INFORMATION SECURITY POLICY

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 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, and may result in disciplinary action in accordance with applicable university policies.

Reason for Policy/Purpose

Information is a vital asset to the university. Non-Public Information requires protection from unauthorized access, modification, disclosure or destruction. In addition, in certain situations the university is required by law to protect particular kinds of information.

Who Needs to Know This Policy

Faculty, staff, students, and all other authorized users.

Table of Contents

<table>
<thead>
<tr>
<th>Table of Contents</th>
<th>Page #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Statement</td>
<td>1</td>
</tr>
<tr>
<td>Reason for Policy/Purpose</td>
<td>1</td>
</tr>
<tr>
<td>Who Needs to Know This Policy</td>
<td>1</td>
</tr>
<tr>
<td>Table of Contents</td>
<td>1</td>
</tr>
<tr>
<td>Policy/Procedures</td>
<td>2</td>
</tr>
<tr>
<td>Website Address for this Policy</td>
<td>5</td>
</tr>
<tr>
<td>Contacts</td>
<td>5</td>
</tr>
<tr>
<td>Definitions and Data Classification</td>
<td>6</td>
</tr>
<tr>
<td>Related Information</td>
<td>7</td>
</tr>
<tr>
<td>Who Approved This Policy</td>
<td>7</td>
</tr>
<tr>
<td>History/Revision Dates</td>
<td>7</td>
</tr>
</tbody>
</table>
Policy/Procedures

1. UNIVERSITY INFORMATION THAT IS NON PUBLIC MUST BE PROTECTED

Non Public Information at the university is classified as Regulated or Restricted. 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:

- Secured at rest.
- Secured in transit.
- Securely destroyed in accordance with record retention policies and university procedures.

2. UNIVERSITY COMPUTING SYSTEMS, EQUIPMENT, AND NETWORKS WITH NON PUBLIC INFORMATION MUST BE SECURED

Any university computing system, equipment, or network 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:
INFORMATION SECURITY POLICY

• Restrict physical and login access to authorized users.
• Maintain up-to-date software patches and anti-virus software.
• Enable and use host-based firewalls if available.
• 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.

3. 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:

• Notify their manager or the appropriate university official and the IT Support Center 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.
• 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.
• Secure your computers using a screen saver or built-in lock feature when you are physically away from your office or work space.
• Maintain possession or control of your mobile devices to the extent possible to reduce the risk of theft and unauthorized access.
• 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.
• Log out when finished using a system.
• 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.

• Do not intentionally damage, alter or misuse any university-owned or
maintained computing systems, equipment, and networks.

For further information on reporting security incidents and implementing security
practices see the Division of IT website at http://it.gwu.edu.

4. 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. If a school or division has questions on
how specific information should be classified, they should contact the
Compliance and Privacy 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 and Privacy Office if they
have any of the following types of Regulated Information:

• Government-issued identification numbers, including social security
  numbers, driver license numbers, and passport numbers.
• Financial account numbers, including credit card numbers and bank
  account numbers.
• Personal health or medical information.

Schools and divisions are also responsible for implementing appropriate
managerial, operational, physical, and role-based controls for access to, use of,
transmission of, and disposal of Non-Public Information in compliance with this
policy.

5. 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 & Privacy 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.

6. 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.

**Website Address for This Policy**

GW University Policies

**Contacts**

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>Information Security and Compliance Services, Division of Information Technology</td>
<td><a href="mailto:infosec@gwu.edu">infosec@gwu.edu</a></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Definitions and Data Classification

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

**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** 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 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.

Please see the [Protecting Information: Guide to Data Storage and Custodial Practices](#) for specific examples of Non-Public Information.
Related Information

System and Individual Responsibilities
Application and System Access Policy
Acquisition of Computer Hardware and Software Policy
GW Web Content Policy
Laptop Computer and Small Electronics Theft Policy
Security Breaches Involving Non-Public Personal Information
GW Mail Policy
Telephone/Wireless Communication Usage Policy
IT Support Center (ITSC)

Who Approved This Policy

Louis H. Katz, Executive Vice President and Treasurer
Steven Lerman, Provost and Executive Vice President for Academic Affairs
Beth Nolan, Senior Vice President and General Counsel

History/Revision Dates

Origination Date: April 21, 2004
Last Amended Date: November 26, 2014
Next Review Date: November 30, 2016