SECURITY BREACHES INVOLVING
NON-PUBLIC PERSONAL INFORMATION

Policy Statement

Actual or suspected Security Breaches involving non-public personal information must be reported immediately to the IT Support Center (ITSC). Once the nature and extent of the breach has been determined, the university will notify affected individuals as necessary. Violations of this policy may lead to disciplinary action up to and including termination.

Reason for Policy/Purpose

Non-Public personal information compromised by a Security Breach may lead to identity theft and invasion of privacy for affected individuals. In the event of such a breach, the university may be required by law to take specific action.

Who Needs to Know This Policy

Faculty, staff, students and contractors

Table of Contents

Policy Statement ..................................................................................................1
Reason for Policy/Purpose ...................................................................................1
Who Needs to Know This Policy .........................................................................1
Table of Contents .................................................................................................1
Policy/Procedures ................................................................................................2
Website Address ..................................................................................................2
Contacts ................................................................................................................2
Definitions .............................................................................................................2
Related Information ............................................................................................2
Who Approved This Policy .................................................................................3
History/Revision Dates ........................................................................................3
Policy/Procedures

All faculty, staff, students, and other authorized individuals that process, store, transmit or otherwise use Non-Public personal information entrusted to the university are required to immediately notify the ITSC in the event of a suspected or actual breach of the confidentiality of such information.

Personal information that is lawfully available to the public from a government record (considered public information) is not subject to this breach notification policy. In addition, personal information rendered unreadable to an unauthorized party through use of encryption is not subject to this breach notification policy. Accordingly, all computers and other electronic data storage devices where non-public, personally identifiable information may reside must be secured in accordance with the Information Security Policy.

Website Address for This Policy

GW University Policies

Contacts

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
<th>Telephone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Breach Notifications</td>
<td>Information Technology</td>
<td>(202) 994-4948</td>
<td><a href="mailto:ithelp@gwu.edu">ithelp@gwu.edu</a></td>
</tr>
</tbody>
</table>

Definitions

For Definitions of Public Information and Non-Public Information and related guidance, please consult the Information Security Policy.

Security Breach

Unauthorized access to or the use of personal information.

Related Information

Information Security Policy
D.C. Consumer Personal Information Security Breach Notification Act
Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. No. 106-102
SECURITY BREACHES INVOLVING NON-PUBLIC PERSONAL INFORMATION

Health Insurance Portability and Accountability Act, P.L. 104-191
Security Breach Notification Laws by State

Who Approved This Policy

Louis H. Katz, Executive Vice President and Treasurer
Beth Nolan, Senior Vice President and General Counsel

History/Revision Dates

Origination Date: October 3, 2007
Last Amended Date: June 30, 2014
Next Review Date: March 31, 2016