Category	Old Policy (2017)	New Policy (2025)	Change Summary / Impact
Document Structure	12 PCI DSS requirement sections (v3.0 structure), detailed technical guidance embedded in each section.	Streamlined to 8 sections (Purpose, Applicability, Policy, Non-Compliance, Audit, Definitions, Approval, References).	Moved from technical procedure style to a governance/policy format; technical implementation now implied to exist in subordinate procedures.
Version Reference	Based on PCI DSS v3.0 / SAQ B-IP (2014).	Explicitly aligned with PCI DSS v4.0 (2022 standard).	Updated to reflect latest PCI DSS version, including risk-based validation and continuous testing expectations.
Scope & Applicability	Focused on limited POS environment; explicitly excludes card data storage.	Applies enterprise-wide: all systems that store, process, or transmit cardholder data, including cloud and vendor environments.	Broader applicability across County systems and vendor integrations; reflects modernization and digital transformation.
Governance Responsibility	IT and Finance Directors jointly responsible.	Finance Director oversees non-technical policies; CISO manages technical compliance and boundaries.	Establishes shared governance, introduces CISO accountability, and aligns with enterprise GRC framework.
Vendor Management	Minimal mention under Requirement 12.8.	Dedicated **Vendor Compliance** and **Third-Party Oversight** sections; mandates annual QSA validation for vendors.	Introduces structured TPRM (Third-Party Risk Management) alignment with PCI DSS v4.0 vendor oversight requirements.
Technical Controls	Explicit requirements for firewalls, encryption, authentication, and patching detailed per PCI section.	Summarized under “Technical Controls” with ongoing validation, segmentation, and continuous testing.	Consolidates granular requirements into higher-level control objectives; assumes technical standards documented elsewhere (e.g., IT Security procedures).
Training & Awareness	Security awareness noted briefly in Requirement 12.6.	Annual PCI-specific training required, including breach and tamper detection.	Expands training to include specialized PCI-focused modules.
Incident Response	Detailed incident response with Visa/Mastercard reporting flow and law enforcement contacts.	Not directly included; implied under overall security governance.	Operational response steps likely migrated to separate Incident Response Plan or playbook.
Audit & Compliance Validation	References quarterly scanning and annual testing under Requirement 11.	States that all County policies may be audited per Internal Auditor’s Statement.	Moves from system-level scan requirements to enterprise audit alignment; indicates a shift to continuous compliance posture.
Definitions Section	Not formally defined.	New section defining terms: CDE, Untrusted Network, Sensitive Authentication Data, Segmentation, QSA.	Improves readability and governance consistency.
References / External Links	None included.	Lists PCI SSC resources, including mapping guides and v3.2.1→v4.0 comparison.	Provides traceability to authoritative standards and cross-framework mapping (NIST CSF).
Board Approval Process	Explicitly dated approvals by IT/Finance and Board.	Structured approval workflow: requires Board approval; version history and origination dates provided.	Standardizes documentation lifecycle under County governance policy format.
Tone and Focus	Technical and compliance-centric (“how to configure systems”).	Policy and governance-centric (“who is responsible and what must be maintained”).	Transitions from implementation document to executive-level policy document.
New Emphasis Areas (v4.0)	—	Continuous monitoring, segmentation validation, risk-based testing, vendor QSA validation, and governance separation.	Introduces risk-based approach and integrated compliance monitoring—aligned with County’s broader GRC and continuous monitoring strategy.