

Information Technology – Administrative Directive

Mobile Device Support

Information Technology is providing this document to define the policy and devices that are supported for remote email retrieval and synchronization with the University's exchange email servers. This policy is essential due to the regulations set by HIPPA and FERPA and to adhere to the best practices concerning mobile messaging.

Currently IT supports the use of blackberry's that are using our Blackberry Enterprise Server (BES) and supporting any device that runs the Windows Mobile operating system version 5 or greater. This includes devices like the PPC-6700 / 6800, Treo's and similar devices running windows mobile and is capable of over-the-air-synchronizing. These devices should have a DATA plan associated with it and should also have the ActiveSync program installed. For configuration of ActiveSync please refer to the document – Windows Mobile 5 Configuration using ActiveSync. (attached)

This policy will be enforced during the configuration and you will be prompted to accept the settings / policy. If you decide not to apply the security settings / policy you **will not** be able to sync your device with our exchange servers.

Policy settings:

Enforce a password	Yes	
Min password length:	4	std setting is for a PIN but can be set to strong (alpha-numeric)
Inactivity Time (minutes):	15	after 15min of no use the device will lock
Wipe Device after failed attempts:	10	will wipe the device after this many failed logins
Refresh settings on the device (hrs):	1	device will look for new policies at this time interval

By enforcing this policy IT has the ability to issue a remote wipe operation which will erase all data on the internal memory of the device should it be lost or stolen.

Please NOTE that on October 1, 2007 your device will be REQUIRED to use SSL to connect and synchronize with our email complex.

There will be a separate email arriving that will cover the SSL change.

SSL or Secure Sockets Layer is an encryption method that ensures the data between the device and the server is unreadable by anyone but the sender and the recipient. You will need to make sure that the device is setup to use SSL. The instructions listed above include using SSL.

NOTE:

If you have a memory card installed in your device and you lose it, the remote wipe will NOT erase the memory card. You should store only NON CONFIDENTIAL data on it. If you have CONFIDENTIAL data on the device it should always be stored in the unit's main memory for data protection to apply in case of accidental loss or stolen devices.