Cloud Computing Services Policy

PURPOSE

This policy outlines best practices and approval processes for using cloud computing services to support the processing, sharing, storage, and management of institutional data at Tufts University.

SCOPE

All Tufts faculty, staff, and students.

This policy concerns cloud computing resources that provide services, platforms, and infrastructure that provide support for a wide range of activities involving the processing, exchange, storage, or management of institutional data. This policy does not cover the use of social media services, which is addressed in the Social Media Policy.

POLICY STATEMENT

Overview

Cloud computing services are application and infrastructure resources that users access via the Internet. These services, contractually provided by companies such as Apple, Google, Microsoft, and Amazon, enable customers to leverage powerful computing resources that would otherwise be beyond their means to purchase and support. Cloud services provide services, platforms, and infrastructure to support a wide range of business activities. These services support, among other things, communication; collaboration; project management; scheduling; and data analysis, processing, sharing, and storage. Cloud computing services are generally easy for people and organizations to use, they are accessible over the Internet through a variety of platforms (workstations, laptops, tablets, and smart phones), and they may be able to accommodate spikes in demand much more readily and efficiently than in-house computing services.

For more details about cloud computing see "The NIST Definition of Cloud Computing"

Considerations Regarding Cloud Computing Services

Most cloud services, such as Google Docs, make it easy for individuals to sign-up and use (self-provision) their services via an end user license agreement (EULA), often at no monetary cost. Tufts also locally or centrally acquires cloud services, such as the survey tool *Qualtrics*, for use by members of the Tufts community.

Tufts faculty, staff, and students must be very cautious about self-provisioning a cloud service to process, share, store, or otherwise manage institutional data (as defined by the Information Stewardship Policy). Self-provisioned cloud services may present significant data management risks or are subject to changes in risk with or without notice. Virtually all cloud services require individual users to accept click-through agreements. These agreements do not allow users to negotiate terms, do not provide the opportunity to clarify terms, often provide vague descriptions of services and safeguards, and often change without notice.

Risks with using self-provisioned cloud services include:

- Unclear, and potentially poor access control or general security provisions
- Sudden loss of service without notification
- Sudden loss of data without notification

- Data stored, processed, or shared on cloud service is often mined for resale to third parties that may compromise people's privacy
- The exclusive intellectual rights to the data stored, processed, or shared on cloud service may become compromised.

In contrast, Tufts negotiates agreements with service providers for locally as well as centrally provisioned services. The terms of these services are more clearly defined and well known by the University. In short, university provisioned cloud services are vetted environments whose risks are better measured and accepted by Tufts.

PROCURING OR LICENSING CLOUD COMPUTING SERVICES

If your division, school, department, office, or lab is looking to provision a cloud services to support its work, the first step is to consult with its Information Steward(s) and TTS Contract and Licensing Services.

Faculty, staff, and students may not self-provision cloud services to store, process, share, or manage Level A: Regulated Institutional Data. Defined by the Information Classification and Handling Policy, regulated institutional data are data that are regulated by information privacy or protection laws, regulations, contracts, binding agreements (such as non-disclosure), or industry requirements. If your division, school, department, office, or lab needs to provision a cloud service to store, process, share, or otherwise regulated institutional data, it must work with TTS Contract and Licensing Services in order to properly evaluate and manage the risks that come with using the service for regulated institutional data.

Using Cloud Computing Services
Using a third party cloud service to handle institutional data does not absolve you from the responsibility of ensuring that the data is properly and securely managed. As noted in the Information Stewardship Policy, "members of the Tufts community are expected to responsibly maintain and use institutional data regardless of the resource used to access or store the data—whether an institutional system, a privately owned resource, or a third-party resource."

The care taken to review a cloud services' security and trustworthiness must match the sensitivity of the institutional data you are looking to support with the service and the data's governing regulatory environment. In order to use a cloud service to store, process, share, or otherwise manage regulated institutional data, you must:

- Work with TTS Contract and Licensing Services to develop the appropriate contractual safeguards
- Monitor changes to the service's safeguards
- Have a clearly designated Information Manager for the institutional data. Defined by the Information Roles and Responsibilities Policy, the Information Manager is the individual charged "to ensure the responsible management and use of institutional data."
- Know the retention period and, when applicable, the destruction date of the institutional data. Retention periods are often defined by the general Records Retention Schedule or other records policies.
- When appropriate, destroy the institutional data securely.

These steps should also guide your use of cloud services for storing, processing, sharing, or otherwise managing other institutional data.

The Information Classification and Handling Policy provides a framework for classifying institutional data as Level A: Regulated, Level B: Confidential, Level C: Administrative or Level D: Public. The table below adapts the classification framework to help inform your decisions on appropriate solutions for storing and

managing information.

Confidentiality Level	Description	Cloud Use
Level A: **Regulated Institutional Data**	All Institutional data that is governed by privacy or information protection mandates required by law, regulation, contract, binding agreement, or industry requirements.	• ***Cannot*** use self-provisioned cloud services to store, process, share, or otherwise manage regulated institutional data without working with TTS Contract and Licensing Services to develop the appropriate contractual safeguards. • Can only use a contractually (locally or centrally) provisioned cloud service once you have confirmed with your Information Steward or TTS Contract and Licensing Services that the service is appropriate for confidential institutional data. Not all centrally and locally provisioned services are designed to handle regulated data.
Level B: **Confidential Institutional Data**	Institutional data that is meant for a very limited distribution—available only to members of the Tufts community on a strictly need-to-know basis.	• Should ***not*** use self-provisioned cloud services to store, process, share, or otherwise manage confidential institutional data without ensuring that a service's safeguards are appropriate for confidential institutional data. • Should only use a centrally or locally provisioned cloud service once you have confirmed with your Information Steward that the service is appropriate for confidential institutional data. Not all contractually provisioned services are designed to handle confidential data.
Level C: **Administrative Institutional Data**	Institutional data that is meant for a limited distribution; available only to members of the Tufts community that need the institutional data to support their work. This institutional data derives its value for Tufts in part from not being publically disclosed.	• Should ***not*** use self-provisioned cloud services to store, process, share, or otherwise manage administrative institutional data without ensuring that a service's safeguards are appropriate for administrative institutional data. • Should only use a centrally or locally provisioned cloud service once you have confirmed with your Information Steward that the service is appropriate for administrative institutional data. Not all contractually provisioned services are designed to handle administrative data.
Level D: **Public Institutional Data**	Institutional data that is meant for members of the Tufts community and in some cases wide and open distribution to the public at large. This institutional data does not contain confidential information.	• May use self-provisioned cloud services to store or manage public institutional data with caution. Should ensure that using these cloud services does not violate any licensing agreements. • May use contractually provisioned cloud services to store or manage public institutional data.

Review Entity(ies)
Information Stewardship Committee
IT Leaders Forum

Approval Date
2014-07-7

Effective Date
2014-07-7

Executive Sponsor(s)
David Kahle, Vice President for Information Technology and Chief Information Officer
Tom McGurty, Vice President for Finance and Treasurer

Policy Manager(s)
Tufts Technology Services
Tufts Finance Division

Responsible Office(s)
Tufts Technology Services
Tufts Finance Division

Revision
The University reserves the right to change this policy from time to time. Proposed changes will normally be developed by the policy managers with appropriate stakeholders. The review entities have sole authority to approve changes to this policy.

Review Cycle
Annually or as required by relevant external regulation.

Distribution
https://it.tufts.edu/cloud-pol