

Information Technology Services Policies and Procedures

Revised August 2010

The mission of the Information Technology Department at Emory & Henry College is to support the academic and administrative technology initiatives of the College. We will provide integrated technological support for all College educational, administrative and student support services in a receptive and courteous manner. Via ongoing research and development, the Information Technology Department will take the lead in identifying, testing and integrating new technologies and formats for the College community in support of the College's academic mission.

Emory & Henry College

Security & Acceptable Use of the Campus Network & Technology Policy

Revised August 2011

The Library and Information Technology Services department, with the oversight of the College's Executive Council, determines the campus network and technology security and acceptable use policy in accordance with the security and preservation needs of the Emory & Henry College, best practices in the IT industry, and in compliance with federal, state, and local legal requirements. All students, faculty, staff, and others affiliated with Emory & Henry College receiving a network access account must adhere to the following policies and guidelines. Employment or enrollment at Emory & Henry College signifies agreement to abide by all rules, regulations and policies of the College. Please note that all policies are subject to change. Notification of changes will be posted. This document will be reviewed and published regularly on the College website and in various official College publications such as the *Student Handbook*, *Faculty Handbook* and the *Staff Handbook*. All network users must adhere to the most current published revision.

Guests of the College utilizing Internet access through the College's network are expected to practice good Internet citizenship in their online activities, so as to avoid reflecting negatively on Emory & Henry College. Specifically, they must adhere to all local, state, and federal laws, not download illegally obtained copyright protected materials, and not access websites or materials which are not in keeping with the teaching, research, and educational goals of the institution. Anyone affiliated with Emory & Henry College who allows minor children to utilize public access computers on campus must be responsible for the actions of those children and should remember that Emory & Henry College does not have any filtering hardware or software in place for Internet content.

All students, faculty, and staff, have a network account assigned to them for their individual use while at Emory & Henry College. Emory & Henry College computerized information systems exist to promote shared access to computing, communication, and information necessary to serve the teaching, research, and administrative needs of the entire campus community. These systems and the data they contain are vital resources of considerable monetary and intellectual value, in addition to important personal information which must be handled in a secure and confidential manner. Access to computer systems and networks, including e-mail and web material placed on or distributed through the systems and networks owned or operated by Emory & Henry College is a privilege, not a right, and requires compliance with College policies and to federal, state, and local laws. Thus, all account holders of the College's information assets have a responsibility to use these systems in a respectful, ethical, professional, and legal manner.

The purpose of the network is to support the teaching, research, and administrative needs of the College. The network is not designed nor intended to support the downloading of copyrighted material, such as, unlawfully obtained music, videos, and software. Such activities are not permitted at any time. Online activities which require disproportionately large amounts of bandwidth (such as online gaming or watching full-length movies online) are strongly discouraged as they require a major portion of the College's available internet bandwidth for the use of a single individual, which can disrupt the research and other legitimate activities of the College community of network users.

This policy pertains to all computers, printers, scanners, networks, Internet connections, and communication systems transmitting voice, data, or video information owned or leased by the College or connected to the College network. Appropriate use is always ethical, reflects academic honesty, the security and confidentiality of personal information, and shows restraint in the consumption of shared resources.

All users of College information assets are required to demonstrate respect for intellectual property, ownership of data, system security mechanisms, and the individual's right to privacy and freedom from intimidation, harassment, and unwarranted annoyance.

While acknowledging a respect for privacy, the College cannot guarantee confidentiality in the use of any College information system. This policy acts as notification that all email accounts are the intellectual property of the College and are for the conduct of College-related business. As such, users are hereby reminded that email accounts should not be used to send or receive emails of a personal nature. Furthermore, the College retains the right to immediately disable or delete all network and email accounts upon either termination of employment or as directed by College officials.

Electronic records retained on College systems are subject to state and federal Privacy Acts, the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (US PATRIOT Act), and *Commission on Accreditation for Law Enforcement Agencies* (CALEA), as well as *Freedom of Information Acts*. World Wide Web information located in designated web directories will be considered public information if "read" access is granted. Access to and the utilization of data contained within College administrative, academic, and student support administrative systems are also subject to *Family Educational Rights and Privacy Act* (FERPA) regulations and authorized users agree under this acceptable use policy to adhere to and abide by FERPA privacy and security guidelines. Student and staff medical and counseling records may be subject to *Health Insurance Portability and Accountability Act* (HIPAA) regulations and must be accessed and handled in accordance with those established guidelines and regulations.

Appropriate Use Guidelines

In making appropriate use of resources Emory & Henry students, faculty, and staff must:

- Be consistent with the purposes of the network. It is designed to support research, education, and administrative needs of students, faculty, staff, and administrative personnel.
- Assume responsibility for material on personal web pages.
- Comply with local, state, and federal laws for materials made available on the Internet.
- Use copyrighted materials only with the prior approval by the copyright holder or in compliance with "Fair Use" guidelines as described in current federal copyright legislation.

- Use resources only for appropriate purposes, such as, but not limited to, assignments given by instructors, college related work, communication. Inappropriate use is described in the section below.
- Discontinue use of a College public-access or lab computer for personal or recreational activities if no other resources are available for students to use for class assignments.
- Protect the individual's user logon ID (user account) from unauthorized use. The individual is responsible for all activities on his or her user ID.
- Access only files and data that belong to the individual user, that are publicly available, or to which the individual user has been given authorized access.
- Use only legal versions of copyrighted software in full compliance with vendor license requirements. Do not make copies of copyrighted software for personal use.
- Be considerate in the use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, or wasting computer time, connect time, disk space, printer paper, bandwidth, or other resources.

In making appropriate use of resources Emory & Henry students, faculty, and staff must NOT:

- Use another person's user logon ID and password at any time.
- Allow another person other than the actual user to access a user account.
- Use another person's files or data without permission.
- Use computer programs to decode passwords or access control information.
- Attempt to circumvent or subvert system security measures.
- Engage in any activity that might be harmful to computers or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files.
- Use College systems for partisan political purposes, such as using electronic mail to circulate advertising for political candidates.
- Transmit, distribute, upload, post, or store any material in violation of any applicable law or regulation, or that encourages conduct that could constitute a criminal offense, gives rise to civil liability or otherwise violates any applicable local, state, national or international law or regulation. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization.
- Transmit, distribute, upload, post, or store any material that is obscene, defamatory, libelous, unlawful, harassing, abusive, threatening, harmful, vulgar, constitutes an illegal threat, violates export control laws, hate propaganda, fraudulent material or fraudulent activity, or invasive of privacy or publicity rights.
- Use College resources to create personal web pages containing (1) pornography or (2) abusive and/or profane language.
- Place digital photographic or recording equipment of any kind in any public space on campus without the prior written permission of the Dean of Students.
- Waste computing resources, for example, by intentionally placing a program in an endless loop or by printing excessive amounts of paper.
- Use the College's resources for moneymaking activities as these can jeopardize Emory & Henry's non-profit status. The network may not be used to advertise a commercial business, or to support a personal business interest. Neither may electronic mail be utilized to circulate advertising for products.
- Engage in any other activity that does not comply with the general principles presented above.
- Peer-to-peer file sharing is now prohibited at Emory & Henry College in compliance with the *U.S. Higher Education Act*. Downloading movies, music, or other copyrighted materials without permission of the copyright holder is strictly forbidden.

There are numerous legal and legitimate sites in the World Wide Web for the downloading of materials, such as iTunes.com and Rhapsody.com. The College recommends that anyone wishing to download music or other copyrighted materials utilize legal means to do so.

- Any non-computing device must be approved and registered through the IT Help Desk before it can be connected to the network. Kelly Library and IT Services reserves the right to restrict devices accessing the network.
- The E&H wireless network does not accept non-College access points. Personal wireless access points, hubs, and routers are strictly forbidden.
- Any computers connected to the Emory & Henry network are strictly forbidden to function as hosts for network services such as peer-to-peer, file-sharing, local area networks (LAN), etc.

Abuse of E-mail Privileges

E-mail and network connectivity are a privilege, not a right. These privileges can be revoked for violations of this *Acceptable Use* policy. Unacceptable behavior includes, but is not limited to:

- Infringement on others' privacy
- Interference with others' work
- Copyright infringement
- Illegal activity
- Use of mass e-mail for commercial or political mailings
- Use of distribution lists for purposes other than teaching, research, and administrative needs of the College.

Penalties for unacceptable behavior range from deactivation of the account through College judicial action or referral to law enforcement authorities. For minor first offenses, the Chief Information Officer/Director of the Library will notify the offender with a simple e-mail warning.

Mass E-mail Guidelines

The ability to send mass e-mail messages to all employees is currently available to each employee with an Emory & Henry e-mail address. In addition, a few individuals have the ability to send mass e-mail messages to all students. Mass electronic mailings shall be concise and to the point, and shall consist of a plain-text message without graphics or bolding, italics, or other formatting. The use of attachments should be limited to small size files, such as MS Word and Excel files. Larger files can be posted on the password-protected section of the website or on the learning management system. To post a document on the web site, please contact Public Relations. If you need assistance with the learning management system, please contact the Instructional Technologist.

Using the All E&H Employees E-mail Distribution List

Mass e-mail is recognized as an important medium for facilitating communication within the Emory & Henry community. However, the potential misuse of mass e-mail is also recognized. The policies and procedures found in this document attempt to provide guidance for the appropriate use of the All Employees e-mail distribution list. Please note that there is a list "EHC Community" that was created for community members who wish to advertise or announce items such as garage sales, items for sale, babysitting services, etc. Membership on that list is voluntary and can be joined by contacting the Help Desk.

Remember that the College's official internal electronic newsletter, *The Scoop* (not e-mail), should be used for all general College-related announcements and for providing information about programs, projects and activities. If you need assistance with including these events

in the College's electronic calendar, please contact Public Relations. In order to have your news or event featured in *The Scoop*, a request should be submitted to Scoop@ehc.edu by 2 p.m. the day before the announcement should appear in the e-newsletter. If you are unsure about where to post an announcement, please contact the Help Desk for assistance.

In addition, discussion forums should be set up through the use of ANGEL or Moodle (not e-mail). If you need assistance with setting up an ANGEL or Moodle account for a discussion forum, contact Harry Baya (hbaya@ehc.edu).

The All E&H Employees list should be used only for the following purposes:

- Instructions from the faculty marshal for all faculty and/or staff that do not seem appropriate for other communication media.
- Communication from the chair of the staff affairs committee for all faculty and/or staff that does not seem appropriate for other communication media.
- Communication from senior administrators for all faculty and/or staff that does not seem appropriate for other communication media.
- Communication from individual faculty or staff of general interest to a majority of faculty and/or staff that does not seem appropriate for other communication media.
- Distribution of faculty and staff surveys
- Reports from faculty or staff committees or task forces of general interest to a majority of the faculty and/or staff.
- Reports from the faculty or staff representative to the Board of Trustees.
- Reports from the governance groups (Faculty Advisory Committee, the Staff Affairs Council, etc.).

Urgent Messages

Urgent mass e-mails are reserved for highly important, time-sensitive emergency notices. In those cases, faculty and staff need to contact one of the following offices and request the message to be distributed to the College-wide community. Urgent messages must be sent in plain text and contain no graphics, bolding, or other HTML formatting. The following is a list of the office authorized to distribute mass e-mails to the campus-wide community:

- President's Office – Roz Reichard, Mark Graham
- VP for Academic Affairs – Linda Dobkins
- VP for Student Life – Pam Gourley
- Campus Security – Scott Poore
- VP for Business and Finance – Dirk Wilmoth
- Chaplain's Office – Mary K. Briggs
- Centralized Student Assistance - David Hawsey
- Physical Plant – Mark Pitcher
- Library/IT – Lorraine Abraham

Urgent messages include the following:

- Messages concerning emergency, health and safety: bomb or terrorist threat; natural disaster alert; mechanical failures; weather closures or delays; crime alerts; and computer virus alerts; health alerts.
- Logistics announcements: construction closures; traffic routing; and ozone or environmental alert notices.
- Messages pertaining to matters of university-wide policy.
- Messages of a timely nature having direct impact on large numbers of faculty, staff, or students.

Web pages on College Servers

The privilege of presenting material on the College web site can be revoked, with or without cause, at the College's discretion. Web pages found to be in non-compliance may be removed immediately by the web administrator or upon failure to revise web pages and conform to these guidelines.

Accessing Data in the Administrative Systems of Emory & Henry College

The College recognizes that personnel must have access to student records and other data that is protected under the *Family Educational Rights and Privacy Act* (FERPA) and the *Health Insurance Portability and Accountability Act* (HIPAA) in order to conduct the legitimate business of the College. All Emory & Henry College administrative system users agree that use of systems maintained by partners, consortia arrangements, etc. is governed by the rules and regulations set forth in this policy. Acceptance of this policy implies cooperation with the spirit and intent of any complimenting acceptable use policies which may be provided by E&H's service providers. College personnel must adhere to the following policies:

- Computers logged into Datatel/Raiser's Edge/Entrisik Informer, or other administrative system applications, must never be left unattended. All users should log out of these systems whenever it is not in active use.
- No faculty or staff, office or department, should share administrative system accounts.
- Student worker access to administrative systems must be strictly supervised and must be conducted only through the use of an authorized student assistant administrative system access account.
- Administrative users should not store any confidential data on hard drives, flash memory sticks, or other portable storage media. All confidential data derived from administrative systems must be stored and shared via secure password-protected folders on the network.
- Confidential data in reports, spreadsheets, or other formats must not be emailed to other personnel. It should be stored and retrieved from password-protected folders on the network.
- Personnel working from remote locations or taking work off campus on laptops or other portable devices must not download any data which falls under the protection of FERPA or HIPAA regulations.
- Students, faculty, employees, and others authorized by consortia partners on shared systems may be provided an account on the partner's information networks. Account privileges may include, but are not limited to, secured network storage, networked applications, databases, and Web services.
- All permanent employees who need access the administrative systems of consortia partners will receive user account information from the consortia partner's network administrators through the Emory & Henry Library and IT department, which is the liaison between the College and the consortia partner. Access will be revoked immediately upon termination or at the end of the last day of employment.
- Users shall under no circumstances represent themselves as others for the purpose of circumventing established policies or security measures, or for any reason without explicit permission of the others. Sharing accounts and/or passwords is a violation of this policy.

Enforcement

The CIO and staff members of the Library and Information Services Department reserve the right to enforce this policy as deemed necessary to protect the security of the network, data and files, as well as the rights and privileges of its users. These policies have been developed in consultation with IT directors from the Council of the Independent Colleges of Virginia member institutions as well as the information technology security officials at The Ohio State University, the University of Chicago, and Loyola University, and represent widespread practices in public and private institutions of higher education throughout the United States.

Emory & Henry College considers any violation of appropriate use principles or guidelines to be a serious offense and reserves the right to copy, examine, and remove any files or information resident on College systems allegedly related to unacceptable use and behavior. Violation of these rules will be reported to the appropriate campus office for further action. Punishments may include temporary or permanent suspension of user privileges on the network and/or disconnection from the campus network, or other sanctions as described in the Faculty and Faculty Status handbooks, or the Staff handbook. Offenders may be prosecuted under laws including (but not limited to) the *Privacy Protections Act of 1974*, the *Computer Fraud and Abuse Act of 1986*, the *Computer Virus Eradication Act of 1989*, the *Interstate Transportation of Stolen Property* statutes, the *Virginia Computer Crimes Act*, the *Electronic Communications Privacy Act*, and the *Telecommunications Act of 1996*.

Cooperation with Law Enforcement Investigations

The proper procedures for staff members in the Emory & Henry Library and Information Services Department regarding cooperation with and participation in investigations of suspected misconduct involving the use of the campus network or technology hardware and/or software are as follows:

- When seeking technical support assistance from Library and Information Services staff, each student must sign a waiver which states that the department may look at the student's personal computer files in the course of completing the requested technical support. The waiver authorizes the department to view the content of the computer's hard drive(s) in the course of completing any requested technical support assistance, if necessary in assisting the computer user.
- Should a department staff member discover potentially illegal activities, data, or files on a computer, he or she are to immediately document what he or she saw, why he or she came into contact with that data or file, and how he or she arrived there in terms of the directory structure. The staff member should take no direct action, but should notify the Chief Information Officer/Director of the Library immediately. If the CIO is unavailable, then he or she should notify the VP for Student Life without delay if a student is involved, or the VP for Business and Finance if an employee is involved. If none of these administrators are available, or if there is a genuine threat to public safety inferred in the discovered materials (e.g. bomb threats, plans for violent activities, etc.), then the staff member is authorized to notify Campus Security, or law enforcement officials directly if Campus Security is not available.
- Staff members are not to confiscate any personal computers or other technology that are not College-owned property.
- Staff members are authorized to remove College-owned technology and return it to the Library and Information Technology department for removal of materials which violate the *Security and Acceptable Use Policy* with the approval of the Chief Information Officer/Director of the Library.

- Staff members are authorized to boot up computers, open files, or examine directories or folders on College-owned and non-College-owned equipment for College officials, if requested, in the investigation of suspected infractions of the *Security and Acceptable Use* policy if the equipment in question has been connected to the Campus network.
- Department staff members are not to release any information, data, or files of any kind to law enforcement authorities without receipt of a properly-executed subpoena compelling the College to cooperate in a criminal investigation.

Any questions or comments can be directed to the Chief Information Officer/Director of the Library.

Disclaimer

Revised August 2010

Emory & Henry College makes no warranties of any kind, whether expressed or implied, with respect to the information technology services it provides. The College will not be responsible for damages resulting from the use of communication facilities and services, including, but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions caused by the negligence of a College employee, or by the user's error or omissions. Use of any information obtained via the Internet is at the user's risk. The College specifically denies any responsibility for the accuracy or quality of information obtained through its electronic communication facilities and services, except material represented as an official College record.

The College reserves the right to append or modify these policies and procedures and also to extend, limit, restrict, or deny privileges and access to its information resources without notice.

Information Support Services for Students

Revised August 2010

E&H Information Technology will help students with network, e-mail and server access problems. Our service is limited to assisting students with connections and access to our college network. We do not help students with general repairs, maintenance, or upgrades to personal computers.

E&H does not recommend any particular local computer service providers and cannot be responsible for making arrangements with vendors on behalf of students.

Hardware Policy

Revised August 2010

All computer equipment purchased by Emory & Henry College for the business use of its faculty, staff and students shall be managed and maintained by the Information Technology Department and shall remain the sole property of Emory & Henry College. Disposal or reallocation of all computer technology at Emory & Henry College shall be at the discretion of the College.

Using Non-College Owned Equipment on Campus

Revised August 2010

Personal equipment that will be used on the College's network must be approved by the Information Technology Department prior to installation. The Department reserves the right to refuse to allow any faculty, staff or student to attach non-approved equipment to the College network.

All student computers will be subject to a security inspection by the Information Technology Department prior to being connected to the College network. No student computer will be allowed to be connected to the College network without updated anti-virus software and a complete registration record of computer identification data.

Emory & Henry College is not responsible for the maintenance, repair or replacement of non-College owned equipment, nor are they responsible for any tangible or intangible losses resulting from any College-owned equipment.

Independent Departmental Servers on the E&H Network

Revised August 2010

The Information Technology Department strongly discourages the use of independent departmental servers which are attached to the E&H network, but understands that some servers have been a part of the network for some time. No new independent servers will be added to the E&H network unless they are located and maintained within the server facilities of the College by the Information Technology Department. All existing independent departmental servers must be located within the firewall security system of the College network. All servers attached to the College network must be inspected and approved by the Information Technology Department to insure that they meet stringent levels of network security. The Information Technology Department reserves the right to refuse to attach any independent server to the College network and to disconnect any server which is deemed by the Department to be a security risk to the College network. Emory & Henry College is not responsible for the maintenance, repair or replacement of non-College owned equipment.

Software Policy and Approved Software List

Revised August 2011

The following is the Approved Software List of the software that Emory & Henry College has approved for use on all College-owned computer technology equipment. Please note that the Information Technology Department reserves the right to remove any third party software installed by the user that is not listed on the Approved Software List. Third party software will be removed if it interferes with the smooth operation of any College-approved software or if violates the Acceptable Use of College Computer Technology Policy.

Approved Software List
Operating Systems

MS Windows 7, all versions
MS Windows Vista, all versions
MS Windows XP, all versions
Apple OS 10.x and above
Word Processing
MS Word for PC's or Macs
Database
MS Access for PC's or Macs
Presentations
MS PowerPoint for PC's or Macs
Spreadsheets
MS Excel for PC's or Macs
Email
MS Outlook
MS Web Outlook
MacMail
Internet Software
MS Internet Explorer
Safari for Macs
Adobe Acrobat and Acrobat Reader
Desktop Publishing
Recent Adobe desktop publishing applications
MS Publisher
*Others as specifically identified, please contact Help Desk for info
Class Specific Software (may change from semester to semester)

SPSS
Mathematica
Sniffy the Virtual Lab Rat
Minitab
ArcView
Adobe Applications

Availability of Software for College Use on Home Computers (Faculty & Staff)

Revised August 2010

The Information Technology Department maintains Microsoft site licensing for the use of faculty and staff. A two-install CD or DVD of Microsoft Office suite of applications can be purchased at a reduced rate for installation on faculty and staff personal computers on which the faculty or staff member conducts College business. Currently, the cost is \$20, but is subject to change per Microsoft. Please contact the Help Desk for information on the availability of these CD's/DVD's.

At the end of each fiscal year, the College must renew the software license with Microsoft. At that time, software installed on home computers may be required to be removed for the College to remain in compliance with its license agreement with Microsoft. Some teaching software may be loaded on the home computers of those faculty members teaching courses utilizing specific course-related software. At the conclusion of the semester during which the course was taught, the faculty member will be expected to remove the software application from his or her home computer. The Information Technology Department is not responsible for installing, maintaining or troubleshooting software borrowed or purchased from the College and installed on home computers.

Anti-Virus Software Policy

Revised August 2010

Maintaining an active and updated anti-virus program on every computer connected to the E & H network is a very important part of the foundation of security for the network. The Emory & Henry College network is set up to automatically verify the presence of updated anti-virus software on all faculty and student computers that connect to our network. In accordance with the *Security and Acceptable Use of College Computer Technology Policy for Emory & Henry College*, to which each user is subject in order to receive a user account, Information Technology must insist on implementing necessary system protection measures. The policy states, "All users of college information facilities are required to demonstrate respect for intellectual property, ownership of data, system security mechanisms..." Anyone who voluntarily connects to our campus network with their personal computer becomes a component of the campus computer network system. In order to

protect the system, we need to have what we consider adequate anti-virus protection in place.

Network Accounts for Students, Faculty & Staff

Revised August 2010

User Accounts

Every student, faculty and staff member will be issued a network account, an e-mail account, and a data storage account on the network. These accounts are required to access all computers and network resources available on the Emory & Henry College campus. These accounts are issued by the Information Technology Department and are subject to College rules and regulations as outlined in the *Security and Acceptable Use of the Network* policy. Please refer to this policy for specific information regarding these regulations.

Each account is assigned for the use of a single user. Sharing of accounts is prohibited. The user for whom the account was created is responsible for the security of that account and all actions associated with that account.

Student e-mail accounts are limited in size. When the account approaches maximum capacity, a warning is issued regarding the account, followed by the system prohibiting the sending of email. At critical capacity, the user cannot send or receive e-mail. It is important for the user to keep his or her mailbox within its space quota by removing unneeded e-mails, and by emptying the "Deleted Items" folder regularly. The Information Technology Department reserves the right to empty mailboxes that are full if they pose a resource problem for the mail server. E-mails from full mailboxes will be deleted and lost in the emptying process, and cannot be retrieved.

Visitor accounts are only available with permission of the Information Technology Department. A request may be made at the Help Desk. The visitor accepts full responsibility and liability for all activity related to the use of the account in accordance with the *Security and Acceptable Use of the Network* policy.

Account Status Changes

The status of an Emory & Henry College network account can be changed for many reasons:

- Currently enrolled students who transfer to another college or withdraw from the College will have their accounts disabled upon withdrawal deleted after 30 days.
- Staff members who resign or are dismissed from the institution will have their accounts deleted upon notification from the Human Resources Office.
- Faculty who resign or are dismissed from the institution will have their accounts disabled and deleted after 6 months or upon request.

Network Security and Password Control

It is important to select a password which is not easily guessed, but that is easy to remember. Do not share your password with anyone else.

If a student, staff or faculty member forgets his or her password, a password change can be requested in person at the Help Desk on the ground floor of the Kelly Library building, upon presentation of a photo ID. Password changes cannot be requested via email or by phone. The user must present his or her Emory & Henry College ID. There will be no exceptions to this rule.

Mandatory password changes occur automatically every 120 days from the date of the last password change. The system will prompt a user several times prior to the expiration of a password so that the user can complete his or her own password changes prior to its expiration. Passwords must contain at least 8 characters with THREE of the following FOUR parameters:

- Capital letters
- Lower case letters
- Numbers
- Special characters such as ! \$ or %

If a user is on campus, they can initiate a password change by pressing the Control + ALT + Delete keys and selecting the "Change Password" tab.

Students may have access to a data storage directory (H:\ drive) on the college network upon request from the help desk. All faculty and staff are issued a data storage directory upon employment at the College. Users are responsible for protecting their own files. The College does not guarantee that data stored on its network will be safe from system failures or operator errors. Furthermore, the College cannot guarantee the protection of any data and thus the user expressly waives any claim or cause of action in regard to the maintenance and protection of the user's data. Personal files stored on the hard drives of lab and classroom computers will be deleted. Users should store their data on removable technology in addition to their H:\ drive directory to ensure data integrity.

Computer Lab Policy

Revised August 2011

Emory & Henry College maintains several Computer Labs located throughout the campus. These shared facilities are available for open access computing and for classroom instruction. Unless reserved for classroom instruction these facilities are available on a first-come first-serve basis to students, faculty, and staff.

Miller Computer Lab
Miller Mass Comm Lab
McGlothlin-Street 231
McGlothlin-Street 233
Byars Lab
Kelly Lab
McGowan Lab

Hours for lab use vary due to the classroom teaching schedule for each classroom lab. One lab is designated the "overnight" lab and is available after hours. Currently this lab is MS 231. Please note that this lab is regularly patrolled and kept under video surveillance by the Campus Security Police.

Downtime & Network Patches & Update Policy

Revised August 2010

The Library and IT Services Department is committed to ensuring reliable Information Technology services. In order to meet this objective, the network needs to be taken offline from time to time to maintain or improve system performance, install important patches and upgrades, safeguard data, or to respond to emergency situations.

The Library and IT Services Department has scheduled downtime at 4:30 pm on Friday afternoons. In order to minimize the inconvenience to network users, this corresponds to the routine downtime of the Datatel system by ICE. Please be sure to be off the network by 4:30 pm every Friday. The IT staff will complete the necessary maintenance and bring the network back online as soon as possible.

Planned Downtime: Fridays at 4:30 pm

Network servers, routers, switches, and other network equipment all need regular maintenance and to have patches and upgrades installed and configured. It is also necessary to reboot network equipment to ensure data integrity and security. The goal of these tasks is to ensure maximum system performance and prevent future system failures. These tasks include:

- Application of patches to operating systems and other applications in order to fix vulnerabilities and bugs, add functionality, or improve performance.
- Monitoring and checking of system logs.
- Security monitoring and auditing.
- Disk defragmentation, disk cleanup, and other general disk maintenance operations.
- Required upgrades to system physical memory or storage capacity.
- Installation or upgrade of applications or services.
- System performance tuning.
- Regular backup of system data for the purpose of disaster recovery.

Exceptions to this downtime policy must be requested in advance and will be authorized only by the Chief Information Officer or the Network Administrator.

Emergency Downtime

The Library and IT Services Department works diligently to keep the Emory & Henry computer network fully functional at all times. Unexpected circumstances may arise, however, when systems or services will be interrupted without prior notice. Every effort will be made to avoid such circumstances, although incidences may arise involving a

compromise of system security, the potential for damage to equipment or data, or emergency repairs.

If possible, IT Services will notify everyone by e-mail when the network needs to be brought offline for unanticipated maintenance and support. Users will receive a telephone message stating that the network is offline if it is not possible to send email. Users will be notified via telephone that the network is back online as soon as the network is restored.

Policy on Software Patches

Software patches are regularly issued by all software and operating system manufacturers in order to fix bugs, to enhance data and system security, and to add additional functionality. The Library and IT Services Department does not automatically apply software and operating system patches immediately. Depending on the type and size of the patch, the IT staff may install the patch on test servers or other equipment in order to ensure that it does not harm the system and to confirm that it works as intended with other software in use on our network equipment. The IT staff may also wait until testing by other software and hardware manufacturers has been completed and that the patch has been determined to be fully inter-operational with all integrated network assets. The IT staff reserve the right to take up to 60 days to install patches and upgrades in order to ensure that these software changes are not harmful to the systems on the Emory & Henry computer network.

The Library and Information Services staff members reserve the right to take up to 60 days to install a patch or upgrade to any and all network assets and systems in order to test the safety and interoperability of the patch.

Revisions

The Library and IT Services Department reserves the right to revise, amend, or modify this Downtime and Patch Policy as necessary.

Website Policy and Standards

Revised August 2011

For current website policies and standards, please contact Jed Arnold, Web Manager, in the Office of Public Relations. Telephone 276-944-6155 or email jarnold@ehc.edu.