EASTERN OKLAHOMA STATE COLLEGE
ACCEPTING AND HANDLING CREDIT AND DEBIT CARD PAYMENTS
POLICIES AND PROCEDURES

This document describes Eastern Oklahoma State College's policy and procedures for the proper handling of credit and debit card transactions processed through automated systems and/or manual procedures. It is intended for:

1. Any College employee, who accepts, captures, stores, transmits and/or processes of credit or debit card payments received for the purchase of products and services, for contributions, etc.
2. Any individual who supports any College effort to accept, capture, store, transmit and/or process credit card information, such as a technical support staff member whose role gives him or her access to computer hardware and software holding credit card information, individuals tasked with shredding credit card information, etc.

This policy and procedures are intended to ensure that credit and debit card information is handled and disposed of in a manner that satisfies the College's obligation to protect such information to the level that meets or exceeds the standards of the Payment Card Industry, known as the Payment Card Industry's Data Security Standard, or "PCI-DSS". Penalties for non-compliance can include but not limited to increased credit card transaction fees, a suspension of credit card privileges, and fines in cases where an account is compromised.

Since any unauthorized exposure of credit or debit card information could subject the College to reputational damage and significant penalties, failure to comply with the policy contained within this document will be considered a serious matter.

POLICY AND PROCEDURES

- **PCI-DSS COMPLIANCE IS MANDATORY FOR ANY DEPARTMENT THAT ACCEPTS, CAPTURES, STORES, TRANSMITS AND/OR PROCESSES CREDIT OR DEBIT CARD INFORMATION.**

  Any College department that accepts credit or debit cards as payment must follow the procedures outlined in this policy (or any future revisions) to ensure the security of cardholder information as required by PCI-DSS.

- **ONLY AUTHORIZED EMPLOYEES MAY ACCEPT AND/OR ACCESS CREDIT OR DEBIT CARD INFORMAITON**

Only Eastern Oklahoma State College employees (non-student, full or part-time) are permitted to accept and/or access credit or debit card information. Authorization to handle such information will be granted only after an employee has read this policy and has been instructed by the appropriate Department Head or Supervisor in the proper handling of credit and debit card information. Each employee being authorized must sign a "Statement of Intent to Comply" to document his or her understanding and commitment to comply with all College policies and procedures. This certification will be maintained in the employee's personnel file in the Human Resource Department.

- **ANY CONTRACTORS DOING BUSINESS WITH THE COLLEGE WITH ACCESS TO CREDIT OR DEBIT CARD INFORMATION MUST ALSO PROVIDE THE COLLEGE WITH WRITTEN VERIFICATION THAT THEY UNDERSTAND AND ARE COMPLYING PCI-DSS STANDARDS**.

Such verification will be maintained by the Vice President of Business Affairs. Any contractor that fails to establish such verification will not be allowed to conduct business with the College until compliancy is assured.

- **CREDIT AND DEBIT CARD PAYMENTS MAY BE ACCEPTED ONLY IN THE FOLLOWING MANNERS:**

    1. in person
    2. via telephone
    3. via physical mail (not e-mail)
    4. via FAX (if received through an analog telephone line; not through an online computer)

Other methods of accepting payments may be added but only with the approval of the Vice President of Business Affairs.

- **EACH PERSON WHO HAS ACCESS TO CREDIT OR DEBIT CARD INFORMATION IS RESPONSIBLE FOR PROTECTING THE INFORMATION**

All College personnel who have access to credit or debit card information are responsible for properly safeguarding the data. The following pieces of information are considered "confidential" and must be protected appropriately from initial capture through destruction regardless the storage mechanisms used (e.g., on computers, on electronic, magnetic or optical media, on paper, etc.):

1. Credit or debit card number
2. Cardholder Verification Value (CVV2) – the 3- or 4-digit code number generally located on the back of the credit or debit card.

3. Cardholder's name, address and/or phone number when used in conjunction with the above fields
4. Credit or debit card expiration date when used in conjunction with the above fields

Special note (1): Only the last four characters of the credit/debit card number may be retained in a database or computer file. If an entire credit/debit card number is recorded on a computer hard drive or on a removable storage media (diskettes, CDs DVD/s, USB Storage devices, etc.), they must be encrypted to allow only the last number visibility.

Special note (2): The use of Social Security Numbers in conjunction with credit or debit card information is strictly prohibited and should never be used.

Point-of-sale devices must be configured to print only the last four characters of the credit or debit card number on both the customer and the merchant receipts, and on any reports that may be produced by the device. Physical documents that contain confidential credit or debit card information should be retained only as long as there is a valid business reason to do so. While the documents are retained, they must be stored in a locked secured area. When an authorized employee leaves the College or whose responsibilities no longer require him or her to access such documents, keys are to be returned and/or combination must be changed to ensure security.

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 physically cut out of the document. Overwriting the credit or debit card number with a marker is not acceptable since the number can still be viewed in certain circumstances.

The three- or four-digit credit or debit card validation code (CVV2) must never be captured in any form.

No lists should be maintained that include entire credit or debit card numbers.

Credit or debit card information may be shared only with authorized employees and individuals who have been authorized via contract to process credit or debit card transactions on our behalf.

- **CREDIT AND DEBIT CARD INFORMATION MUST BE DESTROYED AS SOON AS IT IS NO LONGER NECESSARY**

All credit and debit card information must be destroyed as soon as it is not longer necessary. All physical supporting documents that are no longer necessary must also be shredded using a commercially available shredding device. The merchant duplicate transaction receipts may be retained as part of the college's records. When such files are moved to storage, all individual merchant duplicate transaction receipts must be removed and shredded using a commercially available shredding device.

Any electronic file containing credit/debit card information stored on electronic or magnetic media (computer hard drives, diskettes, USB storage devices, etc.) that is no longer needed must be electronically "shredded" or wiped. Merely deleting the file is not sufficient, as common computer operating systems typically leave deleted information on such media intact.

- **DEPARTMENTS MUST MAINTAIN APPROPRIATE CHECKS AND BALANCES IN THE HANDLING OF CREDIT AND DEBIT CARD INFORMATION**

Departments handling credit or debit card transactions must segregate, to the extent possible, all duties related to data processing and storage of credit and/or debit card information. A system of checks and balances should be put in place in which tasks are performed by different individuals in order to assure adequate controls. All transactions are to be verified with the original supporting detail records and balanced to deposits. Terminal or web-based reports must not be the only supporting detailed record.

- **SUSPECTED THEFT OF INFORMATION MUST BE REPORTED IMMEDIATELY**

When an employee suspects the loss or theft of any materials containing cardholder data, that person must immediately notify the College. The College will then take such security action deemed necessary.

Exceptions to Required Procedures It is understood that a unique situation within an individual department may require a permanent or short-term exception to one or more of the above procedures. Such an exception must satisfy ALL of the following conditions:

1. It must comply with all applicable PCI-DSS requirements.
2. It must be approved by the Vice President of Business Affairs.

Appendix A – Statement of Intent to Comply with the University Policy and Procedures for Accepting and Handling Credit and Debit Card Payments The following page is a statement of understanding and intent to comply with the College Policy and Procedures for Accepting and Handling Credit and Debit Card Payments.

Any College employee who has access to credit or debit card information must sign the form. The signed form will be retained by the Office of Human Resource as a part of the employee's permanent record.

Any contractor who has access to credit or debit card information must also sign the form. The signed form will be retained by the Vice President of Business Affairs along with other supporting documentation that they are in compliance with PCI-DSS standards.

Eastern Oklahoma State College
Responsibilities of Credit/Debit Card Handlers and Processors

As a credit/debit card handler or processor, I agree to abide by the provisions of this document. I recognize that all credit/debit card numbers, expiration dates, and card verification codes are sensitive and that the College is contractually obligated to protect this information against its unauthorized use or disclosure in any manner. Should such information be disclosed to an unauthorized individual, the College could be subject to fines, increased credit and debit card transaction fees and/or suspension of credit/debit card privileges.

As an individual whose roll includes the acceptance, capture, storage, transmission and /or processing of credit /debit card information, I agree with the following statements:

- I have read the requirements stated in EOSC Policy for Accepting and Handling Credit and Debit Card Information ("Policy").
- I understand that I may only accept credit and debit card payments using approved methods.
- I understand that, as an individual who has access to credit and debit card information, I am responsible for protecting the information in the manner specified within the Policy. Further, I understand that I am also responsible for effectively protecting the credentials (IDs and passwords) and the computers that I may use to process credit or debit card transactions.
- I understand that I must destroy credit and debit card information as soon as it is no longer necessary using methods prescribed by Policy.
- I understand that in cases where I suspect that a breach of credit or debit card information has occurred, I must immediately report the breach to the Vice President of Business Affairs.

I commit to comply with the Policy and its documented procedures, and understand that failure to comply with the above requirements may subject me to disciplinary measures, up to and including termination of employment.

Signature:	Date:
Print Name:	

Authorization Granted: _____
Limited_____ ***Vice President of Business Affairs***

Board Approved 08/27/2009

Appendix B – Procedures for In-House Application Systems

All applications and procedures associated with the use of an on-campus system that accepts, captures, store, transmit and/or process credit/debit card information must comply with the following additional requirements:

- System and network controls must be implemented to restrict access to authorized individuals and only on a need-to -know bases. Access is to be immediately revoked for any individual who leaves the College or whose responsibilities no longer require access to such information.
- The three or four digit credit/debit card validation cold (CVV2) must never be captured in any form.
- Credit/Debit card information that is transmitted across a network must be encrypted.
- No reports should be maintained that list entire credit/debit card numbers.
- Only the last four characters of the credit/debit card number may be retained in a database or computer file.
- Any file containing credit/debit card information stored on electronic or magnetic media that is no longer needed must be electronically "shredded" or wiped.
- No computer that has hosted a software application that accepts, captures, stores, transmits or processes credit/debit card information may be repurposed, donated, sold or sent to surplus until all of the hard drives on that system have been removed from the system and physically destroyed. Such hard drives must be protected against theft and unauthorized access through their destruction.
- No computer that has been used to manually enter credit card information received via phone, FAX, mail, etc. into a credit card system hosted by a bank or credit card service organization may be repurposed, donated, sold or sent to surplus until all of the hard drives on that system have been removed from the system and physically destroyed. Such hard drives must be protected against theft and unauthorized access through their destruction.
- Any piece of non-magnetic/non-electronic media (e.g., CDs, DVDs) that has been used to store credit/debit card information must be shredded before being discarded.

Appendix C – Procedures for processing Credit or Debit Card Transactions

The following guidelines are to be followed when processing a credit or debit card transaction. These guidelines are intended to assure adequate control of confidential information and compliance with PCI-DSS standards. They are to be reviewed periodically. If changes are warranted, these changes must be documented and signed by the Vice President of Business Affairs before be added to this policy.

- **Only credit/debit card transactions that are payment on an account or payment for a sale or service are authorized.** *Transactions to secure cash are prohibited.* The only exception will be the Business Office processing College travel transactions using College credit cards.

- **Transactions are to be processed for the amount of the required payment only.**

- **Credit/Debit Card payments may be accepted only in the following manners**
    1. in person
    2. via telephone
    3. via physical mail (not e-mail)
    4. via FAX (if received through an analog telephone line; not through an online computer)

Other methods of accepting payments may be added but only with the approval of the Vice President of Business Affairs.

- **The following credit cards may be accepted for payment:**

    1. Visa
    2. MasterCard
    3. Discover

At this time, the College does not accept American Express credit cards. These and other services may be added in the future if deemed needed and approved by the Vice President of Business Affairs.

- **Credit/Debit Card transactions can originate from the following sources:**

    1. A College department and/or program that does not have a credit/debit card terminal to process the transaction
    2. A College department that does have a credit/debit card terminal to process the transaction but is outside of the Business Office.
    3. The College Business Office.

The following pages outline the procedures for each of these sources.

Appendix C – Part 1 **A College department and/or program that does not have a credit/debit card terminal to process the transaction**

Many department and/or programs collect their own payments for their activities. Payments are then deposited in the Business Office in a timely manner as prescribed by the College. *No department and/or program shall accept credit/debit card payment unless limited authorization to accept such payments has been granted from the Vice President of Business Affairs and the required Statement of Intent to Comply is signed and on file in the Office of Human Resources.* Once authorization has been granted, credit/debit card transactions may only be processed as follows:

Customers should be encouraged to use an alternate method of payment other then credit/debit card if possible. If they prefer to pay by credit/debit card, such payment can be processed by:

1. Phone – The customer may call the College Business Office and convey the necessary information to a College employee authorized to process credit/debit cards. The Business Office employee will then process the transaction immediately and give a confirming receipt number. If the transaction is not to be processed immediately, the Business Office employee will secure such information until the transaction is processed at a later time. Once processed, a copy of the deposit receipt will be sent to the appropriate department for their records. Then, all confidential credit/debit card information will be destroyed as required.

2. Intent to Pay by Credit/Debit Card Statement – If the transactions cannot be processed by phone, then the customer may complete and sign an Intent to Pay by Credit/Debit Card statement. (See Appendix D) The statement is designed to give you assurance that the customer intends to pay by credit/debit card and to collect the necessary information to allow an authorized Business Office employee to contact the customer at a later time to secure the necessary credit/debit card information. The Business Office employee will then secure the information and/or process the transaction as requested. When the transaction is completed, a copy of the deposit receipt will be sent to the appropriate department for their records. A copy will also be sent to the customer upon their request.

SPECIAL NOTE: At no time are you to collect or record in any manner any confidential credit/debit card information.

Appendix C – Part 2 **a College department that does have a credit/debit card terminal to process the transaction but is outside of the Business Office**

- Currently, there are two areas outside the Business Office that are authorized to accept credit/debit card transactions:
    1. College Post Office
    2. College Cafeteria

These departments are required to make daily (or timely) deposits to the Business Office. Credit/Debit card transactions are included as part of their deposited transactions.

- Credit/Debit card transactions in these areas are almost always from personal presentation of a credit/debit card. A phone presentation is possible but not as likely.

- Only authorized employees who have an Intent to Comply statement on file in the Office of Human Resources are allowed to process a credit/debit card transaction.

- All credit/debit card terminals must be configured to print only the last four characters of the credit/debit card number on both the customer and the merchant receipts, and on any reports that are produced by the device.

- The use of Social Security Numbers in conjunction with credit/debit card information is strictly prohibited. Social Security Numbers should never be requested or recorded.

Credit/Debit card payments are to be processing as follows:

Credit/Debit card is presented

1. Customer presents a credit/debit card for payment – Verification should be made as to the identity of the individual presenting the card and compared to the name on the credit/debit card. If different, refuse the card. (The authorized employee should always try to overt placing the College in danger of credit/debit card penalties or reputable damage.)

2. Process the transaction – Swipe the credit/debit card and follow the instructions for the terminal to complete the transaction.

*SPECIAL NOTE: If the terminal asks for a **tax amount**, always enter **$0.00**; if asks for **customer code**, always **enter all 9's**; if asks for address verification information, always enter something. This will lower the credit/debit card transaction rates that the College has to pay for process credit/debit cards.*

3. Credit/Debit card receipts – Have the customer sign both copies of the credit/debit card receipt. (A) If the signature is not legible, print the customers name at the bottom of the merchant copy of the receipt. (B) Record the credit/debit card's expiration date on the bottom of the receipts. (C) Ask for and record a phone number for future contact if needed. This information will be helpful to the Business Office should a transaction be contested.

4. Complete the sale – Record the sale in the cash register. Hand the customer their credit/debit card, the original credit/debit card receipt and the cash register sales receipt. Place the merchant copy of the credit/debit card receipt in the cash drawer and complete the sale.

Credit/Debit Card is Not Presented

If a transaction is process without a card being presented (phone transaction) the process is to be completed as follows:

1. Verification - The authorized employee should try to secure the identity of the credit/debit card information. Sufficient identification should be presented to assure the information is accurate and the transaction is not fraudulent. If sufficient explanation is given, continue with the transactions. If fraud is suspected, refuse the transaction. (The authorized employee should always try to overt placing the College in danger of credit/debit card penalties or reputable damage.)

2. Process the transaction –Using the terminal key pad, enter the credit/debit card number and other pertinent information. Follow the instructions for the terminal to complete the transaction.

*SPECIAL NOTE: If the terminal asks for a **tax amount**, always enter **$0.00**; if asks for **customer code**, always **enter all 9's**. This will lower the credit//debit card transaction rates that the College has to pay for process credit/debit cards.*

3. Credit/Debit card receipts –Print the customers name at the bottom of the merchant copy of the receipt and initial it by you /phone. (B) Record any credit/debit card verification information (received in step 1. above) on the back of the merchant copy of the receipt. (C) Record the credit/debit card's expiration date on the bottom of the receipts. (D) Ask for and record a phone number for future contact if needed. This information will be helpful to the Business Office should a transaction be contested.

4. Complete the sale – Record the sale in the cash register. Place all copies of the credit/debit card receipt in the cash drawer and complete the sale.

All credit/debit card terminals must be closed out and a report printed on a daily basis. The merchant copy of the credit/debit card receipt and the terminal daily report must be turned over to the appropriate department personnel (someone other then the casher) to be included in the daily cash reconciliation and deposit report. They must be kept in a secure location. Once reconciled, all merchant copies of credit/debit card receipts are to be turned over to the Business Office as part of the daily cash deposit. No type of credit/debit card information is to be retrained by the department.

Special Note: If the cash reconciliation and deposit report must be complete by the cashier because of only one individual in a department, then that department's supervisor must perform random audits of the cash drawer to verify that transactions are in being preformed in compliance with required standards.

Appendix C – Part 3 **the College Business Office**

The current database system for the College is Datatel/College, commonly referred to as Datatel. This system has the capability of processing credit/debit card transactions through e-commerce. At this time, e-commerce transactions are not being offered as a means of processing credit/debit card payments to the College. The College does not have the proper security systems in place to be in compliance with PCI-DSS standards if such transactions were processed. Therefore, all employees, whether authorized or unauthorized, are prohibited from entering any confidential credit/debit card information electronically into the database. The following pieces of information are considered "confidential" and must never be entered in to the database in any manner:

1. Credit/Debit card number
2. Cardholder Verification Value (CVV2) – the 3- or 4-digit code number generally located on the back of the credit or debit card
3. Number codes located on the back of the credit/debit card on the magnetic strip preceding the cardholder verification value.

Any violation of this policy will subject the College to significant penalties and suspension of credit/debit card privileges. Therefore, such a violation would be considered a serious matter and grounds for termination of employment. Other legal options may also be perused if deemed necessary by the College.

The College reserved the right to expand payment options to include e-commerce at a later date but only after sufficient safeguards are in place to protect confidential credit/debit card information. These safeguards must insure the College will be in compliance with PCI-DSS standards. At that time new guidelines are to be written and added to this policy once approved by the Vice President of Business Affairs.

Board Approved 08/27/2009

The following credit/debit card information may be entered electronically into the database:

1. Name as shown on the credit/debit card
2. Last four digits of the credit/debit card number
3. Expiration date of the credit/debit card
4. Amount of the transaction.

This information must never be associated in any way with the "confidential" credit/debit card information listed above.

All financial transactions for the College are processed through the Business Office. Credit/debit card transactions may be received by the Business Office through the following sources.

1. Departmental Deposits
2. in Person
3. via Phone
4. via Mail

All faxes are currently being received online through individual computers. The Business Office fax machine is connected to an analog telephone line but is not set up to receive faxes. Therefore, no credit/debit card information is to be transmitted via fax. The Business Office reserved the flexibility to add this feature to the fax machine if needed. Such a change would have to be approved by the Vice President of Business Affairs and appropriate guideline added to this policy.

Credit/Debit card payments are to be processing as follows:

1. Departmental Deposits – This included deposits that are processed for other departments, which may include credit/debit card transactions. The departmental deposit is to be recorded into the database and all funds deposited into the cash drawer. *This included all copies of the merchant credit/debit card receipts on which the cashier is to record the database receipt number (CR#).* The departmental deposit report is then filed with the database receipt. The second copy of the receipt is returned to the department for their file.

2. **In person –**

1. Verification should be made as to the identity of the individual presenting the card and compared to the name on the credit/debit card. If different, refuse the card. (The authorized employee should always try to overt placing the College in danger of credit/debit card penalties or reputable damage.)

2. Process the transaction – Swipe the credit/debit card and follow the instructions for the terminal to complete the transaction.

*SPECIAL NOTE: If the terminal asks for a **tax amount**, always enter **$0.00**; if asks for **customer code**, always **enter all 9's**; if asks for address verification information, always enter something. This will lower the credit/debit card transaction rates that the College has to pay for process /debit cards.*

3. Credit/debit card receipts – Have the customer sign both copies of the credit/debit card receipt. (A) If the signature is not legible, print the customers name at the bottom of the merchant copy of the receipt. (B) Record the credit/debit card's expiration date on the bottom of the receipts. (C) Ask for and record a phone number for future contact if needed. This information will be helpful to the Business Office should a transaction be contested. (Option: This information may be entered electronically into the database instead of being hand written on receipt.)

4. Process the transaction in the database. Hand the customer their credit/debit card, the original credit/debit card receipt and the database (CR) receipt.

5. Cross reference the receipt numbers by recording the credit/debit card transactions number on the face of the office copy of the CR receipt and recording the CR number on the merchant copy of the credit/debit card receipt. Place the merchant copy of the credit/debit card receipt in the cash drawer. The CR receipt is to be retained for reconciliation of the cash drawer at the end of the day.

3. **Via Phone and/or Mail –**

1. Credit/Debit Card Information Sheet - When credit/debit card information is collected by phone or received by mail a Credit/Debit Card Information Sheet (See Appendix E) should be used to record the vital information. The use of this form will help insure that all pertinent information is collected but that no confidential credit/debit card information is permanently maintained.

Once the Credit/Debit Card Information Sheet is completed it must be kept in a secure locked location until the credit/debit card transaction can be processed. Any supporting documentation should be kept with it.

Once the credit/debit card transaction has been processed. The upper portion of the sheet will be attached to the database receipt to be filed in the Business Office. The bottom half containing the confidential credit/debit card information is to be removed and shredded along with any supporting documentation that contains confidential information also.

2. Process the transaction –Using the terminal key pad, enter the credit/debit card number and other pertinent information. Follow the instructions for the terminal to complete the transaction.

*SPECIAL NOTE: If the terminal asks for a **tax amount**, always enter **$0.00**; if asks for **customer code**, always **enter all 9's**. This will lower the credit/debit card transaction rates that the College has to pay for process credit/debit cards.*

3. Process the transaction in the database. Cross reference the receipt numbers by recording the credit/debit card transactions number on the face of the office copy of the CR receipt and recording the CR number on the merchant copy of the credit/debit card receipt. If possible, record the name on the credit/debit card, a phone number and the expiration date on the back of the merchant copy of the credit/debit card receipt. Place the merchant copy of the credit/debit card receipt in the cash drawer. The lower half of the Credit/Debit Card Information Sheet containing the confidential credit/debit card information must be removed and properly shredded. Any other supporting document containing confidential credit/debit card information must be shredded also. Attach the top half of the Credit/Debit Card Information Sheet to the CR Receipt. The CR receipt is to be retained for reconciliation of the cash drawer at the end of the day.

The credit/debit card terminal must be closed out and a report printed on a daily basis. The merchant copy of the credit/debit card receipt and the terminal daily report are to be included in the daily cash drawer reconciliation at the end on the day. Once the cash drawer is reconciled, the cash for the deposit and the merchant copy of all credit/debit card receipts must be kept in a secured locked location over night or until the daily cash deposit is processed.

To insure an appropriate segregation of duties, the cashier is not allowed to prepare the daily cash deposit. Once the deposit is processed, all supporting documentation, including the merchant copy of all credit/debit card receipts, and reports are to be filed within the Business Office. After the bank deposit has been made, the deposit slips are attached to the file and the file is audited for accuracy. The files are then turned over to the accounting assistant for the Vice President of Business Affairs to be used in the month end reconciliation with the state and credit/debit card reports from the merchant banks.

After reconciliation, the deposit files are held in the Business Office until sufficient time has passed and the files are boxed for storage. Prior to sending the files to storage, all individual merchant credit/debit card receipts are to be removed and shredded. This insures that no confidential credit/debit card information will be allowed to be stored in an unsecure location.

Appendix D **- Intent to Pay by Credit/Debit Card Statement**

A College department and/or program that do not have a credit/debit card terminal to process credit/debit transaction can have credit/debit card information collected for them by the College Business Office. The department and/or program needs to secure a signed copy of an Intent to Pay by Credit/Debit Card Statement from the customer. The statement is then submitted to the Business Office for processing.

The Intent to Pay by Credit/Debit Card Statement is designed to give the department and/or program assurance that the customer intends to pay by credit/debit card and to collect the necessary information to allow an authorized Business Office employee to contact the customer at a later time to secure the necessary credit/debit card information.

EASTERN OKLAHOMA STATE COLLEGE
Intent to Pay by Credit/Debit Card Statement

I, _____
(Customer Name)

intend to pay by ***credit/debit card*** for the goods and/or services provided by Eastern Oklahoma State College described as follows:

_____

_____

I understand that Eastern Oklahoma State College Business Office will contact me to collect the necessary credit/debit card information. If I fail to provide the necessary credit/debit card information, I will forfeit all rights and privileges written or implied with the signing of this statement.

_____ $_____
(Phone Number) (Amount)

_____ _____
(Preferred Date) (Preferred Time of Day)

_____ _____
(Customer's Signature) (Current Date)

****

I understand that the above signed customer has agreed to pay by credit/debit card for the goods and/or services described. At this time, I accept this statement as payment in full.

_____ _____
(Department Representative Signature) (Current Date)

Board Approved 08/27/2009

APPENDIX E – Credit/Debit Card Information Sheet

Only an authorized Business Office employee may collect confidential credit/debit card information. Such confidential information, whether received by phone or by mail, should be recorded on a Credit/Debit Card Information Sheet. The use of this form will help insure that all pertinent information is collected but that no confidential credit/debit card information is permanently maintained.

Once the Credit/Debit Card Information Sheet is completed, it must be kept in a secure locked location until the credit/debit card transaction can be processed. Any supporting documentation should be kept with it.

Once the credit/debit card transaction has been processed, the upper portion of the sheet will be attached to the database receipt to be filed in the Business Office. The bottom half containing the confidential credit/debit card information is to be removed and shredded along with any supporting documentation that contains confidential information.

_____	Mail Phone	_____
Employee's Initials	(Circle One)	Current Date

Eastern Oklahoma State College
Business Office
Credit/Debit Card Information Sheet

_____ _____
(Customer Name) (Account Number)

Payment is to be applied to:
_____
_____
_____

Total of Card Transaction: $_____

Last 4 Digits of Credit/Debit Card Number: _____

Credit/Debit Card Expiration Date: _____

Address:_____

_____

Phone Number: _____

Name as shown on Credit/Debit Card: _____

(Explain on back if different than customer's name)

Copy of database receipt forwarded to: _____

This portion is to be filed with database receipt.

This portion is to be shredded once transaction is completed.

_____ _____
Complete Credit/Debit Card Number Verification Number

Board Approved 08/27/2009