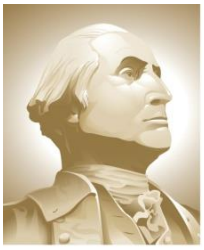

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Responsible University Official: Chief Information Officer
Responsible Office: Division of Information Technology
Last Revised Date: June 8, 2018

INFORMATION SECURITY

Policy Statement

This policy sets forth information security standards for the protection of Non-Public Information at the George Washington University. Maintaining the confidentiality, integrity, availability and regulatory compliance of Non-Public Information stored, processed, printed, and/or transmitted at the university is a requirement of all Authorized Users. This policy applies to information in any format, including electronic and hard copy. Any violations of this policy are to be reported to an individual's manager or the appropriate university official and to the IT Support Center (ITSC), and may result in disciplinary action in accordance with applicable university policies. Any questions or concerns related to this policy may be referred to the ITSC, contact information is documented below in the contacts section of this policy.

Reason for Policy

Information is a vital asset to the university. Certain types of information handled by the university are subject to legal and regulatory requirements and establish restrictions on access, disclosure, or destruction. Non-Public Information requires protection from unauthorized access, modification, disclosure or destruction.

Who is Governed by this Policy

Faculty, staff, students and all other authorized users

Table of Contents

Policy

University Information that is Non-public Must be Protected

Non-Public Information at the university is classified as Regulated or Restricted and may only be disclosed to individuals outside the university in specific situations with appropriate technical safeguards. Definitions of these classifications can be found in the Definitions section of this policy. Examples and required control standards are included in the Protecting Information: Guide to Data Storage and Custodial Practices.

Throughout its lifecycle, all Non-Public Information stored, processed and/or transmitted at the university must be protected in a manner that is consistent with contractual or legal restrictions and is reasonable and appropriate for the level of sensitivity, value, and risk that the information has to the university or members of the university community.

Information that contains data elements from multiple classifications must be protected at the highest level of information represented. For example, a document that contains Regulated and Public Information must be treated as Regulated Information.

Non-Public Information must be secured against disclosure, modification, and access by unauthorized individuals. It must be:

A. Secured at rest.
B. Secured in transit.
C. Securely destroyed in accordance with the record retention policies and university procedures.

University Computing Systems, Equipment and Networks with Non-public Information must be Secured

Any university computing system, equipment, or network, including mobile devices, that is used by Authorized Users to store, process, or transmit university Non-Public Information must be secured in a manner that is consistent with contractual or legal restrictions and is reasonable and appropriate for the level of sensitivity, value, and risk that the information has to the university or members of the university community.

Qualified information technology professionals, such as the Division of IT, must ensure that the following control standards are enabled on every university computing system, university-owned or university-approved equipment, and network with Non-Public Information:

A. Restrict physical and login access to authorized users.
B. Maintain up-to-date software patches and anti-virus software.
C. Enable and use host-based firewalls if available.
D. Perform regular security scans on the computing systems, equipment and networks.

Computing systems, equipment, and networks that contain data elements from multiple classifications must be protected at the highest level of information represented. For example, a system that stores and processes Regulated and Public Information must be treated as Regulated Information.

Authorized Users are Responsible for Non-public Information in their Custody

Authorized Users who have access to Non-Public Information are responsible for protecting that information while it is in their custody in a manner that is consistent with contractual or legal restrictions and is reasonable and appropriate given the level of sensitivity, value, or risk that the Non-Public Information has to the university or members of the university community.

Maintaining the confidentiality, integrity, availability, and regulatory compliance of Non-Public Information stored, processed, and/or transmitted at the university is a requirement of all Authorized Users.

The following requirements are applicable to all Authorized Users with access to Non-Public Information:

A. Notify their manager or the appropriate university official and the IT Support Center (ITSC) immediately if Non-Public Information, passwords or other system access control mechanisms are lost, stolen or disclosed or suspected of being lost, stolen or disclosed.

B. Restrict physical access to laptop computers when you are physically away from your office or work space, by, for example, locking the door or using security cables or locking devices.
C. Secure your computers using a screen saver or built-in lock feature when you are physically away from your office or work space.
D. Maintain possession or control of your mobile devices and apply appropriate safeguards to the extent possible to reduce the risk of theft and unauthorized access. In the event that a personal mobile device containing Non-Public Information is lost or stolen, contact the ITSC immediately.
E. Secure computers and mobile devices by requiring passwords (except for public computers with no Non-Public Information, such as those in the library or in labs). Passwords are integral to security. To minimize the risk of a password being compromised or unauthorized access, follow the IT guide for selecting secure passwords and to resetting passwords at http://identity.gwu.edu.
F. Log out when finished using a system.
G. Use secure methods to transmit Non-Public Information. University-provided email services are enabled with security features for securing emails sent to other university email addresses. Information that is sent by e-mail to non-university recipients is not encrypted and therefore at risk. Please contact the IT Support Center if you require email encryption services to external recipients.
H. Do not intentionally damage, alter or misuse any university-owned or maintained computing systems, equipment, and networks.
I. Understand and follow contractual requirements for data security that apply to themselves or data in their custody.
J. Ensure others with access to secured data follow contractual requirements.
K. Work with IT's Office of Risk and Compliance to review any data use agreements and maintain GWs ability to comply with technical requirements.
L. Do not store export-controlled data in cloud-based applications, such as Google Drive.

For further information on implementing security best practices see the Division of IT website.

Schools and Divisions are also Responsible for Non-public Information in their Custody

Schools and divisions are responsible for reviewing and determining the kinds of Non-Public Information in their custody. Schools and divisions must report Regulated Information in their custody to the Compliance Office in accordance with the Implementing Procedures for the Information Security Policy to Report Regulated Information to Compliance. Schools and divisions are also responsible for implementing appropriate managerial, operational, physical, and role-based controls, in consultation with the Division of Information Technology, for access to, use of, transmission of, and disposal of Non-Public Information in compliance with this policy.

If a school or division has questions on how specific information should be classified, they should contact the Compliance Office.

Schools and divisions will frequently have access to information protected by the Family Educational Rights and Privacy Act (i.e., information maintained by the university that personally identifies a student, with some exceptions). They are responsible for protecting that information while it is in their custody in a manner that is reasonable and appropriate.

Schools and divisions must report to the Compliance Office if they have any of the following types of Regulated Information:

A. Government-issued identification numbers, including social security numbers, driver license numbers, and passport numbers.
B. Financial account numbers, including credit card numbers and bank account numbers.
C. Personal health or medical information.
D. Data, information, or technical specifications not in the public domain that are regulated by export control laws, excluding technology or software that arises during, or results from, fundamental research under Section 734.8 of the Export Administration Regulations (EAR).

Other Information Security Roles and Responsibilities within the University

The Division of Information Technology is charged with developing information security policies.

The assistant vice president of information security and compliance services ("AVPISCS") is charged with the promotion of security awareness within the university community, as well as responsibility for the creation, maintenance, enforcement and design of mandatory and voluntary training on relevant security standards in support of this policy.

The AVPISCS receives and maintains reports of incidents, threats and malfunction that may have a security impact on the university's information systems, and receives and maintains records of actions taken or policies and procedures developed in response to such reports.

The AVPISCS assists the internal audit function, as appropriate, in conducting periodic audits to determine university compliance with this policy.

The University Compliance Office facilitates distribution of this policy, assists in the investigation of alleged violations, and administers the university's 24-hour Regulatory Compliance Help and Referral Line (1-888-508-5275), which provides a confidential method for reporting instances of suspected misconduct or violations of law or university policies.

The Office of the Senior Vice President and General Counsel reviews policies and procedures for compliance with applicable legal requirements, responds to court-ordered releases of information, and is available to advise on specific issues relating to information security.

Violations and Enforcement

Suspected violations of this policy should be reported to the IT Support Center and to the individual's manager or other appropriate university official. In accordance with the Non-Retaliation Policy, the university prohibits retaliation against a member of the university community for making a good faith report of a potential university-related legal or policy violation. Violations of this policy may result in disciplinary action up to and including termination or expulsion in accordance with applicable university policies.

Security Breaches

Actual or suspected security breaches involving Non-Public Information must be reported immediately to the ITSC. Incident response procedures will be initiated to identify the suspected breach, remediate the breach, and notify appropriate parties.

Definitions

Authorized Users: refers to any faculty, staff, student, and other authorized users of university computing systems, equipment, and networks.

Export Control: refers to any regulations governing export of certain technologies, information, and software. For the purposes of this policy, this includes International Traffic in Arms Regulations (ITAR), and the Export Administration Regulations (EAR), excluding any data that is controlled at a level higher than EAR99.

Mobile Device: is any device that can be easily transported and that has the capability to store, process, or transmit data, including but not limited to laptops, portable hard drives, USB flash drives, smartphones, and tablets.

Public Information: is information with no restrictions on access, use, or disclosure under university policy, or contract, or local, national, or international statute or regulation. Public Information includes announcements and press releases, public event information, and public directories.

Non-Public Information: is information that may only be disclosed to individuals outside the university in specific situations with appropriate technical safeguards and

may include but is not limited to information that fits into one of the following categories:

Regulated Information: is information that is protected by local, national, or international statute or regulation mandating certain restrictions. For example, student academic and financial records are regulated by the Family Educational Rights and Privacy Act (FERPA) and certain personal health information is regulated by the Health Insurance Portability and Accountability Act (HIPAA). Other forms of Regulated information include social security numbers, export controlled data and information (excluding technology or software that arises during, or results from, fundamental research under Section 734.8 of the EAR), and credit card information.

Restricted Information: is information that must be limited to appropriate university faculty, staff, students, or other authorized users with a valid business need. This information must be protected from unauthorized access, use, or disclosure due to university policies, contract, or designation, or due to proprietary or privacy considerations. Examples of Restricted Information include payroll and tax information, performance appraisals, and internal directory information.

Security Breach: is any unauthorized access, acquisition, disclosure or use of Non-Public Information.

Please see the Protecting Information: Guide to Data Storage and Custodial Practices for specific examples of Non-Public Information.

Related Information

Application and System Access Policy

Acquisition of Computer Hardware and Software Policy

Export Control Policy

GW Mail Policy

GW Web Content Policy

Health Information Privacy Policy

Implementing Procedures for the Information Security Policy to Report Regulated Information to Compliance Office

IT Support Center (ITSC)

Non-Retaliation Policy

Privacy of Student Records Policy

Record Retention Policy

Telephone/Wireless Communication Usage Policy

University Procedures

Contacts

Contact	Telephone	Email
Information Security and Compliance Services	202-994-4948	infosec@gwu.edu
IT Support Center (ITSC)	202-994-4948	ithelp@gwu.edu
Office of the Senior Vice President and General Counsel	202-994-6503	gwlegal@gwu.edu
Office of the Vice President Research / Export Control	202-994-9329	askovpr@gwu.edu

Document History

- **Last Reviewed Date:** June 13, 2018
- **Last Revised Date:** June 8, 2018
- **Policy Origination Date:** April 21, 2004

Who Approved This Policy

Louis H. Katz, Executive Vice President and Treasurer

Forrest Maltzman, Interim Provost and Executive Vice President for Academic Affairs

Beth Nolan, Senior Vice President and General Counsel

*This policy, as well as all **university policies**, are located on the **Office of Compliance's** home page.*