BMCC INFORMATION SECURITY STANDARDS AND POLICIES

Borough of Manhattan Community College is responsible for ensuring that its network and computer resources are safe from security breaches, to prevent the loss of non-public University information to unauthorized persons, and to maintain the operational integrity of the systems themselves so that they can be used for the business of the College. Therefore, we have established a set of security policies, congruent with NY State and CUNY policies and regulations, to promote the safeguarding of the College's information technology assets and any non-public data stored therein.

In addition to regular system patches and upgrades, host-based computer security suites, and network-based security tools, BMCC's networks and the computers that connect to them must adhere to the following:

1. Non-public University information such as social security number, grades, etc. must not be sent in email text, email attachments, or be left unencrypted on devices subject to theft or loss.
2. Encrypt all sensitive data, either by saving it to your network drive's My Documents folder or by using encryption software. The University licenses McAfee encryption software for our use.
3. Maintain access on a strict need-to-know basis and store non-public University information on a secure server rather than on end point devices such as desktops, laptops, or flash drives.
4. Reports produced containing full social security numbers, except where required for regulatory compliance requirements should be modified to include only the last four digits.
5. Strictly controlling access to SSNs, cleaning out old data, storing data with SSNs on secure file servers and using encryption where full SSN access is absolutely necessary also helps to reduce risk of public disclosure.
6. Lock your computer every time you leave your desk. Desktops managed by the Computer Center are configured for a screen saver with preset timeout and password protection, and their login passwords must be changed every 90 days. Computers connected to our networks must be accessible only via individual login credentials, and standalone computers should be accessible in that way only, also. This helps in the establishment of forensic trails in case someone uses these computers for illicit activities, and provides custom help to users who encounter difficulties using our systems.
7. Back up your data regularly. Data stored in the My Documents folder on networked computers managed by the Computer Center will be automatically backed up periodically.
8. Be cautious when you print or copy sensitive non-public information — do not leave it in an open area, and shred it when not in use.
9. CUNY security policies, procedures, and advisories can be found at http://security.cuny.edu. Report violations and issues when they occur to the College Computer Center Help Desk.

10. Do not give out your social security number to any College department unless it is absolutely necessary.
11. Peer-to-Peer (P2P) applications, such as BitTorrent, are prohibited from use and network facilities are in place to block their use to the Internet. However, such applications evolve rapidly, and blocking technologies often fail to prevent P2P connectivity. Remember that using such software, or for that matter installing any software obtained from untrusted sources, can open your computer to infection and compromise by unscrupulous parties for anything from plain malicious interference to theft of personal data.
12. Computers found to be creating a hazard to the integrity of our networks, or that fail network access control status checks, will be placed in a quarantine network – if possible – until any issues can be addressed and resolved. If, for some reason, a staff computer cannot be networked at all, Help Desk technicians will attempt a standalone fix. In the case of Instructional computers, Instructional Technology IT personnel will attempt the fix.
13. Laptops issued by the College for use by Administrative or Instructional staff, when use may include storing non-public University data on the laptop's local hard drive, must have their hard drives encrypted. The Computer Center is in the process of implementing this policy with McAfee software, and in the near-future, all newly-issued laptops will be suitably configured. We will implement a system through which laptops that have already been issued will be encrypted.

If you encounter a security-related problem, or have a question about these policies, call the BMCC Help Desk as your first point of contact at 212-220-8379.