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	
		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. Refer to the Encryption Standard for more information regarding appropriate encryption: http://www.oit.gatech.edu/sites/default/files/Encryption_Standard.pdf	

Category of Data [1]			Item Ref.	Internal Control	Central Service[3]
I	II	III			
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, as per the Institute Encryption Standard: http://www.oit.gatech.edu/sites/default/files/Encryption_Standard.pdf	
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	
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

Category of Data [1]			Item Ref.	Internal Control	Central Service[3]
I	II	III			
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 15 minutes, require the user to re-enter the password to re-activate the	
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.	
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					

Category of Data [1]			Item Ref.	Internal Control	Central Service[3]
I	II	III			
		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	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.	