Wireless Networking

IT-20

About This Policy

Effective Dates:
09-19-2008

Last Updated:
08-17-2011

Responsible University Administrator:
Office of the Vice President for Information Technology & Chief Information Officer

Policy Contact:
University Information Policy Office, uipo@iu.edu

Scope

This policy applies to all users of Indiana University information technology resources regardless of affiliation, and irrespective of whether those resources are accessed from on-campus or off-campus locations.

Policy Statement

Only wireless networking equipment installed and managed by or under the auspices of UITS or regional campus counterparts is allowed to be connected to the university network.

UITS and regional campus counterparts are responsible for establishing standards and procedures governing wireless networking.

Reason For Policy

Wireless networking offers increased convenience for mobile users. However, wireless networking introduces significant additional risks not associated with wired networks (e.g., exposing the network and its traffic to unauthorized parties external to the physical space within which it is deployed). If not deployed and configured correctly, wireless networking can cause service interruptions and make network problems difficult or impossible to isolate and identify. In addition, if wireless networking services are not properly secured, unauthorized users may be able to access the university network or to monitor network traffic. The installation of these devices must therefore be managed and coordinated.

University Information Technology Services (UITS) and regional campus counterparts are responsible for the university's data, video, and voice communications network. This includes designing, deploying, documenting, monitoring, maintaining, supporting, and troubleshooting the physical data, video, and voice networks of the university, as well as the management of the Internet Protocol (IP) address spaces assigned to Indiana University (including public and private addresses).

Procedure

Campus housing: Installation of wireless network equipment by residents is prohibited in locations where the campus housing network service is provided and managed by the university. Interference: Several categories of devices use radio frequencies in the same range as wireless Ethernet; therefore, other devices that use these frequencies may disrupt wireless network communications. Such devices include cordless phones, microwave ovens, and personal network devices using Bluetooth technology. This interference can be intermittent and difficult to diagnose. UITS or regional campus counterparts will work to resolve frequency conflicts, but cannot be responsible for resolving problems resulting from non-network wireless devices. If a device installed by an individual or unit interferes with the wireless network maintained by UITS or regional campus counterparts, the

owner of the device must cooperate to resolve the conflict (regardless of whether the device is or is not connected to the university network). Indiana University Service Set Identifiers (SSIDs): Only wireless access points that are approved by UITS or regional campus counterparts are allowed to broadcast standard university SSIDs. Exceptions to this policy: Requests for exceptions to this policy should be submitted to noc@iu.edu or to the relevant campus helpdesk. UITS and/or the regional campus counterpart will review requests on a case-by-case basis as appropriate. Approved exceptions to this policy must comply with university wireless networking standards. UITS and regional campus counterparts will maintain a record of approved exceptions to this policy. Consultation: UITS is available to provide consultation or advice related to this policy and may involve the Information Policy and Information Security offices and/or regional Chief Information Officers (CIOs) and others in consultation.

Definitions

SSID stands for "Service Set Identifier," which is a set of characters that identify a wireless network. It is defined in the IEEE 802.11 standards. wireless network is a telecommunications network whose interconnections between nodes are achieved using electromagnetic waves such as radio waves instead of wire or fiber optic cable. Wireless networking equipment includes devices used to set up a wireless network such as wireless hubs, routers, and access points.

Sanctions

Indiana University will handle reports of misuse and abuse of information and information technology resources in accordance with existing policies and procedures issued by appropriate authorities. Depending on the individual and circumstances involved this could include the offices of Human Resources, Vice Provost or Vice Chancellor of Faculties (or campus equivalent), Dean of Students (or campus equivalent), Office of the General Counsel, and/or appropriate law enforcement agencies. See policy IT-02, Misuse and Abuse of Information Technology Resources for more detail.

Failure to comply with Indiana University information technology policies may result in sanctions relating to the individual's use of information technology resources (such as suspension or termination of access, or removal of online material); the individual's employment (up to and including immediate termination of employment in accordance with applicable university policy); the individual's studies within the university (such as student discipline in accordance with applicable university policy); civil or criminal liability; or any combination of these.

History

- Reviewed December 2011.
- Revised August 17, 2011: changed titles in *Sanctions* section to more accurately reflect current usage.
- Revised March 4, 2010: enhancing language in *Sanctions* section
- Approved: September 19, 2008
- Interim: June 26, 2008
- Draft: October 26, 2001
- Revised: December 2007
- Revised: March 2008

Related Information

Temporary Exception 2