CFA Resolution 2004-05A
Resolution on Computer Privacy

Approved by CFA:	October 22, 2004
Reviewed and endorsed by CAPFA:	October 7, 2004
Reviewed and endorsed by CCSA:	October 28, 2004
First Reading, University Council:	December 6, 2004
Approved, University Council:	
Approved, President:	
Approved, Board of Visitors:	
Effective Date:	Upon approval by BOV

WHEREAS, Human Resource Policy 1.75 of the Commonwealth of Virginia states that "No user should have any expectation of privacy in any message, file, image or data created, sent, retrieved or received by use of the Commonwealth's equipment and/or access;" and

WHEREAS, a core value of Virginia Tech is the view of the university as a community of scholars embedded in an environment that protects and nurtures freedom for intellectual inquiry; and

WHEREAS, a policy defining the balance between the university's business needs and respect for employees' freedom of inquiry is needed to guide actions of managers in certain situations and to clarify expectations for all employees about when and how the university may access employees' communications;

THEREFORE, be it resolved that the attached "Privacy Policy for Employees' Electronic Communications" be approved and forwarded to the Board of Visitors for adoption.

Subject: Privacy Policy for Employees' Electronic Communications

1. Purpose

This policy defines the balance between the university's business needs and respect for employees' freedom of inquiry and expression with regard to electronic communications and computer resources owned or provided to employees by the university.

As noted by the 2001 Virginia Tech Strategic Plan, "The core values of Virginia Polytechnic Institute and State University are freedom of inquiry, personal integrity, mutual respect, promoting personal and professional growth, fostering a lifelong commitment to learning, and contributing to society." The core values section of the Strategic Plan also emphasizes the importance of the university as a "community of scholars" embedded in an environment that protects and nurtures freedom for intellectual inquiry.

The Commonwealth of Virginia's Human Resource Policy 1.75 ("HR policy") contains the following statement: "No user should have any expectation of privacy in any message, file, image or data created, sent, retrieved or received by use of the Commonwealth's equipment and/or access." The HR policy further states that Virginia agencies, including its institutions of higher education, have "the right to monitor any and all aspects of their computer systems" and may do so "at any time, without notice, and without the user's permission." While the policy grants Virginia Tech the right to monitor its computer systems, it does not require it to do so, and states that, "Agencies may supplement this policy as they need or desire, as long as such supplement is consistent with this policy."

In recognition of the complex and unique mission of a land grant university, the Virginia Tech privacy policy supplements the commonwealth's electronic communications policy to tailor it to situations that may arise in a university community, and to further the goals of an academic community expressed in the Strategic Plan. However, it does not create any additional or new legal rights, or new or additional legal expectation to privacy for Virginia Tech employees.

2. Policy

The university does not routinely monitor or access the content of electronic communications, computer files, or voice mail of its employees, whether stored on university equipment or in transit on the university network. Content of employees' electronic communications or files will not be accessed during the

execution of systems support, network performance, and related security functions.

However, monitoring or access may be necessary under certain circumstances. This section outlines the legal or administrative circumstances under which access and/or monitoring may occur without further authorization, or when it may occur on a routine basis if specified in an approved departmental policy.

2.1 Legal or administrative circumstances where monitoring and/or access may occur without further authorization are:

- communications or files required to be released by law, by orders of a court, or requested in accordance with the Virginia Freedom of Information Act ;
- approved Internal Audit reviews;
- resolution of technical problems; [Technical staff may inadvertently see or hear potentially illegal content in communications or files while working to resolve technical problems. If so, they are required to report what they have seen or heard to appropriate authorities. Otherwise, the university expects technical staff to treat inadvertently encountered electronic communications and files of university employees as confidential and not subject to disclosure to anyone.]
- emergency situations involving an imminent threat of irreparable harm to persons or property; and,
- resources assigned to a group or publicly available to any user.

2.2 Routine monitoring and/or access in support of essential departmental operations:

If routine monitoring or examination of employee electronic communications or files are an essential part of the work environment, then the department must develop and maintain a clearly written operating policy that is regularly disseminated to the affected employees. Affected employees must be given an opportunity to comment during the development or major revision of such a policy. Prior written approval of such departmental policies is required from the relevant dean or senior manager.

2.3 All other cases of monitoring and/or access require authorization as described in the procedures section in part 3.

Virginia Tech requires all employees to obey applicable policies and laws in the use of university computing and communications technologies. Nothing in this policy changes or supersedes these employee requirements.

3. Procedures

Authorization for non-law-enforcement university personnel to monitor or access electronic communications or files of employees will not be granted casually. Such authorization will require justification based on reasonable business needs or reasonably substantiated allegations of violation of law or policy on the part of the employee. In carrying out retrieval of files or information, due respect should be accorded to confidential or personal information and legally protected files.

Explicit consent never constitutes an intrusion. Employees may freely give consent to other individuals to access information stored on equipment or resources assigned to them. No further authorization is required in such instances.

3.1 Investigations of Violations of Law or Policy

Requests for authorization to monitor or review electronic communications or files because of allegations of violations of policy or law by faculty or staff members may originate with supervisors. They may also originate with an investigatory authority such as the Equal Opportunity Office investigating a claim of sexual harassment. Requests must be made in writing and include the rationale for the request, a description of the information or files to be accessed or retrieved, and the proposed handling and disposition of the files. Authorization in such cases may be granted by the relevant dean or senior manager (including vice presidents/vice provosts), or higher level authority if needed.

The senior manager who is asked to consider authorization for monitoring or reviewing the electronic communications or files of an employee must use his or her best professional judgment in determining if there exist reasonable grounds, considering the surrounding circumstances and environment, to grant such authorization. The senior manager is expected to maintain confidentiality in such a situation. He or she may wish to consult with the Office of the General Counsel or Personnel Services in determining whether to authorize monitoring or review, and in determining if the affected employee or anyone else should be notified that the monitoring or review is taking place.

3.2 Business Needs

Where there is a reasonable need for access to routine business or educational documents and the employee is unavailable, authorization to access that employee's electronic communications should be provided by the department head or director, or next higher authority. Whenever possible, the employee should be informed and asked to help in obtaining the needed business materials. If that help is not reasonably available, then other steps should be considered to respect the confidential or

personal nature of any other materials present. The employee will be promptly notified of the access and the nature of the documents or communications reviewed or obtained.

4. Definitions

Employees include all persons directly employed by Virginia Tech in their capacity as employees. The policy also covers anyone to whom the electronic communications and computing resources of employees have been extended. These include (but are not limited to) recently terminated employees whose communications and computing resources have not yet been terminated, deleted, or transferred, consultants that may be hired, and individuals whose electronic communications and computing resources continue between periods of employment. This also includes student workers, volunteers, and other individuals who are using state-owned equipment and carrying out university work.

5. References

Department of Human Resources Policy 1.75
http://www.dhrm.state.va.us/hrpolicy/policy/pol1_75.pdf

Virginia Freedom of Information Act Title 2.2, Chapter 37
http://legis.state.va.us/Laws/CodeofVa.htm

University Strategic Plan 2001
http://www.unirel.vt.edu/stratplan/01MVV.html

Administrative Data Management and Access Policy—University Policy 2005
http://www.policies.vt.edu/2005.pdf

Acceptable Use and Administration of Computer and Communication Systems—University Policy 2015
http://www.policies.vt.edu/2015.pdf

Acceptable Use Guidelines
http://www.policies.vt.edu/acceptableuse.html

Management of University Records—University Policy 2000
http://www.policies.vt.edu/2000.pdf

Policy on Intellectual Property—University Policy 13000
http://www.policies.vt.edu/13000.html

Campus Security—University Policy 5615
http://www.policies.vt.edu/5615.pdf

Government Data Collection and Dissemination Practices Act, Sec. 2.2-3800 et seq.
http://legis.state.va.us/Laws/CodeofVa.htm

6. Approval and revisions

Information system technology is characterized by rapid evolution and the development of innovative, novel applications. It is the intent of this policy to establish basic principles that will endure through many evolutions of information systems.

The Vice President for Information Technology is charged with the responsibility to periodically review the policy and propose changes as needed for consideration by university governance.

Approved:

University Council: February 21, 2005

Board of Visitors: