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					

Category of Data [1]			Item Ref.	Internal Control	Central Service[2]
I	II	III			
	R	M	5-1	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	
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 15 minutes of inactivity. Login should be required to unlock the screen. Examples where timeout may not be possible include digital signage, kiosks, and scientific	
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.	

M= Mandatory; R= Recommended