Purpose

The purpose of this document is to provide guidelines for consideration when negotiating contracts to provide cloud based technology solutions.

Guidelines

When evaluating a cloud solution for a technology application need, the following criteria must be considered and adopted using the identified solution or a reasonable alternative:

- Implement user authentication using the District's Active Directory and Central Authentication Service or if the entity wants to provide their own authentication use a pseudo-ID provided by us. Never share the Banner ID with cloud providers.
- Establish the data to be stored in the cloud and identify the business need for each data element in writing, preferably in the contract. Make sure the service provider is under the direct control of the district with regard to the use and maintenance of records, and that the provider uses protected information only for the purpose for which the disclosure was made and refrains from disclosure to other parties.
- Assess the level of data privacy for the information to be stored with the cloud provider and determine the appropriate level of security that must be guaranteed by the cloud provider in their Agreement with the District. Information Services has developed Technology Procedure ISP 15.2.2 "Guidelines for Outsourcing Web Hosting Services and Instructional Resources" to assist in the assessment process.
- When Personal Identifiable Information (PII) is to be stored and/or processed by the cloud services provider, consult with legal counsel to ensure that the Agreement with the cloud provider:
    - addresses all applicable federal, state, and local laws and regulations,
    - states that the data is owned by the District,
    - addresses how individuals will be notified in the case of a data breach,
    - provides for e-discovery that is required by law,
    - indemnifies the District for the vendor's own intentional or negligent acts or omissions,
    - guarantees that the vendor will not "data mine" the information,
    - provides the proper security such as firewall, patch management, security monitoring, and other relevant data security measures and procedures,
    - addresses how we are provided access to our data, the timeframe in which we can obtain it, and assures that we can easily migrate the data onto our own servers when necessary,
    - And ensures that the data will be stored within the USA.
- Evaluate the stability of the cloud provider and assure that the Agreement addresses what happens to the data if they go out of business.
- Ensure that all terms and conditions, whether explicitly in the Agreement or linked to the Agreement, are acceptable to the District.

- When implementing a collaborative cloud application such as e-mail, calendar, or shared documents, we must:
  - educate our user community regarding the type of data that should/should not be stored in the cloud including education on the issue of privacy and provisions of district policy,
  - provide a method for encrypting sensitive data to be transmitted and stored in the cloud,
  - And determine the need for additional technology tools and services. For example, archiving of e-mail, tools for scanning the domain for PII, and tools to backup data are not included in the basic e-mail models but are available for an additional cost. If existing user functionality will be lost with cloud e-mail, users should be informed of the change.

Review

The Technology Coordinating Council will annually review these guidelines for currency and effectiveness.

Questions or Assistance

For questions or assistance contact:

Tim Nguyen, Security Analyst at tnguyen@nocccd.edu
Tom Wallace, Technical Services Manager at twallace@nocccd.edu
Deborah Ludford, District Director, Information Services at dludford@nocccd.edu

Approved by Technology Coordinating Council, October 28, 2014