THE FLORIDA STATE UNIVERSITY

Information Technology Services

Technology Guidelines

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

Date: July 2019

Issuing Authority: Information Security and Privacy Office

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), 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 the FSU's Information Technology Services (ITS) or Office of the General Counsel. Clicking on an agreement binds you as an individual and not the University to the terms of use absent authorized and documented University approval.

This document is not an endorsement by ITS for the use of public cloud services to conduct University business. 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 consumer grade/personal 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 protected or private information per 4-OP-H-12 Information Privacy Policy. If FSU (includes faculty and staff) decides to contract a third-party for the processing of protected or private information, this must be regulated in a written agreement, in which the rights and duties of FSU and the third-party contactor in addition to any subcontractors engaged by the primary third-party contractor are specified. A third-party contractor shall be selected that will guarantee the technical and organizational security/privacy measures required in this privacy policy and provide sufficient guarantees with respect to the protection of the information. FSU provides a terms and conditions document containing privacy and security provisions for information sharing agreements involving protected or private information.

- ✓ 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.

- ✓ Consumer grade/personal 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 consumer grade/personal cloud service agreements 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.

- ✓ Consumer grade/personal cloud service users conducting University business should understand provisions of State mandated public records retention and disposal provisions. https://vpfa.fsu.edu/records-schedule

- ✓ 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 or public records request resulting in the cloud service provider forwarding all account material including personal data items to fulfill the request.

- ✓ The individual may lose access to data should a consumer grade/personal 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, 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 consumer grade/personal cloud services should the user terminate employment.

Policy/Legal References

- 4-OP-H-12 Information Privacy Policy
- 4-OP-H-5 Information Security Policy
- 4-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 501.171 Security of confidential personal information.
- Florida Statute 119 and Florida State University Regulation 6C2R-2.023 Administrative Matters for public records