Information Security Services

WSU Guideline: Cloud Computing

Cloud Computing Adoption, Implementation and Utilization

Author(s): Keela Ruppenthall

Date: May 20, 2016

Version: 2.2

WASHINGTON STATE UNIVERSITY

Revision History

Version No.	Date	Description	Author
1.0	5/20/16	Initial Release	Ruppenthall, Keela
2.0	11/02/16	Complete Revision	Ruppenthall, Keela
2.1	3/15/17	Appendix C Update	Ruppenthall, Keela
2.2	10/04/19	Appendix C Update	Ruppenthall, Keela

Approvals

Tom Ambrosi, ITS Senior Director & CISO — Date: 4/20/2017

Dr. Sasi Pillay, VP Information Technology & CIO — Date: 4/20/2017

1. Contents

2. Introduction

This guideline contains the Washington State University (WSU) Information Security Services (ISS) guidelines for using cloud computing services to support the processing, sharing, storage, and management of University data. This document provides recommendations to facilitate successful adoption of cloud computing services using industry best practices.

3. Purpose

"Cloud services" represent a growing variety of useful services available on the internet. Cloud-based service and application offerings from external providers are developing rapidly and they promise to provide useful services and increased efficiencies to WSU faculty, staff and students. The business models and terms of use for these services and applications pose a variety of risks to users.

The primary purpose of this guideline is provide guidance for adopting, implementing and utilizing cloud storage and/or cloud computing services. The National institute of Standards and Technology (NIST) SP 800-145 provides a recommended definition of Cloud computing:

> "Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. "

To be considered a cloud storage and/or cloud computing service, the service provider must offer all 5 essential characteristics outlined in NIST SP 800-145; on-demand self-service, broad network access, use pooled resources, provide for rapid elasticity, and the service must be measured.

The secondary purpose of this guideline is intended to provide recommendations to help individuals make informed choices regarding the appropriate use of cloud-based services for storage and processing University Data.

4. Scope

This WSU Guideline is recommended for use when considering services and applications utilizing the cloud computing model. Cloud computing has three primary service models, Software as a Service (Saas), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) which can be deployed as Public, Private, Community and Hybrid.

This WSU Guideline applies to all WSU data that is shared, processed, stored, accessed, or transmitted by any cloud storage and/or cloud computing service.

This guideline applies to all University data accessible to authorized users, to include faculty, alumni, staff, students and affiliates.

This guideline does not supersede WSU Executive Policies (EP), Business Policies and Procedures Manual (BPPM), Safety Policy and Procedure Manual, Human Resource Policies or any other policy or process prepared and maintained by WSU.

5. External Requirements/Drivers

WSU is required to comply with Federal and/or State laws and regulations related to information security, privacy and data confidentiality. This guideline complies with regulations as defined by:

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH Act)
- Sarbanes Oxley Act (SOx)
- Payment Card Industry Data Security Standard (PCI DSS)
- Protected Personal Information (RCW 19.255.010; RCW 42.56.590)
- Federal Trade Commission (FTC) Red Flag Rule (Identity Theft Regulation)
- Regulations Governing the Protection of Research Data (e.g., FISMA, CUI, Uniform Trade Secrets Act RCW 19.108)
- National Security Information

This Policy satisfies part or all of the following controls from NIST Special Publication 800-53 rev. 4:

- AC -20: USE OF EXTERNAL INFORMATION SYSTEMS
- CA-3 SYSTEM INTERCONNECTIONS
- SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

6. Guidelines

6.1. Acquiring Services

There are a number of information security and data privacy risks to consider when using cloud storage and/or cloud computing services. There are also legal concerns with the use of cloud computing because cloud-computing relationships are governed by contract law. It is important to address the following items prior to entering into any contract to use or purchase cloud computing services.

- Data Definition and Use
- General Data Protection Terms
- Compliance with Legal and Regulatory Requirements

- Service Level Expectations and Performance Metrics

When specific questions about the implications and risks of using an externally hosted service are not answered here, the individual user should consult with the IT organization that supports their area.

6.1.1. Self-provisioned cloud-based services should not be used conduct official WSU business or to share, process, store, access, or transmit WSU data.

6.1.2. All contracted cloud-based services and applications, external to WSU, are required to be reviewed per WSU BPPM 70.24: Acquistion of Computer Equipment, Services, or Software . Appendix B: WSU Data Security and Confidentiality Language should be appended to all contracted services and applications.

6.1.3. Both the University and cloud-computing vendor should understand the type of data that they might transfer back and forth because of their relationship. A contract should have clear terms that define the data owned by each party. The parties should also clearly define data that must be protected.

6.1.4. Many cloud providers utilize a non-negotiated terms of use policy. Prior to adopting a cloud provided service, the cloud service sponsor should review and understand the cloud provider terms and conditions of use.

6.1.5. Consideration should be taken with regards to Control of User Content. A cloud-based service or application that grants the service provider rights to user content is not is not allowed without approval from the appropriate University or legal authority.

6.1.6. The contract should specifically identify University owned data. It should also classify the type of data shared in the contract according to the University's classification schema as described in WSU Executive Policy #8 (University Data Policies). It is recommended to exercise due diligence and closely examine the contractual terms when sharing sensitive or restricted data within a cloud computing service. WSU EP 8 – University Data Policy requires approval of the data steward to release data to 3rd parties for contracting.

6.1.7. Very careful consideration should be taken with regards to Information Security and Privacy. A preliminary risk assessment should be conducted to prevent direct or indirect disclosure of University Confidential, Proprietary, or Privileged data. Vendors are not permitted to use University data in any way that violates federal, state, or local laws and regulations, or University policies.

6.1.8. It is recommened to utilize a service provider that displays a commitment to data security, privacy, and information assurance. Cloud-based contracting language should be included to ensure an appropriate level of information security and privacy protection. Approved University contracting language for cloud-based and external hosting services is shown is Appendix B: WSU Data Security and

Confidentiality Language. Appropriate contract language should include provisions for:

- Evidence of compliance with the appropriate laws, regulations, policies, and standards
- Data transmission and encryption requirements
- Authentication and authorization mechanisms
- Intrusion/breach detection and prevention mechanisms
- Logging and log review requirements
- Incident Response
- Security scan and audit requirements
- Security training and awareness requirements
- Cloud Computing Consumer Guidelines
- Notice of possible data threats or breach

6.1.9. WSU BPPM 90.00 - Records, outlines the University Records Retention requirements. Cloud-based services and applications that store data records listed in BPPM Policy 90.00 are required to meet federal, state and local regulations. Consideration should be taken with regards to the service providers backup and data purging policies and procedures to ensure compliance with BPPM 90.00 for all University records to include, records that fall outside of WSU BPPM policies. Providers cannot delete or destroy records without the permission of the university.

6.1.10. The service provider agreement should address notification when non-negotiated changes are permissible by the terms of use, service, or business model to ensure adequate time to seek supplemental or replacement services and change to the operational environment.

6.1.11. Proprietary data formats may prevent the ability to copy, remove or use the data with other applications. All cloud-based services and applications should to use commonly used data formats. Cloud-based service providers that provide data conversion assistance to facilitate the exit strategy are recommended when using proprietary data formats.

6.1.12. Service level agreements make sure that the contract specifies service level expectations and includes performance metrics. Language regarding service availability time, service outages, routine maintenance timeframes, hardware and software upgrades, and changes to cloud-computing services should be included in the contract agreement.

6.1.13. Faculty, staff or administrators that use a cloud-based service to share, process, store, access, or transmit WSU Non-Public or WSU Confidential Data should utilize cloud-based services and applications authorized by formal University negotiated contractual agreements.

6.1.14. Consolidation of services is encouraged. As such, faculty, staff and administrators are urged to utilize University wide cloud-based services and applications that have been vetted and implemented for the organization as a whole.

6.2. Access

6.2.1. Access to the cloud-based service or application be should be restricted where technically and operationally feasible and based on WSU business need.

6.2.2. Cloud-based services or applications that require users to use their WSU NID for authorization require formal approval in the form of a University negotiated contractual agreement. A formalized engineering review and risk assessment should be preformed.

6.2.3. The use of WSU federated identification systems for authentication and authorization to cloud-based services and applications is recommended for campus-wide services.

6.2.4. Access to the cloud-based service or application should comply with WSU EP-8 University Data Policy and EP-18 User ID and Password policy, where technically feasible.

6.3. Appropriate Use

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered or destroyed without authorization.

6.3.1. WSU data classification levels are outlined in WSU EP-8 University Data Policies and should be used to determine what baseline security controls are appropriate for safeguarding that data.

6.3.2. EP-8 University Data Policy establishes that Data stewards have charge over University data and are responsible for its safekeeping. In turn, faculty, staff, and others with access have a responsibility to appropriately use and effectively protect University data.

6.3.3. Classification definitions for data are outlined in the WSU EP-8 University Data Policies. The WSU Cloud Acceptable Use Matrix - Appendix C is intended to provide information for faculty, staff and students about the considerations and limitations

for using the externally hosted computing services that have been arranged by university IT organizations.

6.3.3.1. While there are examples of specific use cases and data types referenced in this summary, there may be data and concerns that are not addressed here.

6.3.3.2. University organizations should be responsible for publishing any specific guidelines for use of the technologies that they support.

6.3.4. The appropriate use of any technology assumes individual compliance with all university policies, legal and regulatory requirements, and funding agency requirements.

6.3.5. Loss or exposure of data that result from the inappropriate use of technology may be considered a violation of the university's information security or computer use polices, other compliance requirements, or state and federal law.

6.4. Data Protection and Records Retention

6.4.1. EP-8 University Data Policy identifies Non-Public Data and Confidential Data as sensitive. All information users are responsible for protecting and ensuring the security of the information to which they have access.

6.4.2. WSU BPPM Records 90.00; outlines the requirements for retention of electronic data. University Staff and departments are responsible for adhering to all University policies regarding the management and retention of electronic data records as outlined in BPPM 90.00.

6.4.3. Cloud-based services and applications that do not adhere to Appendix B: WSU Data Security and Confidentiality Language, are not approved to receive, process, store, access or transmit WSU Non-Public or Confidential Data.

6.4.3.1. Using a cloud-based service or application **does not** absolve WSU employees, to include faculty and staff, from ensuring data is properly and securely managed.

6.4.4. Use of cloud-based services or applications should comply with all laws and regulations governing the handling of WSU data. This includes, but is not limited to, data protected by State of Washington OCIO policies, WSU Information Security and Data Policies, FERPA, GLBA, or HIPPA.

6.5. Exit Strategy

6.5.1. Exit strategies provide a contingency plan to migrate records securely to another solution, non-cloud or cloud, while maintaining business continuity.

6.5.2. A documented exit strategy is recommended for all cloud-based services or applications.

6.5.3. Cloud-based services and applications authorized by formal University negotiated contractual agreements should have a clearly outlined exit strategy defined prior to implementation.

6.5.4. The exit strategy should consider what data will need to be archived, where it will be archived, the method to transfer it, how it will be destroyed and how destruction will be verified together with the security requirements associated with these processes.

7. Review Cycle

This guideline will be reviewed by ISS at least once annually.

Appendix A: Glossary

Acronyms

Acronym	Definition
BPPM	Business Policy and Procedure Manual
EP	Executive Policy
IaaS	Infrastructure as a Service
ISS	Information Security Services
NID	Network Identifier
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
Saas	Software as a Service
WSU	Washington State University

Terms

Term	Definition
Due Diligence	Due diligence is the process of systematically researching and verifying the accuracy of a statement.
Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited users-specific application configuration settings.

Appendix B: WSU Data Security and Confidentiality Language

Data Security and Confidentiality:

Revised 6/25/2013

As used herein, the term "WSU" shall mean "Client" and the term "Vendor" shall mean "XXXXX". In this Agreement, the party receiving information is generically referred to as the "Receiving Party," and the party disclosing the information is generically referred to as the "Disclosing Party."

a) Confidential Information Defined

In performance of this Agreement, parties may directly or indirectly disclose confidential information, proprietary information, or confidential data ("Confidential Information").

"Confidential Information" shall include any data and/or information that is identified by either party as confidential (either orally or in writing) or is of such a nature that a reasonable person would understand such information to be confidential, including, but not limited to: (1) personal information of customers, employees, students, and/or donors, including but not limited to, images, names, addresses, Social Security numbers, e-mail addresses, telephone numbers, financial profiles, credit card information, driver's license numbers, medical data, law enforcement records, educational records or other information identifiable to a specific individual that relates to any of these types of information ("Personal Information"); (2) business methods, plans, and practices, financial data, or customers lists; (3) trade secrets, inventions, methodologies, research plans, products, product plans, patent applications, and other proprietary rights, and any specifications, tools, computer programs, source code, object code, documentation, or technical information; or (4) any other proprietary information or data the Disclosing Party maintains in confidence.

Confidential Information shall not include information the Receiving Party can prove by clear and convincing written contemporaneous evidence is: (1) publicly known through no fault or negligence of the Receiving Party; (2) rightfully possessed by the Receiving Party prior to disclosure by the Disclosing Party; (3) rightfully obtained by the Receiving Party from a third party in lawful possession of such Confidential Information without obligation of confidentiality; (4) independently developed by the Receiving Party without reference to or use of Confidential Information; (5) required to be disclosed by law; or (6) necessary to disclose to prevent severe physical injury to or loss of life of an individual.

b) Use and Non-Disclosure of Confidential Information; Exceptions

Each party agrees to use the Confidential Information received from the other party only as expressly permitted in this Agreement or when reasonably necessary to perform the party's duties under this Agreement so long as such disclosure is in accordance with applicable law. To the extent permitted by law, neither party will disclose to any third party the other party's Confidential Information, in whole or in part, without the prior written consent of the party, or as provided for in this Agreement and incompliance with all applicable state and federal laws; provided however, Vendor may disclose Personal Information of WSU Students to third party with the written consent of that Student. Notwithstanding the foregoing, either party may

disclose the Confidential Information or portions thereof to their respective attorneys or accountants when seeking legal or financial advice.

Vendor specifically warrants and represents that except as otherwise permitted herein, it will not in any manner disclose, disseminate, copy, sell, resell, sublicense, transmit, assign, or otherwise make available any of WSU's Confidential Information to any third party without the prior written permission of WSU, and further warrants and represents that it will take all reasonable steps necessary to ensure that its authorized agents, employees, contractors or subcontractors having access to the Confidential Information shall not copy, disclose or transmit any of the Confidential Information, or any portion thereof, in any form, to a third party except as necessary to perform the Services under the Agreement.

Vendor acknowledges that WSU, as a state agency, is at all times subject to the Washington Public Records Act, RCW 42.56.010 et seq. as now existing or as amended. If WSU receives a public records request for this Agreement and/or for documents and/or materials provided to WSU under this Agreement, generally such information will be a public record and must be disclosed to the public records requester. However, WSU agrees to notify Vendor if it receives such a public records request and the date WSU plans to release the records. If Vendor fails to obtain a protective order from the applicable court prior to the time WSU releases the records to the public records requester, Vendor gives WSU full authority to release the records on the date specified, and Vendor understands it shall hold WSU harmless with respect to such disclosure.

c) Obligations to Secure Confidential Information

Vendor warrants and represents that it will implement the necessary industry-standard physical, electronic, and managerial safeguards to ensure the confidentiality, integrity, and availability of WSU Confidential Information, including but not limited to, the environment in which the WSU Confidential Information is stored, processed, and transmitted. Vendor further warrants and represents that such safeguards will in no event be less than the level of security Vendor uses to protect its own Confidential Information. Vendor shall require its contractors and subcontractors authorized to access WSU's Confidential Information pursuant to this Agreement to take similar industry-standard precautions in safeguarding the Confidential Information.

Vendor agrees to comply with all applicable state and federal statutes and regulations governing unauthorized access and disclosure of the Confidential Information including, but not limited to: (1) personally identifiable information from education records as defined in The Family Educational Rights and Privacy Act ("FERPA") (20 U.S.C. § 1232g; 34 CFR Part 99), and regulations promulgated thereunder; (2) information that is subject to the security provisions of the Gramm-Leach-Bliley Act, 15 U.S.C.,

Subchapter 1, Sections 6801-6809 (Disclosure of Nonpublic Personal Information); (3) individually identifiable "personal health information" as defined in the Health Information Portability and Accountability Act ("HIPAA") regulations, 45 CFR Parts 160 and 164; and (4) the Washington State Office of the CIO ("OCIO") Standard No. 141.10 " Securing Information Technology Assets" (available at

http://www.ofm.wa.gov/ocio/policies/documents/141.10.pdf) or comparable standard. Any transmission, storage, or transportation of WSU Confidential Information outside of the U.S.A. is prohibited without prior written authorization from WSU.

Prior to execution of this Agreement and once per calendar year, Vendor will provide WSU with the most current SSAE 16 Report or comparable, 3rd party information security assessment report. WSU shall have the right, at its own expense and upon reasonable prior notice to Vendor, to review Vendor's security measures and information security program.

If Vendor will accept and process payment by credit cards or any other form of electronic payment on behalf of WSU pursuant to this Agreement, Vendor agrees to provide evidence of certification for the Payment Card Industries Data Security Standard ("PCI DSS"). Proof of compliance shall be provided to WSU by Vendor on an annual basis for the duration of this Agreement. WSU reserves the right to monitor, audit or investigate said certification. If Vendor fails to achieve or maintain PCI DSS compliant status, Vendor will cease the acceptance and processing of payment cards or any other form of electronic payment on behalf of WSU pursuant to this Agreement, as well as the acceptance of any other Confidential Data or other proprietary data on behalf of WSU.

d) Obligations upon Breach of Security

The Confidential Information, including any Personal Information, is subject to the provisions of RCW 19.255.010 and RCW 42.56.590 and Vendor will comply with those laws. Vendor will report to WSU any breach of security resulting in the unauthorized disclosure, misappropriation or unauthorized access of WSU Confidential Information ("Breach"). Vendor will promptly investigate any Breach affecting WSU Confidential Information and take reasonable measures to identify the Breach's root cause(s), mitigate its effects, and prevent a recurrence. Unless prohibited by law, Vendor will provide WSU with a detailed description of the Breach, the type of data that was the subject of the incident, the identity of each affected person, and other information WSU may reasonably request concerning the affected persons. The parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected persons. If a data compromise and/or identity theft occurs and is found to be the result of Vendor's non-compliance with the obligations to secure WSU Confidential Information, Vendor will assume complete responsibility for customer notification, and be liable for all associated costs incurred by WSU in responding to or recovering from that Breach.

e) Survival of Obligations

The obligation to maintain the confidentiality of the Confidential Information received by the other party will survive termination or expiration of this Agreement, and shall survive for a period of five (5) years thereafter. Except as otherwise set forth below, within sixty (60) days of the expiration or termination of this Agreement, Vendor shall, at Vendor's option: (1) certify to WSU that Vendor has destroyed all WSU Confidential Information in its possession; or (2) return all media containing all WSU Confidential Information to WSU; or (3) take whatever other steps WSU requires of Vendor to protect WSU's Confidential Information. WSU reserves the right to audit, or investigate the use of WSU Confidential Information collected, used, or acquired by

Vendor or its employees, contractors or subcontractors pursuant to this Agreement. Any costs of such audit or investigation are the sole responsibility of WSU.

Appendix C: WSU Cloud Acceptable Use Matrix

WSU Cloud Acceptable Use Matrix

Permitted services have been reviewed to assess security capabilities and are only suitable for use if WSU security control requirements are properly applied.

					CONFIDENTIAL - REGULATED Data Types								
		Public	Human Subjects De-Identified	Non-Public	Student Education Records (FERPA)	Personal Information (RCW 42.56.590)	Human Subjects Identifiable	Student Loan Application Data (GLBA)	Protected Health Information (HIPAA)*	Payment Card Information (PCI)	Export Controlled Research (ITAR/EAR)	Federal Information Security Management Act (FISMA)	EU General Data Protection Regulation (GDPR)
	University Services												
University Services are considered a preferred choice.	Office 365 Email	●	●	●	●*	●*	▲	●*	▲	▲	▲	▲	▲
	Proofpoint Secure Email	●	●	●	●	●	●	●	▲	▲	▲	▲	▲
	ZOOM	●	●	●	●	▲	▲	●	▲	▲	▲	▲	▲
	Zoom Health	●	●	●	●	■	■	●	●**	▲	▲	▲	▲
	OneDrive	●	●	●	●	●	●	●	■**	▲	▲	▲	▲
	Teams - Modern Groups /Sites	●	●	●	●	●	●	●	▲	▲	▲	▲	▲
	Qualtrics	●	●	●	●	●	▲	●	▲	▲	▲	▲	▲
	Redcap	●	●	●	●	●	●	●	■**	▲	▲	▲	▲
	Azure	●	●	●	●	●	●	●	■**	▲	▲	▲	▲
	Amazon Web Services	●	●	●	●	●	●	●	■**	▲	▲	▲	▲
	Other Services												
	Box	■	■	■	■	■	■	■	■	▲	▲	▲	▲
	Dropbox	■	■	■	■	■	■	■	■	▲	▲	▲	▲
	Google Drive	■	■	■	■	■	■	■	■	▲	▲	▲	▲

De minimis Use Rule: Appropriate use of state-provided resources for personal use is defined in WSU BPPM 20.37 – Personal Use of University Resources.

Intuitional data is not permitted to be stored on individual or personal cloud services.

WSU Internal to WSU Internal Only

****Enterprise level BAA exists*** (3rd parties that create, receive, maintain, or transmit HIPAA data on behalf of, or for the benefit of, WSU, whether directly or through another business associate, are required to include a Business Associates Agreement as part of the contract agreement.)

Legend			
●	Permitted (Must comply with all appliable laws, regulations and WSU Policy)		Permitted with Compliance Audit
■	Permitted with contract and must comply with all appliable laws, regulations and WSU Policy	▲	Not Permitted