Access to Information Technology Resources

Purpose

Information Technology Resources (computer hardware, software, telephone systems, cable television, networks, services, data, and other information) are made available at Hamilton to support and facilitate the teaching, research and administrative functions of the College. Access to these resources is provided to employees of the College (faculty, administration, staff, maintenance and operations) and enrolled students consistent with their responsibilities. This policy describes the criteria for assignment of access privileges to these resources and the responsibilities associated with using them.

Scope

This policy applies to all employees, students, alumni and retirees of Hamilton College.

Enforcement

Any employee, student, alumnus or retiree found to have violated this policy may be subject to termination of access privileges.

Policy Revision History

Last revised, September 2015.

Table of Contents

- Electronic Resources
- Convention for User Names
- Access in Residence Halls
- Management of Internet Bandwidth
- Personal Computers on the Network
- Virus Protection
- Operating System Updates
- Network Connections in Departments
- Connections from Off-Campus (through the VPN)

Electronic Resources

Electronic resources include:
Access to electronic resources for employees, students, spouses/partners, and alumni is enabled through username and password provided to individuals according to the following guidelines.

**Non-Faculty Employees** are given access to Group I and Group II resources upon notification of hire. Access to Group III resources is by request from the Department Head.

Non-Faculty employee access to all resources is normally removed at the end of business on the last date of employment. As soon as an employee gives notice, he/she should enable a "vacation" (auto-responder) message to indicate his/her last date of employment and to provide correspondents with an alternate address to which they should address future College business. Employees should also remove any personal e-mail or files from their accounts during this period.

**Faculty** are given access to Group I resources and Group II resources upon notification of hire. Access to Group III resources is by request from the Dean of Faculty.

Faculty access to all resources is normally removed at the end of business three months after the last date of employment. A request for a brief extension of e-mail privileges may be made to the Director of Human Resources.

**Retirees** (employees who leave the College and meet Hamilton's requirements for retirement) may ask to keep their Hamilton email account by contacting the Director of Human Resources prior to retirement. The account must be renewed on an annual basis. The retiree's network account will be removed on the employee's last day unless an extension has been granted.

**Students** are given access to Group I and Group II resources upon making an acceptance deposit to the College. Students who work in administrative offices may be granted limited access to Group III resources.

Student access to all resources is removed three months after withdrawal or graduation. A request for a brief extension of e-mail privileges may be made to the Director, Help Desk and Training Services in LITS.

**Graduates** are eligible for access to a free e-mail forwarding service. Each alumnus keeps his/her username and the forwarding address will be username@alumni.hamilton.edu which will automatically forward e-mail to a personal e-mail account.

E-mail accounts are continued for Hamilton alumni for three months after graduation, and may be extended by special request to the e-mail administrator.

Other individuals, upon submission of a request, may be granted access to some, or all, of Hamilton's IT resources by the Vice President for Libraries and Information Technology. Generally, such individuals will have some association with the College. The terms of access will be stated at the time access is granted.

Under no circumstance may anyone use College IT resources for profit-making activities, in ways that are illegal (e.g. copyright violations), that threaten the College's tax-exempt or other status, or interfere with reasonable use by other members of the College community.
Convention For User Names

The standard Hamilton naming convention for access to electronic systems comprises the first initial of the first name, followed by (up to seven characters of) the last name. If duplicates occur, the middle initial is generally used to resolve ambiguity.

Access in Residence Halls

Residence hall connections are intended to provide students with access to cable television services, and the campus data network. One cable television, and data network connection is provided for each student. Network connections, wiring, equipment, or jacks may not be altered or extended beyond the location of their intended use. Students must provide their own televisions, computers and software. Information on current minimum standards and recommended configurations is available online. Network standards are updated annually. Any costs incurred to repair damages to a network, telephone, or cable television jack in a residence hall room will be divided equally, and billed to the students residing in that room.

Management of Internet Bandwidth

The campus network, including our connection to the Internet, is a critical shared resource for supporting the academic program. Uses of our Internet connection that are central to the academic/administrative mission of the college (e.g. access to Hamilton web, e-mail, and Blackboard Courseinfo servers) always will receive a higher priority compared to non mission related activities.

To ensure sufficient internet bandwidth is available for mission critical activities, internet traffic using the secure wireless network and traffic originating from wired ports in dorm facilities are limited to a maximum of 30Mbps for each IP connection, except for known Peer-to-Peer Internet applications (applications for distributing videos, music, software, etc.) which receive a highly restricted bandwidth.

Hamilton does not monitor the content of traffic on the network. It is the responsibility of each person using college resources, including the network, to do so in an ethical and legal manner. Particular attention should be given to observing copyright laws for digital materials.

Personal Computers on the Network

Internet addresses are provided dynamically through a Dynamic Host Configuration Protocol (DHCP) system.

The rules and regulations contained in this policy pertaining to electronic mail and Internet access are equally applicable to the use of personal machines for file sharing or as servers. If bandwidth or other problems occur, LITS reserves the right to discontinue access to the machine. Computers connected to the network may not be used as servers for private enterprises, commercial activity, or personal profit. Computers connected to the network may not be used to provide access to the Internet for anyone not formally affiliated with the College. If personal computers on the Hamilton network are used as servers, the administrator has the additional responsibility to respond to any use of the server that is in violation of these policies and procedures. Server administrators must take steps to prevent recurrence of such violations and report these violations to the Hamilton Network Administrator (hostmaster@hamilton.edu).
LITS reserves the right to disconnect any network port whose activity causes an adverse effect on the network or on any other user. Network connections may also be revoked in the case of malicious or inappropriate computing activity on the network.

LITS reserves the right to restrict access to the network during expansion, or for diagnostic and maintenance services. Every effort will be made to provide advance notification and to schedule such disruptions during times of minimum impact and traffic.

**Virus Protection**

Hamilton College requires all computers connected to the network to have up-to-date virus protection. Failure to do so will result in the loss of connectivity to the Hamilton College network until the situation is corrected. All college-provided computers have antivirus software installed.

In addition, all attachments to e-mail sent and received to/from the Hamilton e-mail service (Google Mail) are scanned for viruses. A description of Google's approach to virus scanning can be found at: https://support.google.com/mail/answer/25760?hl=en

**Operating System Updates**

All computers connected to the Hamilton College network must be kept up-to-date with critical operating system updates. Failure to do so will result in the loss of connectivity to the Hamilton College network until the situation is corrected. All college-provided computers have automated updating of operating system.

**Network Connections in Departments**

All offices, laboratories, and classrooms on campus are wired for access to the network. If departments request additional network jacks, or if network connections need to be moved to different locations, the department should request this service through LITS. The department will be billed for charges resulting from moves, additions, and changes.

Network connections, wiring, equipment, or jacks may not be altered or extended beyond the location of their intended use. Any costs incurred to repair damages to a network, telephone, or cable television jack in a department will be billed to that department.

**Connections from Off-Campus (through the VPN)**

The Virtual Private Network (VPN) provides secure access to Hamilton information resources from off-campus for Hamilton employees, contractors, and consultants. To use the VPN the individual must have access to an Internet connection and an appropriately configured computer.

It is the responsibility of those with VPN privileges to ensure that unauthorized users are not allowed access to the computer while it is connected to the VPN. The computer connected to the VPN must use up-to-date anti-virus software, and have operating system and security patches installed. Users of computers connected to the VPN should employ the same safeguards as on campus:

- lock your screen when away;
- don’t leave the computer unattended;
- don’t allow unauthorized users to access to the device while connected to the VPN;
- disconnect from the VPN when you are finished;
• use strong passwords.

VPN users will be automatically disconnected from Hamilton College's network after thirty minutes of inactivity. Pings or other artificial network processes are not to be used to keep the connection open. VPN users must install the approved Cisco SSLVPN clients which are provided by LITS.

If you have any questions on securing your personally owned device, you can contact the LITS Help Desk at 315-859-4181.

Return to Policies

Last Updated: September 22, 2015