Data Protection Safeguards - Cloud Computing Safeguards

The following are safeguards which should be implemented for when entering into agreement with a cloud service provider or when utilizing a cloud service with Georgia Tech data. Cloud computing is defined as a network of remote servers or services, hosted by third parties, used to store, manage, and process data.

Section one of these safeguards contains general controls which should be implemented when using a cloud service with Georgia Tech data. Section two contains controls which should be implemented when entering into contract/agreement with a cloud service provider on behalf of Georgia Tech. Please note that the controls listed within section two do not apply when entering into a personal agreement with a cloud service provider through an end user license agreement.

Any deviation from mandatory requirements must be documented with an approved policy exception and covered by adequate compensating control(s). The department of Internal Auditing is available to assist in reviewing compensating controls. For more information on requesting policy exceptions, refer to: http://policylibrary.gatech.edu/policy-exceptions.

References

[1] Safeguard Guidelines by Data Category: M = Mandatory safeguard, R = Recommended

Category of Data [1]			Item Ref.	Internal Control
I	II	III		
1 - Cloud Computing Controls				
R	R	M	1-1	Encrypt all sensitive data being transmitted outside of Georgia Tech networks, as per the Institute Encryption Standard: http://www.oit.gatech.edu/sites/default/files/Encryption_Standard.pdf
R	R	M	1-2	Encrypt data stored on a cloud service provider's systems.
R	R	M	1-3	Use a unique user name and password when logging into the cloud service provider's system.
		M	1-4	Review sponsored research contracts to identify if the data in question can be stored/used in concert with cloud services. Please note the US Commerce Department has determined that ITAR and export controlled data may not be stored in the cloud.
2 - Contract/Agreement Considerations				
R	R	M	2-1	When reviewing and negotiating the terms of an agreement/contract with a cloud service provider, ensure the following items are considered and included in the terms:
R	M	M	2-2	Georgia Tech maintains sole license/ownership of all Georgia Tech data.
R	R	M	2-3	Service provider will immediately notify Georgia Tech in the event of a security breach or data disclosure. The service provider will work with Georgia Tech to quickly resolve any security incidents as well as provide any necessary information in the event we receive a court order or open records request.
R	R	M	2-4	Service level agreements as well as warranties to protect Georgia Tech against loss of service and/or data. The contract must also allow for termination of service if service level agreements are not met.
R	R	M	2-5	Georgia Tech data is backed up either by the service provider, or by Georgia Tech. The contract/agreement must also detail the process and service level agreements for the restoration of data from backups.
R	R	M	2-6	Georgia Tech has the right to reclaim our data in the event the contract is terminated.
R	M	M	2-7	Georgia Tech data will be wiped from the service providers systems/storage when the contract ends, or when the service provider is disposing of their physical media.
R	R	M	2-8	Georgia Tech has the ability to access the data owned by any GT account holder.
R	R	M	2-9	Contract terms protecting Georgia Tech data remain valid in the event the service provider is acquired by another company.
R	R	M	2-10	Georgia Tech may audit the service provider and any subcontractors, or obtain equivalent audit reports.