1. **Policy Statement**
   
   To minimize or prevent unauthorized access to sensitive data, all electronic devices used to access university data must be inaccessible after a period of inactivity.

2. **Reason For Policy**
   
   2.1. As a result of federal laws and security policies from Indiana and Purdue Universities, IPFW has had to put into place additional security controls dictated by a number of federal acts requiring compliance such as:
   
   2.1.1. The Patriot Act: Covers wide areas protecting electronic transmission of information & data
   
   2.1.2. Gramm-Leach-Bliley Act: Covers protection of customer information gathered from financial transactions
   
   2.1.3. Health Insurance Portability & Accountability Act (HIPAA): Protects a person’s health information
   
   2.1.4. Family Education Rights and Privacy Act (FERPA): Protects a student’s educational information.

3. **Who Should Know This Policy**
   
   3.1. All units, students, faculty, and staff of IPFW are governed by this policy.

4. **Definitions**
   
   4.1. Devices – Any electronic device used to access university data. This includes but is not limited to:
   
   4.1.1. PC’s, Macintosh,
   
   4.1.2. iPad/iPod,
   
   4.1.3. PDA,
   
   4.1.4. Kindle,
   
   4.1.5. Galaxy,
   
   4.1.6. Nook,
   
   4.1.7. cellular devices,
   
   4.1.8. smart phones. ETC.

5. **Policy Details**
   
   5.1. University owned PC
5.1.1. The screen saver will automatically lock your network-connected machine after 15 minutes of inactivity. After it takes effect you will be prompted to enter your network password to regain use of your workstation.

5.2. Purdue’s Security Auditors allow no more than 15 minutes of inactivity before invoking the workstation lock.

5.3. Users with access to the IPFW data are required to manually implement such a screen saver on their devices if one does not exist via automatic IPFW imaging.

5.4. Mac
   5.4.1. Macintosh users are required to manually implement such a screen saver on their workstations.

5.5. Tablets / PDA
   5.5.1. iPad/iPod, PDA, Kindle, Galaxy, Nook, etc. users are required to manually implement such a screen saver/password access lock on their devices.

5.6. Cellular Devices
   5.6.1. Most cellular devices provide a security lock option. This may be a password, Personal Identification Number (pin), or a security pattern. Cellular Device users with access to the IPFW network are required to manually implement some type of device lock.

6. Anomalies
   6.1. Classrooms – Depending upon the class situation some temporary exceptions may be granted after approval IT services.

7. Related Information
   7.1. Release of Social Security Number” (Ind. Code § 4-1-10)

   7.2. Purdue Data Handling Requirements
       7.2.1. [http://www.itap.purdue.edu/security/procedures/dataHandling.cfm](http://www.itap.purdue.edu/security/procedures/dataHandling.cfm)

   7.3. Purdue’s Social Security Number Policy
       7.3.1. [http://www.purdue.edu/policies/pages/information_technology/v_5_1.html](http://www.purdue.edu/policies/pages/information_technology/v_5_1.html)

   7.4. Purdue’s Password Policy(change 30 or 120 days)

8. Violations
   8.1. Contact the IT Services Security Officer with your concerns if you are aware of volition.
9. **Contacts** (Consult the phone directory, or contact the IT Services Help Desk for the current name and number for these contacts)

9.1. IT Services Security Officer
10. Policy Approval

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

[Signature]
IT Services Security Officer  
Date: 6/12/13

[Signature]
CIO & Director of IT Services  
Date: 6/12/13