

Information Security Policies  
Macalester college  
St. Paul, MN

**Table of Contents**

1000	Information Security Policies Introduction.....	4
1100	Overview.....	4
1200	Compliance.....	5
1300	Responsibilities.....	5
2000	Security of ITS Resources.....	6
2010	Physical Security.....	6
2020	Controlled Access to the Data Room.....	6
2030	Records of Authorized Entries to the Data Room.....	6
2040	Visitors to the Data Room.....	7
2050	Data Backup.....	7
2060	Laptop Security.....	7
2070	Disposal of Data.....	7
2071	Media Disposal.....	7
2072	Document Disposal.....	8
2080	Firewall Security.....	8
2090	Personal Information Security.....	8
3000	Authentication and Network Security of ITS Resources.....	9
3010	Authentication.....	10
3020	Account Access Administration.....	10

Last Updated – Thursday, May 29, 2008

Information Security Policies  
Macalester college  
St. Paul, MN

3021	Procedure to create usernames and passwords for new accounts .....	10
3022	Procedure to enable new network and email accounts .....	11
3030	Disabling network and email accounts.....	12
3031	Procedure to close student email accounts .....	12
3032	Procedure to close access to student email accounts for a Leave of Absence .....	13
3033	Procedure to re-activate student email accounts .....	13
3034	Email Access for Graduating Seniors .....	13
3035	Procedure to close employee email, network, Banner and other accounts .....	13
3036	Allowing access to accounts after the termination date .....	14
3037	Allowing access to accounts between active assignments and appointments .....	14
3038	Allowing access to accounts for retirees and emeriti faculty.....	14
3040	Procedure to open Banner accounts.....	14
3050	Passwords .....	15
3060	Receipt and acknowledgement of policies by user .....	15
3070	Network Security .....	15
3071	Login Controls.....	16
3072	Login Reporting .....	16
3080	Appropriate Security Measures .....	16
3081	Logging off of Users .....	17
3082	Disabling File and Print Sharing.....	17
3090	Reviewing Access Groups .....	17
4000	Responsible use of Electronic Communications .....	17

Last Updated – Thursday, May 29, 2008

Information Security Policies  
Macalester college  
St. Paul, MN

4010	Policy Violations .....	19
4020	Reporting Violations .....	20
4030	Responsible Use of Email.....	20
4040	Email Procedures .....	20
5000	Mass Electronic Emailing .....	20
5010	Two Forms of Mass Electronic Mail.....	21
5020	Emergency Email.....	21
5030	Non-emergency Email to a Specific Constituency .....	22
5040	Non-emergency Email for Campus-wide Distribution.....	22
6000	Privacy of Information Technology Data .....	23
7000	Reporting Electronic Security Incidents.....	23
8000	Outsourcing.....	24
9000	Emergency Response Plan & Disaster Recovery .....	24
9010	Emergency Response Plan.....	24
9020	Disaster Recovery.....	24
9030	Incident Tracking.....	24

Information Security Policies  
Macalester college  
St. Paul, MN

## **1000 Information Security Policies Introduction**

Each college department is responsible to comply with this document which includes all members of the faculty, staff and student body.

### **1100 Overview**

Macalester college is committed to the principle that information should be shared, subject to privacy and confidentiality requirements, and consequently to an open flow of information within the college and between the college and the public. Macalester recognizes that it is very dependent on digital technologies for communicating, sharing and analyzing information.

Consistent with this principle, Macalester seeks to provide appropriate access to Information Technology Services (ITS) facilities and services for its faculty, staff and students. Access to those facilities and services that are owned, operated, managed by or the responsibility of Macalester imposes certain responsibilities and obligations and is subject to applicable college policies and local, state and federal laws.

This policy provides the primary framework for the management, administration, integrity and effective use of the college's ITS facilities and services. Based on the following premises:

- The ITS facilities and services of Macalester college are intended for use for teaching, learning, research, college-based consultancy and administration in support of the mission of the college.
- Access to the ITS facilities and services of Macalester college is granted as a privilege to college faculty, staff, and students; and the college reserves the right to limit, restrict or extend access to these facilities and services.
- All individuals using the ITS facilities and services must act appropriately and responsibly; and observe the Information Security Policies and statutory requirements applying to these facilities and services.

Last Updated – Thursday, May 29, 2008

Information Security Policies  
Macalester college  
St. Paul, MN

- The ITS facilities and services of Macalester college are not to be used for commercial purposes or non-college-related activities without written authorization from the college.

## **1200 Compliance**

Macalester College may suspend an individual from using ITS facilities and services if after appropriate investigation that individual is found to:

- be responsible for willful physical damage to any of the ITS facilities
- be in possession of confidential information obtained improperly
- be responsible for willful destruction of information
- be responsible for deliberate interruption of normal services provided by ITS
- be responsible for the infringement of any patent or the breach of any copyright
- have gained unauthorized access to accounts and/or passwords
- have shared accounts and/or passwords without authorization
- have gained access to restricted areas without authorization
- be responsible for inappropriate use of the facilities and services, including the Internet
- be knowingly aware of and/or have observed inappropriate behavior and failed to report the incident

## **1300 Responsibilities**

The Macalester college ITS department has the authority to develop and administer information security, data protection and privacy policies and practices for all of Macalester college and outside service providers; and to outline requirements for each college department or outside service provider to ensure those requirements around information security are appropriately followed.

Information Security Policies  
Macalester college  
St. Paul, MN

Each college department head must ensure that their business practices adhere to Macalester's Information Security Policies. Further, they are responsible for ensuring that all applicable individuals under their umbrella of authority have been informed of these policies and practices.

The responsibility for adhering to this policy rests with each college department. College departments are responsible for demonstrating that they have processes in place to manage information security practices in their organization in accordance with this policy and federal, state and provincial laws and regulations.

## **2000 Security of ITS Resources**

### **2010 Physical Security**

Physical access to IT resources is restricted to appropriate individuals. The locations of those IT resources include but are not limited to the Data Room on the third floor of the Humanities Building located on the campus of Macalester College, wiring closets on-campus, and other rooms on-campus which house IT resources that contain sensitive information of Macalester College.

### **2020 Controlled Access to the Data Room**

Access controls are maintained through an automated identification process that includes procedures to add and remove individuals from the list that controls access to the Data Room. These procedures are auditable.

### **2030 Records of Authorized Entries to the Data Room**

Records of who is authorized to access the Data Room; and logs that identify everyone who enters and exits this controlled area will be

Last Updated – Thursday, May 29, 2008

Information Security Policies  
Macalester college  
St. Paul, MN

maintained for a period of 1 year. Entries and exits to the Data Room are to be reviewed on a monthly basis.

**2040 Visitors to the Data Room**

Visitors to the Data Room must be accompanied at all times by an authorized employee. A visitor is any party, whether employed by Macalester College or not, who has not been given explicit authorization for Data Room access.

**2050 Data Backup**

The ITS department's main file servers located in the Data Room of the Humanities Building and any other college departments that have data files containing confidential and sensitive information must periodically backup those files. Those departments must conduct an annual review that includes a successful, complete restoration of a data backup. The results of the annual review will be documented and retained. The backup media must be protected from unauthorized access and stored in a location separate from the originating source. Centrally managed back-up services are available.

**2060 Laptop Security**

Portable computing devices (laptops) shall not be left unattended. Encrypting laptop data may mitigate a security breach if a laptop containing sensitive, personal information is stolen.

**2070 Disposal of Data**

**2071 Media Disposal**

Information Security Policies  
Macalester college  
St. Paul, MN

All data must be removed from electronic media prior to being disposed, released or transferred to another party. Data removal must be consistent with physical destruction of the electronic media, for example, degaussing of the electronic media or overwriting of the data at least three times. A "quick" format or file erasure is insufficient.

Electronic media is defined as any electronic storage device used to record information, including, but not limited to hard disks, magnetic tapes, compact disks, videotapes, audiotapes, and removable storage devices such as floppy disks and zip disks.

### **2072 Document Disposal**

All individuals who handle paper-based documents that contain confidential or sensitive information should use proper disposal methods when disposing of those documents such as shredding (cross-cut shredding is best), disintegration, incineration, pulverization, or a vendor contracted to properly dispose of confidential and sensitive paper documents.

### **2080 Firewall Security**

Macalester College deploys and maintains a network firewall between the Internet and all on-campus computers. Networked computers run a host-based firewall. Each firewall is restrictively configured to deny all traffic unless expressly permitted.

### **2090 Personal Information Security**

College departments must identify departmental computing systems and applications that house personal information such as:

- Personal name along with social security number
- Driver identification number
- Financial account number
- Lists of computer systems IDs and/or passwords
- Information protected by HIPPA and/or FERPA

Personal information must be removed from all computing devices for which it is not required.

Last Updated – Thursday, May 29, 2008

Information Security Policies  
Macalester college  
St. Paul, MN

If personal information cannot be removed from the computing device, the college department must develop a plan specifically outlining how the information and systems will be kept secure. Each college department must take proper care to isolate and protect files containing personal information from inadvertent or unauthorized access or viewing when personal information is stored on devices not configured to operate as serving devices. Measures to protect the information could include removing several digits from the personal identifiers, moving the files to removable media and storing this media in a secure location apart from the computer, or encrypting the personal information.

Any alternative location for serving devices must be reviewed and approved by the Associate Vice President of ITS. An exception will be granted only if the server storing personal information is deemed secure.

Campus units that develop web-based or network-based applications that host personal information must use secure application coding practices as described within OWASP Top Ten Critical Web Application Security Vulnerabilities.

## **3000 Authentication and Network Security of ITS Resources**

Macalester College provides its community with access to information technology (IT) resources such as email, Internet and network devices. To protect these resources from unauthorized use, Macalester requires IT users to obtain college owned and managed electronic identifiers to gain access to these resources and to follow specific rules for obtaining, changing, and terminating these identifiers. In addition, to avoid unauthorized access to IT resources, holders of Macalester electronic identifiers must follow specific rules for creating and using complex passwords that correspond to a Macalester electronic

Last Updated – Thursday, May 29, 2008

Information Security Policies  
Macalester college  
St. Paul, MN

identifier, as well as observe a requirement for reporting of suspected compromises of those passwords.

### **3010 Authentication**

#### **3020 Account Access Administration**

At Macalester College, the Human Resources department and Registrar's office, in conjunction with the ITS department, shall have a suitable process in place to authenticate users. Alumni records are managed by the Advancement office.

#### **3021 Procedure to create usernames and passwords for new accounts**

The Human Resources department creates an active record for each new Macalester staff person, faculty member, and temporary/contract employee by entering his or her personal information into Banner. An automated process within Banner applies an algorithm to each individual's personal information to create a new, unique user name and password.

The algorithm uses the first character of the first name plus the first seven characters of the last name. If there is a duplicate then numeric characters are added to the end of the user name to maintain its uniqueness.

For example, using the name, John Johnson, the algorithm would generate a unique 8-digit alphanumeric user name:

- Jjohnson
- Jjohnso1... jjohnso9
- Jjohns10... jjohns99
- Jjohn100... jjohn199
- Jjoh1000... jjoh1999
- Jjo10000... jjo19999

Information Security Policies  
Macalester college  
St. Paul, MN

Human Resources also emails the new user's information to the User Account mail box:

- User name
- Hiring manager or supervisor
- Start date
- If the employee is overlapping another
- If the employee is a change of status

For students, the user name creation process is slightly different. A list of incoming students (first year students and transfer students) is generated from Banner and validated by the Admissions office and the Financial Aid office. ITS uses this list of students in conjunction with Sungard delivered APIs to create active student records for each deposited student. The same automated process (described above) within Banner creates a new, unique user name and password.

### **3022 Procedure to enable new network and email accounts**

To enable new network and email accounts, an Identity Manager (IDM) software application creates new user accounts and then propagates the new, unique 8-digit alphanumeric user name and randomly-generated, 12-digit numeric password from Banner to the following two systems:

- Novell – Campus Computer Network System
- Macalester Email Account

The following applications authenticate to Novell using the new user name from Banner:

- Google Apps (E-mail / Calendar, other apps) Login
- 1600 Grand – Portal for payroll, employee records, grades, etc.
- Moodle – Learning management tool, class schedules, assignments, etc.
- EZProxy – Gateway to third-party research databases
- Novell – file storage space, both private and shared

Last Updated – Thursday, May 29, 2008

Information Security Policies  
Macalester college  
St. Paul, MN

- Novell – Networked software applications

The network administrator checks the User Account mailbox to verify that IDM has created a new user account. The network administrator then creates a New User Memo (Welcome Letter) containing the individual's user name and initial password to activate his or her new account. The New User Memo is emailed as an attachment to the individual's manager and associated groups:

- Desktop Services
- Telecom
- Administrative Computing
- Training
- Human Resources, Acquisition & Development

### **3030 Disabling network and email accounts**

If an individual's account is disabled or closed, each user name is permanently archived at Macalester College. If an individual's account is ever re-opened, the original user name created in Banner will be reassigned to that account.

### **3031 Procedure to close student email accounts**

Students' email accounts are closed when they do not:

- Register for the next semester (and have not graduated)
- Validate (they have financial, academic or medical holds on their file)
- Complete the appropriate Leave of Absence paperwork

Once an account is closed, a student has up to two weeks to transfer the contents of his or her Macalester.edu e-mail to an alternate email address when provided to the ITS department.

Last Updated – Thursday, May 29, 2008

Information Security Policies  
Macalester college  
St. Paul, MN

**3032 Procedure to close access to student email accounts for a Leave of Absence**

Students taking a Leave of Absence are not allowed access to their email accounts after the Registrar's office notifies the ITS department. Exceptions may be allowed by the Dean of Students, and are noted on the Leave of Absence form.

Students taking a Leave of Absence in the middle of a semester have their email accounts closed two weeks after the processing date. But students who take a Leave of Absence for a full semester shall have their accounts respectively closed for the:

- Spring semester on January 15<sup>th</sup>
- Fall semester on June 15<sup>th</sup>

**3033 Procedure to re-activate student email accounts**

If an email account is closed and a student returns to Macalester, the account can be re-activated. After the student registers for the new semester, the Registrar's office notifies the ITS department to grant the student full access first to 1600grand, and then to email.

**3034 Email Access for Graduating Seniors**

Graduating seniors continue to have access to 1600grand and email until the first day of the following semester. Non-graduating seniors who require access to email to complete their degree may receive an extension with the approval of the Registrar.

**3035 Procedure to close employee email, network, Banner and other accounts**

Human Resources shall notify ITS to close email, network, Banner and other accounts of the terminated employee effective his or her last day

Last Updated – Thursday, May 29, 2008

Information Security Policies  
Macalester college  
St. Paul, MN

of work at Macalester College. Termination is meant as a neutral term in the context of this document. The term employee includes staff person, faculty member, and temporary/contract employee. Please see Section 3.17.3, Termination of Information Technology Resources, in the Human Resources Policies.

**3036 Allowing access to accounts after the termination date**

In the event HR allows an ex-employee to have access to accounts after his or her termination date, HR shall notify ITS there is an extension of services, which is not to exceed one month. Please see Section 3.17.3.1, Extension of Services beyond the Termination Date, in the Human Resources Policies.

**3037 Allowing access to accounts between active assignments and appointments**

If an employee is expected to return to an active assignment or appointment after a short absence, an employee may be granted continued access to his or her accounts at the request of the department head. This situation typically applies to an employee whose job is tied to the academic nine month term. If an employee does not return, Human Resources shall notify ITS to close those accounts. Please see Section 3.17.3.2, Extension of Services between Active Assignments/Appointments, in the Human Resources Policies.

**3038 Allowing access to accounts for retirees and emeriti faculty**

Macalester College allows indefinite, continued access to accounts for retired employees who leave in good standing or faculty who are extended emeriti status. Please see Section 3.17.3.3, Extension of Services for Retirees or Emeriti Faculty, in the Human Resources Policies.

Last Updated – Thursday, May 29, 2008

Information Security Policies  
Macalester college  
St. Paul, MN

**3040 Procedure to open Banner accounts**

Banner accounts are manually opened by the ITS Data Base Administrator (DBA) only for those users who have a valid business purpose and an active network account.

The new user must present to the ITS DBA the Banner Account Request Form (<http://macalester.edu/its/>) completed and signed by the data owner of that specific business entity or user group authorizing the new account opening in Banner.

**3050 Passwords**

- No campus computer network user account shall exist without a password or other secure authentication system.
- Passwords cannot contain the username or the surname of the individual.
- A password must have a minimum of six (6) but no more than fifteen (15) alphanumeric characters.
- Each password must contain at least one (1) numeric character.
- Passwords may contain special characters.

**3060 Receipt and acknowledgement of policies by user**

When new users are added to the system, they will receive and acknowledge the receipt of policies which relate to the use of equipment and accompanying software.

Information Security Policies  
Macalester college  
St. Paul, MN

## **3070 Network Security**

### **3071 Login Controls**

Login services shall provide for positive authentication to ensure that a legitimate user is allowed access to the system or network environment.

### **3072 Login Reporting**

Every login attempt must be logged in a system log.

### **3080 Appropriate Security Measures**

Macalester College expects all individuals using information technology devices connected to the Macalester college campus network to take appropriate measures to manage the security of those devices.

Each computing device connecting to the campus network must have up-to-date anti-virus and anti-spyware software installed.

When a computer first, and at other intervals necessary, connects to the network, it goes through an automated scan and online registration process to ensure certain system requirements are met. These system requirements include but are not limited to: current anti-virus software; an active firewall; specific patches applied; specific versions of operating systems installed. If a computer fails to meet the minimum criteria, that computer is not allowed to access the campus network until the requirements are met. Macalester College will provide the critical security updates or required security software to those computers failing the test.

Information Security Policies  
Macalester college  
St. Paul, MN

Computing devices connecting to the network must keep their operating system and application software up-to-date; keeping current with updates and patches provide an added layer of security.

### **3081 Logging off of Users**

Users shall log off and secure workstations when not in use. Administrators shall create procedures to ensure that unused workstations are secured by logoff or other means when they remain idle for a period of time determined reasonable by a review of the procedures.

**Example:** Where possible, computing devices must be configured to "lock" when left unattended for more than 10 minutes, and require a user to re-authenticate before resuming use.

At the end of the workday, each user must log off of his or her computer. If a job must be run unattended after work hours, precautions must be taken to protect the system from unauthorized access.

### **3082 Disabling File and Print Sharing**

Be sure to disable file and print sharing on office computers, other than the ones that are your actual file and print servers. File sharing allows access to drives/directories/files on your local hard drive. Therefore file sharing should be disabled, restricted or secured.

### **3090 Reviewing Access Groups**

Access groups and roles of access groups must reviewed twice a year. These procedures are auditable.

Information Security Policies  
Macalester college  
St. Paul, MN

## **4000 Responsible use of Electronic Communications**

Macalester College expects all members of its community to use electronic communications in a responsible manner. The college may restrict the use of its computers and network systems for electronic communications, in response to complaints presenting evidence of violations of other college policies or codes, or state or federal laws. Specifically, the college reserves the right to limit access to its networks through college-owned or other computers, and to remove or limit access to material posted on college-owned computers.

The college seeks to enforce its policies regarding harassment and the safety of individuals; to protect the college against seriously damaging or legal consequences; to prevent the posting of proprietary software or the posting of electronic copies of literary works in disregard of copyright restrictions or contractual obligations; to safeguard the integrity of computers, networks, and data, either at Macalester or elsewhere; and to ensure that use of electronic communications complies with the provisions of the campus code of conduct for maintaining public order or the educational environment.

The college recognizes the complexity of deciding what constitutes appropriate use of electronic communications services. What is appropriate or inoffensive to some members of the community may be inappropriate or offensive to others.

The college cherishes the diversity of values and perspectives endemic in an academic institution and so is respectful of freedom of expression. The college does not condone censorship, nor does it endorse the inspection of electronic files other than on an exceptional basis, i.e., if required to ensure the integrity, security, or effective operation of college systems.

Nevertheless, the college reserves the right to place limited restrictions on the use of its computers and network systems in response to complaints presenting evidence of violations of college policies or codes, or state or federal laws. Once evidence is established, the

Last Updated – Thursday, May 29, 2008

Information Security Policies  
Macalester college  
St. Paul, MN

college authorities responsible for overseeing these policies and codes will be consulted on the appropriateness of specific restrictions, which could include the removal of material posted on a computer and/or limiting access to the college's networks.

This policy is in accordance with college policies concerning harassment, use of computers and network systems generally, and related judicial codes. Any restrictive actions taken by the college will be in accordance with guidelines and procedures set forth in these policies, codes, or laws. The restrictive actions pertaining to this policy and described below conform to the Electronic Communication Privacy Act of 1986.

- The college reserves the right to limit access to its networks when applicable college policies or codes, contractual obligations, or state or federal laws are violated, but does not monitor or generally restrict the content of material transported across those networks.
- The college reserves the right to remove or limit access to material posted on college-owned computers when applicable college policies or codes, contractual obligations, or state or federal laws are violated, but does not monitor the content of material posted on college-owned computers.
- The college does not monitor or generally restrict material residing on college computers housed within a private domain or on non-college computers, whether or not such computers are attached to campus networks.

#### **4010 Policy Violations**

Violations of this policy may involve the use of electronic communications to:

- Harass, threaten, or otherwise cause harm to a specific individual(s), whether by direct or indirect reference
- Impede, interfere with, impair, or otherwise cause harm to the activities of others

Last Updated – Thursday, May 29, 2008

Information Security Policies  
Macalester college  
St. Paul, MN

- Download or post to college computers, or transport across college networks, material that is illegal, proprietary, in violation of college contractual agreements, or otherwise is damaging to the institution
- Harass or threaten classes of individuals

As a matter of policy, the college protects expression by members of its community and does not wish to become an arbiter of what may be regarded as "offensive" by some members of the community. However, in exceptional cases, the college may decide that such material directed to classes of individuals presents such a hostile environment that certain restrictive actions are warranted.

#### **4020 Reporting Violations**

If you believe that a violation of this policy has occurred, contact the system or network administrator responsible for the system or network involved, who will report the incident to the college/unit policy officer in accordance with local procedural guidelines, should they exist.

#### **4030 Responsible Use of Email**

The Macalester E-mail system is not to be used for commercial purposes, sending unsolicited e-mail (aka SPAM), or for any illegal activity; or in a way that violates the ITS Responsible Use Policy.

#### **4040 Email Procedures**

When using email, don't open attachments unless you are expecting them and make sure to check any embedded links within emails to verify they point to the expected location.

The single greatest cause of email exposure of sensitive data is sending email to the wrong recipient so carefully check all addresses before sending.

Last Updated – Thursday, May 29, 2008

Information Security Policies  
Macalester college  
St. Paul, MN

## **5000 Mass Electronic Emailing**

Macalester College employs consistent procedures for notification and processing mass electronic mailings to the following constituencies: faculty, staff (academic and non-academic), students, and alumni. The college expects anyone sending mass electronic mailings to any or all of these constituencies to do so in accordance with the procedures outlined in these policies.

The college must exercise appropriate control over electronic communications so that it may properly maintain network performance and limit the number of unsolicited mail messages.

### **5010 Two Forms of Mass Electronic Mail**

Macalester employs two forms of mass email communication:

- Emergency
- Non-emergency

Emergency mailings go to all faculty, staff (academic and non-academic), and students, but not to alumni.

Non-emergency mailings follow one of two tracks:

1. Specific constituencies (faculty, staff (academic and non-academic), students, or alumni), or
2. General campus-wide distribution

**Note:** This policy does not limit or prohibit the use of other methods of email dissemination.

**Note:** The president and the provost are not subject to the approval procedures described in this document.

### **5020 Emergency Email**

Anyone wishing to send an emergency email must do the following:

Information Security Policies  
Macalester college  
St. Paul, MN

1. Receive the approval of the Vice President of Student Affairs. In the absence of the Vice President of Student Affairs, the Provost must validate and approve the email.
2. Depending upon the circumstances, either the individual wishing to send the mailing or the Vice President of Student Affairs will consult with the Director of College Relations as to the substance of the message. In addition, the administrative officer who approved the message (either the Vice President of Student Affairs or the Provost) will attempt to inform managers and deans, as appropriate, of the email to be sent.
3. The approving individual will contact the appropriate office for dissemination of the mass email.

**5030 Non-emergency Email to a Specific Constituency**

Anyone wishing to send an email to a specific constituency, specifically, faculty, staff (academic and non-academic), students, or alumni must do the following:

1. Send the request to the appropriate vice president or Dean of Faculty for that constituency
2. The specific vice president or Dean of Faculty will decide whether it is appropriate for distribution to his or her population
3. If the specific vice president or Dean of Faculty agrees to approve it, he or she should consult with the Vice President of Student Affairs as to the content of the message
4. Only the approving vice president or Dean of Faculty may instruct the Director of College Relations to send the email, by contacting Douglas A. Stone at [stone@macalester.edu](mailto:stone@macalester.edu)
5. The Director will validate the authenticity of message and the sender. Upon validation, the messaging manager will return the email, formatted for distribution to the constituency, to the sender for final approval before dissemination. Once approved, the email is disseminated

**5040 Non-emergency Email for Campus-wide Distribution**

Anyone who has a communication intended for distribution to the entire college community requires the approval and review of the Vice

Last Updated – Thursday, May 29, 2008

Information Security Policies  
Macalester college  
St. Paul, MN

President of Student Affairs. Only that vice president can instruct the Director of College Relations at [stone@macalester.edu](mailto:stone@macalester.edu). The Vice President of Student Affairs will also inform managers and deans, as appropriate, of the message before it is distributed.

## **6000 Privacy of Information Technology Data**

Macalester College recognizes users' reasonable expectations of privacy in information technology (IT) data generated automatically by computer systems and by voice and data network devices. Therefore, the Vice President for Information Technology Services (ITS) will disclose IT data only under the following circumstances:

- In response to a court order or other legal papers
- In the investigation of a legal or policy violation,
- In the event of a health or safety emergency,
- In specific instances of reasonable requests in the interests of the college, such as collaborative research with other institutions
- To maintain the operation and security of the IT network

This policy enables the safeguarding of the privacy of the college's information technology (IT) data by establishing controls over access to such data, including limiting conditions under which that data may be disclosed.

- Nothing in this policy is intended to prohibit or inhibit data custodians who handle IT data from performing their duties in the normal course of business
- The Vice President for ITS has delegated to IT professionals the authority to disclose IT data for the purposes of security, maintenance, or billing
- All data disclosed to assist academic research will be anonymous

## **7000 Reporting Electronic Security Incidents**

Users of information technology devices connected to the Macalester network must report all electronic security incidents promptly and to the appropriate party or office. This includes loss or theft of a device.

Last Updated – Thursday, May 29, 2008

Information Security Policies  
Macalester college  
St. Paul, MN

The campus computer network constitutes a substantial college resource, and the college's missions rely significantly on a secure electronic communication network. Prompt and consistent reporting of electronic security incidents protects and preserves these resources and aids the university's compliance with applicable law.

## **8000 Outsourcing**

College departments providing electronic personal information to a third party must do so by formal agreement. The agreement must include a provision that the party receiving the electronic personal information will abide by Macalester's data standards.

## **9000 Emergency Response Plan & Disaster Recovery**

### **9010 Emergency Response Plan**

The Associate Vice President of ITS is responsible to maintain an emergency and disaster response plan that addresses what will happen in the event of a disaster to organizational facilities. This plan will ensure the integrity of data and the ability to quickly recover after the disaster passes.

### **9020 Disaster Recovery**

The disaster recovery plan will undergo an annual review including a full restoration of a data backup. The results of the annual review will be documented and retained.

### **9030 Incident Tracking**

Production environment incidents will be tracked using Macalester's internal incident tracking software (HelpLine). In the event of application failure an incident report will be created and assigned to the appropriate personnel. Details of the incident (cause, resolution, etc.) are to be recorded in the incident report for future reference.

Last Updated – Thursday, May 29, 2008

Information Security Policies  
Macalester college  
St. Paul, MN

Last Updated – Thursday, May 29, 2008