Private Information Advisory

Protecting the personal private information of our students, faculty and staff is of utmost importance to the University. Exercising due diligence to prevent unauthorized disclosure of private information is the continuous responsibility of all constituents who maintain, use, distribute or share such information – regardless of the form in which the information is stored – electronic or paper. Not only does it make sense to protect the private information belonging to others, such practices are mandated by Federal and State Laws.

Unauthorized disclosure of private information can have a severe adverse impact on the financial profile of our constituents and could lead to significant embarrassment to the University and to those directly responsible for the disclosure. New State Law requires individual notification of those affected and there are other internal University and external reporting requirements.

When private information is disclosed to the Internet and made easily accessible through Internet search engines, it is extremely difficult to remove the private information in an expedited manner and there can be no assurance that this information is no longer accessible through lesser known or privately engineered Internet search engines in far offshore locations. In addition, once the information is published to the Internet it could have been saved to local computers intended to be used for less than ethical reasons. Similar risks can be illustrated if information is stolen or hacked from presumably secure computers.

The CUNY Information Security Management Office has published direct links of major Internet search engines to request the removal of information from their index and cache. Additional resources provide instructions on how to prevent the search engines from collecting your information. Please refer to security.cuny.edu under Security Resources.

Please be aware that this does not prevent the possible theft of information through unethical hacking or poorly implemented access controls. Only prudent security configuration, control over who has access, and maintaining current software patch levels can minimize these risks.

In the event of an unauthorized disclosure (or suspected disclosure) of private information the Breach of Private Information procedure must be followed. This procedure is available at security.cuny.edu under Security Policies.

Examples of private information includes, but is not limited to, social security numbers, driver's license or non driver identification card numbers, credit, debit, or other financial account numbers in combination with access codes permitting access to an individual's accounts. The disclosure of private information in combination with personal identifiers such as an individual's name must be protected.

Please exercise the following security measures:

1. When files contain private information do not allow the files to be searchable and publishable to the Internet search engines.

2. When files include private information and are to be stored on any type of portable device (including a desktop computer) or transmitted, the files must be encrypted and password protected.

3. Do not include social security numbers on displays, reports or spreadsheets unless absolutely necessary. When unique identification is desirable mask the social security number to include only the last four numbers or mask the entire entry if social security number is used as a data entry field for authentication.

4. Delete files and cross-shred documents when no long needed.

5. Do not leave your computer unattended and accessible to others. Either logout or use the screen lock features of your computer.

6. Do not share your password with anyone, do not write it down, and change it regularly.

7. Computer operating systems and other programs should be maintained to current software security patch levels.

8. Keep access to information aligned with individual job responsibilities.

Identity theft is unfortunately very common, very costly and can be damaging to our constituents. Please protect the private information of others as if it were your own.

This advisory is also available at security.cuny.edu under Security Advisories.