DIVISION: **Administration**	
SUBJECT: Cloud Security Use Policy	Page 1 of 14
Policy Number:	Supersedes: **None**
Effective Date:	Previous Issued: **N/A**

Overview

A basic element of any institution of higher learning's information security program is the protection of information resources that support the critical operations of the institution from unauthorized access, modification, or disclosure. The use of cloud solutions is expected to continually increase, thus the importance of adhering to this cloud security policy and subsequent set of guidelines that direct the decision making process to minimize risk is vital.

1.0 Policy Statement

Information Technology Services must be involved in the onboarding process for services that result in LMU content of an administrative nature specifically personally-identifiable information protected by privacy legislation, such as FERPA, being collected, processed, or stored in a non-LMU data center. Services for purposes of an academic nature are excluded from this policy. No individual shall be permitted to collect, process, or store data used for the administration of Loyola Marymount University in a non-sanctioned cloud-based service without written approval by the Chief Information Officer. All procurements for cloud services must be evaluated using the following cloud security guidelines.

2.0 Defining the Cloud

The term “cloud” has been a widely used metaphor to describe a variety of services provided by vendors. These services are categorized into three primary paradigms – Software-as-a-Service (SaaS), Platform-as-a-service (PaaS), and Infrastructure-as-a-service (IaaS).

2.1 Software-as-a-Service (SaaS) - Primarily focused on services for end users with the following characteristics:

- Software is managed in a central location, generally off site
- Licensees and their users do not perform upgrades or patches
- Generally accessible via web rather than through a terminal service
- Software was built for this paradigm model versus the simple hosting of software accessible remotely

Examples of SaaS providers include Google Mail (email); Salesforce (CRM); WorkDay (HR); NetSuite (Finance); Box/DropBox (Content Management); Facebook (Social Media); WebEx (Collaboration); and Blackboard (Learning Management).

2.2 Platform-as-a-service (PaaS) – Primarily focused on services for developers, PaaS provides an environment for developers to create web applications without the need to purchase and support the software and infrastructure needed for development. **Platform-as-a-Service (PaaS)** is primarily focused on services for software developers with the following characteristics:

- Services to develop, test, deploy, host and maintain applications
- Web-based tools to create, modify, test and deploy different UI scenarios
- Web services and databases integration via common standards

Examples of PaaS providers include Google App Engine and Microsoft Azure Services.

2.3 Infrastructure-as-a-service (IaaS) – Primarily focused on services for system administrators, IaaS is primarily focused on services for system administrators with the following characteristics:

- Policy-based resources
- Automation of administrative tasks
- Dynamic scaling

Examples of IaaS providers include Amazon Web Services and Rackspace. IaaS also includes services such as Storage-as-a-Service, Database-as-a-Service, and Security-as-a-Service.

3.0 Confidentiality and Privacy

3.1 Legislation Requirements - Loyola Marymount University is obligated to regulations such as GLBA, HIPAA, and FERPA to protect educational records. Placing those records in the cloud introduces new risks.

"*Education records*...means those records that are: (1) Directly related to a student; and (2) Maintained by an educational agency or institution or by a party acting for the agency or institution". As such, contractual provisions should be made to acknowledge and set the expectation between parties that LMU data is protected by one or more of these regulations and that LMU data stored by a 3rd party does not absolve any party from these requirements.

3.2 Export controls – Legislation (such as the International Traffic in Arms Regulations (ITAR) should be considered when storing information that may be hosted in data centers outside the United States or where foreign nationals may have access to the data even under normal system administration duty scenarios. Therefore, priority should be given to solutions that guarantee storage of data in the United States or guarantee compliance with the Federal Information Security Management Act (FISMA) and Federal Information Processing Standards (FIPS 140-2 Level 4). This particularly pertains to research that may be developed or used for research purposes by the University.

3.3 Stewards of Federal Data - The Federal Information Security Management Act (FISMA) requires federal agencies and those providing services on their behalf to develop, document, and implement security programs for information technology systems and store the data on U.S. soil. This means that, under some federal contracts or grants, information the University collects or information systems that the University uses to process or store research data need to comply with FISMA. Whether data is regulated by FISMA is typically called out in a Request for Proposal (RFP) in contract language or grant language. It is important that researchers review grants and contract language closely to identify FISMA or other information security requirements.

3.1. **Encryption** – Encryption is a crucial part of maintaining confidentiality and privacy of LMU data. Therefore, all data at rest and in transit between a cloud provider and the end user must be encrypted. At the time of this writing, the minimum standard for data at rest is 128-bit AES encryption, though 256-bit AES encryption is preferred. All data in transit must use a public key asymmetric algorithm of which a 1024-bit RSA key is the de

facto standard to be used. The Director of Information Security and Compliance must approve any exceptions.

4.0 Data Breach Responsibilities and Security

4.1 Notification - Data breaches, generally, but depending on the data attributes breached carries with it an obligation to notify. Contractually, LMU will attempt to hold the vendor duty-bound to minimally notify LMU of any breach. Contractually, vendors should assume responsibility for breach notifications:

> (VENDOR) agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of personally identifiable information or other event requiring notification. In the event of a breach of any Customer Data, (VENDOR) agrees to (1) notify Customer by telephone, email, and certified mail of such event within 24 hours of discovery; (2) assume responsibility for informing all such individuals in accordance with applicable law; (3) indemnify, hold harmless and defend LMU and its trustees, officers, and employees from and against any claims, damages, or other harm related to such Notification Event.

5.0 E-Discovery (discovery requests of electronic data and/or legal holds)

5.1 Administrative Access – Consideration is needed in handling e-discovery requests and other litigation holds:

- Will the vendor facilitate these requests?
- Is there a procedure outlined by the vendor for these types of events?

6.0 Risk Evaluation

6.1 *Confidential Information* – Prior to signing any contract with a cloud vendor, all data attributes should be defined and reviewed by the Information Security team (i.e. personally identifying information). Use of social security numbers or driver's license numbers is prohibited. The appropriate data steward should review use of any student data:

> "Confidential Information" means any proprietary or confidential information as such terms are most broadly

> defined under common or federal, state and local law including, without limitation, the Family Educational Rights and Privacy Act ("FERPA") and California Uniform Trade Secrets Act, and shall extend to all personal and private information (and all organizations, listings, distillations and analysis thereof) pertaining to Customer's student data, it's and their personnel data, inventory information and other related data (collectively "Customer Information"). Each party agrees that it (i) will not copy or use any of the other party's Confidential Information in any way, except as permitted by this Agreement or as required to achieve the purposes of this Agreement, (ii) will not disclose any of the other party's Confidential Information to any third party, except as required by law or to that party's attorneys and accountants as reasonably necessary, and (iii) will protect the other party's Confidential Information reasonably and at least as well as it protects its own. Information is not Confidential Information if a party can clearly show that it (i) became known to the receiving party prior to receipt from the disclosing party, (ii) has become publicly known, except through breach of this Agreement, or (iii) is independently developed without reference to Confidential Information.

6.2 Data Mining – Consideration should be made to exclude contractually the ability to mine any data for the benefit of the vendor or vendor's agents (advertisers, etc.).

6.3 Indemnification – Contractually, both parties should have language to indemnify each other:

> (VENDOR) shall indemnify, defend (by counsel reasonably acceptable to LMU) and hold harmless Loyola Marymount University and its officers, directors, agents and employees from and against claims, damages, losses and expenses, including but not limited to attorneys' fees, arising out of or resulting from the negligence or misconduct of Vendor in connection with performance of the work described in this Agreement.

6.4 Warranty – Contractually, the vendor should warrant that the use of their solution does not infringe on a 3rd party.

> (VENDOR) warrants against any claims of infringement from third parties by reason of LMU's use of its service and software.

6.5 Responsibility for End Users – Identify the responsibilities that are forced upon our end users. These may include actions inhibiting use of vendor's intellectual property, disclosing intellectual property or other confidential information, or sharing account credentials. Ensure that all LMU parties are informed of any contractual responsibilities.

6.6 Patent / Copyright Infringement – Contractually, the following clause should be included to protect LMU data that will be stored in the vendor's or sub-contractor's facilities:

> (VENDOR) acknowledges that all Customer Information and related data is owned exclusively by Customer and (VENDOR) shall acquire no ownership or continuing rights in or to said Customer Information and data by virtue of this Agreement or the parties' respective use of the (VENDOR) service, software or forms under this Agreement.

6.7 Choice of Law and Jurisdiction – Ensure that the choice of law and jurisdiction is located in the United States. California is preferable but not mandatory.

6.8 Procurement Practices – The Information Security team should be notified and ample time be provided for an information security assessment prior to any contracts being signed for services that involve vendors collecting information from LMU constituents, storage of LMU data, and/or authenticating LMU accounts.

6.9 Historical Availability – Prior to signing a contract for cloud services, a thorough review of past outages or lack of service availability should be considered:

- Does the vendor have a reputation for service outages?

6.10 Vendor Infrastructure – Understanding the vendor's infrastructure is critical to understanding how services are provided:

- Is there a third-party interdependence to provide the service in which they are contracted to perform?
- Are they sublicensing another vendor's software?
- Does the vendor support their own data center?
- What redundancies are built in to their infrastructure?
- What type of data center do they use as per ANSI/ TIA-942?

Tier Level	Requirements
1	• Single non-redundant distribution path serving the IT equipment • Non-redundant capacity components • Basic site infrastructure with expected availability of 99.671%
2	• Meets or exceeds all Tier 1 requirements • Redundant site infrastructure capacity components with expected availability of 99.741%
3	• Meets or exceeds all Tier 2 requirements • Multiple independent distribution paths serving the IT equipment • Dual-powered and fully compatible IT equipment made with the topology of a site's architecture • Concurrently maintainable site infrastructure with expected availability of 99.982%
4	• Meets or exceeds all Tier 3 requirements • Independently dual-powered cooling equipment, including chillers and heating, ventilating and air-conditioning (HVAC) systems • Fault-tolerant site infrastructure with electrical power storage and distribution facilities with expected availability of 99.995%

6.11 LMU Technology Standards

- Does the vendor's solution adhere to technical standards outlined in the LMU Technical Standards document?

6.12 Cloud Architecture - Private cloud versus Public cloud

- Is the solution that is being procured being fully hosted by the vendor or are there any components that will be placed on site?
- Have the risks been reviewed to address communication between components hosted onsite and those offsite?
- Is the vendor managing the components hosted onsite?
- How will they securely perform those functions?

6.13 Service Management - Contractually, the following clause should be included to assist in managing vendor's material service changes:

> During the life of this contract,(VENDOR) shall notify Loyola Marymount University at an email address provided by Loyola Marymount University within 30 days preceding any material changes to (VENDOR'S) services that affect the infrastructure, security, or user interface.

- Does the vendor subscribe to ITIL practices for managing services and specifically change management?
- Will the vendor be amenable to ensuring changes are completed during acceptable maintenance periods?
- Are these maintenance periods outlined contractually?
- Will we be notified before changes are made?
- Are we sharing the service with other clients or is our "instance" separate from other clients of the vendor?

7.0 Business Continuity

7.1 Suspension/Termination of Services – Consideration should be made for providing business services in the event that the contracted vendor is no

longer able to provide the contracted service due to the incapacity of the vendor's technology infrastructure beyond the scope of a brief outage.

7.2 Service Level Agreements (SLA) – Address clearly the SLA expectations for service if the vendor's services are unavailable. More information is provided in paragraph 8.4 Managing Vendors-Service Agreements.

7.3 Access to Data After Termination – Contractually, expectations should be established for access to data after a contract is terminated:

> If this Agreement terminates, (VENDOR) will provide Customer access to, and the ability to export Customer data immediately and for a commercially reasonable period of time.

8.0 Managing Vendors

8.1 Cloud Paradigm

- What type of provider is being procured?
- Is the solution completely hosted by the vendor or are their components hosted on site?

8.2 Definition of Availability – The definition of availability can be ambiguous at times, but the definition that should be adhered to is that the service is not only online but its basic functionality is available to the end user. Basic functionality being defined as the primary use of the service by the average end user.

8.3 Service Probes (HTTP Get, API, etc.) – During vendor evaluation, it should be determined how LMU can monitor service availability:

- Are we contractually permitted to use monitoring tools or is there a vendor provided API?

8.4 Service Agreements – All contracts should outline expectations of service that include the responsibilities of both parties:

- The availability of services should be no less than 99% uptime (including scheduled maintenance).

Availability %	Downtime per year	Downtime per month*	Downtime per week
90% ("one nine")	36.5 days	72 hours	16.8 hours
95%	18.25 days	36 hours	8.4 hours
97%	10.96 days	21.6 hours	5.04 hours
98%	7.30 days	14.4 hours	3.36 hours
99% ("two nines")	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes
99.9% ("three nines")	8.76 hours	43.2 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes
99.99% ("four nines")	52.56 minutes	4.32 minutes	1.01 minutes
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds
99.9999% ("six nines")	31.5 seconds	2.59 seconds	0.605 seconds

8.5 Vendor Accountability – A process needs to be implemented to actively manage the availability of services not controlled by ITS:

- Who notifies the vendor and is there a process established by the vendor to escalate service availability complaints?

8.6 Notice to LMU Users – A process needs to be implemented in which the vendor notifies LMU ITS when a service outage occurs longer than 10 minutes regardless if it is planned or not. This is to provide ITS an opportunity to notify end users in a proactive manner rather than in a reactive manner when end users are contacting ITS.

8.7 Documentation and Response – A member of ITS management should be assigned to be the liaison for managing the cloud vendor whose responsibility will include but not be limited to understanding the written contract; hold contact information of the vendor; report on service availability annually or upon request; document and escalate service availability issues when necessary.

9 Revision History

Version	Date	New
1.0	March 3, 2014	Draft for Review
1.1	March 21, 2014	Revision after initial ITS Director feedback
1.2	April 2, 2014	Revision to include cloud definitions and ITIL
1.3	April 25, 2014	Revisions to policy statement and formatting changes
1.4	May 19, 2014	Minor grammatical/spelling/format edits. Prepared for wider dissemination.

Version	Date	New
1.5	11/11/14	Formatting and language updates after administrative staff review.
1.6	9/1/15	Added Appendix for Data Classification and Review Type and other changes from initial UTC meeting.
1.7	2/17/16	Few modifications to Appendix A.

Appendix A
Cloud Service Onboarding Assessment Matrix

Prior to onboarding a cloud service for administrative use, review the type of data that will stored or collected in the cloud service. Information Technology Services (ITS) should be consulted prior to using a cloud service to minimize duplication of fees for services that may already be in use by other departments. Additionally, ITS and appropriate data stewards should be notified when data collected will be reused for multiple purposes and/or integrated into an existing database.

Data Collected	Collection Allowed in Cloud Service?	Notify ITS?	Security Assessment Needed?
Social Security Numbers	No, with some exceptions*	Yes	Yes, some critical business processes require collection of SSN. Any SSN collection must be through an approved service managed by ITS.
Driver's License Numbers	No	Yes	N/A
Personal banking account numbers	Yes**	Yes	Yes, any banking information collected must use an approved payment gateway managed by Treasury/ITS.
Credit Card Numbers	Yes**	Yes	Yes, All credit card transactions must use an approved payment gateway managed by Treasury/ITS.
Student Directory Information Student Directory Information – Includes: • Name • Address(es) • Telephone numbers • E-mail address(es) • Date and place of birth • Major field of study • Enrollment status • Participation in officially recognized activities • Dates of attendance • Anticipated degree and degree date • Degrees, honors, and	Yes	Yes	No

awards received • Most recent educational institutions attended • Weight and height of members of athletic teams • Photograph • A student's personal identifier used by the student for purposes of accessing or communication in electronic systems			
Student Information (non-directory)	Yes	Yes	Yes
Non-student information (Name, phone number, Address, email address)	Yes	No	No

* Exceptions can be made for specific business processes where using SSN as an identifier is required.
** Credit cards can only be collected by payment gateways vetted by ITS and Treasury departments.

	Student Directory Information – Includes: • Name • Address(es) • Telephone numbers • E-mail address(es) • Date and place of birth • Major field of study • Enrollment status • Participation in officially recognized activities • Dates of attendance • Anticipated degree and degree date • Degrees, honors, and awards received • Most recent educational institutions attended • Weight and height of members of athletic teams • Photograph • A student's personal identifier used by the student for purposes of accessing or communication in electronic systems	Medium – Consideration should be made regarding students that have filed a *Request for Non-Disclosure of Directory Information* with the LMU Registrar's Office.
3	Non-personally identifiable information	Low – Review of vendor can be expedited by Information Security Team.