comments on Ohio platforms, or the posting of confidential, critical or personally identifiable information. Security incidents, such as the introduction of malware, can also occur. Ohio agencies need to ensure that procedures for capturing evidence and escalating incidents discovered in social media environments are integrated into established incident management processes. Ohio agencies should involve legal and communications in incident management. Agencies must ensure that clear lines of responsibility are determined and communication platforms are clearly conveyed to all state employees involved in maintaining the social media presence.

If a security incident has been identified, agencies need to follow the security incident response procedures that were defined by their agency in response to Ohio IT Policy ITP-B.7, "Security Incident Response."