

Georgetown University Security Newsletter

Produced by the University Information Security Office

October 2009

UIISO Services

Georgetown University's Information Security Office (UIISO) is committed to protecting your data and IT assets. Operating primarily behind the scenes, the office's services are widespread and support the entire campus community. These services that benefit you include:

- Reviewing departmental servers, risks and workstations
- Managing implementation and repair of remote connection and firewall services
- Responding to investigations that involve data thefts, breaches and loss

More about the UIISO and tips about how to protect your data and computers can be found at www.security.georgetown.edu.

The UIISO is a part of University Information Services (UIS). David C. Smith leads the UIISO as the University Information Security Officer.

Other departments within UIS include Network Computing Services, Academic and Information Technology Services, and Enterprise Engineering & Technology Services.

Inside this issue...

UIISO Services.....	1
Policies to know and use.....	1
October is National Cyber Security Awareness Month!.....	2

Policies to know and use

As an employee of Georgetown University, knowing and understanding the policies that protect your data and computer is vital to doing the best job you can. Losing confidential data or a computer that houses important data for your department can be embarrassing and detrimental to the university. Below are a few policies that you should review now and apply to your daily business practices in order to secure your data and computer:

Acceptable Use Policy

Designed to establish acceptable and appropriate use of computer and information systems, networks and other information technology resources at Georgetown University. More importantly, it is meant as an application of the principles of respect and reverence for every person that are at the core of Georgetown's Catholic, Jesuit identity.

Information Security Policy

Serves to create an environment that will help protect all members of the Georgetown University community (the "University") from information security threats that could compromise privacy, productivity, reputation, or intellectual property rights.

Interim Internet Business Policy

This policy sets forth the guidelines for conducting commercial activity via the Internet.

Interim Policy on the Use, Collection and Retention of Social Security Numbers by Georgetown University

Applies to all students, faculty, staff, contractors, consultants, temporary employees, guests, volunteers, and other members of the University community, including those affiliated with third parties, who use Georgetown University information resources,

Over

Policies to know and use cont.

particularly including, but not limited to, those who are entrusted with highly sensitive data and data protected by law or other Georgetown University policies.

Record Retention Policy

Applies only to documents in departments that have primary responsibility for the specific records (retention and disposition) as defined in the documentation mission statement(s), e.g., Financial Aid, Financial Affairs, Benefits, or Human Resources.

Links to these policies in their entirety can be found at <http://security.georgetown.edu/44846.html>.

October is National Cyber Security Awareness Month!

National Cyber Security Awareness Month is a joint effort between the Department of Homeland Security, the National Cyber Security Alliance and the Multi-state Information Sharing and Analysis Center. The purpose of this effort is to shed light on cyber crime and how individuals can protect their information online.

Cybercrime is growing rapidly. Cybercriminals use the computer to carry out organized methods of theft that involve getting you to give up valuable information like your name, Social Security number or bank account password. One such method that is popular on higher ed campuses today is Phishing. Phishing involves using e-mail to obtain personal information. The e-mail can be threatening or disguised to appear as a legitimate request for information from a bank or friend. Once the person responds with their information, the thief uses it to gain access to bank accounts, open credit cards or make purchases – all under the victim's identity.

Social media, on the other hand, is an open gateway for malicious software, or malware, which can be downloaded without the user's knowledge. Malware can take over a user's computer and allow hackers to quietly access the user's data.

The National Cyber Security Alliance (<http://www.staysafeonline.org>) lists the following top tips for staying safe online:

- Use strong passwords.
- Use security software tools (i.e., antivirus, antispyware) as your first line of defense
- Know who you are dealing with online.
- Back up important files. (GU tip: Use an encrypted hard drive for files that contain confidential or sensitive data.)

In addition, Georgetown's University Information Security Office (UIISO) recommends these guidelines:

- Never store confidential or sensitive data in your e-mail inbox or on an unencrypted hard drive.
- Do not use your NetID username and password for accounts outside of Georgetown. If this information is stolen, it can put the university's data at risk as well as any other data you protected with it.
- Turn off your workstation or disconnect it from the Internet when you are not working with it.
- Use your university-issued computer as your work computer only.
- Use your screen saver to lock your computer when you are away from it for any period of time.

Call the UIS Help Desk directly at 202-687-4949 if you have questions or need help protecting your information online.

University Information Security Resources

Find out more about how to protect data and your computer, technology policies and news by visiting security.georgetown.edu or sending an e-mail to security@georgetown.edu.