PURPOSE

This policy is to inform the user community about the procedures and requirements for utilizing personally-owned wireless routers in the OSU Institute of Technology (OSUIT) residence halls.

SCOPE

This policy applies to all students living in any of the residence halls that do not have OSUIT provided wireless access.

POLICY

1.01 Personally owned wireless routers may be connected to the residence hall dorm room Ethernet jacks under the conditions stated within this policy.

DEFINITIONS

2.01 WPA ENCRYPTION – Wi-Fi Protected Access (WPA) encryption is a security standard that protects data transmitted over the wireless network.

2.02 WIRELESS ENCRYPTION PASSWORD – the password used to connect to the resident’s wireless network.

2.03 ADMINISTRATOR PASSWORD – the password used to connect to the router and modify the configuration.

PROCEDURES

3.01 The wireless router must be registered with the designated Residential Life staff member to not only be recorded as an approved device but be properly setup in order to help prevent network impairment.

3.02 The wireless router must be configured for WPA encryption.

3.03 The wireless connection password must be kept private and not shared. The administrator password for the wireless router must be changed from the factory default and not shared.
3.04 The owner of the wireless router is responsible for any network activity emanating from the wireless router including, but not limited to, copyright violations and network disruption. The occupant may be subject to legal action from entities including, but not limited to, the RIAA and/or MPAA, for copyright violations associated with their wireless router.

3.05 Disciplinary actions resulting from misuse or shared connections to the wireless router will follow normal Student Conduct processes for network policy violations. This may include turning off the room and/or suite network privileges.