- Division of Finance is responsible for the acceptance of payment and the making of payment to individuals or institutions located outside of the United States; and
- Division of Information Technology is responsible for communications and data networks and resources.

In order to ensure compliance, the University requires the following:

- Before entering into any transaction, determine whether a person or entity involved in the contemplated transaction is from a country or involves a program on the Embargo List.
- If the country or program is on the Embargo List, consult OFAC's website to determine if the sanctions prohibit the proposed activity, and whether an application for a license must be submitted; and
- Before entering into any transaction, check the names of the persons and entities involved against the SDN list and Executive Orders (either manually using the list published or list search engine on OFAC's website, or through the use of screening software); and
- If there is a valid or potentially valid match between the name of an individual or organization and a name on the SDN List, Embargo List or Executive Order, the University employee should stop the transaction and report the match to the Vice President for Finance and Treasurer who shall contact OFAC as required by applicable law.
- After entering into any transaction, periodically screen person(s) and entities to determine if they or their country have been placed on the Embargo List, SDN List and Executive Orders.

The University expects all staff to be aware of these requirements and to consider them whenever entering into any transactions with or within a foreign country, or with individuals, entities and organizations. Should specific assistance be required, the Office of University Counsel should be contacted.

II. Currency and Banking Reports

A. Mandatory Reporting of Certain Payments Received by the University Over $10,000

The U.S. Patriot Act requires the University to file a report with the U.S. government if it receives more than $10,000 in cash or coin, cashier's checks, money orders or bank drafts in a single transaction, or more than one related transaction. Related transactions would include: 1) those taking place within 24 hours; or 2) tuition and fee payments made in installments. The University is not required to file such a report if it receives a payment of $10,000 or more by personal check.

The University's Office of Student Accounts and the Division of Advancement are locations which may receive payments greater than $10,000 in single and related transactions. In the event this occurs, the University employee receiving the payment shall: 1) prepare IRS Form 8300 which can be found at: http://www.irs.gov/pub/irs-pdf/f8300.pdf; 2) request government

identification from the individual or entity making the payment; and 3) forward the completed IRS Form 8300 and identification to the Vice President for Finance and Treasurer within 5 calendar days after receiving payment.

The Vice President for Finance and Treasurer, or his designee, shall review IRS Form 8300 for completeness and file it with the IRS within 15 calendar days of receipt of the payment by the University. A copy of the IRS Form 8300 and payee identification shall be retained by the University for no less than five (5) years. At the expiration of the five (5) year period, such documents shall be shredded by the University in a manner to prevent unauthorized access to the information contained therein.

B. University Reporting of Suspicious Activity

The University may report suspicious or unusual activity to the U.S. government even if the payment is below $10,000.00 or is not otherwise required by law to be reported.

The following are a list of examples that may cause suspicion and warrant reporting:

- Unusual size, frequency or type of transaction
- Inconsistency with normal student activity
- Payments are beyond the student's financial means
- Funds received by third party check
- Unusual processing instructions
- Unusual use of an intermediary
- Students or payments sent from countries on the Embargo List or Myanmar (Burma) and Nigeria (identified by the U.S. Government as Non-Cooperative Countries and Territories for failing to have adequate procedures to prevent money laundering);
- Customers from narcotic source countries;
-

IV. Prohibition Against Payments to Foreign Officials

The Foreign Corrupt Practices Act ("FCPA") prohibits making a payment, or gift of anything of value to a foreign official for the purpose of influencing the official to give business to or to obtain an improper advantage in securing or retaining business. A "foreign official" could include any employee or contractor of a foreign government. Individuals employed by foreign universities could be characterized as "foreign officials" under the FCPA. The FCPA also states it is unlawful to make a payment to a third party knowing that all or a portion of the payment will go to a "foreign official".

The FCPA does permit a payment to be made to a foreign official to facilitate routine governmental action, such as, the issuance of a visa, permit or license. FCPA also permits the payment or gift to occur if it is lawful under the laws and regulations of the foreign official's country. FCPA permits payment of a reasonable and bona fide expenditure by the foreign official, such as travel and lodging expenses directly related to the promotion, explanation or demonstration of a University's services or the execution or performance of a specific contract, and that have nominal value.

Compliance with the FCPA is dependent upon the facts and circumstances. Please contact the Divisional Vice President or the Office of University Counsel if you have specific concerns regarding compliance with the FCPA. For general information visit the United States Depart of Justice site at www.justice.gov/criminal/fraud/fcpa.

V. Export Controls

U.S. export control laws restrict the ability of the University to grant access to foreign nationals present in the United States to certain types of technology and technical data. Three principal U.S. regulatory laws govern the export of items and technology from the U.S., and the re-export or retransfer of the items outside the U.S.:

- The export or re-export of U.S.-origin items or technologies that are commercial in nature is subject to the Export Administration Regulations ("EAR"). administered by the U.S. Department of Commerce, Bureau of Industry and Security ("BIS"). A copy of the updated set of regulations is available at: http://www.access.gpo.gov/bis/ear/ear_data.html.
- The export, re-export, or retransfer of defense articles and related technical data and defense services (i.e., items or technology that are "inherently military" in nature, as determined by the State Department not by the researcher's intent, as well as most space-related items) is subject to the International Traffic in Arms Regulations ("ITAR") administered by the U.S. Department of State, Directorate of Defense Trade Controls ("DDTC").
- For certain prohibited persons or destinations, the export, re-export, or retransfer of all U.S.-origin items or technologies is generally prohibited under regulations administered by the Department of Treasury, Office of Foreign Assets Control ("OFAC"). See Section 1of this Policy for more details on the Embargo List.

Finally, various other U.S. government agencies administer limited controls on the export, re-export, or retransfer of certain types of items and technologies with which Montclair State