CITY UNIVERSITY OF NEW YORK INFORMATION SECURITY POLICY

Acceptable Use of University Data in the Cloud

Issue Date: 8/19/2019

Issued By:
University Cloud Policy Advisory Group
University Chief Information Officer

Policy Owner:
Computing and Information Services

Purpose and Background

Cloud services potentially offer empowering benefits over traditional computing methods, such as ease of collaboration and sharing of information, lower cost, higher performance and faster delivery of services. This policy endorses the use of *University Data*[1] with cloud services in a manner that sustains the appropriate security standards that the University has adopted for data protection.

Requirements regarding the acceptable use of University Data with cloud services are detailed below. These requirements align with NIST 800-171[2] and other recognized cybersecurity standards, reflect common practices at institutions of higher education and supplement the CUNY *Acceptable Use of Computer Resources* and *IT Security Procedures* policies.

While a *Cloud Service Provider*[1] (CSP) may claim it is secure or compliant with regulations and compliance frameworks, the responsibility for data security and compliance with applicable laws and regulations rests primarily with the *Cloud Customer, Data Owner and Data User*[1], and, institutionally, CUNY. In other words, use of cloud services does not absolve CUNY, including faculty and staff, of the obligation to ensure that data is properly and securely managed.

Scope

This policy applies to all *University Entities*[1] using, or considering the use of, a Cloud Service Provider that can process, manage, create, collect, share or store University Data for any University purpose. Examples of cloud services include, but are not limited to, Internet-based web applications, commercial email and other messaging, social media, document storage and cloud platforms and infrastructure.

Personal use of cloud services on personal accounts is not subject to this policy.

[1] See *Definitions and Terms* below.
[2] See *Related Information* below.

Statement

It is the responsibility of the Cloud Customer, in consultation with the Data Owner, IT and legal counsel, to determine whether a particular cloud service and CSP can suitably maintain the required level of security and regulatory compliance on an ongoing basis. Further, since the use of cloud services involves, to a varying degree, delegating custody and aspects of data security to the CSP, the CSP must be contractually obligated, through a legally binding agreement with CUNY, to assume its delegated responsibilities.

In order to determine security protections commensurate with the level of required confidentiality, the Data Owner is responsible to evaluate, determine, document and share the classification of its University data with Cloud Customers according to CUNY's *Data Classification Standard*.[3] The *Data Classification Standard* defines three classification categories for University Data: *Confidential Data*, *Sensitive Data* and *Public Data*. Refer to the *Data Classification Standard* for detailed descriptions and pre-defined data types for these classification categories.

Sufficient security protections must be implemented to meet the most sensitive data potentially present (i.e., highest data classification) in a particular use of a cloud service irrespective of the presence of less sensitive data. It must not be assumed that University acquired cloud services are inherently suitable to secure any data.

Once a cloud service is implemented, on an ongoing basis the Cloud Customer must periodically assess whether cloud service security requirements remain satisfactorily in effect as required. Such assessments shall be conducted by the Cloud Customer (in consultation with the Data Owner(s) and IT) 1) prior to service renewal, 2) when service terms are changed by a CSP, 3) when the classification of data changes and 4) as otherwise required to support the bi-annual CUNY IT Security Attestation.[4]

Self-provisioned, personal cloud service accounts may not be used for Confidential or Sensitive Data.[5] Regardless of the classification of data used, cloud service accounts must comply with University licensing and legal requirements.

[3] See *CUNY IT Security Policies and Procedures* under **Related Information** below

[4] Ibid. *CUNY IT Security Procedures*

[5] That is, cloud service accounts not associated with a University procured or licensed service approved for use with such data

Classification	Use of Cloud Services
Confidential Data	Confidential Data is **NOT ALLOWED** to be processed, created, collected, stored nor archived in the cloud **UNLESS** the specific use and CSP security protections and certifications have been reviewed and approved by the University's Chief Information Security Officer (CISO) in consultation as necessary with Cloud Customer(s), Data Owner(s), College CIO(s), Information Security Manager(s) and relevant offices possessing expertise on the type of data involved, including Provost(s). Cloud services handling Confidential Data shall be assessed for security protections defined by NIST 800-171[*], including "basic" and "derived" security controls, as applicable.
Sensitive Data	Sensitive Data is **NOT ALLOWED** to be processed, created, collected, stored and archived in the cloud **UNLESS** the service is determined to support security controls as necessary to sufficiently protect the data. The 30 NIST 800-171[*] basic security controls (*Appendix B*) should be used to guide Sensitive Data security requirements. The Data Owner, College CIO and/or College Information Security Manager, or CIS for the Central Office, must be consulted to determine that adequate protections are present in the cloud service with documented approval. The University CISO shall be informed when Sensitive Data is approved to be stored in a cloud service by a campus. The appropriate CIO or designee shall share such approval with the University CISO.[6]
Public Data	Public Data is **ALLOWED** to be freely published, processed, created, collected, stored and archived in the cloud without restriction. Public Data should be made as widely accessible as appropriate to promote data sharing and transparency across the University. While disclosure of Public Data is by definition of little or no risk to the University, nevertheless, access, integrity and availability protections may be desirable for particular Public Data.

[*] NIST 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, defines 14 families of security requirements. (See *Appendix A*.) The 800-171 standard also maps to other recognized information security standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework.

[6] Until a formalized process for security assessment and approval is established, the University CISO should be informed by email to ciso@cuny.edu.

Cloud Service Provider Suitability

To determine whether a CSP can maintain the required level of data security based upon the classification of the data involved on an ongoing basis, and be suitable for the intended purpose, the Cloud Customer, in consultation with, and with the participation of, the Data Owner(s), IT and legal counsel, shall determine whether the CSP can:

- Meet security requirements sufficient to protect the University Data involved and support CUNY's required compliance with applicable laws, regulations and policies.
- Integrate well with University systems as necessary, including identity management.
- Avoid intermingling CUNY's data with that of other cloud customers to reduce the potential for loss of customer segregation and inappropriate disclosure.
- Detect and respond promptly to a data breach and notify CUNY in a timely fashion.
- Assert operational and security competence through attestation by independent auditors, e.g., AICPA SSAE SOC reports.
- Agree to meet required service levels. (Service Level Agreement—SLA)
- Negotiate terms of service that meet CUNY IT and legal requirements and comply with applicable NY State laws.

Cloud Service Contractual Agreement Information Security Terms

The University's agreement with a CSP shall clearly specify contractual data protection terms that address the (non-exhaustive) areas listed below. The terms must ensure that University Data is kept appropriately confidential, is not changed inappropriately and is available to the University as needed. The agreement with a CSP should:

- Define University Data that must be protected and describe how the CSP will protect it.
- Define the relationship and expectations regarding the division of security responsibilities between the Cloud Customer and the CSP.
- Define the data owned by each party, and declare the types of data that might be exchanged and how they will be securely exchanged.
- Indicate whether or how the CSP can use University Data. A CSP cannot use Confidential or Sensitive University Data without agreement by the University or in any way that violates the law or University policies.
- Specify that University Data be physically stored within the boundaries of the United States. (May be legally required to avoid jurisdictional issues.)

- Require the CSP to return University Data to the Cloud Customer upon request in a reasonable, usable format, both during the term of the agreement and upon termination or expiration.
- Require the CSP to securely and irreversibly erase or destroy University Data, unless its retention has been explicitly agreed to, upon termination or expiration of the agreement.
- Require the CSP to notify CUNY promptly of a data breach of CUNY protected information.
- Require the CSP to provide, on an ongoing basis, the results of independent audit reports on security controls.

Related Information

CUNY IT Policies—includes CUNY *Policy on Acceptable Use of Computer Resources*

http://www.cuny.edu/about/administration/offices/CIS/policies.html

CUNY IT Security Policies and Procedures—cybersecurity policies, data breach notification procedure, etc.

https://security.cuny.edu

NIST 800-171, **Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations—** cybersecurity standard for assessment of security protections

https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

NIST Cybersecurity Framework—framework standards, guidelines, and practices to reduce cybersecurity risks

https://www.nist.gov/cyberframework

Definitions and Terms

Affiliate or Affiliated Organization: Any organization associated with the University that uses University resources to create, access, store or manage University Data to carry out business functions. This applies to all third-party vendors under a contractual agreement.

Cloud Customer: The individual or University Entity that procures, or seeks to procure, or is the primary University contact for, a cloud service involving University Data on behalf of the University.

Cloud Service Provider: A Cloud Service Provider, or CSP, is a company that offers some component of cloud computing as a service to other businesses or individuals. See *Cloud Service Models* below.

Controlled Unclassified Information (CUI): A term used by the NIST 800-171 standard, for the purpose of this policy CUI is any University Data that requires protection.

Data Owner: the University Entity (typically a function or department) that can authorize or deny access to certain data, can delegate custody of that data and is accountable for its accuracy, integrity and timeliness. The Data Owner is responsible for appropriately classifying its data as well as implementing security controls that appropriately protect its data resources. Common examples of Data Owners:

Description	Common Data Owner(s)
Student Records	Registrar, Enrollment Management, Bursar, Student Finance, Student Affairs
Employee Records	Human Resources
Research Data	Researcher, Principal Investigator
Financial Data	Finance, Business Office, Procurement
Academic	Faculty, Department Chair, Dean, Provost, Academic Affairs

Data User: Creates, accesses and alters data as well as uses data resources and is responsible to comply with data use requirements.

University Data: Any CUNY institutional data related to CUNY's academic, research and administrative functions either stored on CUNY information technology systems or maintained by, or on behalf of, CUNY faculty, staff, students and *affiliates* in any format or location.

University Entities: All colleges, academic, research and administrative departments and affiliates.

Cloud Service Models

Software as a Service (SaaS)	Users interact with the CSP's application running on its cloud infrastructure. Comparatively, the most responsibility for security is delegated to the CSP in the SaaS model.
Platform as a Service (PaaS)	The Cloud Customer deploys its own application onto the cloud infrastructure using programming languages, libraries and tools supported by the provider. Moderate responsibility is delegated to the CSP in this model.
Infrastructure as a Service (IaaS)	The Cloud Customer provisions processing, storage, networks and other computing resources where it is able to deploy and run arbitrary software, including virtual servers, operating systems and applications. The least responsibility is delegated to the CSP in this model, as the Cloud Customer is responsible for everything but infrastructure and virtualization.

Appendix A

NIST 800-171 Security Control Families

NIST 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, defines 14 families of security controls.

Requirement Family	Description
Access Control	Who is authorized to view this data?
Awareness and Training	Are the Cloud Customer and its users made aware of their information security responsibilities?
Audit and Accountability	Are records kept of authorized and unauthorized access? Can violators be identified?
Configuration Management	Are networks, configurations and protocols baselined and changes approved and documented?
Identification and Authentication	What users are approved to access the data and how are they verified prior to granting them access?
Incident Response	What's the process if a breach or security threat occurs, including proper notification?
Maintenance	Who is responsible to conduct routine maintenance, and how is it scheduled?
Media Protection	How are electronic and hard copy records and backups safely stored? Who has access?
Physical Protection	Who has physical access to systems, equipment and storage environments?
Personnel Security	How are employees screened prior to granting them access to data center environments or to the data?
Risk Assessment	Are defenses tested? Are operations or individuals verified regularly?
Security Assessment	Are security processes and procedures effective? Are improvements needed?
System and Communications Protection	Is information regularly monitored and controlled at key internal and external transmission points?
System and Information Integrity	How quickly are possible threats detected, identified and corrected?

Appendix B

NIST 800-171 "Basic" Security Requirements

Reference No.	Requirements Family	Security Requirement
3.1.1	Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
3.1.2	Access Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
3.2.1	Awareness and Training	Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
3.2.2	Awareness and Training	Ensure that organizational personnel are trained to carry out their assigned information security-related duties and responsibilities.
3.3.1	Audit and Accountability	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.
3.3.2	Audit and Accountability	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
3.4.1	Configuration Management	Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
3.4.2	Configuration Management	Establish and enforce security configuration settings for information technology products employed in organizational information systems.
3.5.1	Identification and Authentication	Identify information system users, processes acting on behalf of users and devices.

Reference No.	Requirements Family	Security Requirement
3.5.2	Identification and Authentication	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
3.6.1	Incident Response	Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
3.6.2	Incident Response	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.
3.7.1	Maintenance	Perform maintenance on organizational information systems.
3.7.2	Maintenance	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
3.8.1	Media Protection	Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.
3.8.2	Media Protection	Limit access to CUI on information system media to authorized users.
3.8.3	Media Protection	Sanitize or destroy information system media containing CUI before disposal or release for reuse.
3.9.1	Personnel Security	Screen individuals prior to authorizing access to information systems containing CUI.
3.9.2	Personnel Security	Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.
3.10.1	Physical Protection	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
3.10.2	Physical Protection	Protect and monitor the physical facility and support infrastructure for organizational systems.
3.11.1	Risk Assessment	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational

Reference No.	Requirements Family	Security Requirement
		systems and the associated processing, storage, or transmission of CUI.
3.12.1	Security Assessment	Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.
3.12.2	Security Assessment	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.
3.12.3	Security Assessment	Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
3.12.4	Security Assessment	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.
3.13.1	System and Communications Protection	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
3.13.2	System and Communications Protection	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.
3.14.1	System and Information Integrity	Identify, report, and correct information and information system flaws in a timely manner.
3.14.2	System and Information Integrity	Provide protection from malicious code at appropriate locations within organizational information systems.
3.14.3	System and Information Integrity	Monitor information system security alerts and advisories and take appropriate actions in response.