



Protecting Data at Georgetown

Georgetown University understands the importance of everyone taking a role in the protection of data. Every member of the University community is a stakeholder in the protection of the University's electronic data assets.

About the Data Security Task Force

The University-wide Data Security Task Force, led by Senior Vice President Spiros Dimolitsas, is designed to engage leaders on all campuses to identify a variety of critical business, academic and research functions that utilize confidential data. The Task Force is responsible for implementing practical changes to enable individuals to use confidential data securely. These changes involve eliminating confidential data wherever it is not absolutely necessary for a business function. Visit Sr. VP Dimolitsas' website at <http://www8.georgetown.edu/admin/svp> to review detailed information about this Task Force.

Data Security Principles

Effectively protecting confidential data at Georgetown University requires collaboration between faculty and staff to be successful. This effort demands a change in the way the University conducts business and handles confidential information. Below are some steps you can take now to protect electronic data:

Data security highlights

1. Meet with your manager or supervisor to verify whether or not using confidential data (i.e. SSNs, credit card numbers) is required for your business function. Find a list of what the University considers confidential data on the Security Resources section of security.georgetown.edu.
2. If you must work with confidential data, ensure that it is maintained on the Phoenix Enterprise File System (EFS), the University's secure storage space. Contact the University Information Services (UIS) Help Desk for more information, 202-687-4949 or help@georgetown.edu.
3. If you work with confidential data, work with it only on a University-issued desktop or a secure laptop that is encrypted.
4. Never download confidential data to a computer not issued to you by the University (i.e., home computer, public kiosk).
5. Never e-mail confidential data to anyone, even through the University e-mail system.
6. Delete files that you are not required to maintain. Refer to the University's Record Retention Policy for guidance.

General steps to ensure data security

1. Use strong passwords to protect access to your computer. Visit security.georgetown.edu to find out how to establish these types of passwords.
2. Lock your computer's screen when you are away from your PC or laptop, even if it is just for a few minutes.
3. Ensure your system is regularly updated with security patches to prevent virus attacks.
4. Do not open e-mail attachments from unknown senders. Attachments can carry malicious viruses.
5. Never click on links sent to you in an e-mail. These links can take you to a site that may put your computer at risk for virus attacks or a data breach.
6. Ensure your PC is shut down when not in use.
7. If you have an office, make sure your door is locked when you leave it for any amount of time.
8. Do not back-up confidential data on portable devices

- over -

Policies to Know and Use

The following policies are key to helping you effectively protect your data. Visit security.georgetown.edu to review and become familiar with each one in order to be a star supporter of the University Data Security effort.

Acceptable Use Policy

This policy is designed to establish acceptable and appropriate use of computer and information systems, networks and other information technology resources at Georgetown University.

Information Security Policy

This policy serves to create an environment that will help protect all members of the Georgetown University community 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. All Internet-based business transactions must be undertaken in accordance with this policy and its associated procedures.

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

This policy serves as a guide for all faculty and staff who collect, use and retain this type of confidential data as part of their day-to-day business process.

Record Retention Policy

The purpose of this policy is to ensure that necessary records and documents are adequately protected and maintained, and to ensure that records that are no longer needed are discarded at the appropriate time.

Inquiries and concerns about these policies can be directed to uispolicy@georgetown.edu.

Resources

For more information about protecting your data, technology policies, and security trends and tips, contact the University Information Security Office at security@georgetown.edu or 202-687-3031.