Draft CUNY Cloud Computing Policy

I. INTRODUCTION AND PURPOSE

This policy describes when and how cloud-based applications and services may be used for University activity.

"Cloud-based applications and services" are computer applications and services made available to Users on demand through the Internet from a third-party provider's servers (i.e. servers not controlled by CUNY or an associated entity such as the Research Foundation). Cloud-based applications and services do not include applications and services solely provided through the University's servers or installed on local desktop computers, although, in some cases, a locally installed application may be used to access a Cloud-based application or service. Cloud-based applications and services include, but are not limited to, file sharing and file storage, social media, and content hosting. Examples of well-known Cloud-based applications and services include Microsoft Office 365, Google Apps, and Dropbox, Twitter and Facebook.

The purpose of this policy is to allow the use of cloud-based applications and services for University activities, while addressing certain information security, data privacy and contractual concerns associated with transmitting or storing CUNY information and/or data on cloud-based applications and services.

In general, cloud-based applications and services may be used to transmit or store "public information," i.e., any information or data that is generally available to the public or that the University would have no concern being publicly disclosed or disseminated. However, any data that could be "Non-Public University Information," as defined below and by CUNY's IT Security Policies and Procedures, present a variety of security and privacy concerns when stored or transmitted in the cloud. These concerns include the following:

- The University no longer protecting or controlling its data, leading to a loss of security, lessened security, or inability to comply with various regulations and data protection laws
- Loss of privacy of data, potentially due to aggregation with data from other cloud consumers
- Non-compliance with legal mandates such as FERPA
- University dependency on a third party for critical infrastructure and data handling processes
- Potential security and technological defects in the infrastructure provided by a cloud vendor

In light of these and other concerns, this policy sets forth rules governing the use of cloud-based applications and services for transmitting or storing different types of information and data in the conduct of University Activities (as defined below).

II. APPLICABILITY

This policy applies to all Users (as defined below).

This policy applies to any use of cloud-based applications and services capable of transmitting or storing protected or sensitive electronic data in the conduct of University Activities, whether paid or freely provided, and whether obtained directly from a vendor or generally made available over the Internet.

III. DEFINITIONS

A. “Non-Public University Information” has the meaning set forth in CUNY’s IT Security Policies and Procedures found at security.cuny.edu, and include:

1. Personally identifiable information such as
    - i. Social security number
    - ii. Driver’s license number or non-driver identification number
    - iii. Passport number
    - iv. Personal characteristics including biometrics
    - v. Home address, email address and telephone numbers
2. Health information such as medical records and disability status
3. Confidential human resources information
4. FERPA-protected information such as student records including grades and scores
5. Financial account numbers including payment card numbers (credit/debit)
6. Citizenship status
7. Passwords and access codes

B. “User” means anyone using a cloud-based application or service to transmit or store CUNY data or information for a University Activity. This includes all current and former CUNY faculty, staff and students, as well as University affiliates, the CUNY Research Foundation, consultants, and others, that are conducting University Activity.

C. “University Activity” means any administrative or academic work (including both teaching and research) conducted in furtherance of the University’s mission and/or in the course of University employment or pursuant to a contract with the University (whether directly or as an employee, agent, representative or subcontractor of a primary University contractor).

IV. RULES FOR USE OF CLOUD-BASED APPLICATIONS AND SERVICES

A. Permitted Uses

Users may use cloud-based applications and services to conduct University Activity if the following conditions are met:

i. the use is within the scope of the authorization granted by the University with respect to such specific cloud-based application or service;

ii. the use of the cloud-based application or service to store or transmit the particular data or information involved is permissible because

  a. The data or information to be stored or transmitted is public data that presents no risk to CUNY or its current or former offices, employees, students, or applicants if exposed (e.g. published research; government census data; aggregate, non-personally-identifiable enrollment information); or

  b. The data or information to be stored or transmitted is Non-Public University Information, such as personally identifiable information, FERPA protected data including grades and class membership, or financial transactions, and prior authorization by the University's Chief Information Security Officer (CISO) or designee has been acquired per Section V below and the use is within the scope of authorization;

iii. the use is within the scope of the User's employment or other relationship with the University;

iv. the cloud-based applications and services have been procured in accordance with the law and all CUNY policies, including those set forth in V below;

v. the use is not otherwise prohibited by this or any other University policy or applicable law.

B. Prohibited Uses

1. Users are prohibited from accessing, transferring, exposing, storing or using any CUNY data classified by law as sensitive or protected, or by CUNY security policy or practice as Non-Public University Information by means of a cloud-based application or service, unless such cloud-based application or service was provided and expressly authorized by the University and the User's activities fall entirely within the constraints of that authorization.

2. Cloud-based applications and services may not be used for any purpose or in any manner that violates CUNY rules, regulations or policies, or federal, state or local law. Users are responsible for complying with all laws, rules, policies, contracts, and licenses applicable to a particular cloud-based application and service use.

3. Unless specifically authorized, Users are prohibited from using cloud-based applications and services provided by or through affiliation with CUNY for personal use; private business purposes, whether commercial or not-for-profit; advertising of products or services; any activity meant solely to foster personal gain; or political activity.

4. Users are prohibited from using cloud-based applications and services obtained personally, and not provided by or expressly authorized by the University, for any University Activity.

V. ADDITIONAL REQUIREMENTS PRIOR TO USE OF CLOUD-BASED APPLICATIONS AND SERVICES

A. Authorization for Storing and Transmitting Non-Public University Information

Prior authorization by the University's Chief Information Security Officer (CISO) or designee is required for use of any cloud-based application or service that transmits or stores Non-Public University information, such as personally identifiable information, FERPA protected data including grades and class membership; or conducts financial transactions.

Cloud-based applications and services are authorized on a case-by-case basis. Authorization for the use of a cloud-based application or service does not imply that the application or services may be used for any other purpose than the one covered by the authorization. Users are responsible for ensuring that Non-Public University Information is transmitted or stored only as authorized by the CISO.

B. Acquisitions and Agreements

Acquisition of cloud-based applications and services on behalf of the University is always considered a procurement (even when the application or service is free) and is subject to University procurement policy.

No contract may be entered into on behalf of the University for cloud-based applications and services without having been approved through the appropriate contract review process as defined by the University Office of General Counsel.

Users are not authorized to accept a contract on behalf of the University, including "click through" licensing terms. Acceptance by Users on behalf of CUNY without proper authority can lead to legal, privacy, and security issues for CUNY, and may subject a User to criminal, civil and financial liability.

The Office of General Counsel will consider for approval agreements for use of cloud-based applications and services if the following criteria are met:

- The agreement expressly sets forth the types of data that may be transferred
- The agreement clearly defines the ownership of the data
- The agreement clearly defines how the vendor may use University data, if at all
- The agreement clearly defines what data must be protected, whether all data or a subset, and must set forth the level of data protection that vendor must provide
- If any Non-Public University Data will be transferred or stored, the agreement clearly sets forth the vendor's liability for unauthorized exposure of Non-Public University Data
- If any Non-Public University Data will be transferred or stored, the agreement specifies that the data may not be transmitted or stored outside of the boundaries of the continental United States.

VI. ADHERENCE TO POLICY

Users of cloud-based applications and services authorized by the University in the conduct of University Activities and in full compliance with University policies and recommended use practices shall receive the University's support in that use.

Use of unauthorized cloud-based applications and services, or use of authorized cloud-based applications and services in a manner that is not in compliance with University policies and recommended use practices, is done at the sole and exclusive risk of the User. The University shall not be obligated to provide support for the cloud-based application or service, assist in the recovery of lost data or response to information security breaches, or protect or hold harmless Users from losses arising from any of the foregoing or from any claims that arise from such User's unauthorized or non-compliant use of cloud-based applications and services.

In cases where an employee is charged with a violation of this policy the matter shall be referred for disciplinary action in accordance with the applicable CUNY policies, rules and collective bargaining agreements. Penalties for employees include reprimand, suspension or termination of employment following applicable disciplinary procedures.

If protected or sensitive data is exposed through the use of cloud-based applications and services, the User may be held criminally and civilly liable for any resulting harm and financially responsible for all resulting claims against and losses suffered by the University, including the cost associated with the breach notifications required by New York State law.

APPENDIX

The following cloud services and applications are NOT approved for University Activity. This listing is meant to serve only as a partial list. As noted in the CUNY Cloud Computing Policy, any application or service that has not been expressly approved in accordance with University procedures should be assumed to be not approved:

- Dropbox
- iCloud
- Amazon Cloud Drive
- Google Drive
- SurveyMonkey
- MailChimp