The Faculty Senate

March 3, 2005

The Faculty Senate will meet on Friday, March 11, 2005, at 2:10 p.m., in the Marvin Center, Room 310.

AGENDA

1. Call to order

2. Approval of the minutes of the regular meeting of February 11, 2005, as distributed

3. Resolutions

   A RESOLUTION FOR THE APPROPRIATE REGULATION OF HONORS, AWARDS, OR DISTINCTIONS BY UNITS OF THE UNIVERSITY (04/9); Professor Barry L. Berman, Acting Chair, Honors and Academic Convocations Committee (Resolution 04/9 is attached)

4. Introduction of Resolutions

5. Update on Academic Technology Security: Chief Information Officer David W. Swartz and Chief Technology Officer Guy L. Jones (Information attached)

6. Report on the School of Engineering and Applied Science: Dean Timothy W. Tong

7. Remarks by Vice President for Advancement Laurel Price Jones

8. General Business:

   (a) Nominees for election to the Nominating Committee for the Executive Committee for the 2005-06 Session (nominees to be announced)

   (b) Report of the Executive Committee: Arthur E. Wilmarth, Jr., Chair

9. Brief Statements (and Questions)

10. Adjournment

Elizabeth A. Amundson
Secretary
A Resolution for the Appropriate Regulation of Honors, Awards, or Distinctions by Units of the University (04/9)

WHEREAS, it is of the first importance that any honor, award, or distinction linked with the name of The George Washington University continue to deserve the high regard of the entire academic community and the world at large; and

WHEREAS, it is essential therefore that such honor, award, or distinction be conferred with due deliberation on individuals or associations properly deserving of that honor, award, or distinction; and

WHEREAS, to that end it is desirable that in the conferral of such honor, award, or distinction a degree of uniformity in standards, criteria, and deliberation be maintained throughout the University; NOW, THEREFORE

BE IT RESOLVED BY THE FACULTY SENATE OF THE GEORGE WASHINGTON UNIVERSITY:

1) That only Schools of the University should be authorized to confer honors, awards, or distinctions (that is, not individual Departments or other academic subdivisions, Institutes, or Centers, or other components, including 'schools within Schools', although these could well suggest or initiate consideration of such), subject to some appropriate procedures to be established by and within each School for that purpose, such procedures to be approved by the Executive Vice President for Academic Affairs; and

2) that nominees for School awards should be vetted and approved by the Committee on Honors and Academic Convocations of the Faculty Senate on the basis of materials submitted in support of the honor to be conferred by the School, much as that Committee now vets nominations for the award of honorary degrees submitted by the various Schools.

Appendix: Guidelines for Conferral of Honors, Awards, or Distinctions

1) The awardee must have achieved distinction in his or her profession. "Distinction" can be measured in a variety of ways: winning significant prizes for professional or scholarly work; achieving national or international recognition for professional or scholarly work; or displaying the kind of professional or scholarly skills or abilities, character, and integrity that might cause the nominee to be considered to be a role model for students.

2) The awardee must have made the kind of contribution to his or her profession that has measurably enhanced or improved the profession. The awardee must have set a new standard for accomplishment, found new ways to deliver the benefits of the profession, or otherwise brought recognition to the profession.

3) A connection with GW and the School proposing the honor, award, or distinction would be an important positive factor.

Committee on Honors and Academic Convocations
Barry L. Berman, Acting Chair
February 16, 2005
To: GWU Faculty Senate Members  
From: Arthur E. Wilmarth, Jr., Chair  
GWU Faculty Senate Executive Committee  
Re: GWU Information Security Policy

On Friday, February 25th, 2005, the Faculty Senate Executive Committee met with Mr. David Swartz, Chief Information Officer, and Mr. Guy Jones, Chief Technology Officer, in anticipation of Mr. Swartz's upcoming presentation to the full Senate on Friday, March 11th, 2005. The Executive Committee felt, and Mr. Swartz agreed, that sharing the following questions (posed by the Executive Committee) and answers (provided by Mr. Swartz) would be appropriate to inform the Senate about the underlying issues involving Information Security Policy.

1. What generic types of computer programs are currently mandated on all academic machines under the University academic technology policy (...a copy of any such policy would be very helpful).

The security software requirements and recommendations can be found in the Information Security Policy. A copy can be accessed from:


For systems that contain confidential and/or sensitive information such as social security numbers, educational records, and credit card numbers as examples, encryption technology and enhanced security measures is required.

The Information Security Policy states that systems should be patched and anti-virus software used. Operating system patches and software patches are generally freely available from the manufacturer for valid operating system and software licensed users. The George Washington University has a site license for antivirus software (Symantec) that is freely available to faculty, students, and staff.

The Information Security Policy highly recommends the usage of personal firewalls but does not mandate the use of it. GW has a site license for Symantec AV Corp Edition 9.0.2 + Firewall 7.0.2 available from http://helpdesk.gwu.edu/software/download.html.

2. How, and when, were the mandates cited in (1) approved by a representative, elected Faculty body and what is the relationship of that body to the Faculty Senate;

The Information Security Policy went into effect on April 21, 2004. The policy was reviewed by the ISS Policy committee, the AITC (Administrative Information Technology Committee) and the RITC (Research and Instructional Technology Committee). The document was also developed after significant discussions with departmental LSP representatives.

3. Does current academic technology policy require specific vendors (e.g., *Symantec* antivirus checker) or does the policy prescribe only generic categories (e.g., "you must have a virus checker on your machine")

The Information Security Policy does not require specific vendors product.
However, GW has a site license for anti-virus and personal firewall software that is available from the helpdesk website. It must be noted that ISS will only provide support to approved software listed under http://helpdesk.gwu.edu/software/supported.html.

(4) Does the University have site licenses for *all* mandated software identified in (1), and if so, could you provide the *specific* URL to access and download that software?

Yes, for the desktop. Desktop software is available at the ISS helpdesk website for download at http://helpdesk.gwu.edu/software/download.html. However, the Security Policy states that sensitive and/or confidential information must use encryption technologies and other safeguards beyond what is needed for the desktop. SSH and VPN clients (for wireless) is available to encrypt the transmission of sensitive and/or confidential information. Other measures are targeted toward the use of sensitive information on servers. These measures fall under best practice and vary for each type of computer platform. Desktops should not be used to provide open access to sensitive and/or confidential information. Use of a desktop as a server would require that it follow guidelines for server use to include having a designated system administrator.

(5) What procedures are in place, or are proposed, to ensure Faculty compliance with academic technology policy, and are these procedures fully consistent with the Faculty Code?

Compliance with security recommendations at the desktop for the faculty is not monitored today. Instead we use Intrusion Detection and Prevention Systems to monitor malicious traffic such as worm and virus activities. Desktops that are compromised are referred to the local LSP for rebuild. If the identified desktop compromise is not corrected the desktop is removed from the network after one week.

There are two projects in place to ensure desktop compliance with the security policy.

Patchlink is currently being tested by ISS users to verify anti-virus software installation and operating system and software patch update level. This software has been successfully used by Gelman library staff to almost entirely eliminate their desktop virus/Trojan problem. ISS is now working with ResNet to deploy the Patchlink product to the student residents for the 2005 Fall semester. We are also working with departmental LSPs to provide this service later this summer or fall to the departments for voluntary use but our first priority is the student residence halls. Each LSP will determine whether to use Patchlink based on their needs and desires of their Deans/Department heads.

The Cisco Clean Access Solution Initiative is the second program that will be deployed to the student subnets this fall. Clean Access requires that a user either log into the network or have their desktop scanned prior to being allowed full access to the Internet.

By implementing these programs to verify that the security policies are implemented and are working effectively we can reduce the incidence of compromise of University desktops. Patchlink and Clean Access Scanning serve as the verification piece.

The Faculty Code states that "Faculty shall enjoy the freedom of investigation subject only to legal restrictions and guidelines as shall be recommended by the Faculty Senate, and adopted by the University".

Faculty Senate Office
1918 F Street, N.W. ♦ Suite 312 ♦ Washington, DC 20052 ♦ (202) 994-7198 ♦ Fax (202) 994-1523
The University is required by regulation and board mandate to maintain an adequate level of security i.e. due diligence and due care to minimize negligence claims against the University due to crimes such as Identity Theft and the Invasion of Privacy from stolen information.

The implementation of the security technologies listed under question 1 and found in the Information Security Policy (Patches, Encryption, Antivirus software, personal firewalls (recommended)) are seen as a privacy enabler for students, staff, and faculty members. Without these security technologies, true privacy can not exist as the desktop computers are left open to hacker attacks and intrusions.

(6) What generic types of computer programs beyond those currently mandated is ISS proposing to mandate on all academic machines

The Patchlink and Clean Access projects are targeted at the student residence halls this fall. Patchlink will be made available to academic departments for voluntary use this summer. Patchlink requires the participation of the department IT support group to identify users and provide administrative management.

(7) As a specific corollary to (6), is there (or is it contemplated that there will be) a proposal to place any kind of program (active or passive) on each Faculty member's computer to ensure compliance with academic technology policy

Patchlink and Clean Access will be available for expanded use in the future. It is envisioned that ISS will work with the academic or administrative departmental LSPs on which, if either, of these projects would be appropriate in their areas. The Patchlink solution in particular requires direct participation of the group providing desktop support. Clean Access has not been funded beyond the student subnets.

If the answer to (7) is yes:

(8) What is/are those proposed programs?

1. Patchlink on a department by department voluntary basis
2. Cisco Clean Access Solution. (unfunded)

(9) Under the proposal, what is their scope?

Student subnets will be covered by both projects this fall. Participation by other academic and administrative departments will be coordinated on a voluntary basis. ISS and Gelman library are already using the Patchlink solution.

(10) Under the proposal, what is the timetable for implementation?

Patchlink Implementation:
Gelman Library Staff and ISS Staff 11/04 thru 5/05
Students 08/05 forward
Departments on voluntary basis 05/05 forward

Clean Access:
Student subnets 08/05
Other departmental subnets unfunded
(11) At what other universities has a proposal such as this been universally adopted and implemented with respect to the *Faculty*?

Approximately 140 higher education institutions have adopted the Cisco Clean Access Solution. We contacted a reference set of Universities to compare how they implemented their solution.

The normal implementation was for student subnets, wireless and public connections. The reference universities have not implemented a universally adopted solution with respect to Faculty. However, some universities listed are planning to include Faculty in future implementations and are beginning discussions with faculty.

Reference Universities:
- Stanford University
- Fordham University
- University of Mary Washington
- University of Cincinnati
- James Madison University
- Arizona State University

(12) Under the proposal, will the proposed resident program(s) be capable of making any changes to a Faculty member's machine without his/her knowledge and/or concurrence, and if so, what is the proposed scope of those changes?

Patchlink is capable of 'pushing' patches down to each desktop. The initial rollout to the student subnet will be set to monitor anti-virus and patch level. Gelman now 'pushes' patches to its system and ISS is using a mix of monitor and push depending on type of desktop.

Clean Access will also monitor the existence of anti-virus and patch level before allowing access to the network. There is an additional capability to allow access after logging in without scanning. Clean Access does not 'push' but can redirect the user to a website to download the required software.

(13) Under the proposal, would an individual Faculty member have the option of declining to have such a resident program operating on his/her machine, and if so what would be the implications of opting to decline?

a.) The implementation of Patchlink will be dependant on the departmental LSP / management decision. Policies on use will be made by the department. Patchlink requires the direct participation of the desktop support group.

b.) Clean Access is currently not funded beyond the student subnets. If funding becomes available it is envisioned that the entire network will be covered. Clean Access has the ability to exclude individual systems and allowing network log-in for full Internet access.

(14) Under the proposal, in what way would the Faculty (as a group) actively participate to ensure that such any such resident program is limited to exactly, and only, the tasks consigned to it and approved by the Faculty?

The technical coordination of these projects rests with departmental LSPs. They have the knowledge of who and where the faculty are and what their needs and requirements are. ISS is striving to provide flexible solutions that can be used in partnership with the departments to provide cost effective protection.

Each of these solutions depends on the active participation of each department's IT support group to manage and deploy.

Faculty Senate Office
1918 F Street, N.W. • Suite 312 • Washington, DC 20052 • (202) 994-7198 • Fax (202) 994-1523