SECTION 1500.02
PCI (PAYMENT CARD INDUSTRY) COMPLIANCE

Policy Statement:
Lake Region State College allows departments to accept credit/debit cards for purchases of goods or services only in accordance with the procedures outlined in this document.

Purpose:
The College recognizes that accepting credit/debit cards as payment for goods or services has become a common practice that improves customer service, brings certain efficiencies to Lake Region State College's cash collection process, and may increase the sales volume of some types of transactions. In addition, the use of technology, such as the World Wide Web, provides easy access for many, and the use of credit cards is essential when sales are conducted electronically.

Scope of Policy:
This policy applies to all members of the Lake Region State College community.

Related Documents/Policies:

Gramm Leach Bliley Act	http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
Lake Region State College Customer Information Safeguarding Program (Gramm Leach Bliley Act)	Lake Region State College Policy & Procedure Manual
Payment Card Industry Standards	https://www.pcisecuritystandards.org/tech/index.htm
Lake Region State College Information Security Response Policy	Lake Region State College Policy & Procedure Manual
Lake Region State College Identity Theft Prevention Program (Red Flag)	Lake Region State College Policy & Procedure Manual
"What To Do If Compromised" VISA USA Fraud Investigations and Incident Management Procedures	www.usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf

Definitions:

Department	A Lake Region State College department that accepts credit cards to conduct business.
Gramm Leach Bliley Act	Key rules under the Act govern the collection and disclosure of customers' personal financial information.
Payment Card Industry Standards (PCI)	A multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.
Credit Card Processing Machine	A machine or device used to process credit/debit card transactions. *Examples may include: Zon, Trans330, Trans380, Trans460, Omni3200SE.*

Principles:
Overview - Many departments on campus process credit/debit card transactions, either infrequently or in the course of daily business. It is the College's responsibility to protect the privacy of its customers, as well as maintain compliance with the Gramm Leach Bliley (GLB) Act and Payment Card Industry (PCI) Standards.
Departments that transact business by accepting credit cards for goods or services are expected to adhere to the attached procedures to help ensure the integrity and security of all credit/debit card transactions. Failure to follow the procedures may result in the revocation of departmental authorization to accept credit cards and departmental responsibility for paying all related penalties.

Acceptable Credit/Debit Cards - The College is required to process credit/debit card transactions through the Bank of North Dakota. Any exceptions must be approved, in writing, by the Bank of North Dakota. All requests to contract with a processer other than the Bank of North Dakota must be submitted to the Lake Region State College Vice President of Administrative Affairs.
Credit card types that departments may request to be accepted within the department for goods and services include MasterCard, VISA, and Discover.

Credit Card Fees - The College is charged fees on all credit card transactions. The fees vary and are based on the card type accepted and the method of acceptance (swiped versus manually entered). Merchant fees are generally charged to the funding source that the revenue is credited to at the time of the transaction. Fees will be charged to the departmental fund via journal entry/import on a monthly basis by the Business Office.
As departments are developing rates (fees for goods or services) they should recognize the credit card merchant fee as a cost of doing business. Should the department choose to recover the fee, they must build it into the overall rate structure. In other words, departments cannot assess an additional fee to the customer if the customer pays via a credit card.

SECURITY - If a department suspects that credit/debit card records may have been compromised in any way, whether through malicious intent or due to a weakness in the handling and processing of credit/debit card transactions, they are to notify the Business office immediately.
All security incidents will follow the Lake Region State College Information Security Response. The document "What to do if Compromised", VISA USA Fraud Investigations and Incident Management Procedures will be utilized as a reference for any security incident.

Contracts with Vendors/Internet Service Providers - Prior to entering into a new contract with a vendor/internet provider for acceptance of credit/debit cards, a department needs to take the following steps:

1. Submit a brief synopsis of the business rationale to the Business Office and Information Technology (IT). The rational needs to include:
    a. How it will interface with other campus/NDUS systems.
    b. Justification of the approach chosen.
    c. Description of any alternatives seriously considered and explanation of why those alternatives were not chosen.
2. The Business Office/IT will determine if existing credit card collection methods can accomplish the goal.
3. If existing methods can accomplish the goal, the Business Office and IT will work with the department to construct the set-up.
4. If existing methods cannot accomplish the goal, the department must:
    a. Have a secured website and must provide certification that the internet site/provider is PCI compliant prior to entering into a contract with the vendor/internet provider. This certification should be obtained from the vendor/internet provider and submitted to the Business Office Administration. Certification must be provided on an annual basis, or as requested.
    b. Have a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service provider possesses
    c. Maintain a program to monitor service providers' PCI DSS compliance status.
    d. Have the contract approved by NDUS Legal Counsel.

Procedures:
Obtaining Authorization to Accept Credit/Debit Card Payments - Departments must obtain prior approval from the Business Office Accounting Supervisor to accept and/or process credit/debit card transactions within the department. Requests should be made via e-mail to the Accounting Supervisor. If approved, the Business Office will assist the department in obtaining a credit card processing machine and will provide procedures that must be followed when processing credit card deposits. If a department has not obtained approval to accept credit/debit card payments, they must not be accepting credit/debit card information.

Methods of Processing Transactions - There are four accepted methods for processing credit/debit card transactions:

1. In person.

2. By telephone – must obtain the CVV code from the back of the card, but must be shredded after the transaction is processed; must verify the address if sending merchandise; may choose to have return receipt to confirm delivery of goods.
3. By mail.
4. Via a secured College-approved internet or firewall-protected and encrypted database application – a department accepting credit card information over the internet must provide a certification that the internet site/provider is PCI compliant prior to entering into a contract with the vendor/internet provider. This certificate must be submitted to the Business Office on an annual basis, or as requested.

Credit/debit card information cannot be requested or sent electronically (i.e. e-mail). If a cardholder sends credit card information electronically, departments are required to reply (deleting the card information) to the cardholder with the following verbiage:

"It is important that Lake Region State College protects the privacy of our customers, and therefore, does not accept credit/debit card information electronically, as the e-mail system is not a secured site. Because we have already received it, we will process this payment, but please discontinue sending credit card information electronically. You may contact the department providing the goods or services to request available payment options."

Departments must attach a copy of the response to the merchant copy of the transaction being processed and retain in accordance with the records retention policy.

Credit/debit card information needs to be kept confidential and must never be left lying in an area where unauthorized persons may view it.

When issuing credits to customers, the credit should be processed in the same payment method as the original charge.

Departments must not store any credit/debit card information, including CVV codes or PIN numbers, in a customer database or electronic spreadsheet. All CVV codes, PIN numbers, and other documents containing credit card information, must be shredded immediately after the transaction has been processed.

ATM Terminal - An ATM terminal is located at Lake Region State College. Lake Region State College works with ATM Network to provide the service. Lake Region State College is responsible to keep the machine filled with money. Money is transferred from the customer's bank to a Lake Region State College bank account. To reconcile these items, reports are run which include credit card numbers. Those reports are kept in a locked cabinet.

Refunds - When an item or service is purchased using a credit card, and a refund is necessary, the refund should be credited to the credit card from which the purchase was made. If a refund in the form of a check is necessary, it should be approved by the departmental head/manager on a case-by-case basis. No cash refunds will be issued for returned items originally purchased with a credit/debit card.

Disputed Charges / Chargebacks - Occasionally, the Bank of North Dakota will send notification to the College indicating a disputed charge. A copy of this chargeback notification will be forwarded to the appropriate department by the Business Office. The department is required to provide all requested

information in response to the notification by the due date indicated. Failure to provide requested information in a timely manner will result in the department being charged for the transaction in question and the department cannot appeal the chargeback.

Recording and Reconciling Transactions - When submitting deposits to the Business Office, please include the following:

1. Merchant copy of the sales slip, which includes the signature, should only include the last four digits of the credit card number.
2. Daily Totals Report - this includes only the totals for MasterCard, VISA, and Discover; no credit card numbers are included.
3. Daily Detail Report - this includes the entire credit card number for all transactions.
4. Batch Settlement Report - this indicates the amount settled successfully.
    a. Departments should transmit and settle their batches daily.

Retention Periods - Documents supporting the credit card transaction must be retained by the department according to the College's Records Retention Policy.

The Business Office should retain the following documents for receipts processed with a Tender Type selection of Credit Card:

1. The merchant copy of the sales slip, which includes the signature, should only include the last four digits of the credit card number.
    a. Retention period is current fiscal year plus two prior fiscal years.
2. Daily Totals Report includes only the totals for each card type (MasterCard, VISA, Discover, and American Express); not credit card numbers are included.
    a. Retention period is current fiscal year plus two prior fiscal years.
3. Daily Detail Report includes the entire credit card number for all transactions.
    a. Retention period is current fiscal year plus two prior fiscal years.
4. Daily Batch Settlement Report indicates the amount settled successfully.
    a. Retention period is current fiscal year plus two prior fiscal years.

All Transaction documents, as stated above, must be secured, for example, in a locked cabinet/room with limited access.

Network Scans - Departments using networks or servers for credit cards transactions must follow PCI standards. Additional scans may be requested by the Bank of North Dakota.

PCI Self-Assessment Questionnaire - The Business Office is required to complete a PCI Self-Assessment Survey on an annual basis for each method of accepting credit cards. This policy will be reviewed at that time for possible changes. Service providers will be monitored to assure PCI DSS compliance status.

Responsibilities:

• Business Office	• With the assistance of Information Technology, grants authorization to departments to accept and process credit/debit card transactions. • Provides procedures for daily reconciling of credit card transactions. • Retain documents supporting credit card transactions as required.

	• Reconciles transactions on a monthly basis.
• Department Accepting Credit Cards for • Goods or Services	• Request/obtain prior approval from the Business Office/Information Technology to accept and/or process credit/debit card transactions. • Credit/debit card information must never be left in an open area where unauthorized persons are able to view it. • Notify the Business Offices immediately if there is a suspicion that credit/debit card records may have been compromised in any way. • If accepting credit/debit card information over the internet, a department must provide certification that the internet site/provider is PCI compliant prior to entering into a contract with the vendor/internet provider. The certificate must be submitted to the Business Office on an annual basis, or as requested. • Should take merchant fees into consideration when determining rates for goods and services. • Must follow the procedures for processing credit/debit card deposits. • Must not store any magnetic stripe information, including security codes, CVV/CVC, PIN number, CVV2/CVC2. • Reconcile and transmit credit/debit card transactions on a daily basis. • Retain all required credit/debit card documents in a secured location according to the records retention policy. • Do not request credit/debit card information via e-mail. When credit/debit card information is received by the department via e-mail, departments are required to notify the sender to discontinue sending such information via e-mail, as it is not a secured location. The transaction can still be processed. • When disposing of credit/debit card information, all documents must be shredded.

Plan Responsibility, Review, Updates and Approval - Responsibility for Lake Region State College's PCI (Payment Card Industry) Policy is assigned to the Information Security Response Team (see Information Security Response Policy).
These positions will work together and be responsible for coordinating Lake Region State College's PCI (Payment Card Industry) Policy including the following:

1. Annual review of the policy.
2. Complete PCI Self-Assessment Questionnaires.
3. Oversee scans of equipment.

History
Administrative Council Approved Update 06/11/15