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

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.