Georgia Institute of Technology
Data Protection Safeguards
Version: 2.0

Purpose: The purpose of the Data Protection Safeguards is to provide guidelines for the appropriate controls that should be in place to protect the Georgia Institute of Technology (Georgia Tech) data housed within the system in question. This document is intended to support the Georgia Tech Data Access Policy (DAP).

The controls defined in this document are based on control objectives required by regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Family Education Rights and Privacy Act (FERPA),and the Gramm-Leach-Bliley Act (GLBA). The controls are also defined from various information security and privacy standards such as ISO-27001/ISO-27002 and the Georgia Tech Internal Controls Guide (http://www.audit.gatech.edu/resources/internal-control-guide).

Note: The controls contained within this document are not sufficient for the processing of credit cards (Category IV data) and are not encompassing of the controls necessary as part of the PCI-DSS. It is the strategy of Georgia Tech to outsource the processing of credit cards and limit the storage of sensitive credit card data. For a complete list of the controls required by PCI-DSS please refer to the PCI website (https://www.pcisecuritystandards.org/). In addition, all systems which process or store credit cards at Georgia Tech must be approved on an annual basis by the Chief Information Security Officer.

Usage: The configurations and controls detailed in this spreadsheet are first categorized by the type of computing system: Servers, Endpoints (e.g. Desktop Computers, Laptop Computers, Workstations, USB Storage Devices), Mobile Devices (e.g. Smart Phones, Tablet Computers, Personal Digital Assistants, Handheld Scanners), Cloud Computing.

Each page in the spreadsheet contains a matrix outlining the specific configurations or controls, as well as whether the configuration or control is Mandatory or Recommended based on the category of data being stored on the computing system in question.

Data classification categories are consistent with the categories defined within the DAP. For clarification on data types and their classifications, please refer to the DAP as well as the Data Classification Handbook.

Data Protection Safeguards - Server Safeguards

The following are the safeguards which should be implemented for Georgia Tech servers. A **server** is defined as any computer system, cloud computer system, or networking equipment that hosts a campus unit or institute wide service, or acts as an authoritative source of data for the institute or campus unit. Several controls within this document apply only to servers located in a data center. A **data center** is defined as a multidepartmental server room with 24/7 operational support.

Any deviation from mandatory requirements must be documented with an approved policy exception request 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

[2] A multidepartmental server room with 24/7 operational support. For example, the following are considered data centers: Rich, BCDC, GTRI, CoC, and French. If you are unsure if your specific server room would qualify as a data center, or if you are creating a new data center, please send an email to dap@gatech.edu.

[3] Those controls marked in the central service column represent controls which can be achieved by utilizing a central campus service.

Category of Data [1]			Item Ref.	Internal Control	Central Service[3]
I	II	III			
1 - Control Physical Access To Data					
	R	M	1-1	Server must be located in a permanently physically secured location which is protected by either badge reader or keyed locks. Central Service: Refer to list of data centers location in the definition of data center above.	X
		M	1-2	Badge or key access to permanently physically secured locations containing sensitive data must approved by the manager of that secured location as well as the manager of the person requesting access. Access to these locations should be reviewed periodically to ensure that individuals who no longer require access are prevented from accessing. Central Service: Refer to list of data centers location in the definition of data center above.	X
		M	1-3	Constant monitoring is in place using video cameras in data centers[2] to monitor entrance and exits from the secured location. Video cameras are also recommended for non-data center locations housing servers. Central Service: Refer to list of data centers location in the definition of data center above.	X
		M	1-4	Employees and visitors must display an ID badge at all times while inside of a data center. Displaying ID badges is also recommended for non-data center locations housing servers. Visitor ID badges do not permit unescorted access to physical areas that store sensitive data.	
		M	1-5	1. ID badges clearly distinguish employees from visitors/outsiders	
		M	1-6	2. Visitor badges contain a fixed expiration date.	
		M	1-7	3. Visitors are asked to surrender their ID badge upon departure or upon the expiration date.	

		M	**1-8**	Log all physical access to data centers. Log can be both a system log of badge swipes or a paper log for visitors. Retain this log for a minimum of three months. Central Service: Refer to list of data centers location in the definition of data center above.	X
		M	**1-9**	All paper and portable electronic media backups of sensitive data must be stored in a physically secured location or encrypted. Encrypt using modern cryptography that is aligned with FIPS 140-2.	
2 - Install And Maintain A Working Firewall To Protect Data					
M	**M**	**M**	**2-1**	Network firewalls must be configured to block all ports except those which are necessary for services running on the server. Firewall configuration settings should be reviewed for continued appropriateness on an annual basis. Central Service: OIT Firewall Program. Firewalls managed at https://fw.noc.gatech.edu	X
R	**R**	**M**	**2-2**	Host based firewalls must be installed, and configured to block all ports except those which are necessary for services running on the server. Firewall configuration settings should be reviewed for continued appropriateness on an annual basis.	
3 - Keep Security Patches Up To Date					
M	**M**	**M**	**3-1**	Install all applicable operating system and application security patches.	
R	**R**	**M**	**3-2**	1. Test all security patches before they are deployed or placed in production. Testing can either take place in a dedicated test environment or through research of how the patch behaves in other environments.	
M	**M**	**M**	**3-3**	2. Install new/modified security patches within one month of release, or document reason(s) why it cannot be done.	
4 - Encrypt Data Sent Across Public Networks					
R	**R**	**M**	**4-1**	Encrypt all sensitive data being transmitted outside of Georgia Tech networks using modern cryptography that is aligned with FIPS 140-2.	
5 - Use And Regularly Update Antivirus					
R	**R**	**R**	**5-1**	Where appropriate, Use active anti-virus mechanisms with current signatures on servers which are intended primarily for storing user files (e.g. mail servers or file servers)	
6 - Controlling Access Based On "Need-To-Know"					
	R	**M**	**6-1**	Only appropriate users should be provisioned with elevated access to sensitive servers. Access approval should be obtained from the employee's manager or data owner as appropriate, and approval documentation should be maintained for a period of six months. Access should be immediately removed when no longer appropriate.	
7 - Uniquely ID Each Person Or System					
	M	**M**	**7-1**	Verify personnel identity prior to creating user accounts allowing access to the server. Central Service: Identities are verified prior to the issuance of the primary GT account. servers which authenticate via central authentication (e.g. Active Directory, Central Authentication Services (CAS)), are in compliance with this control.	X
R	**M**	**M**	**7-2**	Authenticate all authorized personnel for remote access or access via server console by using the following or comparable methods:	
R	**M**	**M**	**7-3**	1. Unique user name and password Central Service: Servers which authenticate via central authentication (e.g. Active Directory, Central Authentication Services (CAS)), are in compliance with this control.	X

		R	7-4	2. Two-Factor authentication for interactive login	
	R	M	7-5	Ensure proper user authentication and password management by ensuring the following practices:	
	M	M	7-6	1. Control the addition, deletion, and modification of user IDs, credentials, or other identifier objects.	
	M	M	7-7	2. Passwords must comply with the institute Password Policy and Standard: http://policylibrary.gatech.edu/passwords Central Service: Servers which authenticate via central authentication (e.g. Active Directory, Central Authentication Services (CAS)), are in compliance with this control.	X
M	M	M	7-8	3. Where possible, encrypt or hash all stored passwords for accounts that allow interactive login.	
R	R	M	7-9	4. Monitor failed authentication logs for high rates of failed authentication. Take appropriate action to limit inappropriate access to accounts which appear to have a high rate of failed authentication attempts. Central Service: Servers which authenticate via central authentication (e.g. Active Directory, Central Authentication Services (CAS)), are in compliance with this control.	X
	R	M	7-10	5. If a server terminal has been idle for more than 20 minutes, require the user to re-enter the password to re-activate the terminal.	
8 - Server Configuration Practices					
M	M	M	8-1	Change the vendor-supplied defaults for servers or devices on the network (i.e., passwords, SNMP community strings, remove unnecessary accounts, well known server defaults which are easily exploited, etc.).	
	R	R	8-2	Implement only one application, service or primary function per server.	
M	M	M	8-3	Review all active services on the server and disable any unnecessary services.	
M	M	M	8-4	Enable the appropriate audit subsystems such as servers and application change logs and security event logs. These logs must be maintained for a period of at least six months. Logs should be maintained on a separate server in order to preserve their integrity. Examples of useful security event logs include the following types of logs: root or admin level actions, accessing audit logs, login attempts.	
R	R	R	8-5	Regularly review server logs looking for any inappropriate activity. Central Service: Servers which provide their logs to the central SIEM service for log correlation and alerting are in compliance with this control.	X
M	M	M	8-6	Establish a process to identify and address the latest security vulnerabilities and other issues for the server.	
9 - Regularly Test Security Systems And Processes					
M	M	M	9-1	Run internal vulnerability scans at least monthly and external vulnerability scans at least semi-annually. Central Service: OIT offers vulnerability scanning using the Qualys vulnerability management system. Servers protected by the central firewalls are automatically scanned and are in compliance with this control.	X
R	R	R	9-2	Use intrusion detection systems to monitor all network traffic and alert personnel to suspected compromises. Central Service: All servers on the Georgia Tech network are protected by the network perimeter Intrusion Prevention Systems, and are in compliance with this control.	X
		R	9-3	Deploy file integrity monitoring to alert personnel to unauthorized modification of critical system files.	
R	R	M	9-4	Document disaster recovery procedures to allow for the recovery of the server in the event of failure or data loss. Procedures should include the following:	

M	**M**	**M**	**9-5**	1. Data should be backed up to either logical storage or physical tape backups.	
R	**R**	**R**	**9-6**	2. Critical servers should be configured as redundant server pairs with failover.	
M	**M**	**M**	**9-7**	3. Server backups should be tested at least annually to ensure that data can be recovered from backup. If recoveries have been performed within the year, that shall server as a successful test of the backups.	
10 - Notify OIT Information Security Of Servers Housing Sensitive Information					
		M	**10-1**	Servers storing sensitive or highly sensitive data must register their server as a sensitive server with OIT Information Security. Central Service: Servers which are protected by the central firewalls may register their server on the central firewall management website.	X
11 - Disposal Of Servers And Server Hardware					
R	**R**	**M**	**11-1**	Implement data disposal procedures:	
R	**R**	**M**	**11-2**	1. Shred or incinerate hardcopy materials when they are no longer required and have surpassed their retention date. Refer to the Board of Regents retention schedule for more information: http://www.usg.edu/records_management/schedules/A	
R	**R**	**M**	**11-3**	2. Turn over electronic media to central receiving to either surplus, or destroyed if the media contains sensitive data. Central Service: Central receiving provides disk and media destruction services for all surplus items.	X
12 - Virtual Machines Hosted On Campus					
R	**R**	**M**	**12-1**	The following controls must be implemented for virtual machines: Section 2, Section 3, Section 4, Section 5, Section 6, Section 7, Section 8, Section 9 and Section10	
R	**R**	**M**	**12-2**	All controls apply for virtual machine hosts and hypervisors.	

Data Protection Safeguards - Endpoint Safeguards

The following are the safeguards which should be implemented for endpoints containing Georgia Tech data. An **endpoint** is defined as laptop computers, desktop computers, workstations, group access workstations, usb drives, personal network attached storage, small servers, or cloud hosted virtual machines. Laptops and usb drives were selected as endpoints and not mobile devices because the controls necessary to protect them are similar to desktops and small servers.

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

[2] Those controls marked in the central service column represent controls which can be achieved by utilizing a central campus service."

Category of Data [1]			Item Ref.	Internal Control	Central Service[2]
I	II	III			
1 - Control Physical access to data					
R	R	M	1-1	Keep endpoints either in your possession or in a physically secured location at all times.	
R	R	R	1-2	Obtain and use a security cable to secure endpoints located in publicly accessible locations.	
R	R	R	1-3	Install and configure device location and recovery software on laptop computers. (e.g. computrace or lojack for laptops)	
M	M	M	1-4	Georgia Tech owned endpoints which are lost, stolen or misplaced, must be reported immediately to the police department responsible for the area in which the endpoint was lost or stolen. Employees must obtain a police report. The employee must also report the loss of the endpoint to their management and provide the police report to their management.	
		M	1-5	Personal endpoints containing Georgia Tech data or that are used to access Georgia Tech information technology resources, which are lost, stolen or misplaced, should be reported immediately to their CSR or Georgia Tech Information Security.	
2 - Host Based Firewall					
R	R	M	2-1	Install a host based firewall, or use the native operating system firewall. Configure firewall appropriately to limit open ports to only those which are necessary.	
3 - Keep Software Up to date					
R	R	M	3-1	Keep operating system and applications up to date by downloading and installing security patches.	
M	M	M	3-2	Georgia Tech computers must run operating systems which are currently supported by the vendor or an appropriate third party developer. Examples of systems which may not be able to run a supported operating system include systems which support scientific instruments. Systems which are not able to run supported operating systems should document the exception with a policy exception request: http://policylibrary.gatech.edu/policy-exceptions.	
4 - Protect stored data					
		M	4-1	Implement one of the following types of data protection:	

		M	**4-2**	1. Whole disk encryption	
		M	**4-3**	2. Permanently physically secure the endpoint (e.g. keep the endpoint in a locked office at all times)	
		M	**4-4**	3. Store category 3 data on approved GT storage and not on the endpoint. (e.g. Tsquare)	
R	**R**	**R**	**4-5**	Systems which have implemented whole disk encryption should escrow encryption keys in a location accessible to a systems administrator or computer support representative for systems that are owned by Georgia Tech. Personally owned systems which utilize encryption should escrow the encryption key through a method of the users choosing.	
5 - Encrypt data sent across public networks					
	R	**M**	**5-1**	Encrypt all sensitive data being transmitted outside of Georgia Tech networks using modern cryptography that is aligned with FIPS 140-2.	
6 - Remote Access					
M	**M**	**M**	**6-1**	Remote access to endpoints located on the Georgia Tech network should take place using secured methods over strongly encrypted communication channels and authenticated with Georgia Tech credentials. Examples of acceptable remote access include GT-credentialed SSH or VPN. Examples of Third Party remote access software which are NOT authorized include GoToMyPC and LogMeIn.	
7 - Use and regularly update anti-virus software					
R	**M**	**M**	**7-1**	Use active anti-virus mechanisms with current anti-virus signatures, except where best practices suggest otherwise. Georgia Tech owned endpoints must run OIT recommended anti-virus.	
8 - User Account Management					
R	**M**	**M**	**8-1**	Where possible, endpoints should be configured to require login using a unique user name and password. (Refer to campus Password Policy for details on password requirements). Examples where unique login may not be possible include digital signage, kiosks, and scientific instruments.	
R	**M**	**M**	**8-2**	Where possible, endpoints should be configured to lock the screen automatically after 20 minutes of inactivity. Login should be required to unlock the screen. Examples where timeout may not be possible include digital signage, kiosks, and scientific instruments.	
R	**R**	**M**	**8-3**	Periodically review user accounts and disable any accounts which are no longer necessary.	
R	**R**	**M**	**8-4**	Where possible limit the use of Administrator accounts for system administration purposes only.	
9 - System Backup					
R	**R**	**M**	**9-1**	Regularly perform backups of either critical files or the entire hard disk. Central Service: Crashplan	X
10 - System Disposal					
R	**M**	**M**	**10-1**	Electronically wipe or physically destroy all drives and other forms of electronic storage (e.g. USB drives) prior to disposal.	
R	**M**	**M**	**10-2**	Per policy, surplus all Georgia Tech owned computers and devices. http://www.policylibrary.gatech.edu/disposal-property	X
M	**M**	**M**	**10-3**	Georgia Tech endpoints must be returned to a manager prior to termination of employment with Georgia Tech.	

Data Protection Safeguards - Mobile Device Safeguards

The following are the safeguards which should be implemented for mobile devices containing Georgia Tech data. A **mobile device** is defined as cellular telephones, smart phones (e.g. iPhones, Android Phones, BlackBerrys), tablet computers (e.g. iPad, Kindle, Kindle Fire, Android Tablets), wearable devices (e.g. Google Glass, watch devices), personal digital assistants or any other mobile device containing Georgia Tech data (e.g. handheld scanning devices)

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 - Physical Security				
R	R	M	1-1	Mobile devices should be kept in your possession or locked in a secure location at all times.
M	M	M	1-2	Georgia Tech owned mobile devices which are lost, stolen or misplaced, must be reported immediately to the police department responsible for the area in which the device was lost or stolen. Employees must obtain a police report. The employee must also report the loss of the device to their management and provide the police report to their management.
		M	1-3	Personal mobile devices containing Georgia Tech data or that are used to access Georgia Tech information technology resources, which are lost, stolen or misplaced, should be reported immediately to their CSR or Georgia Tech Information Security.
2 - Passwords				
R	R	M	2-1	Mobile devices must be password, pin or swipe code protected and timeout features, which lock the device, must be enabled.
3 - Electronic Wiping and Device Disposal				
R	R	M	3-1	If available, remote wipe and device recovery services features must be enabled.
R	M	M	3-2	Mobile devices must be electronically wiped or physically destroyed prior to disposal.
M	M	M	3-3	Georgia Tech mobile devices must be returned to a manager prior to termination of employment with Georgia Tech.
4 - Encryption				
	R	M	4-1	Encrypt all sensitive data being transmitted outside of Georgia Tech networks using modern cryptography that is aligned with FIPS 140-2.
	R	M	4-2	Where possible, install and/or configure hardware or software encryption.
5 - Anti-Virus				
R	R	R	5-1	Install an anti-virus app where available. Users should scan their device for viruses periodically.
6 - Device Configuration and Updates				
R	R	R	6-1	Bluetooth and Wi-Fi services should be turned off on mobile devices when not in use.
R	R	R	6-2	Install software or apps from trusted sources only. Configure apps to limit the information available to the app (e.g. turn off location based services).
R	R	R	6-3	Periodically update the operating software and apps installed on mobile device.
7 - Backup				
R	R	R	7-1	Periodically backup mobile devices. When considering backing up mobile devices to cloud storage, refer to the controls listed within the Cloud Computing Safeguards tab of this document.

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 using modern cryptography that is aligned with FIPS 140-2.
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.