Electronic Data Security Breach Reporting and Response Policy

Effective Date: March 1, 2007

Policy Statement
Any suspected or confirmed compromise of protected electronic data must be reported to the Information Technology Security and Policy Office and to the local system administrator.

The Office of the General Counsel is responsible for overseeing legal compliance in the case of a compromise of protected data.

Any individual responsible for a system containing protected data that may have been compromised must take immediate steps to secure that system and preserve it without change according to the appended procedure.

Reason(s) for the Policy
Federal and state statutes require the notification of governmental agencies and affected individuals when there is reason to believe that legally protected data held by or for the University was acquired by someone without valid authorization.

This policy establishes measures that must be taken to prepare and respond to data breach incidents including the determination of the systems or applications affected, if data has been corrupted, what specific data was compromised, and what actions are required for forensic investigation and legal compliance.

Primary Policy to Which This Policy Responds
This policy responds to all applicable federal and state statutes pertaining to breaches of the security of protected, electronic data. These statutes include, but are not limited to, the New York State Information Security Breach and Notification Act, the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the PCI Data Security Standard (PCI DSS).

Responsible University Officer and Office
Compliance Responsibility: Office of the General Counsel
Policy and Technical Support: Columbia University Information Technology Security Office

Revision History
This policy was established in February 14, 2007. This policy was updated in May 2011 to include PCI DSS in the list of statues.

Who is Governed by This Policy
This policy applies to all individuals who access, use, or control a University information technology resource. Those individuals covered include, but are not limited to, staff, faculty, students, those working on behalf of the University, guests, and visitors.

Electronic Data Security Breach Reporting and Response Policy- 05092011.doc
Who Should Know This Policy
All individuals, particularly those with broad management responsibilities including Senior Executive Officers, Deans, Vice Presidents, Data Stewards, Chairs, Directors, Senior Administrative Officers, Departmental Administrators, Researchers, and IT support staff

Exclusions & Special Situations
None

Policy Text
Columbia University is committed to compliance with all applicable legal statutes pertaining to the breach of security of protected electronic data. Compliance includes all actions and notifications defined by the governing federal or state statutes as well as University policies associated with data security and privacy.

Responsibilities

Reporting
It is the responsibility of all users to report promptly all suspected or confirmed breaches of sensitive electronic data to one of the contacts listed below in “Contacts”

Compliance and University Response
The University has established a University Response Team to deal with data breaches. The core University Response Team (URT) consists of representatives of the following units:

- Columbia University Information Technology Security Office
- General Counsel
- Public Safety
- Public Affairs
- Human Resources

The Chief Information Security Officer, her delegate, or other cognizant representative of the URT will convene the URT upon receiving a report of a possible breach. An individual will be appointed to manage the ensuing investigation.

The General Counsel is responsible for all legal issues associated with an actual or suspected compromise of protected data.

The Office of Public Safety is responsible for all contacts with law enforcement and for non-technical aspects of any investigation.

The Office of Public Affairs is responsible for all internal and external communications and media relations.

Human Resources will advice on personnel issues and communications to University staff.
The University Response Team will establish detailed internal procedures for compliance, external and internal communications, and oversight of the investigation and technical support associated with a suspected or actual breach of protected electronic data.

The core URT will call on any necessary additional offices and resources required to carry out the investigation and remediation of any breach. This expanded URT will be responsible for the investigation of the incident and any technical support required. Incident team members will include representatives of affected data owners, any other units responsible for the devices or data involved, and any associated information technology or investigative resources.

The following major data owning units will participate in the development of procedures for an investigation, in periodic reviews of these procedures and in regular training.

<table>
<thead>
<tr>
<th>Unit</th>
<th>Area of Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Counsel</td>
<td>Legal compliance</td>
</tr>
<tr>
<td>Public Safety</td>
<td>Investigation</td>
</tr>
<tr>
<td>Public Affairs</td>
<td>Communications</td>
</tr>
<tr>
<td>CUIT</td>
<td>Technical support</td>
</tr>
<tr>
<td>Internal Audit</td>
<td>Audit issues</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Risk issues</td>
</tr>
<tr>
<td>Provost</td>
<td>Academic data</td>
</tr>
<tr>
<td>Finance</td>
<td>Financial data</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Human resources data</td>
</tr>
<tr>
<td>Student Services</td>
<td>Student data</td>
</tr>
<tr>
<td>UDAR</td>
<td>Alumni/development data</td>
</tr>
<tr>
<td>Libraries</td>
<td>Libraries data</td>
</tr>
<tr>
<td>Research</td>
<td>Research data</td>
</tr>
<tr>
<td>CUMC</td>
<td>CUMC data</td>
</tr>
</tbody>
</table>

Definitions

Breach--The actual or probable exposure of protected data to an unauthorized person by any means, including the unauthorized action of a person authorized to access the data.

Device -- Devices include computers and any other equipment such as PDAs, smartphones (TreoS, Blackberry, Palm devices), copiers, printers, disk drives, diskettes, CDs, USB (“thumb”) drives, or other devices that store or display data.

Incident--A report of a possible breach and its follow-up investigation and remediation.

User--Any individual who accesses, uses, or controls a University electronic information resource. Users include, but are not limited to, staff, faculty, students, those working on behalf of the University, guests, and visitors.
Sensitive/personal/protected data/information - Credit card numbers or any information in or sourced from electronic information systems likely to result in an identity theft, for example a unique identifier (name, UNI, address, dates of birth, phone number) in combination with Social Security Numbers, bank account information, driver's license numbers, etc.

Contacts
To report a possible data breach:
  * Columbia University Information Technology
  * Web: [http://www.columbia.edu/cuit/support/](http://www.columbia.edu/cuit/support/)
  * Email: security@columbia.edu
  * Telephone: 212-854-1919

For legal issues:
  * General Counsel
  * Telephone: 212-854-4974

Cross References to Related Policies

Electronic Information Resources Security

See the Administrative Policy Library Information Technology (CUIT) section: [http://policylibrary.columbia.edu/node_browser/nodes_by_category/term/7](http://policylibrary.columbia.edu/node_browser/nodes_by_category/term/7)