

GA 44. Network Security Policy

Title:	Network Security Policy
Policy Number:	GA 44 / 07.18
Effective Date:	July 24, 2018
Approval and Review:	Revised and approved on October 22, 2024
Issuing Authority:	VP for Development

1. RATIONALE

This policy is intended to protect the integrity of the campus network, to mitigate the risks and losses associated with security threats to computing resources and to ensure secure and reliable network access and performance for the University community. This policy is necessary to provide a reliable campus network to conduct the University's business and prevent unauthorized access to institutional, research or personal data. In addition, the University has a legal responsibility to secure its computers and networks from misuse.

2. POLICY

- RHU faculty, staff or students may not connect, nor contract with an outside vendor to connect, any device or system to the University's networks without the prior review and approval of IT/IS. Colleges or departments that wish to provide Internet or other network access to individuals or networks not directly affiliated with the University must obtain prior approval from IT/IS.
- In order to maintain reliable network connectivity, no other department may deploy wireless routers, switches, bridges, and/or DHCP (Dynamic Host Configuration Protocol) services on campus without prior review and approval of IT/IS.
- Users are not permitted to attach personal devices to the network.
- Unauthorized access to University networking equipment (firewalls, routers, switches, etc.) is prohibited. This includes port scanning or connection attempts using applications such as SSH/SNMP, or otherwise attempting to interact with University network equipment.
- Unauthorized access to University equipment/cabling rooms is also prohibited.
- IT/IS will take action to prevent spoofing of internal network addresses from the Internet. IT/IS will also take action to protect external Internet sites from source address forgery from devices on the University's network.

- The University's external Internet firewall default practice is to deny all external Internet traffic to the University's network unless explicitly permitted.
- Access and service restrictions may be enforced by device, IP address, port number or application behavior.
- IT/IS reserves the right to decrypt SSL traffic which transits the University network.
- IT/IS may investigate any unauthorized access of computer networks, systems or devices.
- All devices connecting to the network must have adequate security installed/maintained and must be configured and maintained in such a manner as to prohibit unauthorized access or misuse.
- IT/IS reserves the right to quarantine or disconnect any system or device from the University network at any time.
- Network usage judged appropriate by the University is permitted. Some activities deemed inappropriate include, but are not limited to, attaching unauthorized network devices, engaging in network packet sniffing or snooping, Setting up a system to appear like another authorized system on the network (trojan).
- Any device found to be in violation of this policy, or found to be causing problems that may impair or disable the network or systems connected to it, is subject to immediate disconnection from the University's network
- The University reserves the right to test and monitor security, and to copy or examine files and information resident on university systems related to any alleged security incident or policy violation.
- IT/IS will maintain and monitor traffic logs for all network devices and systems for security auditing purposes.
- IT/IS reserves the right to monitor, access, retrieve, read and/or disclose data communications when there is reasonable cause to suspect a University policy violation,
- IT/IS may perform penetration testing of any University owned devices or systems on its networks in order to determine the risks associated with protecting University information assets.

3. RELATED DOCUMENTS

> IT Manual