County of Bedford, Virginia **Payment Security Policy**	
Treasurer's Office	**Issue/Effective Date: May 9, 2023** **Approval Date: April 24, 2023** **Approved By: County Administration**

I. Overview and Policy Purpose

Bedford County, VA accepts credit and debit card payments from customers and should protect the information on these cards to the greatest degree possible. Bedford County departments that accept credit card and debit card payments must comply with important rules that govern its acceptance of cards. This policy is established as required by those rules and applies to all employees who have access to card-processing systems and customer credit and debit cards while performing their jobs, as well as those employees who administer this policy. (PCI 12.1)

II. General Provisions

A. Definitions

Card	A customer credit or debit card.
Cardholder Data	The information (1) visible on a Card, i.e., the cardholder's name, expiration date, multi-digit card number, and verification digits; and/or (2) stored electronically on a Card; and/or (3) cardholder address. The cardholder's name and address, when either is separate from other Cardholder Data, is not considered Cardholder Data.
Card-Present Transaction	Payment is made when the cardholder and Card are present at our facilities.
Card-Absent Transaction	Payment is made when the cardholder and/or Card are not present at our facilities.
Card Rules	Payment Card Industry Data Security Standards, and the terms and conditions of agreements under which Bedford County, VA is contractually obligated related to Card- processing.
PCI-DSS	Payment Card Industry Data Security Standards and related guidance documents. (Note: references in this policy to specific PCI-DSS requirements are referred to herein in the format of "(PCI ##.#)"

B. Sensitive Information

Cardholder Data is highly sensitive and confidential. Anyone who has all Cardholder Data may have the ability to make payments, either by the cardholder or by someone else fraudulently. Cardholder Data has the highest sensitivity rating in Bedford County, VA financial policies, along with certain employee payroll information.

C. Authorization to Accept Cards as Payment

This policy expressly authorizes Bedford County, VA, and, its employees to accept payment from customers using Cards, in compliance with this policy.

D. Authorization to Establish Procedures

This policy expressly authorizes *County Administrator and Treasurer,* or any person duly authorized by these officials, to establish any procedure that may be required to enforce or ensure compliance with this policy. No other employee can establish or change procedures concerning this policy.

If departments have additional PCI policies and procedures, then they will need to be reviewed and approved by the compliance officer and cannot conflict with the overall Payment Security Policy.

E. Compliance Officer

The policy of the Bedford County, VA is to comply with Card Rules. The Treasurer shall serve as the Compliance Officer under this policy, shall review our compliance as required by Card Rules, and document all known instances of noncompliance for the purpose of remediating such noncompliance. The Compliance Officer shall establish a PCI- Compliance File to contain all documentation required by this policy. (PCI 9.1 and 12.1)

F. Annual Review

The Compliance Officer will review this policy and related procedures at least once each year, and update those as appropriate to reflect the latest Card Rules. The annual review and any policy updates shall be documented by the Compliance Officer. (PCI 12.1.1)

G. Policy Distribution

The Compliance Officer shall distribute this policy to all employees having card-processing responsibilities as it is updated. (PCI 12.1)

III. Card-Processing Devices

A. Authorized Devices

The following devices are authorized to process Card payments:

1. Payment Terminals - these machines accept Cards from cardholders and are always attended by Bedford County, VA employees (e.g. Clover terminal and Ingenico terminals), and shall be approved in accordance with PCI-DSS.
2. eCommerce sites – ACI Official Payments and Citizen Self Service – Tyler Payments
3. Other devices - other devices may be authorized by the Compliance Officer under any procedure issued under this policy.

B. Device Inventory

The Compliance Officer shall maintain an inventory of devices to this policy, which shall include

(PCI 9.9.1):

1. Make, and model of the device.
2. Location of device.
3. Device serial number or another method of unique identification.

C. Device Usage

Authorized employees who use card-processing devices shall comply with the following usage rules:

- Prevent user credentials or Cardholder Data from being viewed when entered into a device.
- Prevent unauthorized physical access and/or use of a device.
- To the degree within an employee's control, protect devices from the installation of unauthorized software or malware as directed by the Bedford County, VA Information Security policy and training.
- Ensure devices are in a locked or otherwise secure state when not in use.
- Report the loss or theft of a device to the supervisor.
- Ensure the secure disposal of devices retired from service.

D. Protection of Devices

Department supervisors and employees must help ensure the protection of Card-Processing Devices in their departments. The Information Technology Department shall protect physical access to electronic systems that process card transactions.

These procedures shall be followed (PCI 9.1, 9.9.2, 9.9.3):

- Devices should be inspected monthly to detect tampering or replacement of a device and documented on the inspection log. Supervisors shall submit the department's monthly log to the Compliance Officer upon request.
- Only persons authorized by the Compliance Officer or his/her designee shall be allowed to modify, troubleshoot, install, replace or repair Devices.
- Employees should be aware of suspicious behavior around Devices. Report suspicious behavior and indications of device tampering or substitution to the Compliance Officer.
- All Devices must be secured in a protected area when not monitored
- The Compliance Officer shall retain inspection logs in the PCI-DSS Compliance File for a rolling twelve-month period.
- The Compliance Officer shall direct personnel who are not involved with a particular Device's use to conduct random inspections of the Device.

IV. Cardholder Data Retention, Storage, and Disposal

Devices shall:

1. Not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.

2. Not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.

3. Not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.

4. Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.

5. Mask personal account number (PAN) when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.

Employees responsible for processing cardholder data shall <u>not</u>:

1. Write Cardholder Data on any document that the employee does not personally destroy, or personally deliver or communicate by phone to a County employee. For example, this includes:
    a. Throwing a document with Cardholder Data in the trash when no longer needed.
    b. Sending a document with Cardholder Data by interoffice mail.
    c. Leaving a document with Cardholder Data in an office inbox.
    d. Storing any document with Cardholder Data in any files in the employee's department
    e. "Destroy" means to shred the document containing Cardholder Data with a crosscut shredder.
2. Use any electronic device to process payments or access Cardholder Data **<u>UNLESS</u>** that device is approved by Bedford County, VA policy and procedures.
3. Save or transmit Cardholder Data by electronic means, including the following:
    a. Personally save or ask anyone else to save Cardholder Data on any Bedford County, VA, or another electronic device, like entering and saving it in a Microsoft program, or tablet/cell phone text message or memo.
    b. Copy a Card or Cardholder Data with any device – phone, tablet, copier, scanner, etc.

c. Email or ask any other person to email Cardholder Data to anyone. (If an employee receives unsolicited Cardholder Data via email, the employee will promptly delete the email from all mail system folders and inform the supervisor).
d. Fax from Bedford County, VA, or ask any other person to fax to the Bedford County, VA any Cardholder Data, except on a fax device specifically approved for such use by this policy or by the Compliance Officer AND is labeled as "APPROVED FOR CREDIT CARD USE."
e. Fax from Bedford County, VA or ask any other person to fax to Bedford County, VA any Cardholder Data using fax- via-email.
f. Otherwise ask a cardholder to Fax Cardholder Data to any other person.

4. Share Cardholder Data in any manner with any person not directly involved in the customer transaction.

The Compliance Officer or designee will review the Cardholder Data Retention, Storage, and Disposal section on a quarterly basis to confirm that no credit card data is stored or written down in compliance with this policy.

V. Information Security

1. Unprotected personal account numbers are not to be sent via end-user messaging technologies.
2. Access to Card-processing system components and Cardholder Data is restricted to only those individuals whose job requires such access.
3. Access to privileged user IDs is restricted to the least privileges necessary to perform job responsibilities.
4. Access to Card-processing system components is assigned based on the employee's job classification and function.
5. Usage policies shall comply with section 2.3 of this policy.
6. The Compliance Officer will grant explicit approval for employees to use Card-processing devices.
7. An inventory of Card-processing devices and employees with access shall be maintained.
8. Acceptable uses of the devices will be established.

VI. Credit Card Processing and Credit Card Providers

A. Authorized Providers

This policy expressly authorizes Bedford County, VA to purchase and use hardware and software systems from outside vendors that are designed to process Card transactions ("Providers"). All Providers must be compliant with PCI-DSS, and the Compliance Officer will review the certification of each Provider annually to verify compliance.

The Compliance Officer will exercise due diligence in the selection of Providers and review their compliance practices. This oversight may include a Provider's reporting practices, breach-notification and incident response procedures, details of how PCI-DSS responsibilities are

assigned between each party, how the Provider validates its PCI-DSS compliance, and what evidence of compliance it provides.

VII. Employee Responsibilities

A. Authorized Employees

Only an employee authorized by this policy and who must perform Card-related activities may use Bedford County, VA devices and systems for Card-related activities. The Compliance Officer shall determine which employees are authorized by this policy, pursuant to their job classification, and publish and disseminate.

Employees who are authorized to access electronic systems containing Cardholder Data will be granted access to such with a unique username and password, and access and privileges will only be granted to the least necessary to perform their job responsibilities.

B. Employee Training

The Compliance Officer shall establish and conduct training procedures concerning this policy for Bedford County, VA employees. The training shall be performed at least annually, and when new employees are authorized under this policy. Documentation of training events shall be maintained Bedford County, VA.

The Compliance Officer or designee shall establish a separate usage procedure for each approved device.

C. Employee Responsibilities

Bedford County, VA employees who have card-related responsibilities must comply with the following:

1. Shall not give their username and/or password for accessing any Bedford County, VA electronic system.
2. Shall not allow another person to observe the employee's entry of login information into any Bedford County, VA electronic device.
3. Shall use Card-processing devices as described in the Payment Security policy.
4. Shall not ignore, prevent or disable the installation of software updates to devices accessed and/or controlled by the employee that are used in Card-processing, to the extent the device provides notification of a needed update.
5. Shall protect card-processing devices as in Payment Security policy, as directed by their supervisor.
6. Safeguard and protect Cardholder Data as described in the Payment Security policy.
7. Follow the Card-Present, Card-Absent, and Recurring Billing policies of this section.

D. Employee Responsibility to Report

Any employee that has knowledge of or suspects (1) a violation of this policy, (2) a loss or theft of Cardholder Data, or (3) suspicious activity related to the use of Cards must report that as soon as possible to his/her supervisor, noting that the supervisor should notify the Compliance Officer.

E. Department Inspection of Credit Card Devices

Bedford County departments who have card-related responsibilities will be responsible for inspecting devices for tampering on a monthly basis at a minimum. Departments may do more frequent checks.

F. Card-Present Transaction

A Card-Present Transaction is where payment is made when the cardholder and Card are present at our facilities. This can be while an employee is present during the transaction, like with the Payment Terminal, or not, like when a customer uses a parking exit machine. The specific procedures for handling Card-Present Transactions shall be developed for the various situations to which they apply. In general, a Bedford County, VA employee present during a Card-Present Transaction shall do the following:

- Use a Bedford County, VA-approved device, in accordance with the training provided.
- Do not allow any other person to observe the entry of login information into the device or system.
- Instruct the cardholder to use the device for making payment - the employee should not handle the Card unless absolutely necessary.
- If the Card is declined, inform the cardholder, and make alternative payment arrangements.
- Report any suspicious behavior to your supervisor.
- Logoff system and device, if applicable.

G. Card-Absent Transaction

A Card-Absent Transaction is where payment is made when Cardholder and Card are not present at our facilities, which will be by phone. This includes when a Cardholder is present and does not have the Card but does have the Cardholder Data.

An employee handling a phone payment shall do the following:

- Use a Bedford County VA-approved device, in accordance with the training provided.
- For mobile devices, access the Bedford County VA-approved system, in accordance with the training provided.
- Do not allow any other person to observe the entry of login information into the device or system.

- Prior to accepting any Cardholder Data from the caller, the employee should have access to a card-processing device, or transfer the caller to an employee who does.
- If an employee has access to a device:
  - Ask the caller for Cardholder Data and enter the information into the device while on the call.
  - Report the results of the processing to the caller.
  - Retain the authorization information.
- If the employee does not have access to a device, the employee must request that the Cardholder call back or permit the Bedford County VA to call the Cardholder when a card-processing device can be available during the call.
- Logoff system and device, if applicable.

VIII. Incident Response

See Incident Response Policy

IX. Policy Enforcement

The Bedford County, VA Treasurer is the policy administrator and will ensure this process is followed. Additionally, department heads and managers are responsible for compliance with County policy within their respective administrative areas.

Robert Hiss
County Administrator