DEPARTMENTAL MERCHANT PROCEDURES - *SAMPLE*

This document is intended to be used as a guide for Merchants when creating departmental processes and procedures.

Department Name:	
Senior Business Officer:	
MID(s):	

Cardholder Data (CHD) Handling Procedures

- CHD will be treated as confidential.
- CHD that is not absolutely necessary for conducting business will *not* be retained/stored in any format.
- If storage is necessary, CHD will be stored in a secure location with access to the CHD restricted to only those with a valid reason to conduct business.
- Card-validation codes (i.e., the three or four-digit code) used to validate a card-not-present transaction, personal identification number (PIN) or encrypted PIN block will **NEVER** be stored under any circumstances.
- CC account numbers will be masked if and when displayed (i.e., no more than the first six and last four digits of the credit card numbers).
- We will not accept, request, or retain CHD via e-mail or other electronic means.
- If courier services are used to transmit CHD, track and document the chain of custody of such data.
- CHD no longer required for business purposes will be destroyed by approved methods according to University Policy.
- Appropriate segregation of duties between employees handling credit card processing, the processing of refunds and the reconciliation of accounts should be established.
- All Third Party Service Providers that may affect the security of CHD or the Cardholder Data Environment (CDE) are properly documented by:
    - A list of those external service providers is maintained
    - A written agreement is executed and retained which defines the provider's responsibility related to the security of this information
    - Any new service provider will be thoroughly vetted by Procurement and Treasury personnel and others as appropriate, before engagement to ensure that the provider can meet these requirements
    - Every service provider's PCI-DSS compliance status is reviewed on an annual basis. Instances of non-compliance are reported to the Office of the Treasurer at creditcards@columbia.edu for assistance in determining appropriate follow-up actions

System Configuration at the Department Level

- CVV and Address verification will be performed for all online and card not present transactions.
- Access will be granted to systems only on a "business-need-to-know" basis.
- Remote access by third party service providers to our CHD environment is strictly prohibited.

These procedures apply to all technologies, processes, and personnel within or that have access to our CHD environment. All personnel affected by these procedures are aware of these responsibilities and are trained on an annual basis.

The most recent version of this document (which can be found **HERE**) should be reviewed on an annual basis by all personnel with access to your departmental Merchant environment, and acknowledged by signing where indicated below. (separate copy should be kept on file for all such personnel)

Signed documentation illustrates that Senior Business Officers have communicated policies and procedures to their staff with operational responsibility.

Merchant Personnel/Representative Name: ______________________________

Signed: ______________________________

Senior Business Officer Name: ______________________________

Signed: ______________________________