Draft: Workstation Privileges Policy

1. **Policy Statement**
   1.1. The policy is to grant every user all of the access to their workstation required to perform their daily job.

2. **Reason For Policy**
   2.1. This policy exists to protect university data, university workstations, and university networks.

3. **Who Should Know This Policy**
   3.1. All IPFW employees should be aware of the details of this policy as all employees are affected by it.

4. **Definitions**
   4.1. **Office workstation** – any desktop, laptop or tablet PC owned by the university and used by an employee—on or off campus—for business purposes.
   4.2. **Principle of least privilege** – assigning the lowest level of user privileges in order to minimize the risk of exploits and compromises. In many cases, viruses, malware, etc. take advantage of users having heightened access, whether the user initiates the install or it happens automatically. The concept is to only grant enough privilege as is needed for the person to accomplish their daily tasks.
   4.3. **User Privilege** - should be given access only to information (and software) they expressly need to do their jobs.
   4.4. **Administrator Privilege** –An administrator is a local account, or local security groups, with complete and unrestricted access to create, delete, and modify files, folders, and settings on a particular computer. An administrator account is used to make system wide changes to the computer, such as:
      4.4.1. Creating or deleting user accounts on the computer
      4.4.2. Creating account passwords for other users on the computer
      4.4.3. Changing others' account names, pictures, passwords, and types
      4.4.4. Installing software and upgrades

5. **Policy Details**
   5.1. In general, users of IPFW workstations do not have access to administrator privileges on their workstation

5.2. Some users, by virtue of their work, need administrator privileges on their machine. Such privileges will be provided by ITS upon the written request from the user's vice chancellor to the CIO. Those users need to:

5.2.1. Practice the principle of least privilege.

5.2.2. Enable administrative privileges only when it is needed.

5.2.3. Realize that running your computer as an administrator (or as a Power User in Windows) leaves your computer vulnerable to security risks and exploits.

5.3. When a user who does not have administrator privileges has a need to perform a task which requires administrative privileges, a person with administrator rights will be available to assist through ITS.

6. **Related Information**

6.1. URL to related resources page.

7. **Contacts**

7.1. Initial contact for questions: IT Services Help Desk

7.2. Policy clarifications: IT Services Security Officer

8. **Policy Approval**
   8.1. The signers of this document agree that their responsible areas approve this policy.

IT Services Security Officer	*Date*
CIO & Director, IT Services	