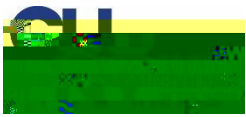


CITY UNIVERSITY OF NEW YORK INFORMATION SECURITY POLICY	
	Issue Date:8/19/2019

Acceptable Use of University
Data in the Cloud

Issued By:

CITY UNIVERSITY OF NEW YORK INFORMATION



Acceptable Use of University Data in the Cloud

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)

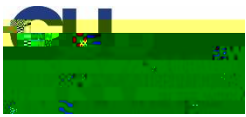
- Negotiate terms of service that meet CUNY and legal requirements and comply with applicable NY State laws.

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 G 0 G 0 G [(a)4(r)-6(e)4(a)



Acceptable Use of University Data in the Cloud

Related Information

CUNY IT Policies Šincludes CUNY Policy on Acceptable Use of Computer Resources

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

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

<https://security.cuny.edu>

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

<https://csrc.nist.gov/publications/detail/sp/8001/rev1/final>

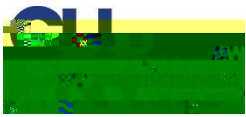
NIST Cybersecurity Framework Š framework standards, guidelines, and practices to reduce cybersecurity risks

<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, is the primary University



Acceptable Use of University Data in the Cloud

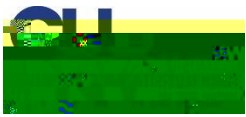
Appendix A

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 network 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 the data?
Risk Assessment	Are defenses tested? Are operations individuals verified regularly?
Security Assessment	Are security processes and procedures effective? Are

CITY U

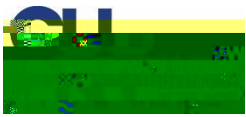


Acceptable Use of University Data in the Cloud

Reference No.	Requirements Family	Security Requirement
		systems and the associated processing, storage, transmission of CUI.

3.12.1

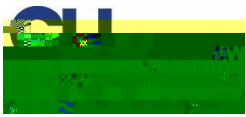
CITY UNIVERSITY OF NEW YORK INFORMATION SECURITY POLICY



Data Classification Standard

Description	Common Data Owner(s)
Student Records	Registrar, Enrollment Management, Bursar, Student Finance, Student Affairs
Employee Records	Human Resources
Research Data	Researcher, Principal Investigator

Data Classification Standard



Data Classification Standard

access to education records except when used in conjunction with one or more fac
W K D W D X W K H Q Identify, SWH Has Password Personal identification number
(PIN), or other factor known or possessed only by the authorized u

4. Protected Health Information (PHI)

Health information about an individual including medical records, health status, and records covered by health privacy laws.

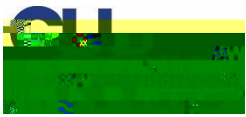
5. Citizenship

, Q I R U P D W L R Q D E R X W D Q L Q G L Y L G X D I O f m a t e e , E L W L] H Q V K I

6. Personnel Records

P

Data Classification Standard



Data Classification Standard

Appendix B

Examples of Sensitive Data

- x Email and other communications regarding internal matters which have not been specifically approved for public release
- x Proprietary financial, budgetary or personnel information not explicitly approved by authorized parties for public release
- x Identities of donors or other third party partner information maintained by the University not specifically designated

