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
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, as per the Institute Encryption Standard: http://www.oit.gatech.edu/sites/default/files/Encryption_Standard.pdf
	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.