Mobile Data Sync - Policy

1. **Policy Statement**
   1.1. It is the responsibility of any employee of the university who uses a mobile device to access university resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct university business be used appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account.

2. **Reason For Policy**
   2.1. The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business uses for connecting mobile device to the university's network and data. This mobile device policy applies, but is not limited to, all devices and accompanying media that fit the following classifications:
   - Smartphones
   - Other mobile/cellular phones
   - iPads/iPods/iPhones
   - Tablets
   - E-readers
   - Portable media devices
   - PDAs
   - Portable gaming devices
   - Laptop/notebook/ultrabook computers
   - Any other mobile device capable of storing university data or connecting to a network

   2.2. This policy applies to any mobile hardware that is used to access university resources, whether the device is owned by the user or by the university.
   2.3. The overriding goal of this policy is to protect the integrity of the student and the university's data that resides within the university's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it could potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, and damage to the university's public image. Therefore, all users employing a mobile device connected to the university's network, and/or capable of backing up, storing, or otherwise accessing university data of any type, must adhere to university processes for doing so.

3. **Who Should Know This Policy**
   3.1. All faculty and staff, who use a mobile device to access, store, back up, or relocate any university data.

4. **Definitions**
   4.1. **Threats:** Malware, viruses, trojans, worms, spyware, malware, and other threats could be introduced to or via a mobile device.
   4.2. **Data Theft**: Restricted or sensitive university data is deliberately stolen.

5. **Policy Details**
   5.1. The most effective method of protecting the data on your mobile device is to protect the device itself. Always keep your mobile device on your person or in a secure physical location. This can prevent not only malicious access to your data, but inadvertent or accidental loss of your data or device. Additionally, you should also keep records of all identifying data for your device, such as its MAC address, serial number, and BlackBerry PIN, and the date and place of purchase. This information may help authorities track or identify a stolen device.
   5.2. If the mobile device is compromised by a threat, or data theft it may be necessary to wipe the device to protect IPFW resources, using the device's wipe capabilities.
      5.2.1. When a remote wipe is initiated by the user or by the IT department with the user's knowledge, the user's mobile device will be wiped of all data and restored to its factory default settings.
      5.2.2. **The wipe is not limited to corporate data**. Data that the employee has added to the device for personal use will also be deleted. This data is not recoverable on the device itself, but can usually be restored from a backup (e.g. on a personal computer or a cloud service) if the mobile device remains in or returns to the user's possession, or a new device is able to store the backup.
      5.2.3. **It is recommended that users back up their personal data frequently to minimize loss if a remote wipe is necessary.**
      5.2.4. A remote wipe will only be initiated if the IT Services Security Officer deems it absolutely necessary.

6. Violations
   6.1. Contact the IT Services Security Officer with your concerns.

7. **Related Information**
   7.1. IPFW follows the Purdue Data Classifications found at:
   http://www.purdue.edu/policies/information-technology/viib6.html

8. **Contacts** (Consult the phone directory, or contact the IT Services Help Desk for the current name and number for these contacts)
   8.1. IT Services Security Officer

9. **Policy Approval**

10. The signers of this document agree that their responsible areas approve this policy.

11. _____ _____
IT Services Security Officer *Date*

12. _____ _____
CIO & Director of IT Services *Date*