Responsibilities of Credit Card Handlers and Processors

As a credit card handler or processor for Virginia Commonwealth University, I agree to abide by the provisions outlined in this document. If I need further clarification, I will refer to the General Credit Card Rules, Regulations and Guidelines located at **http://www.vcu.edu/treasury/CreditCardMerchantAccount.htm** and the Information Security Policy located at **http://www.ts.vcu.edu/kb/3408.html**.

I will DO the following:
1) Change a vendor-supplied or default password if I have access to a computer and/or application with credit card information;
2) Password-protect my computer if I have access to credit card information on my computer;
3) Restrict access to cardholder data to business need-to-know only;
4) Escort and supervise all visitors, including VCU personnel from other departments, into my area where cardholder information is maintained;
5) Store all physical documents containing credit card information behind a layer of security (such as in a locked drawer/file cabinet, safe which is bolted to the floor, locked office, or behind a badge secured area);
6) Follow the policies and procedures set by Treasury Services and Information Security; and
7) Report any credit card security incident immediately to my supervisor, Treasury Services, and the VCU Information Security department, if I know or suspect credit card information has been exposed, stolen, or misused.
   a) This report must not disclose any credit card numbers, three- or four-digit validation codes by e-mail or fax. It must include a department name and contact number.
   b) I will notify my supervisor via e-mail and a telephone call.
   c) I will notify Treasury Services at (804) 828-6533 or by fax at (804) 828-0329.
   d) I will notify the Information Security department via the VCU Help Desk by e-mail at help@vcu.edu or by phone at (804) 828-2227.

I will NOT do the following:
1) Acquire or disclose any cardholder's credit card information without the cardholder's consent, including but not limited to the full or partial 16-digit credit card number, the three- or four-digit validation code (CVC, usually located on the back of credit cards), or PINs (personal identification numbers);
2) Transmit cardholder's credit card information by e-mail or fax;
3) Electronically store any credit card information on a University computer, server or electronic flash drive or optical storage (e.g., CD, DVD);
4) Use an imprint machine to process credit card payments. (An imprint machine is a non-electronic portable device that slides over a customer's credit card and displays the full 16-digit credit card number on the customer copy);
5) Share a login and password if I have access to a computer and/or application with credit card information; or
6) Leave any paper copies containing payment card data in an unsecured area.

_____   _____
Signature   Date

_____   _____
Print Name   Department

_____   _____
Supervisor's Signature   Date