

Georgetown University Security Newsletter

Produced by the University Information Security Office

September 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
Security sense for teleworking.....	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>.

Security sense for teleworking

With the flu season upon us, everyone is preparing for health and human resource emergencies. Telecommuting is a popular and viable option for many university faculty and staff who have flu-like symptoms and need to work from home. Here are some common sense security precautions that we need to take in order to protect university-owned computers and data while working off campus.

1. If you are working with confidential data (i.e. Social security numbers, credit card numbers, driver's license numbers) you must have a secure, encrypted laptop. This type of laptop can only be purchased through the purchasing department. Visit the Hoya Computing page on <http://www.uis.georgetown.edu> for more information on how to purchase this type of computer.

NOTE: You must be approved to work with confidential data. Contact UIS Privacy Officer, Heidi Wachs, for questions or concerns at uispo@georgetown.edu.

2. Confidential data must be worked with in Phoenix EFS only. It can be securely stored in Phoenix EFS and GUShare.

3. Never e-mail confidential data. This type of data can only be sent to university employees via GUShare as a password-protected link.

4. If you are not using a secure or secure, encrypted computer purchased through UIS, ensure that you have the appropriate security controls in place. You can download antivirus and anti-spyware software on our website at <http://www.security.georgetown.edu>. Spyware is software that covertly gathers user information and sends it through the Internet without the user's knowledge or authorization.

5. In order to access files or folders on the Georgetown University network, you must have access to SafeConnect, or Cisco for Mac users. Request forms for both services can be found on the UIS website at <http://www.uis.georgetown.edu>.

6. Use your computer for work purposes only. Save leisure technology activities (i.e. surfing the Web, twittering, blogging) for your home computer.

7. Never open links sent to you via e-mail or IM (instant message). These links can take to you unsafe sites on the Internet that can make your computer vulnerable to malicious viruses and worms.

8. Disconnect from the Internet and "lock" your screen when your computer is not in use.

9. Contact the UIS Help Desk for technology assistance: (202) 687-4949 or help@georgetown.edu

Visit <http://www.security.georgetown.edu> for more tips on how to protect university and personally-owned computers and data while telecommuting.

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.