Approved by I.T. Board of Advisors 10/18/2010
Reviewed by College counsel 11/08/2010

Manhattan College

Data Security Policy

Manhattan College recognizes that certain data maintained by it and accessible by authorized employees using College systems involves confidential and/or sensitive information and/or personally identifiable information. As such, special attention is required in order to maintain security and privacy for these restricted data elements. These data elements include:

- *Social Security numbers*
- *Credit or debit card numbers*
- *Bank account/financial account numbers*
- *Driver's license numbers*
- *State/Federal ID card numbers*
- *Student loan information*
- *Passport numbers*
- *Individually identifiable donor data*
- *Protected health information*
- *Individually identifiable health information*
- *Passphrases/passwords, PINs, and security/access codes*
- *FERPA protected educational records (see below)*

Sometimes, but not always, one of the above data elements needs to be accompanied by an individual's name or other personally identifiable information in order to result in harm if released to 3rd parties inadvertently or without prior authorization. However, as a general rule and in accordance with College policy, none of the above listed data elements shall be released to third parties or even to other College offices or employees without prior authorization. College employees are also precluded from storing any of these data on personal *(non-College owned)* systems including desktop and/or notebook computers, portable storage devices *(e.g. USB "thumb drives")* or telecommunication devices *(e.g. PDAs, data phones)*

No member of the Manhattan College community is permitted to electronically store or maintain any of the above listed data except as required as part of their job description and authorized by their supervisor. When required and authorized, such data shall only be

stored in or on College-owned systems. The Controller's Office in cooperation with Computer Services must approve the use of any system or application that electronically processes, stores, or transmits credit card data.

The use of paper documents containing credit card data is strongly discouraged. If used, such documents shall be secured in a locked office and/or stored in a locked cabinet. In an open office environment paper documents shall be stored in locked cabinets. Paper documents should not be left in an unsecured office after work hours.

All credit card processing (e.g., online, phone, mail, over-the-counter, card-swiping) must be reviewed and approved by the College's Controller.

The following confidential data types shall only be electronically stored on a College managed server and can only be accessed from a College managed computer.

- Social Security number
- Driver's license number
- State/Federal ID card number
- Passport number
- Financial account numbers (checking, savings, brokerage, CD, etc.)

Should an exception be necessary in order to carry out the business of the College, the user shall obtain written approval from his/her supervisor who shall notify the appropriate area Vice President.

It is recommended that, when required and necessary for the transaction of College business, all confidential, sensitive and/or restricted data be electronically stored or accessed from the one of the following list of devices, in order of preference: College's ERP system *(presently Sungard Banner),* College managed servers, College owned and managed desktop computers, College owned encrypted laptops/notebooks.

When handling physical documents containing any confidential, sensitive and/or restricted data types, the documents must be in your possession at all times; otherwise they should be stored in a secure location *(e.g. room, file cabinet, etc.)* to which only specifically approved individuals have access through lock and key. When the information is no longer needed, the physical documents shall be shredded using a College-approved device prior to being discarded; or destroyed by a College-approved facility.

Confidential, sensitive and/or restricted data shall not be taken or stored off-campus unless the user is specifically authorized to do so by a Vice President and only for good and justifiable cause.

In event that such data is found in unauthorized locations, a Security officer will follow-up with the responsible Vice President to remedy the situation.

These data shall also not be transmitted through any electronic messaging *(i.e. email, instant messaging, text messaging)* even to other authorized users.

All faculty, staff, and student JasperNet account passwords must be complex. A password must meet the following criteria:

- Length at least 8 characters
- Include at least 3 of the following character types:
  - Lower case letter [a-z]
  - Upper case letter [A-Z]
  - Number [0-9]
  - Symbol [~!@#$%^&-_ etc...]

When selecting a password, please avoid using dictionary words or common patterns such as "abc" or "123". When using common words, break them up and separate by other characters (paSS737WOrd).

Passwords should not be written down or displayed. Passwords shall not be shared with others.

Users who are authorized to access or maintain confidential, sensitive or restricted data must ensure that it is protected to the extent required by College policy or law after they obtain it. All such data users are expected to:

- Access data only in their conduct of College business.
- Request only the minimum amount of data necessary to perform their College business.
- Respect the confidentiality and privacy of individuals whose records they may access.
- Observe any ethical restrictions that apply to data to which they have access.
- Know and abide by applicable laws or policies with respect to access, use, or disclosure of data.

Compliance with these data protection policies is the responsibility of all members of the College community. Violations of these policies will be dealt with seriously and will include sanctions, up to and including termination of employment. Users suspected of violating these policies may be temporarily denied access to the data as well as College information technology resources during investigation of any alleged abuse. Violations may also be subject to prosecution by state and federal authorities. Suspected violations of Manhattan College's data security policy must be reported as follows:

For Faculty: to the Executive Vice-President & Provost

For Employees: to the Vice-President for Human Resources

For Students: first to the Dean of the School in which the student is enrolled who in turn shall notify the Executive Vice-President & Provost

For Vice-Presidents: to the College President

For the President: to the Chairperson, Board of Trustees

FERPA

This provision supplements the College's FERPA policy maintained by the Registrar's Office.

The Family Educational Rights and Privacy Act (FERPA) of 1974 applies to personally identifiable education records. The term "education records" is broadly defined by FERPA to describe records maintained by or for the College (or a party acting for the College), directly related to a student, and containing personally identifiable information. This includes transcripts, papers, exams, student databases, class schedules, financial records, correspondence, email, and handwritten notations. Education Records may be maintained in any medium. Education records do not include law enforcement or physician treatment records, which may be protected by other laws or regulations. "Personally identifiable" is defined as information that would reveal the identity of a student or make the student's identity easily traceable.

Anyone who maintains or accesses education records on behalf of the College is responsible for using those records in compliance with FERPA and this policy.

As a general rule, anyone releasing education records (other than FERPA directory information) to a third party (i.e., someone other than to the student or a College official with a legitimate interest in the information) without the consent of the student must first be authorized to make such a disclosure and then maintain a record of the request for and/or release of this information. The record will indicate the name of the party making the request, any additional party to whom it may be re-released, and the legitimate interest the party had in requesting or obtaining the information.

FERPA does *not* prohibit instructors from having students use third-party tools as part of the course activities. Content created by students when using such tools to fulfill course requirements (e.g., creating blogs on WordPress or posting videos to YouTube) does not constitute "student education records" under FERPA. However, copies of such records that are maintained by an instructor in his or her own files *do* constitute FERPA-protected

"education records." Instructors submitting student work for review of its originality (e.g. turnitin.com) shall redact any personal identifiers if submitting the work themselves.

Contact the Registrar and/or Associate Provost should any clarification be required as to when or if FERPA protected education records may be released without prior consent.

Breaches

Any State Entity, Person or Business which does business in New York and that owns or maintains private information must comply with the *Security Breach and Notification **Act*** (Chapter 442 and 491 of the Laws of 2005). These Chapter Laws are codified in Section 208 of the State Technology Law (STL) and Section 899-aa of the General Business Law (GBL). The law applies to what New York State deems to be "Private Information" which is defined as: an individual's unencrypted personal information + 1 or more of the following:

- Social security #
- Driver's license number or non-driver ID
- Account number, credit or debit card number + security code, access code or password which permits access to an individual's financial account

and requires that the College disclose to a New York resident when their private information was, or is reasonably believed to have been, acquired by a person without valid authorization. Such notice must be provided in the most expedient time possible without unreasonable delay and after necessary measures to determine the scope of the breach and restore integrity have been undertaken. A delay is possible if law enforcement determines that such notice would impede a criminal investigation.

A breach of the security under the NY law shall mean unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. Good faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others:

- indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
- indications that the information has been downloaded or copied; or

- indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

The College shall comply with the *Security Breach and Notification Act* upon receipt of notice pursuant to this policy or other actual knowledge that would trigger the required notice.

—