Data Protection for Mobile Devices

To avoid the risk of identity theft and other confidentiality breaches, it is vital that appropriate data protection measures be taken to protect the personal information of CUNY employees and students.

The University’s IT Security Procedures require that non-public University information, including social security numbers, protected health information, and confidential financial, administrative and research data must be encrypted and password protected when present on laptops and other mobile devices such as tablets, smartphones and USB storage devices. Because these portable devices are more susceptible to loss or theft, the failure to encrypt and password-protect such information puts this information at great risk.

To avoid potential breaches, it is best not to store confidential data on mobile devices. When there is a University need to do so, however, encryption software for both PC and Macintosh is centrally licensed for use by CUNY employees at no additional cost. This encryption software can be obtained and installed through your campus IT department.

Information breaches are costly in terms of University resources, expense, legal exposure and loss of institutional reputation. Even more importantly, they undermine the trust which our faculty, staff and students place in CUNY to maintain the confidentiality of their personal, academic and professional information in a secure and appropriate manner.

Published: August 2014

The above is derived from a memo entitled “Data Protection for Mobile Devices” issued July 29, 2013 by Senior Vice Chancellor and General Counsel, Frederick Schaffer, and Associate Vice Chancellor and University Chief Information Officer, Brian Cohen