Office of Finance and Treasury
How to Securely Handle and Store Cardholder Information

1) Individuals who capture, store, transmit, or have access to credit or debit card information are responsible for properly safeguarding the data and must comply with all requirements of this procedure and the University's Information Security Policy to protect the integrity and privacy of such information.

2) Types of confidential information
   a) The following pieces of information are considered "confidential" within the meaning of the Information Security Policy and must be protected appropriately regardless of the storage mechanisms used (e.g., on computers, on electronic, magnetic or optical media, on paper, etc.):
      i) Credit or debit card number
      ii) Credit or debit card expiration date
      iii) Cardholder Verification Value (CVV2) – the 3- or 4-digit code number generally located on the back of the credit or debit card.
      iv) Personal identification number (PIN)
      v) Cardholder's name, address and/or phone number when used in conjunction with the above fields

3) Destruction Requirements:
   a) All credit or debit card information must be destroyed as soon as it is no longer needed for legal, regulatory, or business purposes, and may not be retained for more than 90 days after the transaction is processed. In the event of a critical business need, or for legal or regulatory reasons, cardholder data needs to be retained for longer than 90 days, approval must be obtained from Cash and Investment Services.
   b) All physical documents that are no longer necessary must be cross-cut shredded using a commercially available shredding device approved by the Information Security Office.
   c) Applications residing in the PCI Computing Environment must securely dispose of cardholder data, in accordance with all requirements set forth in Section 3 of SAQ D – Protect Stored Cardholder Data. If the application cannot be configured to automatically delete cardholder data after 90 days, Departments with Applications residing in the PCI Computing Environment must manually delete stored cardholder data according to the parameters above.

4) Storage Restrictions
   a) By University policy, credit and debit card information may NOT be stored on the hard drive of any personal computer, laptop, tablet or smartphone, on the hard drive of any computer server or network storage device, or any removable storage medium, such as DVDs, CDs, thumb drives, USB keys, etc. However, in cases where there is a compelling business need and there is no reasonable alternative, Finance Technology and the Office of Information Security may grant an exception allowing a department to capture, process and/or store credit card information in the University's PCI Computing Environment.
   b) Point-of-sale devices must be configured to print only the last four characters of the credit or debit card number on both customer and merchant receipts, and on any reports that may be produced by the device.
   c) The storage of Social Security Numbers in conjunction with credit or debit card information is strictly prohibited. The use of social security numbers is highly restricted by University Information Security Policy. As such, social security numbers should never be used without the approval of the appropriate information guardian.
   d) Neither three- or four-digit credit or debit card validation codes (CVV2) nor Personal Identification Numbers (PIN) may ever be stored in conjunction with credit or debit card information in any form.

5) Storage of and Access to Webservers, Approved Terminals and Devices and Physical Documents
   a) University webservers hosting websites that accept online payment be credit or debit card must be located in a secure environment approved by OIT, located outside of the University's PCI Compliant Computing environment

b) Point-of-sale devices must be stored in a secure location and inspected periodically for tampering and substitution.
c) Physical documents, such as customer receipts, merchant duplicate receipts, reports, etc., that contain credit or debit card information should be retained only as long as there is a valid business reason to do so, and no longer than 90 days.
    i) While the documents are retained, they must be stored in locked cabinets located in secured areas with access restricted to authorized individuals on a need-to-know basis.
    ii) Keys that allow access to such containers must be immediately collected from any individual who leaves the University or whose responsibilities no longer require him or her to access such documents.
    iii) When combination locks are used, the combination must be changed when an individual who knows the combination leaves the University or no longer requires access to perform assigned work.
    iv) For any physical documents that contain credit or debit card information all but the last four digits of the credit or debit card number must be redacted from the document. Overwriting the credit or debit card number with a marker is not acceptable.
    v) No lists should be maintained that include more than the last four digits of a credit or debit card number.
    vi) If there is a business reason that requires storage of cardholder data other than as set forth in this procedure, contact the Information Security Office or Finance Technology.
    vii) "Media" containing cardholder information including but not limited to computers, removable electronic media, paper receipts, paper reports, faxes, and answering machines that contain cardholder should not be moved from a secure area, or distributed, without prior approval from Cash and Investment Services, and the use of secure delivery methods that log and track the Media.

6) Requirements for Departments with Applications in the University's PCI Computing Environment
    a) Departments with Applications residing in the University's PCI Computing Environment must conduct a due diligence call on the Application software with Finance Technology, OIT and the vendor, and document and implement procedures established by OIT and Finance Technology for their Merchant Location and software application.

7) Sharing Restrictions and Suspected Security Breaches
    a) Credit or debit card information may be shared only with individuals who have been authorized to access such data by the appropriate academic or administrative manager, dean or director.
    b) If a breach of credit or debit card information is suspected or has occurred, the Department Manager will immediately report the breach to the OIT Support and Operations Center at 258-HELP.