Ibn Sina University
Network Connectivity Policy

Ibn Sina University Information Systems & Services Network Connectivity Policy

Contents

Ibn Sina University Information Systems & Services

Purpose

The purpose of this policy is to ensure that effective measures are in place to protect devices and users connecting to the ISU network. Protection should be in place to avoid the unauthorised access or damage to:

- The ISU network infrastructure
- Devices connected to the network
- Data stored on these devices
- Data being transmitted across the network.

Scope

ISU has made a significant investment in network infrastructure, creating a facility to enable electronic communication within ISU, the linked colleges of ISU and through Internet, the National Research and Education Network, to the wider Internet community. This network plays a critical role in the running of the university and, as such, it is essential that the network is protected and managed appropriately. This document defines the policy for connecting devices to the ISU Computer network with a view to maintaining Network security, high levels of availability and to ensure that the network can be managed and supported in an efficient manner.

This policy applies to all equipment being connected to the network, including, but not limited to:

- PCs
- Laptops
- Printers
- Network Devices (hubs, switches, routers, wireless equipment)
- Servers
- PDAs/Phones
- Photocopiers
- Scanners

Policy

All devices attaching to the ISU network must comply with relevant ICT Security policies as outlined at: Ibn Sina University Information Systems & Services

http://www.ISU.EDU.SD/policies/index.shtml and to ISU approved standards relating to software, hardware, protocols and network connectivity. In particular your attention is drawn to the following security policies:

- ICT Compliance Policy
- Mobile Computing Security Policy
- Code of Conduct

If you are connecting to the network from a remote location, please consult the following:

- Remote Access Policy

When connecting any device to the wired network (outside of the Residences), please confirm its compliance with current standards by contacting the ISU Information Systems and Services (ISS) Department or your local ICT support. ISU reserve the right to disconnect from the network any device causing interference or performance problem.
The attachment of wireless access points and wireless broadband routers to the ISU network is specifically prohibited, unless installed and operated by nominated and sanctioned IT administrators. IT administrators, nominated locally, should be communicated to the ICT Security Implementation Group. ISS currently manages the unlicensed RF spectrum on the University campus. Devices which are likely to cause interference with the University wireless networks should only be operated following consultation with the ISS Department.
Devices connecting to the ISU Network may be subject to an assessment and software audit.
ISU staff, students and all other users connecting to the ISU network must ensure that anti-virus and/or anti-spyware applications are installed on the computing devices they are using.

Anti-Virus

All computing devices MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system.

Anti-Spyware

All computing devices MUST have an anti-spyware application installed that offers real-time protection to the target system unless they meet one or more of the following conditions:

- The system they are using is locked down using a product such as Deepfreeze and the user does not have the ability to install applications which will persist across a reboot.
- The system is used for a specific purpose (eg. Collecting data from a scientific instrument) and is not used for web browsing.

Definitions

TERM DEFINITION

Computing Device For the purposes of this policy, a computing device is any computer system attached to the ISU network. In addition, this includes any PDA or smartphone. This includes, but is not limited to all devices running: Microsoft Windows and all permutations, Apple OS-X and all permutations and any Linux/Unix based operating systems.

Malware Software designed to infiltrate or damage a computer system without the owner's informed consent. It is a blend of the words "malicious" and "software". The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Spyware Broad category of software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has also come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

Anti-virus Software Consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware).

Document Change Management

Ibn Sina University believes that it is important to keep this policy current in order to ensure that it addresses security issues accurately and is up-to-date with evolving business issues and technologies. This policy is a living document that will be reviewed annually and/or updated as needed.
The Director of Information Systems and Services will draft necessary changes and have them reviewed and approved by the Executive Group of ISU as appropriate. The Director of ISS and the members of the ICT Security Implementation Group will communicate changes to the University communities. Anyone in the University can determine the need for a modification to the existing policy. Recommendations for changes to this policy should be communicated to the Director of ISS.