Extending the University Data Network Policy

1. **Policy Statement**
   1.1. Individuals or units may not deploy network devices that add to the university network, or secure or isolate parts of the university network, without review and approval by Information Technology Services (section 8.1).

2. **Reason For Policy**
   2.1. Certain network devices, if not deployed and configured correctly, can cause service interruptions and make network problems difficult or impossible to isolate and identify. In addition, if not properly secured, these devices can give unauthorized users access to the university network, or the ability to monitor network traffic. The installation of these devices must therefore be managed and coordinated through IT Services.
   2.2. IT Services is responsible for the university's data, video, and voice communications network. This includes designing, deploying, documenting, monitoring, maintaining, supporting, securing and troubleshooting the physical data, video, and voice networks of the university, as well as managing the Internet Protocol (IP) address spaces federally assigned to IPFW (including public and private addresses).

3. **Definitions**
   3.1. Network device: Equipment that allows a connection to the network, physical or virtual. This includes but is not limited to hubs, bridges, switches, routers, firewalls, wireless access points (WAPs), network address translators (NATs), remote access servers (RAS), and virtual private network (VPN) servers; or workstations, servers or devices to provide any of this functionality.

4. **Who Should Know This Policy**
   4.1. This policy applies to all users of IPFW information technology resources, regardless of affiliation, and irrespective of whether those resources are accessed from on-campus (including student housing) or from off-campus locations.

5. **Emergency Actions**
   5.1. IT Services engineers may temporarily suspend or isolate access to an information technology resource or network device when it reasonably appears necessary to protect the confidentiality, security, integrity, or availability of the resource or device or data, or to protect other computing resources, devices, or data, or to protect the university or others from potential harm.

6. **Interference with the University Network**

Extending the University Data Network Policy

6.1. Several categories of user devices use radio frequencies in the same range as wireless Ethernet and may disrupt wireless network communications. These devices include cordless phones, microwave ovens, and personal network devices using Bluetooth technology. This interference can be intermittent and difficult to diagnose. IT Services will work with the user to resolve frequency conflicts, but cannot be ultimately responsible for resolving such problems to owner satisfaction. Preservation of network reliability and security is primary. If a device installed by an individual or unit interferes with the wireless network maintained by IT Services, the owner of the device must expediently cooperate to resolve the conflict (regardless of whether the device is or is not connected to the university network).

7. **IPFW Service Set Identifiers (SSIDs)**

7.1. Only wireless access points that are approved by IT Services are allowed to broadcast standard university SSIDs. These include but are not limited to IPFW, IPFW-WRLS, IPFWGuest and IPFW-WRLS-GUEST.

8. **Exceptions to this Policy**

8.1. Requests for exceptions to this policy should be submitted to helpdesk@ipfw.edu. IT Services will review requests on a case-by-case basis as is appropriate. Approved exceptions to this policy must comply with university networking standards. IT Services will maintain a record of approved exceptions to this policy.

9. **Consultation**

9.1. IT Services is available to provide consultation or advice related to this policy and may involve the IT Security Officer; Chief Information Officer; Security, Policy and Planning team; and others in consultation.

10. **Contacts**

10.1. Initial contact for questions, consultation, exceptions: IT Services Help Desk

10.2. Policy clarification: IT Services; IT Security, Policy and Planning