

Electronic Data Security Breach Reporting and Response Policy

Appendix A

A breach of security means the unauthorized acquisition of data that compromises the security, confidentiality or integrity of personal/sensitive/protected information.

Compromise of systems means an apparent exploit of vulnerability in system software, hardware or a procedural weakness that may provide unauthorized access to the system environment.

Any unit or individual aware of a potential breach of security or compromise of systems containing personal/sensitive /protected information must report to the Information Technology Security and Policy Office and to the local system administrator.

Initial Procedures

Upon notification of a breach, the University Response Team is responsible for:

- Designation of the URT incident leader and incident team to manage the investigation
- Initial evaluation of whether a breach has occurred
- If a breach has occurred, notification of University executives , including at least:
 - Senior Executive Vice President
 - Provost
 - General Counsel
 - EVP for Student and Administrative Services
 - EVP for Development and Alumni Relations
 - EVP for Health and Biomedical Science
 - EVP for Research
 - VP for Information Technology
- Conduct of the investigation.
- Appropriate notification to individuals whose data was compromised or believed to have been compromised
- Appropriate notification of governmental agencies

Securing a Possibly Compromised System

Step 1: Remove the system from the network

Step 2: Pull plug on system – do not go through normal shutdown procedure
– do not edit or delete any information on the system.

Step 3: Contact CUIT Security as note above or send to security@columbia.edu for information and help on what to do next. Make sure to include your phone number – we will want to speak with you.

Governing Laws

The following are major laws which require reporting of breaches and notifications of governmental agencies and affected individuals:

New York State Information Security Breach and Notification Act

Summary: <http://assembly.state.ny.us/leg/?bn=A04254>

Text: <http://assembly.state.ny.us/leg/?bn=A04254&sh=t>

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99). Regulates the keeping and dissemination of student records at all institutions that receive federal funds or who have students receiving federal funds. Protected information includes social security numbers, race/ethnicity or gender.

<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

The Gramm-Leach Bliley Act (Financial Services Modernization Act of 1999)

Governs the collection, safeguarding, and disclosure of customers' personal financial information.

<http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Requires securing all protected health information (PHI). It establishes standards for information privacy, electronic transactions, security, and unique identifiers for individuals.

http://www.cms.hhs.gov/HIPAAGenInfo/02_TheHIPAALawandRelated%20Information.asp#ToPage