August 2004

To: Faculty and Staff
From: Peter N. Stearns, Provost
J. Thomas Hennessey, Jr., University Chief of Staff and Chair, Privacy and Security Compliance Team
Re: Privacy and Security Implementation

In an effort to create a more security conscious environment even as we implement new Banner administrative software, we offer the following operational instructions:

Social Security Numbers: The university has abandoned use of the Social Security number as the primary identifier for students and faculty. Instead, we use an assigned “G” number, a capital G followed by eight digits. Do note that the *Family Educational Rights and Privacy Act (FERPA)* requires that alternate identifiers be kept just as secure as Social Security Numbers, and must be guarded against inadvertent or unauthorized exposure. In no case should individuals’ Social Security numbers and G numbers be associated.

Securing Academic Records: Please exercise vigilance regarding students’ academic records in any format, including paper. They must be kept secure, disposed of only in a secure manner, and shared only with those who have a legitimate educational need. The university’s Privacy and Security Team, under the leadership of Tom Hennessey, will be releasing more specific guidelines in the next few months. They will be available at the Registrar’s Faculty and Staff Services web site at http://registrar.gmu.edu/fss/pweb.

Laptop and Desktop Computers: Wherever possible, avoid downloading privacy information to desktop or laptop computers. Since they are harder to secure than servers, they present a greater risk of compromise. Since many of us need to work on large “privacy information” files on our desktops, one method found to work is to save all files on a securely managed server and not on the desktop. As we add more information to the student course lists provided by the registrar, the sensitivity of that information grows. So too, should the care and security of that information increase. Leaving a desktop that is signed on to the network and or an unattended laptop means that anyone can access the information that is available to the user.

Confidentiality Indicator: Although we are committed to the privacy of all students’ records, *FERPA* allows students to elect an even higher level of privacy for their education records. You will see the designation “confidential” on class rosters for such students. This status in no way precludes you from contacting the student regarding class business. It does, however, mean that sending a group e-mail to your class in a system that lists the e-mails of all recipients would result in a violation of their privacy rights. For these students, you will need to send individual messages or a blind copy. If your course requires that students communicate with each other via e-mail, you must include this information prominently in the syllabus. Students with a confidentiality indicator may choose not to take the course.

G-number and PIN: Guard the confidentiality of your own G number and PIN, as together they constitute your access to grade students. Use the built-in Security Question in Banner to full advantage, as protection should you forget your PIN. Often greater security results in less convenience: do not expect the Support Center, or anyone at the university, to re-set your forgotten PIN based on a telephone request.

Grading: The new Patriot Web system offers a relatively easy and user friendly interface for instructors of record to enter student grades. That entry is the responsibility of each faculty member. Please exercise great restraint in having anyone else enter such sensitive data. Each department will have a grading coordinator who can enter grades for professors through a user-unfriendly and inconvenient part of Banner. While we have been accustomed to wide use of "proxy" graders, we must limit the use of graders in Banner to absolute emergencies. Teaching and grading are at the core of the university. Faculty members are responsible for the integrity of grades for their classes. This should extend to reasonable measures to protect your password and login from abuse or even casual misuse.

Feedback: Your comments are welcome. Please direct them to banner@gmu.edu.