IAM Procurement Resources

7/13/2015

# Background

The IAM Technical Advisory Group (IAM-TAG), in conjunction with DoIT and UW System Legal, has developed several resources for application and business process owners seeking to procure applications that will integrate effectively into our UW System identity and access management infrastructure. These resources include a set of recommended RFP language and sample contract language for use with cloud vendors.

# Sample RFP Language

This language was developed to assist UW System application providers in assessing the IAM capabilities and challenges associated with a particular vendor’s product. They are intended to be used in conjunction with a Subject Matter Expert (SME) from the IAM Support Team that can assess the vendor’s response and provide the UW System application provider with an estimate of relative ease or difficulty of integrating the proposed product with our UW System IAM infrastructure.

Application providers or business owners seeking to procure applications that will integrate with our UW System IAM infrastructure should contact the IAM Support Team at iaa-requests@lists.wisc.edu to request a consultation.

# Sample Contract Language

This draft contract language was developed to address specific concerns raised by the IAM Steering Committee in providing identity data to cloud providers. This language is provided as a template to demonstrate the terms and conditions that should be set forth in any contract that provides identity data to an outside provider.

Application providers and business process owners that are engaged in contracting for cloud services may reference the contract language as a template or may include the language in their contracts but should take care that the entire contract is reviewed to ensure consistency with the following requirements:

1. Provider will not disclose confidential information to 3rd party without explicit written approval from UWSA.
2. Provider will inform UWSA of any request by 3rd party for confidential information. Provider will refer requests for data to UWSA unless compelled by lawful subpoena, in which case provider will notify UWSA.
3. Provider must comply with all applicable regulations based on the nature of the data (FERPA, HIPAA, GLBA, PCI, etc)
4. Provider must apply commercially reasonable practices to protect UWSA confidential data.
5. Provider must notify UW System immediately of any unauthorized disclosure of UWSA data.
6. Provider must provide remedy for breach of UWSA data held by provider, including reimbursement of UWSA’s financial costs related to breach.
7. On termination of contract, provider must destroy all copies of UWSA confidential data.