



The University of Georgia

Credit/Debit Card Processing Policy Bursar's Office Point of Sale Self Assessment

Instructions: This questionnaire is a tool to be used to assess your risk. Please complete questionnaire on an annual basis.

General Control	Y/N	Comments
Is any sensitive credit/debit card information stored on your point of sale device? If yes, please explain.		
Are receipts stored in a secure, limited access area? Please describe.		
If credit/debit card information is taken by fax, is fax machine monitored on a frequent basis?		
Are copies of receipts the exception?		
Are receipts shredded using a cross cut/confetti shredder?		
Are voicemails processed that leave detailing sensitive information?		
Are ID badges, office keys used in identifying who has access to the building/office?		
Is credit/debit card information repeated in front of others?		
Are strangers identified?		
Is all sensitive material removed from your work area when you are not using them and at the end of the day?		
Is a glare screen used to minimize what others may see you inputting?		
Do you avoid taking sensitive cardholder data given on a cell phone?		
How long are receipts kept in storage prior to destroying them?		

Card Present	Y/N	Comments
Are the card security features checked?		
Do you match the embossed number on the card against the four digits of the account number displayed on the terminal?		
Do you check to see if the embossed account number on the front matches the number indent printed on the back?		
Do you check the expiration date to make sure the card has not expired?		
Is the card only swiped in one direction to obtain authorization?		
Do you check the authorization response-approved, denied, call, pick up or no match?		
If approved, do you require customer to sign the sales receipt?		
Do you check the signature on the card to the one on the transaction receipt?		
If denied, do you return the card and ask for another form of payment?		
If Call/Call Center, do you call the phone # given and follow the instructions?		
If PickUp, do you keep the card if you can do so peacefully?		
If No Match, do swipe the card and rekey the last 4 digits? If no match appears again, do you call in Code "10"?		
Do you key-enter the card account data when the card cannot be swiped?		

Card Not Present	Y/N	Comments
Do you obtain expiration date to process the authorization?		
Do you use address verification service (AVS)?		
Do you verify the card verification value2 (CVV2)? (last 3 digits imprinted on back of the card)		

Recurring Transactions	Y/N	Comments
Have you been granted approval to keep sensitive information on file?		
Do requests from clients to hold their credit card information on file indicate an expiration date?		
Is cardholder data stored in a secure, limited access area? Please describe.		