UB RESNET ACCEPTABLE USE POLICY

Category: Information Technology
Responsible Office: Chief Information Officer
Responsible Executive: Chief Information Officer

Date Established:
Date Last Revised: 8/12/11
Date Posted to Library: 9/2/2011

Summary

ResNet is a wired data communications network exclusive to UB's residence halls and apartments. In this document are the responsibilities and accepted behavior specific to people who use ResNet.

Policy

BACKGROUND

To provide the highest quality access to information technologies, Campus Living and Computing & Information Technology (CIT) maintain computing networks that can connect each resident's personal computers and entertainment devices to the Internet. The wired network (not wireless) is called ResNet.

POLICY STATEMENT

ResNet users are responsible for all network traffic originating from their computers, including email, Internet browsing, file transfers, peer-to-peer file sharing, instant messaging, video conferencing, social networking, and connections to other machines.

ResNet users are required to follow all University at Buffalo, Computing & Information Technology and Campus Living rules and policies.

ResNet residents must ensure that their computers present no identifiable risk to the network, i.e. the computer has anti-virus software installed and up-to-date critical operating system updates applied.

ResNet users must be aware that:

1. ResNet must be used in accordance with all copyright laws. This includes, but is not limited to, refraining from using your computer in a way that would violate those laws such as operating unlicensed software or media distribution servers.
2. ResNet communication services, wiring and other hardware may not be modified or tampered with in any way, e.g. installing an unauthorized wireless access point.
3. ResNet may not be used to post advertisements for personal business, or for the sale of products or services for commercial gain.
4. Harassment of other users, by any method, is a violation of the law and will not be tolerated.
5. ResNet cannot be used to misrepresent or hide your personal identity, e.g. email sent from a fake or unauthorized address.

PROCEDURE

To initially connect to ResNet, users must insure that each computer presents no identifiable risk to the network, i.e. has anti-virus software installed and up-to-date and operating system patches applied to date.

At any time that there is credible evidence that a ResNet user's computer has become a risk to the network, the user will be required to re-certify the computer's safe operation at his/her expense.

ResNet users are also expected to be responsible network citizens. ResNet is a shared resource and as such, users should refrain from using any application that may interfere with the legitimate use of the network by others.

Think of your personal computer as your computing home. It is advisable to "lock the front door" so that people cannot use your machine without your supervision. Using a power-on password, or a screen saver password are good ways to control physical access to both the information on your computer, and your computer's access to ResNet.

COMPLIANCE

At any time that there is credible evidence that a ResNet attached computer has become a risk to the network, ResNet access will be denied and the resident will be required to re-certify the computer's safe operation at his/her expense.

Violating any of these conditions of use may result in suspension or loss of ResNet usage privilege, expulsion from university residence halls or apartments, discipline from other university bodies such as the Student Judiciary, or criminal charges. Damage or theft of ResNet wiring or hardware is the financial responsibility of the residence members. If responsibility is traced to any individual or particular group of individuals, then they will be held personally responsible for the theft or damage.

POLICY REVIEW AND UPDATE

The Chief Information Officer or his designee will periodically review and update this policy as needed. Questions concerning this policy should be directed to the Office of the Associate VP for Information Technology.

Contact Information

Office of Chief Information Officer
517 Capen Hall
University at Buffalo
furlani@ccr.buffalo.edu
(716) 645-7979

Related Information

University Documents:

- UB Computer and Network Use Policy
- UB's Digital Millennium Copyright Act (DMCA) Policies
- UB Password Policy