Precautions for Handling Sensitive and Restricted Information at the University of Georgia

TO: Vice Presidents, Deans, Department Heads, and Administrative Directors

FROM: Timothy M. Chester, Vice President for Information Technology

RE: Precautions for Handling Sensitive and Restricted Information at the University of Georgia

The University of Georgia is committed to protecting the personally identifiable information of its students, faculty, and staff as its first and foremost business requirement for all IT systems. Our best advice is to avoid, if at all possible, the receipt, transmission, or storage of sensitive or restricted information, such as Social Security numbers (SSNs) or credit card numbers. If handling this information is required for business purposes, the University has made the following tools available to all units. These tools will reduce your risks associated with handling this information:

Secure Reports is an encrypted repository for receiving and storing restricted information (such as SSNs or credit card numbers) via email or regular reports. If you need to receive or send this type of information, you should do so using Secure Reports. Units are encouraged to store files containing restricted information on this service.

Send Files is an encrypted repository for receiving and storing other types of sensitive information. If you need to receive or send this type of information, you should do so using Send Files instead of email. Units are encouraged to store files containing sensitive information on this service.

Data Loss Prevention (DLP) Software is a software service that, like anti-virus software, resides on your computer and monitors, protects, and manages sensitive information wherever it is stored. The DLP software alerts administrators whenever information is received, transmitted, or stored in a way that is inconsistent with University policy.

ArchPass is a multifactor authentication system for systems on which sensitive and restricted information is stored. The ArchPass network provides an additional firewall around these systems, which users must access by using their MyID, password, and a random six-digit code provided by a physical device that only those users possess.

Secure Virtual Desktop (VDI) supports secure computer workstations hosted in the Boyd Data Center, thereby providing a more secure desktop environment for those who must regularly handle sensitive and restricted information, such as SSNs or credit card numbers. The use of Secure VDI allows employees to accomplish their business functions knowing that the data they handle never leave the security of the Boyd Data Center.

All these tools, with the exception of the Secure VDI service, are available free of charge. The Secure VDI service requires a modest monthly fee to support the software licenses that make the service possible.

This year, we are also emphasizing the use of database or file system encryption by units storing restricted information, such as SSNs or credit card numbers, on their computer systems outside of the Boyd Data Center, in order to protect this information in the event of equipment loss or theft. This would include servers, as well as desktop PCs and laptops. Use of the Secure VDI service (mentioned previously) will negate the need to take this additional step. Our Office of Information Security provides guidance on the use of encryption technologies here: *http://eits.uga.edu/access_and_security/infosec/pols_regs/policies/encryption_guidelines/*

The Office of Information Security's website (infosec.uga.edu) outlines policies, standards, and guidelines related to information security. Recent changes required by the Board of Regents' policy include those related to handling sensitive personally identifiable information, the data classification and protection standard, and guidelines for classifying and protecting UGA ID numbers (also commonly called 810 or 811 numbers). Employees who handle UGA ID numbers, Social Security numbers, credit card numbers, or records related to students, donors, alumni, and prospective students are encouraged to review these guidelines and standards.

The University of Georgia has made significant strides over the past four years in remediating its legacy IT systems, with the goal of providing both increased business efficiency and greater protections for personally identifiable information. Information security success is not something that can ever be fully accomplished, but threats to this security can be minimized through constant diligence and awareness on the part of all students, faculty, and staff. Our greatest information security risk is complacency, and the tools described above can help your units reduce their business process risks associated with handling sensitive and restricted information.

I encourage all UGA Vice Presidents and Deans to have discussions with their IT staff to review the risks and mitigations employed within their unit to protect restricted information. Both I and the University's Information Security Officer are available to provide guidance and assistance with these conversations and our recommendations.

For more information on these resources, please visit http://infosec.uga.edu and click on Tools or contact Mr. Brian Rivers, the Associate Chief Information Officer for University Information Security, by email at brivers@uga.edu.

Cc: Jere W. Morehead, President
Pamela Whitten, Senior Vice President for Academic Affairs and Provost
Information Technology Managers Forum
UGA Network Managers Group

##

Administrative Memos are coordinated through the Office of the Senior Vice President for Academic Affairs and Provost. For more information, contact Sam Fahmy at sfahmy@uga.edu.