PCI DSS Compliance Policy

Contents

1. **Purpose** 1
2. **Applicability** 1
3. **Policy** 1
4. **Policy Non-Compliance** 2
5. **Audit** 2
6. **Definitions** 2
7. **Approval and Revision History** 2
8. **Background** 3

1. Purpose

The Payment Card Industry Data Security Standard (PCI DSS) v4.0 requires Buncombe County to maintain robust credit card security measures to protect cardholder data and ensure continued eligibility for payment card services. Adoption of PCI DSS v4.0 strengthens the County's ability to address evolving threats, improve security outcomes, and promote a sustainable compliance program. Buncombe County management remains committed to implementing, maintaining, and continuously improving these security measures in support of organizational objectives and the protection of resident data and therefore requires all County employees and agencies that handle credit card payments on behalf of the County to adhere to this policy

2. Applicability

This policy applies to all Buncombe County agencies, departments and employees who handle credit cards and credit card data, unless there is a conflict with GS 153A-103 related to hiring, discharging, and supervising employees. Such exclusion is noted at the end of this policy. Otherwise, departments may adopt and enforce policies that are more restrictive than County Policy.

3. Policy

3.1. **County Compliance:** Buncombe County will comply with PCI DSS v4.0 requirements for all systems and processes that store, process, or transmit cardholder data within the County domain. This includes, but is not limited to, on-premises infrastructure, vendor-hosted platforms, and web-based applications. All systems must meet or exceed baseline security expectations as outlined in PCI DSS v4.0 and associated implementation guidance.
Implementation of PCI DSS v4.0 controls is governed through the County's IT Security Policy framework. Each PCI control domain is mapped to its corresponding County policy as listed in Addendum A. Those policies represent the authoritative standards for operational enforcement.

3.2. **Vendor Compliance:** Vendors processing payment data must provide proof of PCI DSS v4.0 compliance verified by an independent Qualified Security Assessor (QSA) within the past 12 months.

3.3. **Governance:** The Director of Finance shall oversee the maintenance of non-technical PCI DSS policies and coordinate with IT and Customer Service teams for compliance alignment. The Finance Director and Chief Information Security Officer (CISO) will jointly coordinate compliance validation activities and periodic self-assessment reviews.

This is a controlled document intended for Buncombe County Government use. Any documents appearing in paper form are not controlled and should be verified with the electronic file version prior to use. For support related to this policy and procedures, contact the Finance Department.

3.4. **Technical Controls:** The CISO shall define PCI DSS boundaries, manage segmentation controls, oversee quarterly vulnerability scans and annual penetration testing, and ensure technical controls are continuously tested and enforced across the enterprise.

3.5. **Third-Party Oversight**: The CISO, via the Third-Party Risk Management (TPRM) process, will review and validate vendor PCI compliance during acquisition, renewal, or changes to scope.

3.6. **Significant Changes**: Any changes to the cardholder data environment (CDE), including network architecture or payment workflows, will initiate a re-validation of applicable PCI controls.

3.7. **Training:** All employees who handle cardholder data or operate payment systems must complete annual PCI DSS-specific training, including data breach and tamper detection content.

3.8. **Scope Maintenance:** All PCI DSS control areas applicable under v4.0—including but not limited to strong access control, vulnerability management, secure system design, and continuous monitoring—will be implemented and periodically tested for effectiveness.

4. **Policy Non-Compliance**
Employees willfully violating the terms and conditions of this policy may be subject to appropriate disciplinary action, up to and including dismissal.

5. **Audit**
All policies for Buncombe County may be subject to audit or review as outlined in the Internal Auditor's Statement.

6. **Definitions**
6.1. **Cardholder Data Environment (CDE) -** The people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data.
6.2. **Sensitive Authentication Data -** Security-related information (e.g., full track data, card verification codes, PINs) that must not be stored after authorization.
6.3. **Segmentation -** The process of isolating the CDE from out-of-scope networks or systems using firewalls, VLANs, or other technical controls to reduce PCI DSS scope.
6.4. **Qualified Security Assessor (QSA) -** A PCI SSC-approved entity qualified to assess compliance to the PCI DSS standard.

7. **Approval and Revision History**

Policy Origination Date:	July 1, 2017
Requires Board Approval:	☐Yes ☒No
Board Approval Dates:	6/21/2016; 9/21/2021
Policy Exceptions:	None
Revision History:	11/12/2017 – added PCI requirement 11.3.4 11/14/2025 – rewrite to include new version of PCI-DSS Standard (v4.0) Initial version was v3.0. -Corrected approval from board approved to county manager approval.

8. **Background**

For a full listing of requirements, please visit http://pcisecuritystandards.org/. Additional standards details can be found at the links below:

8.1. Difference between v3.2.1 and v4.0 - Data Security Standard (pcisecuritystandards.org)
8.2. Version 4.0 - Payment Card Industry Data Security Standard (pcisecuritystandards.org)
8.3. Version 3.2.1 - PCI DSS-v3-2-1-r1.pdf (pcisecuritystandards.org)
8.4. Version 3.2.1 ROC reporting template - PCI DSS-v3_2_1-ROC-Reporting-Template.pdf (pcisecuritystandards.org)
8.5. Mapping PCI DSS v3.2.1 to the NIST Cybersecurity Framework v1.1 - Microsoft Word - Mapping-PCI DSS-v3_2_1-to-NIST-Framework_24Jun2019_clean.docx (pcisecuritystandards.org)

Addendum A – PCI DSS v4.0 Control Policy Cross-References

The following table identifies how Buncombe County's existing IT Security Policy framework supports and satisfies PCI DSS v4.0 control domains. Each referenced policy or procedure represents the authoritative source for implementation and enforcement of the associated control area.

PCI DSS v4.0 Requirement Domain	Control Intent (Summary)	Referenced IT Policy / Procedure	Primary Owner
1. Network Security & Firewalls	Ensure segmentation, boundary protection, and secure connectivity for cardholder systems.	IT Network Security & Firewall Management Policy (Section 4.1–4.3)	IT Infrastructure Manager
2. Secure Configuration & Defaults	Remove vendor defaults, enforce configuration baselines, and secure system builds.	System Hardening & Configuration Management Policy (Section 5.2)	IT Systems Engineering
3–4. Cardholder Data Protection & Encryption	Encrypt stored and transmitted cardholder data; prohibit storage of sensitive authentication data.	Data Encryption & Handling Policy; Data Classification Policy	CISO / Data Governance
5. Malware & Endpoint Protection	Maintain anti-malware, EDR, and patch controls on all endpoints in scope.	Endpoint Security & Threat Protection Policy	IT Security Operations

6. Vulnerability Management & Patch	Identify and remediate vulnerabilities and apply patches timely.	Vulnerability Management Policy; Patch & Update Procedure	IT Security Operations
7–8. Access Control & Authentication	Restrict access to the CDE by business need; enforce MFA and unique credentials.	Identity & Access Management (IAM) Policy; Remote Access Policy	CISO / IAM Admin
9. Physical Security	Protect physical access to payment systems and media.	Physical Security & Environmental Controls Policy	Facilities / Finance
10. Logging & Monitoring	Collect, review, and retain logs of all CDE system activities.	Security Monitoring & Incident Detection Policy	SOC / IT Security
11. Testing & Assessments	Conduct quarterly vulnerability scans and annual penetration tests.	Continuous Monitoring & Assessment Policy; Testing Procedure	CISO / GRC
12. Security Governance, Training, and Incident Response	Maintain policies, awareness programs, and formal IRP for security events.	IT Security Governance Policy; Incident Response Plan; Training & Awareness Program	CISO / Finance Director
13. Third-Party Risk Management	Validate vendor PCI compliance and security posture.	Vendor & Third-Party Risk Management Policy	Procurement / CISO