

University Information Technologies

[University Information Technologies \(UNIT\)](#) maintains a variety of policies governing the use of University computing and communication resources. Every member of the University community is bound by these policies and is expected to be thoroughly familiar with them. Persons found in violation of these policies will be subject to the full range of disciplinary sanctions, up to and including expulsion. In order to retain necessary flexibility in administration of policies, the University reserves the right to interpret, revise, or delete any of the provisions of these policies, as the University deems appropriate in its discretion. All changes in policy are approved by appropriate governing bodies of the University prior to publication.

Complete copies of all UNIT policies are available in the [Villanova Policy Library](#) and include, but is not limited to: copyright infringement and illegal file sharing, email policy, and acceptable use.

1. Misuse of IT systems may include but is not limited to:
 - Unauthorized entry into a voice/email mailbox.
 - Unauthorized use of another individual's username or password.
 - Sharing of University-provided username or password with other faculty, staff, students or individuals.
 - Use of University telephone/email/Internet to send abusive, harassing or obscene messages.
 - Use of browsers, programs , or extensions to hide or change your network address in an attempt to create privacy while connected to the University network or resource.
 - Use of personal routers (wired or wireless).
 - Probing or scanning the University network or services or attempting to cause a denial of service.
 - Consumption of a disproportionate amount of network bandwidth.
 - Attempting to connect to systems or using data from systems where access or usage has not been authorized.
 - Accessing personal information of others without authorization.
2. Students are responsible for maintaining the security of their personal computing devices including updating the device with security patches, enabling the default protections on the device such as antivirus or firewall, and updating installed software to mitigate vulnerabilities.

If you have any technology questions or concerns, [submit a help request](#) or contact the UNIT Service Desk at support@villanova.edu or 610-519-7777, or stop by the [UNIT Tech Zone](#) for assistance.