Acceptance of Credit Cards Policy

Purpose

The District accepts Credit Cards for payment of goods and services under controlled conditions to protect against the exposure and possible theft of account and personal cardholder information that has been provided to Fargo Public Schools; and to comply with Payment Card Industry (PCI) requirements. The District must adhere to these standards to limit its liability and continue to process payments using payment cards.

Scope

This policy applies to all Fargo Public Schools departments, employees, contractors, consultants, temporaries, and other workers. This policy is applicable to any area that processes, transmits, or handles cardholder information in a physical or electronic format. All computers and electronic devices at Fargo Public Schools involved in processing payment card data are governed by the PCI Data Security Standard. This includes servers which store payment card numbers, workstations which are used to enter payment card information into a central system (for example, ordering tickets over the phone or activity fee payments), and any computers or credit/debit card swipe devices through which the payment card information is transmitted.

Policy

All transactions that involve the transfer of credit card information must be performed on systems approved by the Business Office and IT Department and will include a compliance and security review. Any specialized servers that have been approved for this activity must be housed behind a Fargo Public Schools firewall, approved by the Business Office and IT Department, and must be administered in accordance with the requirements of all Fargo Public Schools and PCI policies.

Departments involved with the acceptance of and processing of credit cards for payment of goods and services must design adequate processes to ensure the following are maintained:

- Approval of the Business Office before entering into any contracts or purchases of software and/or equipment related to credit card processing. This requirement applies regardless of the transaction method or technology used (e.g. e-commerce, POS device).
- Departments must comply with the Payment Card Industry Data Security Standard listed below.
- Establish departmental procedures for safeguarding cardholder information and secure storage of data. This pertains to ALL transactions initiated via the telephone, over the counter, mail order, Internet, etc.
- Credit card numbers must not be transmitted in an insecure manner, such as by e-mail, unsecured or stored fax (including Right Fax or similar networked fax servers), or through District mail.
- Sensitive cardholder data [i.e., full account number, card type, expiration, PIN, and card-validation code (three-digit or four-digit value printed on the front or back of the card)] will not be stored in any school system, personal computer, or e-mail account.
- Do not print the entire credit card number on either the merchant copy or customer copy of any receipts. Old receipts with the entire credit card number should have all but the

last four digits blacked out with permanent marker. Do not print the full credit card number under any circumstances.

- All documentation containing card account numbers must be stored in a secure environment until processed. Secure environments include locked drawers and safes, with limited access to only individuals who are processing the credit card transaction.
- Processing should be done as soon as possible and the credit card number should immediately be blacked out to the last four digits and the card expiration date must be masked.
- Stored credit card information will be retained according to the approved document retention policy of the District (see AP 3208 Record Retention Schedule). All media used for credit cards must be destroyed when retired from use. All hardcopies must be shredded prior to disposal.
- Background checks must be performed prior to hiring of any positions with access to stored cardholder information.
- Credit card handlers and processors must agree (in writing) not to disclose or acquire any information concerning a cardholder's account without the cardholder's consent, and to follow all PCI standards.
- Require all personnel involved in credit card handling to attend card security training every year in conjunction with required PCI audits.
- Assign an individual to administer the control of log-in privileges, limit software access to secure locations, delete access to software for terminated employees, and do not use vendor-supplied defaults for system passwords.
- Units using third-party software, including cash register systems, are prohibited from storing complete payment card numbers on District computers at any time.
- Contractually require all third parties with access to cardholder data to adhere to PCI security requirements and provide proof of PCI certification to the merchant department.

Procedures

All credit card and debit card processing contracts and renewals, including web-based procurement, must be initiated and approved through the Business Office. Because the sale of goods and services to entities outside the District may raise special considerations (e.g. unrelated business tax, accounting, legal, etc.), business plans concerning credit sales should also be reviewed by the Business Office. Please contact the Business Office to initiate or change services.

The District has a web-based solution for credit card sales. After review by the Business Office, a specialized Merchant Number will be established for the secure payment mechanism. The department will work with the Business Office and IT Department for integrating the payment mechanism. Once the payment program is properly configured to pass the required parameters, secure payment will be executed, and approval codes and other related elements will be returned to the originator. Accounting entries must be forwarded to the Business Office for entry into the finance system if not formally integrated.

Departments who need to accept credit/debit cards through a physical terminal or a Data Capture machine for either swipe or key transactions need to contact the Business Office to execute the required paperwork, obtain a Merchant Number, receive training, and be given direction as to the

accounting of those transactions on the books of the District. Data Capture machines must be configured according to PCI requirements to meet security standards and certified by District policy.

Under no circumstances will it be permissible to obtain credit card information or transmit credit card information by e-mail.

The Business Office reviews all proposed business plans involving credit card sales over the internet in conjunction with the IT Department and requesting area ,which includes:

- Reviewing each proposal for intended business purpose, consistency with the District's mission and policies, and selling department's ability to support an E-commerce activity.
- Following review and approval, the Business Office will notify the requesting department of approval status, determine the appropriate accounts and revenue object codes to be credited for sale proceeds, and issue a unique merchant ID identifier for the selling department.
- Any significant changes to approved Business Plans must be reviewed and approved by the Business Office prior to implementation. Changes may include such items as products or services to be sold, intended customer base, anticipated transaction volume, outside advertising, application software, or changes in the departmental contacts responsible for the e-commerce business plan. Proposed changes should be routed to the Business Office.

Sanctions
Departments not complying with this policy may lose the privilege to serve as a credit card merchant. Additionally, fines may be imposed by the affected credit card company, beginning at $50,000 for the first violation.

Persons in violation of this policy are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary action, suspension, termination of employment and legal action. Some violations may constitute criminal offenses under local, state, and federal laws. The District will carry out its responsibility to report such violations to the appropriate authorities.

Definitions and Resources
A. *PCI:* The PCI Standard is the result of collaboration between the four major credit card brands to develop a single approach to safeguarding sensitive data. The PCI standard defines a series of best practices for handling, transmitting and storing sensitive data.

B. *Cardholder data:* Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, or Card Validation Code (e.g., three-digit or four-digit value printed on the front or back of a payment card (e.g. CVV2 and CVC2 data)).

C. *Merchant*: any person or department accepting money for goods or services. Includes conference registrations, memberships, fees, etc.

D. Resources

Please see the PCI Security Standards Council website for resources and further information regarding security standards.

Payment Card Industry Data Security Standard (PCI DSS)

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data and sensitive information across open public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

What to Do If Compromised

In the event of a security incident, merchants must:

1. **Take immediate action to investigate the incident and limit exposure**.
    a. Contact the Business Office and IT Department to prevent further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information. To preserve evidence and facilitate the investigation:
    b. Do not access or alter compromised systems (i.e., do not log on to the machine and change passwords).
    c. Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable).
    d. Preserve logs and electronic evidence.
    e. Log all actions taken.

   f. If using a wireless network, change the Service Set I Dentifier (SSID on machines that may be using this connection with the exception of any systems believed to be compromised.
   g. Be on "high" alert and monitor all systems with cardholder data.
2. **Notify credit card companies immediately, and report investigation findings**. Be sure to contact:
   a. Your internal information security group, the Business Office and IT Department.
   b. Your merchant bank.
   c. If you do not know the exact name and/or contact information for your merchant bank, notify your credit card processer immediately.
   d. Your local office of the United States Secret Service.
   e. Your local office of the Federal Bureau of Investigation.
   f. Your local law enforcement agency.
      i. Your various card associations such as Visa, Mastercard and Discover.
3. **Provide all compromised accounts to your merchant bank within 10 business days.** All potentially compromised accounts must be provided and transmitted as instructed by your merchant bank and credit card issuers.
4. Within 3 business days of the reported compromise, provide an Incident Report document to your merchant bank.

Note: The credit card company, in consultation with your merchant bank, will determine whether or not an independent forensic investigation will be initiated on the compromised entity.

Adopted 1/11/11
Reviewed 7/23/13
Revised 7/2017
Revised 7/2022

FARGO PUBLIC SCHOOLS PCI SIGNATURE FORM

Fargo Public Schools employees working with credit cards must read and agree to the following:

A. Approval must be obtained from the Business Office before entering into any contracts or purchases of software and/or equipment related to credit card processing. This requirement applies regardless of the transaction method or technology used (e.g. e-commerce, POS device).
B. The Department must comply with the Payment Card Industry Data Security Standard.
C. Departmental procedures must be established for safeguarding cardholder information and secure storage of data. This pertains to ALL transactions initiated via the telephone, over the counter, Internet, etc.
D. Credit card numbers must not be transmitted in an insecure manner, such as by e-mail, unsecured or stored fax, or through mail (sealed envelopes must be used).
E. Sensitive cardholder data [i.e., full account number, card type, expiration, PIN, and card-validation code (three-digit or four-digit value printed on the front or back of the card) should not be stored in any system, personal computer, or e-mail account.
F. The entire credit card number must not be printed on any receipts. Old receipts with the entire credit card number should have all but the last four digits blacked out. Do not print the full credit card number under any circumstances.
G. All documentation containing card account numbers must be stored in a secure environment until processed. Secure environments include locked drawers and safes, with limited access to only individuals who are processing the credit card transaction. Processing should be done as soon as possible and the credit card number should immediately be blacked out to the last four digits and the card expiration date must be masked.
H. Stored credit card information will be retained according to the approved document retention policy. All media used for credit cards must be destroyed when retired from use. All hardcopies must be shredded prior to disposal.
I. Background checks must be performed prior to hiring of any positions with access to stored cardholder information.
J. I will not disclose or acquire any information concerning a cardholder's account without the cardholder's consent.
K. I will follow all PCI standards.
L. I agree to attend required card security training every year in conjunction with yearly PCI audits.
M. The District has assigned an individual to administer the control of log-in privileges, limit software access to secure locations, delete access to software for terminated employees.
N. I will not use vendor-supplied defaults for system passwords.
O. The complete payment card number is not stored in any third-party software, including cash register systems, and it is prohibited to store complete payment card numbers on District computers at any time.
P. All third parties with access to cardholder data are contractually required to adhere to PCI security requirements and provide proof of PCI certification to the merchant department.

I have read the above and understand Fargo Public School's security policies and procedures:

_____
Printed Name

_____ _____
Employee Signature Date

FARGO PUBLIC SCHOOLS PCI SIGNATURE FORM FOR STUDENT WORKERS AND CASHIERS

Fargo Public School students/cashiers who are taking credit cards for payments must read and agree to the following:

- Sensitive cardholder data [i.e., full account number, card type, expiration, PIN, and card-validation code (three-digit or four-digit value printed on the front or back of the card)] should not be stored in any District system, personal computer, or e-mail account.
- All documentation containing card account numbers must be stored in a secure environment until processed. Secure environments include locked drawers and safes, with limited access to only individuals who are processing the credit card transaction. Processing should be done as soon as possible and the credit card number should immediately be shredded or blacked out to the last four digits and the card expiration date must be masked.
- Credit card numbers should be written down only if necessary for processing a transaction and only if it has been approved by your supervisor/teacher. The number must be processed and shredded immediately.
- I will not disclose or acquire any information concerning a cardholder's account without the cardholder's consent.

I have read the above and understand Fargo Public School's security policies and procedures:

_____
Printed Name

_____ _____
Signature Date