

933 COMPUTER NETWORK/SERVER SECURITY POLICY

933.1 Overview. Indiana State University provides network services to a large number and variety of users – faculty, staff, students, and external constituencies. Security compromises for any campus-networked system can have a detrimental impact to other systems housed on the University network infrastructure. The Office of Information Technology (OIT), in cooperation with University constituents, has campus-wide responsibility to maintain the integrity and security of networking systems and to provide the wiring, cable and wireless network infrastructure supporting voice, data and video services.

933.1.1 Application of Policy. This policy is necessary to ensure the stability, performance and security of the Indiana State University network environment. Data is an institutional asset. Therefore, it is appropriate and applies to establish policies to ensure the protection, integrity, and reliability of data. This policy encompasses all systems directly connected to OIT-maintained networks or systems on networks that receive network service from Indiana State University network resources. The policy includes, but is not limited to, campus local area network connections, modem pools and DSL connections. OIT is required to provide reasonable protection consistent with federal and state laws placing fiduciary obligation on ISU to protect the privacy, use and security of select data. Laws include, but are not limited to: Electronic Communications Privacy Act (ECPA), Computer Fraud and Abuse Act (CFAA), Gramm-Leach-Bliley Act (GLBA), the United States Patriot Act (USPA), Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA) and others. This policy is intended to define the limits of that obligation and the duties and responsibilities of University employees to safeguard information that constitutes protected data to all ISU computer network resources.

933.2 Definitions.

933.2.1 Indiana State University Computers and Networked Resources. Indiana State University Computers and Networked Resources refers to all computers and network resources (e.g. routers, switches, firewalls, print servers, remote access servers) owned or operated by or on behalf of Indiana State University.

933.2.2 Network Traffic. Network Traffic (defined broadly) is the flow of data within the confines of the Indiana State University network, and traffic flowing from the ISU network through the Internet service provider.

933.2.3 Network Server. Network Server (defined broadly) is a computer physically connected to the ISU data network for the purpose of sharing or distributing its resources such as printers, files, and programs. This definition is not intended to include desktop workstations that are supporting peer-to-peer file or printer sharing.

933.2.4 Network Servers Residing in High Risk Area. Network Servers Residing in High Risk Area consists of those servers that sit between the Internet and the ISU network's line of defense which are commonly some combination of firewalls or

similar network security appliance.

933.2.5 Host Based Intrusion Detection Systems. Host Based Intrusion Detection Systems are systems that use an automated tool or set of tools designed to detect security violations by analyzing the data source and to respond with appropriate actions.

933.2.6 Wireless Network Access. Wireless Network Access means unlicensed spread spectrum radiofrequency wireless local area network access. This access permits connectivity to the ISU network.

933.2.7 Remote Access. Remote access means the ability to get access to a computer or a network from a remote location. This may occur via telephone lines or a secondary internet service provider.

933.2.8 Network Management. Network Management means the execution of the set of functions required for controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a data network.

933.2.9 Physical Network Security. Physical Network Security means controlled access to areas which house network infrastructure components such as data electronics and physical cable plant.

933.3 Statement of Policy. OIT will monitor all network traffic (intra-campus, inbound and outbound Internet, DSL service, and modem connections) to ensure proper network management and performance. The Chief Information Officer or her/his designee will determine, with the advice of the Information Technology Advisory Council (ITAC), criteria for proposed changes to traffic limitations and recommend those that are consistent with the academic and business goals of the University.

933.3.1 Registry of Servers. OIT will maintain a registry of all servers resident on the ISU network in order to ensure proper accountability and communications between all parties responsible for server support and operation.

933.3.2 Academic Department Servers. Servers used and managed by academic departments for instructional and/or research purposes are permitted. Registration of such servers is required and can be accomplished using the online form located at the OIT website. Such registration is intended for the identification of the resource on the network to facilitate communications and is not intended to imply control over the functional use of the server.

933.3.2.1 OIT Assistance. OIT will assist academic departments in determining the proper level of security to implement on servers residing in high-risk areas. Systems behind the firewall must be secured. This will minimize the potential for damage by intruders. Academic departments establishing servers will consult with OIT to determine appropriate security solutions for their environment. OIT

will provide one or more valid IP addresses for dedicated systems, depending on demonstrated need. OIT will configure and maintain all network firewall devices. Information concerning changes to individual unit firewall services configuration and routine maintenance actions will be communicated to departmental contact person(s).

- 933.3.3 All Other Servers.** All other servers (those that support administrative, business, or office functions or process, servers that house institutional data subject to federal, state or local law, or servers that act as the primary repository for institutional data) shall be administered and managed by OIT.
- 933.3.4 Failure to Register Server.** If servers are placed on the University network without proper registration, OIT staff will attempt to contact the appropriate individual(s). If contact cannot be made, OIT personnel are authorized to disconnect the server from the University network until such time as proper registration is completed.
- 933.3.5 Server Guidelines.** Servers shall conform to guidelines set forth in the server High Risk Area document located at the OIT website. Server configuration parameters are published on the OIT website. This is the University Office of Information Technology recommended configuration document library. This library contains general and operating system-specific guidelines.
- 933.3.6 Network Filtering Devices.** Network filtering devices will not be set up as a firewall without approval from OIT.
- 933.3.6.1 Problems with Network Filtering Devices.** While these type firewall systems can provide excellent functionality, there are a number of potential problems with using them. These problems include, but are not limited to: 1) the security of the host system itself must be maintained; 2) Operating System firewall systems are often difficult to configure and maintain, requiring significant system administration skills and may result in excessive coordination responsibilities for OIT staff; and 3) an improperly configured operating system firewall may cause problems for other systems on campus. If problems exist with a network filtering device, OIT personnel will attempt to contact the appropriate individual(s). If contact cannot be made, OIT personnel are authorized to disconnect the system from the University network until such time that a technical resolution is found.
- 933.3.7 Host Based Intrusion Detection Systems.** Host based intrusion detection systems will be installed on all mission critical desktop systems. OIT shall provide an initial configuration that will be used by University personnel during first time installation. Deviations from the initial configuration for an individual or a department host based intrusion detection system shall be documented by OIT personnel. A list of currently supported host based intrusion detection systems may be obtained by contacting the OIT help desk.

933.3.8 Wireless Networks. To ensure the technical coordination required to provide the best possible wireless network for Indiana State University, OIT will be solely responsible for the management of 802.XX and related wireless standards access points and wireless access security on the campus. Departments may deploy 802.XX or related wireless standards access points after appropriate coordination with OIT.

933.3.8.1 Registration. When deploying any wireless access point, departments must register the access point device with OIT. Departments are strongly encouraged to utilize OIT services for all activities related to wireless network access. These activities include pre-engineering/consultation, site survey, installation, and management. A registration form is available at the OIT website and further wireless network access guidelines may be found there.

933.3.8.2 Unregistered Wireless Access Points. OIT will perform network scans for unregistered wireless access points. If an unregistered wireless access point is identified, OIT personnel will attempt to contact the appropriate individual(s). If contact cannot be made, OIT personnel are authorized to disconnect it from the University network until such time as the access point is properly registered. Any department wireless access point that interferes with another system will be disconnected until the problem is resolved.

933.3.9 Remote Access. OIT provides remote access services to the University community and while OIT encourages departments to use this service, remote access does present a security issue. When a department identifies the need for remote access, it must register the remote access device(s) with OIT.

933.3.9.1 Registration and Guidelines. A registration form is available at the OIT website. Remote access system guidelines are contained in the OIT recommended configuration document library found at the OIT website.

933.3.9.2 Failure to Register. If remote access servers or systems are placed on the University network without proper registration, OIT personnel will attempt to contact the appropriate individual(s). If contact cannot be made, OIT personnel are authorized to disconnect these from the University network until such time as proper registration is completed.

933.4 Responsibilities of OIT. As the central support entity for the Indiana State University data network, OIT is assigned the following responsibilities and authority:

(a) OIT, or its designee, is authorized to perform a security audit of any ISU network device(s) at any time.

(b) OIT is the primary contact for all network security related activities.

(c) OIT will prepare network recommendations and guidelines and will post them on OIT web pages. OIT will publish security alerts, post vulnerability notices and patches, and disseminate other pertinent information to assist in preventing security breaches.

(d) OIT will coordinate investigations into any alleged computer or network security compromises, incidents, and/or problems. Suspected security problems and issues may be reported to OIT via e-mail to itcert@isugw.indstate.edu, or by calling extension 2910.

(e) OIT will monitor backbone network traffic in real-time as necessary and appropriate to detect unauthorized activity or intrusion attempts. All monitoring will be carried out in compliance with the policies contained in the Indiana State University Handbook.

(f) If network scans or monitoring identify security vulnerabilities that could jeopardize the University or the ISU network, the cooperation of the system owners and system managers will be solicited to accomplish necessary corrective action. If the appropriate contact cannot be made, the head of the system owner's/system manager's department will be notified. When a server experiences a problem that constitutes a serious security issue or negatively impacts the ISU network on a global basis, OIT will take steps to disable network access to that system and/or device until the problem(s) has/have been rectified.

933.5 Access to Network Distribution Centers. To ensure physical network security, access to network distribution centers is limited to those individuals whose work requires access to rooms that house network electronics and physical cable plant.

933.6 No Exceptions. There are no exceptions to this policy.