Payment Systems
Standard Operating Procedures

See also the Colorado College PCI Compliance Policy

1. General Security Requirements

1.1 Cardholder Data (CHD) Handling
Cardholder Data must never be stored in any electronic format including emails, spreadsheets, systems, screenshots, or handwritten notes that are later digitized. Only truncated PAN (last four digits) may be retained on paper when required for reconciliation or legal purposes. Departments must ensure no full card number, CVV, or expiration date is retained under any circumstance.

1.2 Access Control
Access to all payment systems must be role-based and approved by the Finance Department. Each user must have a unique ID and credentials must never be shared. Multi-factor authentication (MFA) is required for all systems. Passwords must be at least 12 characters, include complexity, and be rotated every 90 days. Access must be revoked immediately upon termination or role change.

1.3 Training Requirements
All personnel involved in payment processing must complete PCI DSS awareness training prior to being granted access and annually thereafter. Please reach out to the IT and Finance office for new employee training.

1.4 Monitoring and Review
Departments must perform monthly transaction reviews to ensure accuracy and reconciliation. Quarterly reviews must validate user access, confirm no CHD storage, and verify that all third-party providers remain PCI compliant.

1.5 Network and Device Security
All payment devices must operate on secure, segmented networks and use encrypted communication such as P2PE or E2EE. Devices must be approved and inventoried by Finance and IT and cannot be transferred between departments without approval.

1.6 Incident Response
Any suspected breach must be reported immediately to Finance and IT. Departments must not investigate independently. Finance and IT will manage response and escalation.

2. Payment Process Procedures

2.1 Card-Present Transactions
All in-person and terminal-based payments must be processed through PCI-approved devices. Staff must verify cardholder identity if necessary, ensure receipts are issued, and confirm no data is stored. Daily inspections of devices must include serial number verification, tamper seal checks, and visual inspection for skimming devices. Devices must be secured when not in use.

2.2 Online Transactions
All online transactions must be fully outsourced to PCI-compliant providers such as CyberSource, PayPal, Ticketmaster, or other approved providers. Customers must be redirected to secure payment pages. Users must access systems via secure devices with multi-factor authentication (MFA) enabled. Quarterly reviews must confirm online transaction providers remain PCI DSS compliant (via Visa's Service Provider List https://www.visa.com/splisting/searchGrsp.do).

2.3 Phone Transactions
No card details can be communicated via phone.

2.4 Email Transactions
Email payments are strictly prohibited. Any card data received via email must not be processed, and the email must be deleted immediately. Customers should be notified using a separate communication method.

2.5 Data Retention and Storage
Only truncated card data may be stored in paper format for legitimate business needs. Records must be secured in locked cabinets with restricted access. Data must be reviewed quarterly and destroyed when no longer required.

2.6 Secure Disposal
All paper records containing card data must be cross-cut shredded immediately after retention periods expire. Disposal must be monitored and documented.

2.7 Refund Procedures
Refunds must be processed through the original payment method and system. All refunds require documentation and must be approved. Standard refund window is 30 days and processing may take 7–10 business days.

2.8 Reconciliation, Settlement, and Chargebacks
Departments must reconcile transactions monthly and settle batches daily. Records must be retained for audit purposes. Chargebacks must be responded to promptly with supporting documentation when required.

2.9 Physical Security
Devices must be secured, inspected daily, and only accessed by trained personnel. Staff must be trained to identify suspicious behavior and unauthorized access. Daily inspections of devices must include serial number verification, tamper seal checks, and visual inspection for skimming devices. Devices must be secured when not in use. No troubleshooting may be performed outside IT oversight.