





**Associate Vice Chancellor
for Technology and CIO**

395 Hudson Street
New York, NY 10014
tel: 212-541-0365

Date: July 29, 2013

To: Council of Presidents
Academic Council
Council of Vice Presidents of Administration
UFS Chair
IT Steering Committee
Enrollment Management Council
Council of Registrars
Council of Bursars
Council of Vice Presidents of Student Affairs
IRB Members
College Research Integrity Officers

From: Frederick Schaffer, Senior Vice Chancellor and General Counsel 
Brian Cohen, Associate Vice Chancellor and University Chief Information Officer 

Subject: Data Protection for Mobile Devices

The University has experienced several incidents in which University laptops were stolen containing personally identifiable information of CUNY employees or students. Those laptops also lacked appropriate data protection for that information, putting the information at risk of identity theft and other confidentiality breaches.

We must remind you that 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, McAfee disk 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.

Please share this important information with your constituent audiences.

cc: Chancellor's Cabinet
Robert Berlinger, Acting Chief Information Security Officer