Hamilton College
Administrative Information Systems
Security Policy and Procedures

Approved by the IT Committee
(December 2004)

Table of Contents

We acknowledge the help of Amherst College whose Project Possibility document was the starting point for our work.

Summary

- Administrative Information is categorized into three levels: Confidential, Sensitive, and Public. (Page 5)
- Employee Information (other than directory information as published in the *Hamilton College Telephone Directory*) is confidential and must be protected. The Family Educational Rights and Privacy Act (FERPA) and the Gramm-Leach-Bliley Act (GLBA) specify obligations that Hamilton College must fulfill with respect to information security. (Page 6)
- All requests for administrative system account activity (adds, changes, or deletions) must be submitted using the new web form available on the ITS website. (Page 7)
- Every employee (including student employees) must access the system using their assigned account and password. Passwords must NEVER be shared for any reason! (Page 8)
- Administrative information is available in WebAdvisor, the My Hamilton portal, and in other web-based applications and is subject to the same privacy restrictions. (Page 9)
- Department Security Managers are responsible for authorizing and monitoring access to the administrative system in their respective areas. They must work with ITS to promote this policy and assist users in their area with understanding the appropriate use of information resources. (Page 9)
- All Hamilton College owned computers must be equipped with up-to-date Anti-Virus software and must be current on Critical Security Patches. (Page 9)
- Users must log out when leaving their computers unattended. (Page 10)
- Equipment, especially laptops and portable devices must be secured from theft. Data should be stored on a network drive rather than on the physical drive in the computer. (Page 10)
- Printed reports containing administrative data must be secured and appropriately disposed of when they are no longer needed. (Page 10)
- Security of administrative information is a partnership between ITS, the Designated Security Managers and all users of the information resources. (Page 10)

Overview

Electronic information at Hamilton College is stored on central servers and on individual desktop computers. This networked environment also poses significant risk to the security of information. Protecting this College resource is a shared responsibility between Information Technology Services (ITS) and the individual users of that information. This policy covers information maintained by administrative offices of the college related to the business of the college and accessed by members of the college community.

Network security, including firewall technology, has been implemented to protect servers and departmental workstations from unauthorized access through the Internet. Staff in administrative offices connect to secured computers through a firewall. The IP address of each administrative computer is registered in the firewall, permitting the user of that computer to access the Datatel system. The person still needs a valid username and password to access information on the system. Off-campus access to these servers is currently in the testing stages and will be provided through a secure Virtual Private Network (VPN) complete with encryption and an additional layer of password security.

Desktop computers in administrative offices provide the most vulnerable point of access to administrative information. Staff in administrative offices must physically protect their computers, including laptops, from unauthorized access and theft. All administrative information including word processing documents, spreadsheets, databases, schedules, etc. must be backed up on a regular basis to protect information from inadvertent deletion or computer failure.

In addition to network security, a fundamental layer of protection is the logical security plan. This plan is the key to protecting administrative information and describes the procedures by which system privileges are granted, passwords maintained, security monitored and issues communicated.

Access to information will be authorized by the department head or designated *Department Security Manager* and centrally assigned by System Administrators in ITS. Inquiry Access to administrative information will be authorized on a 'need to know' basis. Maintenance Access to processes will be authorized based on job responsibilities.

Employees, including students, granted access to institutional data may do so only to conduct College business. In this regard, employees must:

- Respect the confidentiality and privacy of individuals whose records they access
- Observe ethical restrictions that apply to the data to which they have access
- Abide by applicable laws or policies with respect to access, use, or disclosure of information

Employees, including students, may <u>not</u>:

- Disclose data to others, except as required by their job responsibilities
- Use data for their own personal gain, nor for the gain or profit of others
- Access data to satisfy their personal curiosity

Employees and students who violate this policy are subject to the investigative and disciplinary procedures of the College.

Definition of Administrative Information

Administrative information is any data related to the business of the College including, but not limited to, financial, personnel, student, alumni, communication, and physical resources. It includes data maintained at the departmental and office level as well as centrally, regardless of the media on which they reside. *Administrative information* does not include library holdings or instructional notes unless they contain information that relates to a business function.

The College recognizes *administrative information* as a College resource requiring proper management in order to permit effective planning and decision-making and to conduct business in a timely and effective manner. Employees are charged with safeguarding the integrity, accuracy, and confidentiality of this information as part of the condition of employment.

Access to administrative systems is granted based on the employee's need to use specific data, as defined by job duties, and subject to appropriate approval. As such, this access cannot be shared, transferred or delegated. Failure to protect these resources may result in disciplinary measures being taken against the employee, up to and including termination.

Requests for release of administrative information must be referred to the office responsible for maintaining those data. The College retains ownership of all administrative information created or modified by its employees as part of their job functions. Administrative information is categorized into three levels:

Confidential information requires a high level of protection due to the risk and magnitude of loss or harm that could result from disclosure, alteration or destruction of the data. This includes information whose improper use or disclosure could adversely affect the ability of the College to accomplish its mission as well as records about individuals requiring protection under the *Family Educational Rights and Privacy Act of 1974* (FERPA), *and Gramm-Leach-Bliley Act (GLBA).*

Confidential information includes, for example, salary information, social security numbers, alumni gifts and student academic records.

Sensitive information requires some level of protection because its unauthorized disclosure, alteration, or destruction might cause damage to the College. It is assumed that all administrative output from the administrative database is classified as sensitive unless otherwise indicated.

Sensitive information includes, for example, class lists, facilities data and vendor data information.

Public Information can be made generally available both within and beyond the College. It should be understood that any information that is widely disseminated within the campus community is potentially available to the public at large.

Public information includes, for example, directory information.

Employee Information

All aspects of personnel records are confidential. "Directory information for faculty and staff as published in the *Hamilton College Telephone Directory* is public (this includes the printed and Web directories). Directory information **will** include the following: **Printed directory:** name, home address, home telephone, department, position title, campus address, campus phone and email address. Employees may request that **home address and home telephone** remain confidential and not appear in the printed directory. **Web (on-line) directory:** name, photo, department, position title, campus address, campus phone and email address. Employees may request that **their photo** not appear in the Web directory."
All other employee related data, especially that which is available to users outside Human Resources such as social security number and birth date, must be vigilantly safeguarded and treated as confidential.

Family Educational Rights and Privacy Act (FERPA)

The *Family Educational Rights and Privacy Act* (FERPA) of 1974 governs all information about students, current and former, maintained by Hamilton College. FERPA generally requires that Hamilton College have the student's written permission to release any information from their records except certain types of "directory information."

Student "Directory Information", as defined by FERPA

Certain information, classified as "directory information", is available for public consumption unless the student specifically directs that it be withheld. The student should direct the Registrar's Office not to disclose such information prior to the fourteenth calendar day of each semester. Former students should contact the Communications and Development Office.

Public directory information as defined by the law and the College includes: student's name, home and campus address, e-mail address, telephone listing, parents' name and address(es), date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, photograph and the most recent previous educational agency or institution attended.

Gramm-Leach-Bliley Act (GLBA)

This law mandates extensive new privacy protection for financial information colleges maintain about individuals. The college must "develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards" appropriate to the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of any customer information at issue. (NACUBO Advisory Report, January 13, 2003)

One of the required elements of this security program (as detailed in the NACUBO Advisory Report) is the designation of an employee to coordinate the information security program. Any questions or issues with this policy should be addressed to the program coordinator:

Martin Sweeney
Director, Central Information Services
367 Burke Library
Hamilton College
Clinton, NY 13323
(315) 859-4164
msweeney@hamilton.edu

Security Administration

Department Security Managers (department heads or their designee) are responsible for authorizing system access by employees. System Administrators in ITS will assign that access.

The *Administrative Account Request Form* must be completed by the Department Security Manager to authorize, modify or remove user privileges. Security is established in discrete "levels" within a department. For example, the Admission Office may have pre-established security classes called ADM.STUDENT.EMPLOYEE, ADM.DATAENTRY, ADM.ADMISSION.OFFICER, and ADM.MANAGER. It is acceptable and desirable to place employees into the security profile that is appropriate for the job functions they will perform. Note that requesting the same access as [person x] (where person x is another employee with the same job functions within the department) is allowable. If you do not specify a particular "level" of security or "same as person x", you must provide a detailed list of the menus and mnemonics that the employee should be granted access to. Security is explicitly granted by individual menus, screens and processes within the Datatel system.

The *Administrative Account Request Form* is a web form and is available on the *ITS web site at* http://my.hamilton.edu/college/its/colleague_benefactor/account_requests/default.html After the form has been submitted, it is automatically forwarded to the System Administrator for action. Requests for account actions are usually completed within one business day. If you have any reason to follow up with additional information after submitting the form, you may send an email message to cis@hamilton.edu or call 5CIS (5247).

Procedure for creation of NEW accounts:

1. Department Security Manager explains the Security Policy to the new employee and provides a written copy of the Security Policy.
2. The employee signs the Security Policy Acknowledgement/Employee Confidentiality Agreement form. This form is sent via campus mail to the CIS team.
3. Department Security Manager fills out the *Administrative Account Request Form* on the ITS website containing specific details about the Administrative processes the user should have access to.
4. System Administrator creates the login and assigns the appropriate security classes.
5. System Administrator sends the login and password in a sealed envelope, or delivers, to the new employee.
6. System Administrator files the signed Security Policy Acknowledgement/Employee Confidentiality Agreement form and the *Administrative Account Request Form (copy of email).*
7. Department Security Manager provides training and documentation to employee.
8. Employee must change password upon first login.

Procedure for Modification or Termination of existing accounts:

1. Department Security Manager fills out the *Administrative Account Request Form* on the ITS website with instructions (modify or terminate).
2. System Administrator makes the appropriate changes.
3. System Administrator files the *Administrative Account Request Form (copy of email).*
4. System Administrator replies to Department Security Manager indicating that security has been modified or removed.

On a periodic basis, ITS System Administrators will review reports identifying failed login attempts, "super user" logins and origins of login.

Annually, Department Security Managers will be required to review a complete list of all system privileges assigned in their area. The cover page of this report must be signed by the Department Security Manager and returned to the CIS team within two weeks.

Passwords

The most effective way to protect administrative information is through the vigilant use of user-defined passwords.

Passwords must conform to the following standards:

- Password must have at least 6 characters. Only the first eight characters are significant
- Password must contain at least 2 alphabetic and at least one numeric or special character
- Password must differ from the login name and any reverse or circular shift of that login name
- New passwords must differ from the old one by at least 3 characters
- Passwords must be changed by the user every 120 days

It is your responsibility to protect your password from disclosure. Every individual, including student employees, must have a unique user login. Passwords must not be shared with any other person. If you suspect that your password has been compromised, please change it immediately and contact the CIS team at 5CIS (5247) or send an email message to cis@hamilton.edu to report the security breach.

After five consecutive failed login attempts, the system will stop issuing a login prompt and will close your connection to the Administrative system. If you require your password to be reset, please contact the CIS team at 5CIS (5247) or send an email message to cis@hamilton.edu.

Student Employees

It is critical that anyone accessing the Administrative System have their own login and password. ITS System Administrators will create a separate account for each student employee that requires access to the Administrative system to perform their job function. The accounts created for student employees will be of the format [department_code + ws1, ws2, ws3] or [department_code + int1, int2, int3]. For example, if the Admission office employs three student employees who require access to the Datatel system, ITS will create the following three accounts: admws1, admws2 and admws3.

As student employees terminate their employment with an administrative office, the password for the account must be reset to insure that future access is denied. All accounts for student employees will be reset by ITS at the conclusion of every academic year. It is the responsibility of the department head or Department Security Manager to inform ITS whenever a student employee terminates employment with the administrative office.

The administrative office that employs the student is responsible for tracking which student is using which account. Recall that there can be no sharing of accounts - every employee must have a unique account. Upon demand from ITS, the department head or Department Security Manager must be able to match a student employee name to an account for a particular date or range of dates.

The department head or Department Security Manager is responsible for monitoring all student employee access to the system and insuring appropriate and accurate work is being performed. The department may choose how to best monitor student employee access to the administrative system either via distributing the account information to the student employee or by logging into the system for the student employee using the student's designated account.

Web Access to Information

Access to institutional data is also available through Datatel's Web Advisor applications and through the MyHamilton portal. Usernames and passwords may be made available for applicants, students, faculty, employees and alumni volunteers. It should be noted that the web presentation method in no way diminishes the importance of protecting the institutional data. Web browsers allow you to save passwords used to access external sites. You should be wary of using this feature. If you choose to save a password, be aware that anyone using your PC will be able to gain entry to that site using your password.

Department Security Manager Responsibilities

The department head of each administrative office must assign a Department Security Manager and an alternate who is responsible to authorize and monitor access to the administrative information.

An *Administrative Account Request Form* must be completed for each individual who is provided access to the administrative system. This same form must be completed to modify or remove access. It is just as important to remove access to the administrative system, as it is to authorize access to the administrative system. The Department Security Manager should document the completed *Administrative Account Request Form.*

Annually, the Department Security Manager will be required to review all security authorizations for the department. A report will be produced and distributed by the System Administrators. The cover page must be signed and returned within two weeks to the CIS team indicating the security is accurate. ITS System Administrators reserve the right to deactivate the Department Security Manager's access to the administrative system, if the review of security authorizations is not completed in a timely manner.

Anti-Virus Software

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.

In addition, all attachments to e-mail sent to the Hamilton mail server are scanned for viruses. If an attachment is found to be infected it is deleted and a text file is attached to the e-mail message (called substitute.txt) informing the receiver that the attachment was infected with a virus. The receiver can then contact the sender to have the message retransmitted after the attachment has been cleaned of the virus.

For more information on Anti-Virus software please visit the ITS policies web page.

Critical Security Patches (Windows computers only)

The Windows Software Update Service is an automated process to enable users of computers running the Windows XP and 2000 operating systems to apply critical updates from Microsoft on their machines.

For more information on the Windows Software Update Service please visit the ITS policies web page.

Unattended Computers

You must logout from the client software (User Interface) when leaving your PC unattended. This software only requires one password verification. Once logged in, access is provided to all applications you are authorized to use.

An industry "Best Practice" is to shutdown or logoff your PC prior to leaving it unattended. If you do not shutdown, be aware that your email, printers and network drives are readily available to anyone who may walk up to your PC. If your office resides in a building within the firewall, there is an increased risk of gaining unauthorized access to the administrative information system.

You may run multiple copies of the client software (*User Interface*) from your PC (i.e., more than one login session.) Please be aware that there is a limit to the number of concurrent login sessions available at any given time (100). Once that limit has been reached, other users across campus will be blocked from login. As a courtesy to others, please logout sessions that are not active. During certain peak processing times such as during Web Registration, ITS may request that you limit your connection to one (1) session.

Equipment Security

All computer equipment in your office should be reasonably secured from theft. Laptops and other portable devices are obviously the most vulnerable. By storing data on the network drive rather than physical drive C: on your PC, you not only provide additional security for your information if your laptop should be stolen, but you can then access your information from off-campus through the Virtual Private Network. Caution should be used when storing administrative information on portable computers.

Specific buildings on campus are inside the firewall that protects administrative servers. Be wary of providing access to Ethernet taps to those outside your office (i.e., students, vendors, friends, alumni, etc.)

Modems installed on on-campus PC's provide a significant security threat. Only individuals who require a modem as part of their job responsibilities should have them. The "auto-answer" feature must always be turned off.

Printed reports

Reports containing confidential and sensitive data, either test data or live production data, must be secured within the office. Reports should not be left on the printer or desktop in open view. Any report that is no longer needed which contains confidential and/or sensitive data must be shredded or stored securely until it can be shredded.

Communication

The security of administrative information is a shared responsibility among the Hamilton College staff that use and support technology - all have a role to play. Vigilance is a daily activity. Effective, on-going communication of this security policy and office procedures will play an essential part in our success.

Department Security Managers are responsible for discussing this policy with each user at the time system privileges are issued.

Hamilton College
Administrative Information Systems
Security Policy

Acknowledgement Form

Please sign below and return to your Department Security Manager

"I have read the Administrative Information Systems Security Policy and agree to abide by it."

_____	_____
Employee Signature	Date
_____	_____
Printed Name	Department Name

Hamilton College

Employee Confidentiality Agreement

As an employee of Hamilton College, I may have access to confidential or sensitive information about students, staff, faculty, alumnae, donors, volunteers and customers. Confidential information is protected by college policy and by law.

I acknowledge that I fully understand that the intentional disclosure by me of this information to any unauthorized person could subject me to criminal and civil penalties as imposed by law. I further acknowledge that such willful or unauthorized disclosure also violates Hamilton College's policy and could constitute just cause for disciplinary action including termination of my employment regardless of whether criminal or civil penalties are imposed.

I will safeguard and will not disclose my username and password. Any access to Hamilton College electronic systems made using my username and password are my responsibility. If I believe someone else has used my login, I will immediately report the breach to the CIS team in ITS and will immediately reset my password.

My obligations under this agreement to protect confidential information continue after termination of my employment.

_____	_____
Employee Signature	Date