THE FLORIDA STATE UNIVERSITY

Information Technology Services

Technology Guidelines

Title: The Use of Personal Cloud Computing Services for University Business

Date: April 2013

Issuing Authority: ITS Security Manager

For this document the term 'personal cloud computing services' refers to information technology services that are usually accessed via an Internet connection and whose use is not officially approved or contracted by the University. Examples include blogs, wikis, office productivity tools (Google Apps, Hotmail, Yahoo Mail), file storage (assignment/file drop box services such as Dropbox and Box.com), content hosting (publishers text book add-ons services such as VitalSource), and computing resources on demand (Amazon EC2, Rackspace). They typically require the individual user to commit to a service agreement or terms of use through a 'click-to-accept' agreement in order to access the service. Please note these agreements have not been reviewed or approved by FSU's Information Technology Services (ITS) or Office of the General Counsel. Clicking on an agreement without authorized and documented University approval binds you as an individual, not the University, to the terms of use. In addition, the ability to procure a service with a University purchasing card (P-Card) does not automatically confer your right to obligate FSU to a service agreement. The P-Card purchaser still needs proper management approval to bind the University contractually.

It is recommended you consult with your supervisor or legal staff for appropriate approval prior to utilizing these services for University business.

Considerations for the use of public cloud services to conduct University business include but are not limited to:

- ✓ The personal licensing for these products should be authorized or contracted by appropriate Florida State University management when used for official University functions involving data classified as sensitive or confidential information per OP-F-7 Policy on Safeguarding of Confidential Financial and Personal Information (Section B). Confidential or sensitive information transferred to cloud services must also utilize the same protections employed on the University system storing the original data. For example, if the data is stored in an encrypted format on a University system, then it must also be encrypted on the cloud service.

- ✓ Most cloud services vendors provide consumer grade security controls that do not meet the additional contractual (PCI DSS) or regulatory (FERPA, HIPAA, and GLB) data protection requirements. The data owner must ensure the cloud service provider specifically meets all required contractual or regulatory security protections prior to the transfer of data to the cloud service.

- ✓ The FSU username (FSUID) assigned to you and your account password are unique identifiers needed to access select University data systems. Whenever possible, do not use your FSUID as your user name on public cloud services. Exceptions include services requiring the use of your FSU e-mail address which incorporates your FSUID as part of the address. Never reuse your FSU OMNI/Blackboard password on personal cloud services.

Using your FSUID and FSU system password on these services increases the risk of your University accounts being compromised should the cloud service provider suffer a security breach.

- ✓ Public cloud service providers may utilize data centers and network resources outside of the United States to transmit, store, or process data. Verify required research, contractual, or legal agreements concerning possible geographical restrictions on data activities prior to engaging these services for University business.

- ✓ Note, most public cloud service contacts allow the vendor the right to view, catalog, and parse any data stored on their devices. This process could initiate University compliance issues with select State, Federal, and contracted obligations for data safeguarding and privacy should a user move certain data items into the public cloud. In addition, these entities may employ individuals with access to data that have not gone through appropriate background checks or signed confidentiality agreements as a control.

- ✓ Public cloud service users conducting University business should understand provisions of State mandated public records retention and disposal provisions.

  http://vpfa.fsu.edu/Quicklinks/Records-Management-Program/Records-Disposal

- ✓ Users of University management approved public cloud services conducting University business must understand the State of Florida and University requirements for responding to public records requests, as well as discovery in the litigation process. Users should also be familiar with the criminal and civil penalties that can be imposed for noncompliance with these laws and policies.

- ✓ Access to your personal cloud services account could be subpoenaed during an E-discovery litigation request for University data resulting in the cloud service provider forwarding all account material including personal data items.

- ✓ The individual may lose access to data should the cloud service provider shut down unexpectedly. It is unlikely the individual can reclaim data from the cloud service provider under such circumstances.

- ✓ The ability to assess risk mitigation controls and determine the viability of disaster recovery procedures and incident response procedures of the cloud service provider may be limited due to poor vendor transparency, inflexible terms of service, lack of a negotiated contract with the vendor, or lack of right to audit.

- ✓ Campus units may lose access to University data stored on the cloud service should the user terminate employment.

Policy/Legal References

- OP-F-7 POLICY ON SAFEGUARDING OF CONFIDENTIAL FINANCIAL AND PERSONAL INFORMATION
- OP-H-12 PRIMARY IDENTIFIER POLICY
- OP-H-9 INFORMATION TECHNOLOGY SECURITY
- OP-D-2-G PAYMENT CARD POLICY
- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
- Gramm-Leach-Bliley Act, 15 USC, Subchapter I, Sec. 6801-6809
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules
- PCI Data Security Standard (PCI DSS)
- Florida Statute 817.5681 Breach of security concerning confidential personal information in third-party possession; administrative penalties
- Florida Statute 119 and Florida State University Regulation 6C2R-2.023 Administrative Matters for public records