1. **Purpose**
   1.1. IT Services has the responsibility to protect the university systems and data from compromise. This process has been established to ensure the safeguard of the campus network health.

2. **Audience**
   2.1. This process covers students, faculty, staff, and all individuals that have access to the IPFW network through a personally owned or university issued computer.

3. **Definitions**
   3.1. Infected Personally Owned Computer: a private computer that was contaminated with an infectious program, such as virus or malware.
   3.2. Infected University Owned Computer: a university issued computer that was contaminated with an infectious program, such as a virus or malware.
   3.3. Severe/critical threat: the infectious program is propagating across multiple computers and network resources, gathering, destroying and/or sending sensitive data off site, causing physical damage to hardware, and potentially rendering the campus network inoperable.
   3.4. High threat: the infectious program is gathering, destroying and/or sending sensitive data off site, causing physical damage to hardware and/or propagating to other computer on campus or is otherwise putting the university at risk.
   3.5. Moderate threat: the infectious program is isolated to one component, it is not propagating information, and the user productivity is negatively affected
   3.6. Low threat: the infectious program is affecting a personal computer only, but not the campus network.
   3.7. Radius access: access to the campus wireless network.

4. **Obligations**
   4.1. Severe/critical threat level
      4.1.1. All occurrence:
         4.1.1.1. Personally Owned Computer: The IT Services Help Desk will immediately disconnect the infected machine from the campus network without notice. The IT Services Help Desk will try to contact the owner to inform that in order to reactivate radius access; the computer’s owner will need to provide the IT
Services Help Desk documentation stating that the machine was cleaned by a professional.

4.1.1.2. University Owned Computer: The IT Services Help Desk will immediately disconnect the infected machine from the campus network without notice. An IT Services Help Desk Technician will be dispatched to the faculty or staff member’s location and execute the proper procedures before the system is allow back on the campus network.

4.2. High threat level

4.2.1. First occurrence:

4.2.1.1. Both Personally Owned Computer and University Owned Computer: The IT Services Help Desk will use Banner to determine if the account is for a professor, and if the professor is teaching a class. If the professor is scheduled to be teaching a class no action will be taken until after the class is completed.

4.2.1.2. Personally Owned Computer: The IT Services Help Desk will try to contact the owner to inform that within 30 minutes the infected machine will be disconnected from the campus network. In order to reactivate radius access, the computer’s owner will need to provide to the IT Services Help Desk documentation stating that the machine was cleaned by a professional.

4.2.1.3. University Owned Computer: The IT Services Help Desk will contact the faculty member to inform that within 30 minutes the infected machine will be disconnected from the campus network. An IT Services Help Desk Technician will be dispatched to the faculty member’s location and execute the proper procedures before the system is allowed back on the campus network.

4.2.2. Subsequent Occurrences: The same procedures for step High Threat – First occurrence will be taken. Further, the computer’s owner will need to provide to the IT Services Security Officer documentation stating that the machine was cleaned by a professional. The user may also agree to rebuild his or her workstation to remove the threat.

4.3. Moderate threat level

4.3.1. It is the responsibility of the owner of the equipment to correct the problem

4.4. Low threat level
4.4.1. It is the responsibility of the owner of the equipment to correct the problem.

5. Violations
   5.1. Contact the IT Services Manager of Security, Policy, and Planning (itssecurityofficer@ipfw.edu) with your concerns.

6. Related Information
   6.1. Incident Response Policy

7. Contacts
   7.1. IT Services Help Desk: Kettler Hall, room 206, (260) 481-6030, or helpdesk@ipfw.edu