



THE GEORGE
WASHINGTON
UNIVERSITY
WASHINGTON DC

Responsible University Official:
Chief Information Officer
Responsible Office: Division of
Information Technology
Origination Date: April 21, 2004

INFORMATION SECURITY POLICY

Policy Statement

Maintaining the security, confidentiality, integrity, and availability of information stored in the University’s computer networks and data communications infrastructure (“University systems”) is a responsibility shared by all users of those systems. All users of University systems are responsible for protecting those resources and the information processed, stored or transmitted thereby as set forth in this policy. Violations of this policy may result in disciplinary action up to and including termination or expulsion.

Reason for Policy/Purpose

Information is a vital University asset and requires protection from unauthorized access, modification, disclosure or destruction. This policy sets forth requirements for incorporation of information security practices into daily usage of University systems.

Who Needs to Know This Policy

Faculty, staff and students

Table of Contents	Page #
Policy Statement	1
Reason for Policy/Purpose	1
Who Needs to Know This Policy.....	1
Table of Contents	1
Policy/Procedures	2
Website Address	4
Contacts.....	4
Definitions.....	4
Related Information	5
Who Approved This Policy	5
History/Revision Dates	5

Policy/Procedures

Users of University systems are responsible for protecting the information processed, stored or transmitted over or on those systems, and for incorporating the following practices into their daily activities.

A. Maintaining the Integrity of Information

The soundness and completeness of information on University systems must be maintained during its transmission, storage, generation, and/or handling. Information that is corrupted or modified may be impossible to use or lead to errors in decision-making. To maximize the integrity of data, information technology (IT) computing resource users shall adhere to the following:

1. Screen all non-text files downloaded from the Internet with anti-virus software prior to usage to minimize the risk of corruption, modification or loss of data.
2. Notify the Chief Security Officer in the Division of Information Technology (IT) immediately if passwords or other system access control mechanisms are lost, stolen or disclosed, or are suspected of being lost, stolen or disclosed.
3. Forward information pertaining to security-related problems to the Chief Security Officer immediately. DO NOT further distribute this information.
4. Use information obtained from the Internet with caution. Before using free Internet-supplied information for business decision-making purposes, corroborate and confirm the information by consulting other reliable sources.

B. Protecting Confidential Information

All members of the University community are obligated to respect and protect confidential data, and to follow the [Data Classification Security Policy](#). The University strongly discourages storage of any confidential or sensitive data on any computer or network-attached device that has not been explicitly approved by personnel from the Information Security Office within the Division of IT. IT computing resource users must adhere to the following:

1. Employ adequate encryption technology for sensitive or critical information such as educational records, Social Security Numbers, identification numbers (GWID), and credit card numbers in accordance with the [Mobile Device Security Policy](#). For specific information regarding encryption technology options, e-mail the Division of IT at infosec@gwu.edu.

INFORMATION SECURITY POLICY

2. Notify the Chief Security Officer at abuse@gwu.edu if sensitive or critical University information is lost or disclosed to unauthorized parties, if any unauthorized use of University systems has taken place, or if there is suspicion of such loss, disclosure or unauthorized use.
3. DO NOT post University material such as software, internal memos, or other non-public information on any publicly-accessible computer or website unless first approved by the appropriate authority.
4. DO NOT store Confidential Data in any computer unless the persons who have access to that computer have a legitimate need-to-know the information involved.
5. DO NOT save fixed passwords in web browsers or e-mail clients when using a University system. This may allow unauthorized users to access critical or sensitive information such as that contained in Banner, the Enterprise Accounting System or the Advancement System.
6. DO NOT distribute critical or sensitive University communications to external entities. Only distribute to internal entities on a need to know basis.
7. DO NOT establish Internet or other external network connections that could allow non-University users to gain access to University systems with critical or sensitive information unless prior approval has been received from the appropriate authority.
8. DO NOT discuss information security-related incidents with individuals outside of the University, or with those inside the University who do not have a need-to-know.

C. Utilizing Strong Passwords

Passwords are an integral part of overall security. To minimize the risk of a password being compromised and data being lost due to unauthorized access, follow the guidance in [Password Do's and Don'ts](#). For password reset instructions see <http://helpdesk.gwu.edu/helpdesk/accounts/password.html>.

D. Securing Information on Workstations

Users of University systems must adhere to the following procedures to minimize the potential for theft, misuse, or corruption of data:

1. Always use a security cable or locking device with laptop computers and secure mobile devices in accordance with the [Laptop Computer and Small Electronic Device Theft Policy](#), particularly when away from their office or work space.
2. Secure personal computers by requiring a password when the computer is turned on and when the screen saver is deactivated (public computers with no critical or sensitive information, such as those in the library or in labs, are excluded).
3. Log out of the system when finished working.

INFORMATION SECURITY POLICY

4. Use secure means to transmit confidential data. Email is not a secure means to deliver information. Information that is sent by email is at risk. Avoid using e-mail to transmit confidential data.
5. Keep all computer software up to date with the latest software maintenance releases.
6. DO NOT intentionally damage, alter, or misuse any University-owned or maintained hardware, software, or information.
7. DO NOT test security controls in place at the University or any other location (including ethical hacking) without authorization from the Information Security Office within the Division of IT.

Though not required, use of a personal firewall also is recommended (see <http://helpdesk.gwu.edu/helpdesk/security/firewall.html>)

Individual divisions, schools or departments may impose additional information security requirements beyond those set forth in this policy. For further information on reporting security incidents and implementing security practices see the Division of IT website at <http://infosec.gwu.edu/>

Website Addresses for This Policy

[GW University Policies](#)

Contacts

Subject	Contact	Email Address
Information Security	Information Security Office, Division of IT http://infosec.gwu.edu	infosec@gwu.edu
Reporting Security Incidents	Information Security Office, Division of IT	abuse@gwu.edu

Definitions

Confidential Data Confidential Data is information protected by statutes, regulations, University policies or contractual language. Managers may also designate data as Confidential. Any disclosure of Confidential Data must be authorized by senior management and/or the Senior Vice President and General Counsel. By way of illustration only, some examples of Confidential Data include:

- Medical records
- Student records and other non-public student data

INFORMATION SECURITY POLICY

- Social Security Numbers
- Bank account numbers and other personal financial information
- Personnel and/or payroll or records
- Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction.

Related Information

[Code of Conduct for Users of Computing Systems and Services](#)

[Data Classification Security Policy](#)

[Laptop Computer and Small Electronics Theft Policy](#)

[Mobile Device Security Policy](#)

[Glossary of Security Related Terms](#)

GW Helpdesk: <http://helpdesk.gwu.edu>

[Password Do's and Don'ts](#)

Password reset instructions: <http://helpdesk.gwu.edu/helpdesk/accounts/password.html>.

[What is a Security Incident?](#)

Who Approved This Policy

Louis H. Katz, Executive Vice President and Treasurer

History/Revision Dates

Origination Date: April 21, 2004

Last Amended Date: August 31, 2010

Next Review Date: September 30, 2012