Breach of Private Information Procedure, *V07.18.2006*

PURPOSE

The purpose of this protocol is to outline the steps that must be followed once a possible breach of personal privacy is identified.

PROCEDURE

When a possible privacy breach has occurred, immediate action should be taken. The following procedure will assist in controlling the situation and ensuring that, if a breach of privacy occurs, steps will be taken to minimize the risks of a similar breach from happening again.

Step 1) Confirm and Contain. Confirm the validity of the suspected information breach. If the breach can be reasonably ascertained, containment should occur immediately. Containment includes, but is not limited to, disconnection of the host (e.g., server or other device) from the network or shutting down an application. Care should be taken not to destroy data, but to preserve it without any form of network connection. Re-connection of the device to the network is not allowed until such time as remedial steps have been completed and re-connection is specifically approved by the University Chief Information Officer or the University Chief Information Security Officer.

Step 2) Report. The following individuals are required to be informed as soon as possible:

a) The College President or Central Office Vice President for the effected area.
b) The College Legal Affairs Department and Central Office, Office of General Counsel.
c) The College or Central Office department head from which the information was breached.
d) The College Chief Information Officer or IT Director.
e) University Chief Information Officer
f) University Chief Information Security Officer.

The report should indicate whose personal information was disclosed, to whom it was disclosed, when it was disclosed, how it was disclosed/accessed, and what steps have been taken in response to the disclosure.

Step 3a) Retrieve. Any documents or contents of electronic documents that have been disclosed to, or taken by, an unauthorized recipient should immediately be retrieved and/or secured (electronic documents or paper documents in facsimile form or printed e-mail messages) or taken offline. Documents, in any form, should not be destroyed until specific instruction is received. This may require personal attention to secure the documents and return them to their original location, remove them permanently from electronic storage, or send them to the intended authorized recipient.

Step 3b) Remove. Private information taken offline (Step 1 and Step 3a) may still be accessible and discoverable on the Internet via Internet Search engines (e.g., Google).

The usual time periods for information to be removed by the search engines through routine web crawling techniques is too elongated (e.g., weeks) and requests must be made to remove the information from search engine indexes and cache directly to the Internet Search engines companies. These requests must be made as quickly as possible. Support request procedures for the major search engines are available as links at security.cuny.edu under Security Resources. This step will be coordinated with the University Chief Information Security Officer.

Step 4) Notify. In cases where the breach results in the disclosure of personal information, New York law may require that the University notify the individuals affected.

Determination of the reporting requirements will be made by the Office of the General Counsel with the College Legal Affairs Designee on a case-by-case basis. All notification letters must be reviewed the Office of the General Counsel prior to being sent. Notification letters should include the information sheet from the Federal Trade Commission entitled "What to do if your personal information has been compromised."

Step 5) Investigate. The College's Legal Affairs Department, the Vice President for the affected area, the College CIO or IT Director, The University Chief Information Officer and The University Chief Information Security Officer will investigate the details of any breach, for the purpose of determining and recording all the relevant facts concerning the breach and making recommendations. The objectives of this investigation should include: a review of the circumstances surrounding the event as well as the adequacy of existing policies and procedures in protecting personal private information.

Step 6) Management Review. The College Legal Affairs Department with the Vice President of the effected area will document and report the detail of the breach of privacy and remedial steps to the President of the College. The Legal Affairs Department in collaboration with the University Chief Information Officer will report on recommendations and actions to the appropriate parties within the Chancellor's office. Additional incident reporting will occur by the University Chief Information Security Officer to comply with internal incident reporting policies.

CONCLUSION

A breach of private information is a serious matter. College staff and faculty and Central Office departments must make every reasonable effort to prevent breaches from occurring. If one does occur, staff and faculty must ensure that compliance with this procedure is followed.