Impact Statement
For Proposed Policy: Privacy of the Network

Submitted: February 16, 2005
Revised: Post-EPFRG Meeting – February 23, 2005
Responsible Executive: Vice President for Information Technologies
Representing Office: IT Policy Office, Office of the Vice President for Information Technologies

Background
This proposed policy on the privacy of the network represents the next step towards completion of the IT Policy Framework. Two main principles drive this policy: the university’s position on monitoring its network and computers, established in University Policy 5.1, Responsible Use of Electronic Communications; and the conditions under which information technology data may be disclosed to third parties, pursuant to the authority given to the Vice President of Information Technologies (IT) in University Policy 4.2, Data Stewardship and Custodianship.

With respect to the first principle, University Policy 5.1, Responsible Use of Electronic Communications (originally promulgated in 1995) is a first-generation information technology policy. A number of its specifics have been refined into distinct policies following subsequent policy development. (For more information on this point, please see the IT Policy Framework [http://www.cit.cornell.edu/oit/policy/framework.html](http://www.cit.cornell.edu/oit/policy/framework.html)) One of the specifics of “Responsible Use” is the university’s position on monitoring, posting or removing content material from its networks and computers. It is proposed that this consideration form one of the bases of a new policy on privacy.

The IT Policy Framework distinguishes this provision from user obligations, which will be retained in a revised “Responsible Use” policy that will be renamed “Responsible Use of Information Technology Resources.”

With respect to the second principle, this proposed policy presents the opportunity for the Vice President of IT, as steward, to establish policy stipulating the conditions under which information technology data may be disclosed to third parties.

Policy Statement
The university as a practice does not monitor or restrict the content of material transmitted on the university network, or posted on university-owned computers, but reserves the right to limit or remove access to its networks and to material posted on its computers, when applicable university policies or codes, contractual obligations, or state or federal laws are violated.

As steward of the university’s information technology data, the Vice President of Information Technologies (IT) designates the following limited conditions under which information technology data may be disclosed to third parties: (1) in response to a court order, or other compulsory legal process; (2) upon the request of an appropriate university official in the investigation of a legal or policy violation; (3) to maintain operation and security of the network; (4) in the event of a health or safety emergency; and (5) in specific instances explicitly approved by the Vice President, for purposes of research that is to be shared with appropriate parties in other institutions of higher education.
Impact Statement
For Proposed Policy: Privacy of the Network

Reason for Policy
This policy contributes to the protection of confidential and legally-protected data and to the fostering of an environment of trust for and about the university’s network.

Consistency with Cornell University’s Mission and Goals and Other Policies
This policy falls within the IT Policy Framework that attempts to establish a balance between IT security and privacy of the data network.

Related existing university policies are:
- University Policy 4.4, Access to Cornell Alumni Affairs Information
- University Policy 4.5, Access to Student Information
- University Policy 4.7, Retention of University Records
- University Policy 4.12, Data Stewardship and Custodianship
- University Policy 5.1, Responsible Use of Electronic Communications
- University Policy 5.4.1, Security of Information Technology Resources
- University Policy 5.4.2, Reporting Electronic Security Incidents
- University Policy 5.7, Network Registry

Scope of Policy
The Cornell University network and its information technology resources represent the physical scope of this policy and the Vice President of Information Technologies is the steward for information technology data.

Entities, Offices and Other Cornell Community Members Affected by this Policy
Endowed Ithaca and Contract Colleges of the University and the Weill Medical College.

Impact on the University
No known financial or administrative burdens are known to exist for this policy. To the contrary, by making the rules regarding the appropriate use and disclosure of these administrative data, implementation of this policy may increase administrative efficiencies.

Stakeholders Who Will Be Consulted in Developing This Policy
- IT Policy Advisory Group
- IT Manager’s Council
- IT Security Council
- University Audit
- University Counsel
- Office of Risk Management and Insurance
- College Business Officers/Business Service Center Directors
- Office of Human Resources
- Dean of the Faculty
- Faculty Advisory Board for Information Technology (FABIT)
- Administrative Systems Planning Group (ASP)
- Cornell Computing Directors (CCD)
- Weill Medical College, James R. Kahn, Deputy University Counsel
Impact Statement
For Proposed Policy: Privacy of the Network

Compliance Mechanisms
University Audit and University Counsel will audit and review compliance.

The IT Policy Office will oversee education and training of policy principles and procedures.

Timing Requirements
This policy should be issued and promulgated as soon as possible for timely achievement of its goals.