Remote Access Policy

ROWAN UNIVERSITY POLICY

Title: *Remote Access Policy*
Subject: *Information Security*
Policy No: *ISO:2013:15*
Applies: ***University-Wide***
Issuing Authority: Senior Vice President for Information Resources and Technology and Chief Information Officer
Responsible Officer: *Director of Information Security*
Adopted: ***07/01/2013***
Amended: ***06/01/2014***
Last Revision: 7/2/2018

I. PURPOSE

A. Rowan University provides secure remote access technologies that enable authorized users to remotely access the university network and its internal resources.

B. The purpose of this policy is to define standards for connecting to the Rowan University network from any remote host. These standards are designed to minimize the potential exposure to the University from damages which may result from unauthorized use of university resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical internal systems, etc.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer and the Director of Information Security shall implement and ensure compliance with this policy.

III. APPLICABILITY

A. This policy applies to all University employees, students, and affiliates including vendors and agents with a university owned or personally-owned computer or workstation used to connect to Rowan University network. This policy applies to remote access connections used to do work on behalf Rowan University or for personal business, including reading or sending email and viewing intranet web resources.

B. Remote access implementations that are covered by this policy include, but are not limited to, dial-up modems, DSL, FIOS, VPN, SSH, WiFi and cable modems, etc.

IV. DEFINITIONS

A. *Cable Modem* - Cable companies such as Comcast provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps.

B. *Dial-up Modem* - A peripheral device that connects computers to each other for sending communications via the telephone lines.

C. *Digital Subscriber Line (DSL)* - Is a form of high-speed Internet access used over standard phone lines.

D. *Fiber Optic Service (FIOS)* - Is a data communications service provided by Verizon that uses fiber optic cables to transfer data.

E. *Remote Access* - Connection to a data-processing system from a remote location, for example through a virtual private network.

F. *Secure Shell (SSH)* - Is a secure network protocol for secure network communication services between two networked computers.

G. *Virtual Private Network (VPN)* - Extends a private network across a public network, such as the Internet using secure communication.

H. *Wi-Fi* - Wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. A Wi-Fi enabled device such as a PC, mobile phone, or PDA can connect to the Internet when within range of a wireless network.

V. REFERENCES

A. Information Security Policy

VI. POLICY

A. Remote access is provided for university related activity only. All devices that are used to connect to the university network through an approved remote access technology are considered to be extensions of the university network and are subject to all applicable university policies, standards and rules.

Students will not be granted remote access privileges.

Affiliates (personnel that are not faculty or staff at the University) who require remote access privileges will be granted access on a case by case basis. Affiliations may be requested by faculty and staff and are subject to an annual approval process.

The purpose of this policy is to define standards for connecting to the Rowan University network from any remote host. These standards are designed to minimize the potential exposure to the University from damages which may result from unauthorized use of university resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical internal systems, etc.

B. Technology Configuration and Management

1. All university remote access technologies will be configured and managed by the university Information Resources Technology (IRT) team.
2. All university remote access technologies must be configured to automatically disconnect after a preset amount of inactivity and/or after a predetermined length of time.
3. All university remote access technologies must employ a secure authentication mechanism.
4. Devices that are used to remotely connect to university administrative applications must also be managed by IRT.
5. The following configuration requirements must be enabled on all devices that support them:
    a. Antivirus software must be installed and configured to scan on a recurring schedule.
    b. The latest antivirus definitions must be updated and installed on a recurring schedule.
    c. The latest available patches for the remote access device’s operating system and applications must be configured to automatically download and install on a recurring schedule.

6. The deployment of new remote access technologies must be approved by the Information Security Office (ISO) and IRT management.

C. Authorization

1. All new or current employees, faculty and staff that require remote access as a function of their job must have their supervising manager or director send an email to the university Helpdesk (support@rowan.edu) requesting access.
2. All contractors and vendors that require remote access as part of their job requirements with the university must fill out and sign the university remote access request form and Non-Disclosure Agreement (NDR). Each request will be reviewed and approved by the ISO and IRT management.
3. Any exceptions to the authorization process or access model must be reviewed and approved by the Director of Information Security and Director of Networks & System Services.

D. Requirements:

1. Non-University owned devices cannot be used to store (save) data on any devices used for remote access. (Refer to university Data Governance Policy for full details on data types and appropriate usage.)
2. Remote access to internal university applications and networks is currently limited to Citrix technologies, authorized VPN technologies and Internet Web Access technologies.
3. Remote access users must not share their login credentials and should take all reasonable efforts to avert accidental disclosure.
4. In order to connect to remote access technologies from off campus a high-speed internet connection is recommended (i.e. cable modem, DSL, FIOS).
5. Faculty, Staff and affiliates with remote access privileges must ensure that their University owned or personal computer or workstation, which is remotely connected to the university network, is not connected to any other external network at the same time.
6. Affiliates that require a permanent remote access connection must be approved by the Director of Information Security and Director of Networks & System Services, and must be configured to use VPN tunneling.

VII. NON-COMPLIANCE AND SANCTIONS

A. Violation of this policy may result in disciplinary action up to and including termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers.

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer