STAMFORD INTERNATIONAL UNIVERSITY

The Difference is Real

A member of LAUREATE INTERNATIONAL UNIVERSITIES

CLOUD STORAGE POLICY

IT-P-013

Date: 31st July, 2014

STAMFORD
INTERNATIONAL
UNIVERSITY

The Difference is Real

A member of LAUREATE INTERNATIONAL UNIVERSITIES

Stamford International University
Email Usage Policy

Purpose

The purpose of this policy is to provide advice and establish best-practices for appropriate usage of cloud computing services to support the processing, storage, and management of Institutional data at Stamford International University (henceforth, referred to as "Stamford" or "STIU"). This policy also outlines any limitations / restrictions placed on usage of such services for sharing sensitive Institutional / Corporate Data (henceforth, referred to as "Institutional Data").

Scope

This policy applies to all employees of STIU in all locations including the temporary employees, part-time and contractors.

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 other policies.

Policy Information

Responsible Office: Department of Information Technology, Stamford International University
Issued Date: 31st July, 2014

Revision History

Revision Number	Document Number	Description	Effective Date
00	IT-P-013	New Release	31st July, 2014

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.

Recommendation and Approvals

Drafted by:

Name: Chavanath Chatchaiyan
Position: Technology Services Manager
Date: 31st July, 2014

Approved by:

Name: Sourjya Sankar Sen
Position: Director, Information Technology
Date: 31st July, 2014

Name: Gilles Mahe
Position: CEO, Stamford International University
Date: 31st July, 2014

Name: Dr. Boonmark Sirinaovakul
Position: President, Stamford International University
Date: 31st July, 2014

Policy

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: **Wikipedia's definition of Cloud Computing**.

Acquiring Cloud Computing Services

Most cloud services, such as Google Docs, Dropbox, Box etc. 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. STIU also centrally acquires cloud services for use by members of the Stamford community.

Stamford faculty, staff, and administrators must be very cautious about self-provisioning a cloud service to process, share, store, or otherwise manage institutional data. Self-provisioned cloud services are often unvetted environments with significant unmeasured 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 end-user license 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 are 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, Stamford 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 Stamford International University**.

Faculty, staff, and administrators may not self-provision cloud services to store, process, share, or manage regulated Institutional Data. Regulated institutional data are data that are regulated by information privacy or protection laws, regulations, contracts, binding agreements (such as non-disclosure or data use agreements), or industry requirements. If your division, department, office, or lab is looking to provision a cloud service to support its work, it must mandatorily consult the Department of Information technology prior to subscribing to such services. If your division, department, office, or lab needs to provision a cloud service to store, process, share, or otherwise manage regulated institutional data, it must work with the Department of Information Technology and Stamford / Regional Legal Counsel in order to properly evaluate and manage the risks that come with using the service for regulated institutional data. This will help ensure that agreements with cloud service providers have the appropriate provisions, such as notification of changes to the service's protective measures and assurance that the service properly destroys deleted data.

Contact information for the Department of Information Technology

Email: support@stamford.edu

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. Members of the Stamford 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:

- Have a clear and compelling need for using a cloud service
- Work with Department of Information Technology and local / regional Legal Counsel to develop the appropriate contractual safeguards
- Have a clearly designated Information Manager from your division, department or office for the institutional data. An 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.

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

Information Classification Framework

The following table provides a simple framework for classifying institutional data as Regulated, Confidential, Administrative, or Public and can help in 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.	• May not use self-provisioned cloud services to store, process, share, or otherwise manage regulated Institutional data without working with the IT Department & local / regional Legal Counsel to develop the appropriate contractual safeguards. • Can only use a contractually (locally or centrally) provisioned cloud service once you have confirmed with your Information Manager, the IT Department and local / regional Legal Counsel 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 Stamford 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 Manager as well as the IT Department and local / regional Legal Counsel 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 Stamford community that need the data to support their work. Such data derives its value for Stamford 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 Manager and IT Department 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 Stamford 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.