Appendix A: PCI DSS Definitions

1. **Cardholder Data**: At a minimum, cardholder data consists of the full PAN. Cardholder data also may appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code. See the definition of “Sensitive Authentication Data” for additional data elements that constitute account data and may be transmitted or processed (but not stored) as part of a payment transaction. As generally used in this policy, cardholder data refers to all of the information specified above.

2. **Cardholder Data Environment**: The people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components.

3. **Payment Card**: Any payment card, including debit cards, which is issued by one of the leading payment card brands or associations.

4. **Merchant**: Any person or entity (such as a school/unit) that accepts payment cards bearing the logos of any of the five founding members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services.

5. **Payment Application Data Security Standard (PA DSS)**: Requirements and security assessment procedures that apply to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement where these payment applications are sold, distributed, or licensed to third parties. This standard includes what a payment application must support to facilitate an entity’s PCI DSS compliance.

6. **Payment Card Industry Data Security Standard (PCI DSS)**: A comprehensive set of requirements established by the PCI SSC for enhancing payment account data security. It is a multifaceted standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical safeguard measures.

7. **PCI Security Standards Council (PCI SSC)**: The organization founded by American Express, Discover, MasterCard, JCB and Visa that defines credentials and qualifications for assessors and vendors, as well as maintaining the PCI DSS.

8. **Point of Sale (POS)**: Hardware and/or software used to process payment card transactions at merchant locations.

9. **Primary Account Number (PAN)**: The composite number code of 14 or 16 digits embossed on a bank or payment card and encoded in the card’s magnetic strip. The PAN identifies the issuer of the card and the account including part of the account number, and contains a check digit that verifies the authenticity of the embossed account number.

10. **Report on Compliance (ROC)**: Report containing details documenting an entity’s compliance status with the PCI DSS.

11. **Self Assessment Questionnaire (SAQ)**: Tool used by any entity to validate its own compliance with the PCI DSS.

12. **Sensitive Authentication Data**: Security-related information including, but not limited to, card validation codes/values (e.g., three-digit or four-digit value printed on the front or back of a payment card, such as CVV2 and CVC2 data), full magnetic-stripe data, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions. Sensitive authentication data must not be stored after authorization.
Appendix B: NYU Approved Payment Card Processing Technologies

1. Payment Gateway

The NYU Payment Gateway is the preferred service for accepting online electronic payments at NYU.

The NYU Payment Gateway is NYU's Electronic Payment processing system. It is a transaction-based system that accepts ePayment transactions for both one-time and recurring payments. This service may be implemented to receive payment for items such as online gift donations, conference registration, and specific fees related to a university event, or other products and services.

Specific instructions to establish this service for your school/unit are available at www.nyu.edu/epayments.

Note: The Payment Gateway service provides only electronic payment processing. Additional functionality, such as event enrollment or inventory sales, is not specifically provided by this service. Alternative technologies for accepting online electronic payments must be approved by the University Bursar.

2. Standalone Point of Sale (POS) terminals

Standalone POS terminals will be used to process card-present, phone order, mail order, and faxed credit card payments. These terminals, which have a built in key pad and magnetic card reader, encrypt cardholder data at the point of swipe or entry and can be configured to communicate via an IP network, a plain old telephone service (POTS) line, or a cellular wireless connection.

The following are approved standalone terminals at NYU:

- VeriFone's Vx570
  - Supports wired, IP or POTS, connectivity
- First Data's FD400
  - Supports wireless, GPRS or CDMA, connectivity
Appendix C: Roles and Responsibilities

The following tables contain recommended roles and responsibilities for compliance activities within NYU PCI Compliance Program. The tasks, which have been broken down by their frequency, are standard activities that would be required of any merchant who processes payment cards.

Quarterly Activities

<table>
<thead>
<tr>
<th>Quarterly Activities</th>
<th>PCI Support Framework</th>
<th>PCI Compliance Manager</th>
<th>Responsible Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review logging and monitoring summary reports</td>
<td>Maintain documentation</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Review and confirmation of all storage locations for payment card data and systems inventory</td>
<td>Maintain documentation</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Review change control effectiveness and completeness</td>
<td>Maintain documentation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure any stored cardholder data that exceeds its data retention timeline is removed</td>
<td>Assess, maintain documentation</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Review of all network operating procedures</td>
<td>Assess, maintain documentation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Annual Activities

<table>
<thead>
<tr>
<th>Annual Activities</th>
<th>PCI Support Framework</th>
<th>PCI Compliance Manager</th>
<th>Responsible Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy review</td>
<td>Coordinate review, maintain documentation</td>
<td>X</td>
<td>X     X</td>
</tr>
<tr>
<td>Review of individual risk assessments for any changes to the payment card processing environment</td>
<td>Maintain documentation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit information security program, i.e. ensure all aspects of this document are updated as appropriate and completed</td>
<td>Maintain documentation</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Employee and 3rd party security awareness training</td>
<td>Coordinate awareness program, ensure participation, maintain documentation</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Review and test incident response plan</td>
<td>Review, maintain documentation</td>
<td>X</td>
<td>X     X</td>
</tr>
<tr>
<td>Employee acknowledgement of understanding and acceptance of the company’s security policies</td>
<td>Ensure participation, maintain documentation</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Review service provider PCI compliance</td>
<td>Maintain documentation</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Complete SAQ</td>
<td>Ensure participation, maintain documentation</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Other Ongoing PCI Compliance Manager Activities

- On-boarding merchants to the PCI Compliance Program
- Training and supporting merchants to use the proposed compliance tool
- Monitoring compliance tool activities
- Coordinating/ assembling SAQ for submission to the acquiring bank
- Fielding and addressing compliance questions
- Maintaining an inventory of payment systems and coordinating upgrades as necessary
- Tracking merchant accounts for deactivation
- Ensuring merchants have appropriate access control to cardholder data
Appendix D: Other Applicable Law

New York State Law

Schools/units accepting payment cards for goods and services in New York must apply with New York state law. In summary, current New York State law mandates that:

A. A merchant in a sales transaction is prohibited from imposing a surcharge on a purchaser who elects to use a credit card in lieu of payment by cash, check, or similar means.

B. A merchant who accepts credit cards and who imposes minimum purchase amounts for use of a credit card or excludes card payments for discounted items must conspicuously post such limitations or conditions and include them in all advertisements that otherwise mention that credit cards are accepted.

C. A merchant must use paper forms for payment card transactions which do not produce carbon copies or render a separate piece of paper that readily identifies the cardholder by name or number, except as necessary to allow the merchant to complete the transaction. A merchant is prohibited (i) from writing or requiring a cardholder to write any personal identification information (such as an address or phone number) on such form or any attachment to it that is not required to complete the sales transaction (such as a shipping address) and (ii) from printing the expiration date of the card or more than the last five digits of the card number on any receipt provide to the cardholder.

See the following sections of New York General Business Law for further information.

- New York General Business Law §520-a. Certain credit and debit card transaction forms required.

Schools/units accepting payment cards in or from other jurisdictions should contact the Office of General Counsel regarding applicable law.