Ibn Sina University
Remote Access Policy

Contents

Purpose

The purpose of this policy is to define standards for connecting remotely to the ISU network from any host. These standards are designed to minimize the potential exposure to ISU from damages which may result from the unauthorised use of University resources, including the loss of sensitive or confidential data, theft of intellectual property, damage to the public image of the institution, or corruption of critical ISU internal systems.

Scope

This policy applies to all ISU employees, students, contractors, vendors and agents using remote access connections to connect to the ISU network. Exisitng and remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

General Remote Access Policy

General

1. Authorised, remote access to ISU networks can be given toindividuals and organisations. Requests for authorisation should be submitted to the Director of Information Systems & Servicesor a relevant authorised network manager for the area beingaccessed. Where appropriate the ICT Security Implementation Group will be consulted as part of decision making process.
2. The authorised user must ensure that the remote link is not usedby other parties.
3. The authorised user bears responsibility for the consequences should this access be misused.
4. Authorised users should be familiar, and comply with:
a. ICT Security Policy
b. Network Connectivity Policy
c. Mobile Computing Policy

Requirements

1. Secure remote access to critical business systems must bestrictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. Access to administration systems should be through the University Virtual Private Network.
2. For information on creating a strong pass-phrase see the Password Policy.
3. At no time should any ISU employee, student or authorized user, provide their login or email password to anyone, not even family members.

4. ISU employees, students and other authorised users with remote access privileges must ensure that their connected devices do not connect to other devices at the same time.
5. Routers for dedicated ISDN lines configured for access to the ISU network must meet minimum authentication requirements of CHAP (Challenge-Handshake Authentication Protocol).
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. All devices that are connected to ISU networks via remote access technologies must use the most up-to-date anti-virus software (see http://www.ISU.EDU.sd/ict/security-anti-virus/anti-virus.shtml).
8. All devices used to connect to ISU's networks must be running a supported, up-to-date operating system and must be patched to the latest level.
9. Organisations or individuals who wish to implement non-standard Remote Access solutions to the ISU networks must obtain prior approval from the Information Systems & Services Department.

Document Change Management

Ibn Sina University believes that it is important to keep this Remote Access 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, Services & Communication (ICT) 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 ICT.