



CALIFORNIA OFFICE OF INFORMATION SECURITY & PRIVACY PROTECTION



(916) 445-5239
WWW.INFOSECURITY.CA.GOV

USE OF WEB SERVICE OFFERINGS
INFORMATION SHEET NO. 4
JUNE 16, 2008

Use of Web Service Offerings

Many state agencies may consider implementing Web service offerings to expand their public outreach efforts, take advantage of new technologies, and be seen as forward thinking. These offerings can enhance functionality, increase user experience, reach the younger generation, may be low or no cost, usually result in rapid deployment, may require limited technology support, and are typically considered cutting edge. These offerings include, without limitation, the following types of services:

- FeedBurner for enhanced really simple syndication / rich site summary (RSS) subscription and processing service for delivering regularly changing web content.
- YouTube videos for web-based video storage, conversion, and playback services sometimes used for training or public outreach.
- MySpace and FaceBook for marketing or public outreach.
- Social Bookmarking sites like Delicious and AddThis.
- Google Maps for mapping services, utilities, and Application Programmer Interfaces.
- Blogs, forums, and survey tools, such as Survey Monkey, etc.

Associated Requirements and Risks

State agencies must remain cognizant of the information security and privacy policy requirements applicable to the use of these service offerings. The State Administrative Manual Section 5305.1 requires a risk analysis process for those agencies that employ information technology (IT). Therefore, prior to implementation, agencies must consider and mitigate the risks associated with using them. Some of the high level risks associated with using these service offerings include:

- The harvesting of customer information, including IP addresses, and the retention and sale of that information.
- An implied endorsement and/or relationship with the vendor through the product's use.
- A potential for increased liability to the state. Unlike a traditional state outsourcing agreement, these service offerings often require agreement with the vendor's terms and conditions that impose all risk of liability on the agency (and the state), and significantly limit, or eliminate, any potential liability of the vendor (the provider).
- The need for additional port openings to provide the functionality.
- Accessibility issues; confusion by customers when linking to an outside source from a state web site; the risk of virus or malware infection from an outside source; and commitment of state resources for ongoing support, monitoring, and maintenance of the selected service in order to support the customer experience.

Risk Mitigation

As part of the agency's risk analysis, reasonable questions include "Why was this service offering used?" and "What precautions did your agency take to mitigate the risks associated with such use?" The recommended mitigation strategies for agencies include:

1. **Identify a valid business reason.** Ensure that the effort, the approach, and the associated risks to the state are based on justifiable, supportable business needs.
2. **Define the scope of the content.** Early in the process, identify and document the scope of the content and make sure that future content complies with that scope. With very few exceptions, the state must provide content that is suitable for a general audience with only public information provided (must not include confidential, sensitive, protected, or mission critical information).
3. **Understand the Terms of Use and Privacy Policies and clearly define the state/vendor relationship.** Using any service offering creates an agreement to the vendor's terms of use and privacy policies. Before implementation, at a minimum, it is highly recommended that the Chief Information Officer, the Information Security Officer, and your legal staff review and approve the plan, all terms of use and the privacy policies. The Department of General Services State Contracting Manual Volume 3 for IT provides guidance to agencies on Acquisition planning at: <http://www.pd.dgs.ca.gov/polproc/SCMVol3.htm> Understand the nature and extent of the potential for collection and subsequent use of customer's personal information. Before agreeing to the provider's terms of use and privacy policies, ensure that they are the type of agreement to which your agency is permitted to agree. For example, does the business reason for using the service offering outweigh the risks and liability associated with such use?
4. **Review existing Web filtering and employee use policies and standards.** We strongly recommend that agencies continue to use their established acceptable use policies and standards, such as not allowing employees to access these sites for non-state business purposes. Straying from them will increase risk to the state, including the potential downloading of malware and employee access to inappropriate content. Conversely, applicable employees will need access to them for maintenance purposes. Agencies must consider a reasonable approach to allowing these employees this access.
5. **Develop and implement an enterprise internal policy and procedures for using these services.** Document the policy and procedures for approving the use of these service offerings. Ensure employees are aware of them and adhere to them.
6. **Define the security, backup and recovery, and monitoring requirements.** Understand that loosening your existing security policies on your agency's network infrastructure (such as opening firewall ports) to allow for these service offerings increases risk to state information assets. In addition, consider prohibiting the public from posting comments since it may result in inappropriate content being posted. Identify and document any backup and recovery requirements for the source material. Finally, agencies must monitor the outsourced content in a timely manner to ensure ongoing compliance with laws, state security and privacy requirements, and internal policies. The cost associated with such monitoring should be included and considered in the initial risk analysis.
7. **Keep it simple and accessible.** Keep the design as simple as possible. Comply with accessibility requirements in Section 508 of the Rehabilitation Act of 1973. If the web site and/or content are not accessible, have an alternative available.
8. **Coordinate with the eServices Office.** They can link to your channels and videos and provide you guidance and assistance when necessary.
9. **Inform the customer.** When you link these services to your agency's state web site, inform the customer that they are leaving the state web site for an external service.
10. **Pilot the use.** Conduct a pilot on other than the ca.gov domain to make sure it works as expected.
11. **Document the use and approval.** Document the plan, the approach, and obtain management and your agency's Information Security Officer's approval. Update the document as web content changes.
12. **Monitor the site.** Agencies must monitor their site and consider the cost of doing so when deciding to use these services. To the maximum extent possible, identify and remove inappropriate postings or links as soon as possible.

Related Links and Resources

The following organizations provide additional information and resources:

- California eServices Office at www.eservices.ca.gov
 - <http://www.webtools.ca.gov/Accessibility/Background.asp>
- California YouTube Help at www.webtools.ca.gov/Help/YouTube.asp
- Office of Information Security and Privacy Protection at www.infosecurity.ca.gov
- Webcontent.gov - Your Guide to Managing U.S. Government Websites at http://www.usa.gov/webcontent/technology/other_tech.shtml