

# Georgetown University Security Newsletter



Produced by the University Information Security Office

January 2012

## UIISO Services

Georgetown University's Information Security Office (UIISO) is committed to protecting information and technological resources. The office's services are widespread and support the entire campus community. These services include:

- Providing consultation to departments on information security requirements and standards
- Reviewing departmental servers, applications 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](http://www.security.georgetown.edu).

The UIISO is a part of the Office of Information Services. University Information Security Officer David C. Smith leads the UIISO.

## Policies to know and use

As an employee of Georgetown University, knowing and understanding the policies that protect university information and computers 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 to you and detrimental to the university. Below are a few policies to review now and apply to your daily business practices:

### Acceptable Use Policy

This Policy defines and describes acceptable and appropriate use of computers, systems, networks and other information resources at Georgetown University for all members of the University community.

### Information Security Policy

Provides a framework to implement best practices for information security in order to secure and protect the university's information resources.

### 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

States that Social Security Numbers (SSNs) may not be captured, retained, communicated, transmitted, displayed or printed, in whole or in part, except where required by law, or permitted in accordance with the standards outlined in the policy.

## Inside this issue...

UIISO Services.....	1
Policies to know and use.....	1
Password Management 101.....	2

Over

## Policies to know and use cont.

### Record Retention Policy

Designed to ensure that necessary records and documents are adequately protected and maintained, and that records that are no longer needed or of no value are destroyed at the appropriate time. This policy is also intended to preserve University history.

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

## Password Management 101

“Weak” or easy-to-guess passwords can allow a hacker quick access to your personal information or other confidential data. In today’s world where anti-virus and anti-malware solutions abound, hackers can still gain access to sensitive information easily by guessing someone’s password. Why does happen?

For many people, it is a challenge to remember several passwords; one for a bank account, another for Amazon.com, another for access to a personal computer. The process of memorizing them can easily become frustrating. As a result, many people decide to write their passwords down on stick notes or use easy-to-remember passwords such as their mother’s maiden name or a word from the dictionary. These choices all prove a significant risk to the protection of personal and confidential information.

In order to better secure confidential, legally-protected and sensitive information, individuals need to learn how to manage the development of “strong” passwords. Following are some steps you can take to create and manage “strong” passwords:

1. Think of phrase that is meaningful to you such as, “I like red roses in summer.”
2. Take the first letters of each word in the phrase and add at least one number and a symbol:  
Ilrris9\$. **Note that your password should be at least 8 characters long.**
3. **IMPORTANT:** Your password should not be a word that can be found in the dictionary nor a common/historical phrase.

4. For each account, use a variation of that mixture to make each one unique but similar enough for you to remember without you having to write it down. (i.e., Ilrris9\$, Ilrris\$9, 9\$Ilrris)

5. If you have to write down the passwords, keep them in a locked safe, cabinet or drawer.

6. Never tell anyone your password. If you transfer to another department or leave the university, contact the UIS Help Desk (202-687-4949) to securely facilitate access to your information for an authorized individual.

7. **Never use your NetID password for other accounts! This password should only be used for NetID-protected systems such as MyAccess and GUShare.**

For more information about how to create “strong” passwords, please contact the UISO at 202-687-3031 or [security@georgetown.edu](mailto:security@georgetown.edu).

## Current Information Security News Headlines

*Google announces plans to track user activity, no opt out option (01/25/2012)*

New approach will impact all Google products

*Technology and Stalking (01/18/2012)*

Find out how to prevent stalking via technology during National Stalking Awareness Month.

*Student data in peril (12/21/2011)*

Changes to FERPA law may pose risks to student data .

Find out more details about these news topics, information about security-related policies, how to protect your data and computers, and trends in information security at <http://security.georgetown.edu>.

We are now on Facebook! Please visit us at <https://www.facebook.com/pages/Georgetown-University-Information-Security-Office/201803226551926>

## University Information Security Resources

Find out more about how to protect data and your computer, technology policies and news by visiting [security.georgetown.edu](http://security.georgetown.edu) or sending an e-mail to [security@georgetown.edu](mailto:security@georgetown.edu).