Identity Theft Prevention Policy
(“Red Flags Rule”)

Policy Statement

U.S. Congress has provided protection for consumers from identity theft by enacting the Fair and Accurate Credit Act (“FACTA”), Fair Credit Reporting Act (“FCRA”), Red Flags Rule, and the Red Flag Clarification Act of 2010. The risk to the College, its employees and students from data loss and identity theft is a significant concern that can only be reduced through the concerted efforts of College personnel and affiliated third parties by establishing an Identity Theft Prevention Policy.

There are three sections of the Red Flags Rule: (1) 16 C.F.R. § 681.1 users of consumer reports; (2) 16 C.F.R. § 681.2 financial institutions and creditors; and (3) 16 C.F.R. § 681.3 issuers of debit or credit cards.

The College is a “user of consumer reports” but not a “creditor” or “issuer of debit or credit cards.” With the adoption of the Red Flag Clarification Act, the College adopts this Policy to:

- Approve and establish an Identity Theft Prevention Policy;
- Identify, prevent and mitigate identity theft in compliance with the Rules;
- Appoint an Identity Theft Prevention Policy (“Policy”) Administrator who has primary responsibility for oversight of the Policy;
- Ensure periodic updates that reflect changes in associated risks.
Entities Affected by the Policy

All College students, employees, and other constituents, including vendors and contractors, having access to Personally Identifying Information as well as any Covered Account.

Policy Background

No comprehensive policy addressing this issue previously existed.

Policy Procedures

I. OVERVIEW

A Red Flags Rule Policy must include four basic elements within a framework designed to address the threat of Identity Theft:

- Identify potential Red Flags (suspicious events, patterns or practices) for Covered Accounts and Records that contain PII that the College offers or maintains; Detect Red Flags;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft;
- Ensure that the Policy is updated periodically to reflect changes in risks to the College and to the affected entities

II. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the College considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and previous experience with Identity Theft. The following Red Flags are examples of potential indicators of fraud; this list is not exhaustive. Any time a Red Flag, or a situation closely resembling a Red Flag, is apparent, it should be investigated for verification.

- Alerts, Notifications, and Warnings from Credit Reporting Agencies
  - Examples:
    - Report of fraud accompanying a credit report;
    - Notice or report from a credit agency of a credit freeze on an individual;
    - Notice or report from a credit agency of an active duty alert for an individual;
    - Receipt of a notice of address discrepancy in response to a credit report request; or
- Indication from a credit report of activity that is inconsistent with an individual’s usual pattern or activity.

- **Suspicious Documents**
  - Examples:
    - Identification document or card that appears to be forged, altered or inauthentic; or
    - Other information on the document that is not consistent with existing information.

- **Suspicious Personal Identifying Information**
  - Identifying information presented that is inconsistent with external sources of information. Examples are:
    - Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
    - Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
    - A person fails to provide complete personal identifying information on an application and fails to respond to additional notices; or
    - A person’s identifying information is not consistent with information that is on file, e.g., an address does not match any address on file with the College.
    - A person is unable to provide authenticating information beyond what is generally available, e.g., cannot answer a challenge question.

- **Unusual Use of, or Suspicious Activity Related to, a Covered Account**
  - Examples:
    - Change of address for an account followed by a request to change the account holder’s name;
    - Account is used in a manner that is not consistent with prior use;
    - Mail sent to the person is repeatedly returned as undeliverable;
    - Notice to the College that mail sent by the College is not being received;
  - Notice to the College of unauthorized charges or transactions in connection with an individual’s Covered Account;
  - Breach in the College’s computer system security involving personal information;
  - Unauthorized access to or use of account information;
  - Alerts from others; e.g. the College receives notice from victims of Identity Theft, law enforcement authorities, or other persons regarding Identity Theft.

- **Other Information Commonly Used in Identity Theft**
  - Information which may be considered public or proprietary, used in conjunction with confidential information:
    - Payroll information, including but not limited to paychecks, pay stubs, flexible benefits plan check requests and associated paperwork;
- Medical information, including but not limited to health care provider names and claims, insurance claims, prescriptions, and any related personal medical information;
- Other personal information belonging to students and employees, including but not limited to name, date of birth, address, phone numbers, maiden name, customer number, bank routing number or account number.

III. DETECTING RED FLAGS

- **New Covered Accounts (Student Enrollment)**
  In order to detect any of the Red Flags identified above associated with a new Covered Account, College personnel will take the following steps to obtain and verify the identity of the person opening the account:
  - Require certain identifying information such as name, date of birth, academic records, home address or other identification;
  - Verify the student’s and employee’s identity at time of issuance of College identification card (review of driver’s license or other government-issued photo identification).

- **Existing Covered Accounts**
  In order to detect any of the Red Flags identified above for an existing Covered Account, College personnel will take the following steps to monitor transactions on an account:
  - Verify the identification of students who request information (in person, via telephone, via facsimile, via email);
  - Verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes;
  - Verify changes in banking information given for billing and payment purposes.

- **Employee Information**
  In order to detect any of the Red Flags identified above for employees, College personnel will take the following steps to protect employee information:
  - Verify the identification of employees if they request personal information (in person, via telephone, via facsimile, via email);
  - Verify the validity of requests to change addresses or phone numbers by phone or email;
  - Verify outside requests for verification of employee confidential information (employment verifications).
IV. RESPONDING TO RED FLAGS -- PREVENTION AND MITIGATION

- **Protecting Against Identity Theft**
  In order to prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect student and employee identifying information:
  - Ensure that its website is secure or provide clear notice that the website is not secure;
  - Ensure complete and secure destruction of paper documents and computer files containing student account and employee information when a decision has been made to no longer maintain such information;
  - Ensure that office computers with access to Covered Account information are password protected;
  - Avoid use of social security numbers;
  - Ensure computer virus protection is up to date;
  - Require and keep only the kinds of student and employee information that are necessary for College purposes.

- **Responding to Identity Theft**
  Once a potentially fraudulent activity is detected, the College must act as quickly as possible to protect students, employees and the College from damages and loss.
  - All related documentation should be gathered and a description of the situation should be written. This information should be presented to the Vice President for Finance for determination;
  - The Vice President for Finance will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic;
  - If a transaction is determined to be fraudulent, appropriate actions may include the following:
    - Continue to monitor a Covered Account for evidence of Identity Theft;
    - Contact the individual;
    - Change any passwords, security codes, or other security devices that permit access;
    - Reopen a Covered Account with a new account number;
    - Not open a new Covered Account;
    - Close an existing Covered Account;
    - Not attempt to collect on a Covered Account or otherwise place into debt collection;
    - Notify law enforcement;
    - Determine that no response is warranted under the circumstances.
V. POLICY ADMINISTRATION

- **Periodic Updates**
  At periodic intervals, the Policy will be re-evaluated to determine whether all aspects are up to date and applicable in the current business environment. Periodic reviews will include an assessment of which accounts are covered by the Policy. As part of the review, Red Flags may be revised, replaced or eliminated. Defining new Red Flags may also be appropriate. Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the College and its population.

### Definitions

**Covered Account**
- Includes all student financial accounts or loans designed to permit multiple payments or transactions that are administered by the College. Also any other account that a college offers or maintains for which there is a reasonably foreseeable risk to the safety and soundness of the college or its constituents from Identity Theft, including financial, operational, reputation or litigation risks. 16 C.F.R. § 681.1(b)(3)(ii).
- College Covered Accounts include all student, faculty or staff accounts or loans for personal, family or household purposes that permit deferred or multiple payments or transaction, and are administered by the College or an authorized service provider.
- The College has determined the following are Covered Accounts:
  - Perkins Loans
  - College Tuition Payment Plan
  - College Student Account Receivable
  - Donor Records

**Covered Entity**
- A Covered Entity is an entity that acts as a Creditor by regularly extending, renewing, or continuing credit and by regularly arranging from the extension, renewal, or continuing of credit or by being a user of a consumer credit report or by being an issuer of debit or credit cards.
- The College has determined it is a Covered Entity since the College is a “user of consumer reports” but not a “creditor” or “issuer of debit or credit cards.”

**Credit**
- “[t]he right granted by a creditor to a debtor to defer payment or to incur debts and defer payment or to purchase property or services and defer payment therefore.” 15 U.S.C.A. § 1691(a)(d).

**Credit Report**
• A document used regularly and in the ordinary course of business that details the credit history of an individual
• The College may use credit reports during the employee hiring process if job-related.

Creditor
• “…[any] person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal or continuation of credit; as any assignees of an original creditor who participates in the decision to extend, renew or continue credit.” (Emphasis added). 15 U.S.C.A. § 1691(a)(e).
• The College has determined that the College is not a “creditor”.
• The College has determined that the College is not an “issuer of credit cards”.
• The College has determined that third party providers to the College and to students are “creditors”.

Debit Card –
• Any card issued by a financial institution to a consumer for use in initiating an electronic fund transfer from the account of the consumer at such financial institution, for the purpose of transferring money between accounts or obtaining money, property, labor, or services. 15 U.S.C. § 1681a(r)(3). In the preamble to the Rules, the FTC states that stored value cards are not considered debit cards.
• The College has determined that the College is not an “issuer of debit cards.”
• The College’s ID card is a stored value card.

Financial Institutions and Creditors –
• A financial institution or “creditor” who offers or maintains one or more “covered accounts” must develop and implement a written Identity Theft Prevention Policy that will identify, detect, prevent and mitigate damages resulting from identity theft in connection with a “covered account.” 16 C.F.R. § 681.2.
• The College has determined that the College is not a financial institution or creditor but is a user of consumer credit and has Covered Accounts.
• The College has determined, based upon the law and best practices, that the College will develop and implement a written Identity Theft Prevention Policy.

Identifying Information
• Any name or number that may be used alone or in conjunction with any other information to identify a specific person, including: name, address, telephone number, social security number, date of birth, driver’s license or identification number, national identification numbers, alien registration number, passport number, employer or taxpayer identification number, and bank account numbers.
• The College has determined that a student or an employee identification number is not identifying information if used for business at the College.
Identity Theft

- Fraud committed or attempted using the identifying information of another person without authority.

Personally Identifiable Information

- Information that, alone or in combination, is linked or linkable to a specific individual that would allow a reasonable person who does not have personal knowledge of the relevant circumstances, to identify the individual with reasonable certainty. Any information concerning an individual which because of first name, or initial, and last name in combination with any one or more of the following data elements (so long as the information is not otherwise publicly available:
  - Social Security Number
  - passport number, alien registration number
  - driver’s license number or other non-driver identification card number
  - maiden name
  - mother’s maiden name
  - account number, credit or debit card or financial account information
  - full date of birth
  - any security code, access code or password that would permit access to an individual’s financial account
  - results of background or criminal history checks
  - payroll and salary information
  - medical information
  - accommodation requests and related information
  - biometric data (such as fingerprint, voice print, retina or iris images), and/or digital or other electronic signature files

- The College has determined that items identified as Directory Information are not Personally Identifiable Information. FERPA 34 C.F.R. § 99.3., 20 U.S.C. 1232 (g) and 23 NYCRR 500.

- The College has determined that the Manhattanville College employee identification number or student identification number alone are not gateways to accessing data, so, Manhattanville College ID numbers are not PII.

Record

- Written or printed instrument, regardless of format, that contains information regarding specific College educational and business transactions

Red Flag

- A pattern, practice or specific activity that indicates the possible existence of Identity Theft.
User of Consumer Reports

- Someone who obtains a consumer report from a consumer reporting agency for legally permissible purposes, such as employment screening or background checks or credit purposes.
- The College is a user of consumer reports as defined in the Rules.

Responsibilities

Vice President for Finance

- Has administrative responsibility for developing, implementing, overseeing and updating the Policy;
- Is responsible for ensuring Identity Theft training for all requisite employees. Employees should continue to receive additional training as changes to the Policy are made.
- Reports annually to the President on the operations and effectiveness of the Policy, and presents any recommended changes for approval.

Departments with Covered Accounts

- Have operational responsibility for the Policy;
- Determine training to be conducted for all employees for whom it is reasonably foreseeable may come into contact with Covered Accounts or personally identifiable information that may constitute a risk to the College, its students, faculty, staff and other constituents.

Office of Information Technology

- Should ensure that the activities of all vendors are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft. A vendor that maintains its own Identity Theft prevention Policy, consistent with the guidance of the Red Flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements. Any specific requirements should be addressed in the appropriate contract arrangements.

Students, Faculty, Staff

- Should report specific incidents of identity theft to the Vice President for Finance.

Violations of the Policy
Violations of this Policy will be handled in accordance with the procedures in the Employee Handbook or Student Handbook.

### Interpreting and Implementing Authority

Vice President for Finance

### Statutory or Regulatory References

“Red Flag Rules” Fair Credit Reporting Act, 16 C.F.R §681.1
Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500

### Relevant Links

[https://www.law.cornell.edu/cfr/text/16/appendix-A_to_part_681](https://www.law.cornell.edu/cfr/text/16/appendix-A_to_part_681)

Appendix A to Part 681 – Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

### Policy Adoption Review and Approval

Drafting team meetings on February 17, 2017; March 6, 2017; March 22, 2017; April 5, 2017; April 18, 2017; April 27, 2017; May 4, 2017; and June 12, 2017
Recommended approval by President’s Cabinet on June 15, 2017
Notification to Faculty Council, Staff Council, SGA, President’s Council, and Board on June 15, 2017
Posted on public comment period website on June 15, 2017
Approved by President’s Cabinet on XX
Approved by President on XX