I. Introduction

This Policy describes the requirements for appropriate and approved use of externally hosted Columbia University Systems and/or Data (as each is defined in the Columbia University Information Security Charter (the “Charter”) http://policylibrary.columbia.edu/information-security-charter. Capitalized terms used in this Policy without definition are defined in the Charter.

II. Policy History:

The effective date of this Policy is April 20, 2015.

III. Policy Text

External hosting of Systems and/or Data can be categorized as the following models:

Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

Platform as a Service (PaaS) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

Infrastructure as a Service (IaaS) is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it.

For the purpose of this document, the term cloud computing services is used to encompass SaaS, PaaS, and IaaS

For external hosted Systems and/or Data, each System Owner shall ensure that the Systems protections described in Section B and, if applicable, Sections C, D and E of the Registration and Protection of Systems Policy http://policylibrary.columbia.edu/registration-and-protection-systems-policy are implemented as well as compliance with requirements in the Data Classification Policy http://policylibrary.columbia.edu/data-classification-policy
If Sensitive Data and/or Confidential Data are stored on cloud computing services, the relevant contracts must be approved by the University’s Procurement Services and such System’s protections must be assessed by the applicable Information Security Office prior to implementation and reassessed on a periodic basis thereafter, as determined by the level of risk.

In addition to other University policies, the following requirements which must be followed in the use of cloud computing services:

**Pre-requisite Requirements**

- Consult with appropriate data owners, process owners, stakeholders, and subject matter experts during the evaluation process. Also, consult with the Office of the General Counsel or the applicable Information Security Office for guidance.

- Contractual requirements:
  
  o Both the University and vendor must declare the type of Data that they might transfer back and forth because of their relationship. A contract must have clear terms that define the Data owned by each party. The parties also must clearly define Data that must be protected.

  o The contract must specifically state what Data the University owns. It must also classify the type of Data shared in the contract according to the University’s Data Classification policy requirements. Departments must exercise caution when sharing Sensitive or Confidential Data (as defined by Columbia’s Data Classification Policy) within a cloud computing service.

  o The contract must specify how the vendor can use University Data. Vendors cannot use University Data in any way that violates the law or University policies.

- Ensure a Service Level Agreement (SLA) with the vendor exists that requires:
  
  • Clear definition of services;
  • Agreed upon service levels;
  • Performance measurement;
  • Problem management;
  • Customer duties;
  • Disaster recovery;
  • Termination of agreement;
  • Protection of sensitive information and intellectual property; and
  • Definition of vendor versus customer responsibilities, especially pertaining to backups, incident response, and data recovery.
• Cloud computing services should not be engaged without developing an exit strategy for disengaging from the vendor and/or service while integrating the service into normal internal business practices and/or business continuity and disaster recovery plans. The University must determine how Data would be recovered from the vendor.

• A proper risk assessment must be conducted by the applicable Information Security Office prior to any third party hosting or cloud computing service arrangement.

Intellectual property and copyright materials

• Columbia University marks, images, and symbols are owned by the University and may not be used or reproduced without the permission of the Office of Communications.

• Review copyright information [http://policylibrary.columbia.edu/copyright-information-network-users](http://policylibrary.columbia.edu/copyright-information-network-users) and understand the appropriate use of intellectual property including copyrights, trademarks, and patents.

Privacy and data security

• Information that the University has classified as “Sensitive Data”, “Confidential Data”, “Internal Data”, or “Public Data” may be used only in accordance with the policy related to the classification of information which may be found in the Data Classification Policy [http://policylibrary.columbia.edu/data-classification-policy](http://policylibrary.columbia.edu/data-classification-policy)

• Personally Identifiable Information (PII) may only be used in compliance with information protected by federal, state or local laws and regulations or industry standards, such as HIPAA, HITECH, FERPA, the New York State Information Security Breach and Notification Act, similar state laws and PCI-DSS.

• Student information may only be used in compliance with FERPA guidelines.

• Protected Health Information (PHI) may only be used in compliance with HIPAA requirements.

• Export Controlled Information may only be used in compliance with U.S. export control regulations (ITAR, EAR).

Data availability and records retention

• Ensure that all academic, administrative, or research related data are retained according to the records retention requirements.

• Back-up data regularly to ensure that records are available when needed, as many providers assume no responsibility for data-recovery of content.
Supplemental Requirements

The requirements lists set forth in this Policy are not comprehensive and supplemental controls may be required by the University to enhance security as necessary.

IV. Cross References to Related Policies and Other Documentation

The Information Security Policies and certain additional documentation referred to in this Policy are listed in Appendix A hereto.
Appendix A

Related Policies and Other Documentation

Business Continuity and Disaster Recovery Policy

Data Classification Policy
http://policylibrary.columbia.edu/data-classification-policy

Electronic Data Security Breach Reporting and Response Policy

Information Resource Access Control and Log Management Policy
http://policylibrary.columbia.edu/information-resource-access-control-and-log-management-policy

Information Security Charter
http://policylibrary.columbia.edu/information-security-charter

Information Security Risk Management Policy

Registration and Protection of Systems Policy
http://policylibrary.columbia.edu/registration-and-protection-systems-policy