(1) DEFINITIONS

(a) Payment Card Industry Data Security Standards (PCI-DSS): A set of standards established by the Payment Card Industry Security Standards Council to develop a single approach to safeguarding sensitive data. The PCI-DSS defines a series of best practices for storing, processing or transmitting cardholder data.

(b) Cardholder Information: Any personally identifiable data associated with a cardholder or a payment card. Examples include but are not limited to: account number, expiration date, name, address, social security number and the three- or four-digit value printed on the front or back of payment cards (MasterCard Card Validation Code CVC 2, VISA Card Verification Value CVV2, Discover Card Member ID or American Express Card Identification Number CID).

(c) Point of Sale Terminal: An electronic retail payment device which (1) reads a customer's bank's name and account number when a bank card or credit card is swiped (passed through a magnetic stripe reader), DIP (card chip is entered into reader), TAP (contactless payment technology using mobile wallets) or entered directly into payment application, (2) contacts the bank and (if funds are available) transfers the customer approved amount to the seller's account and (3) may print or email a receipt.

(d) Credit Card: A plastic card issued to concede to the holder, upon presentation to authorized stores or service providers, products or services on credit.

(e) Debit Card: A plastic card that may be used for purchasing goods and services or obtaining cash advances for which payment is made from existing funds in a bank account.

(f) “Need to Know”: Access to the information must be necessary for the conduct of one's official duties.

(2) DUTIES AND RESPONSIBILITIES

(a) Head of Information Technology

(i) Provides oversight of information security policy, procedures and standards in accordance with applicable laws and standards to secure data and information systems.

(ii) Establishes an appropriate level of visibility for the policy, procedures and standards, and information risk assessment to the College.

(b) Information Technology (IT) Director(s)

(i) Complies with information security policies and procedures. Manages and monitors information systems that support the College's information security infrastructure.

(ii) Maintains awareness of the security resources and ensures that security-related activities are well documented and completed in a consistent, auditable manner.

(iii) Conducts periodic reevaluation of current operational methods to identify areas for improvement.

(iv) Evaluates security risks of new and existing systems along with the information security team in accordance with applicable policy and procedures.

(v) Implements appropriate security controls commensurate with the acceptable level of risk.

(c) Head of Information Security

(i) Partners with constituencies across the campus community to develop and implement strategies, plans and programs for security compliance. Serves as a liaison for regulatory compliance on behalf of the College.

(ii) Develops procedures, standards and practices for securing information systems.

(iii) Conducts risk assessments and analysis in accordance with applicable laws and standards to secure the College's information systems.

(iv) Ensures completion of corrective action plans and information system integrity is not compromised.

(v) The head of Information Security reserves the right to restrict access to vulnerable systems in accordance with applicable policy and procedures.

(d) Administrators and supervisors of cardholder data environment

(i) Complies with College policies and procedures governing the security of the resources they manage.

(ii) Helps to maintain an adequate inventory of all equipment and serves as a point of contact for the information technology team as it pertains to processing credit card transactions.

(iii) For purposes of this procedure and applicable policy, department administrators and supervisors include individuals and College employees within College departments, clinical sites and all others in the campus community that oversee the use of payment card processors and credit card transactions.

(iv) Ensures only authorized personnel have access to payment card applications and data.

(v) Ensures payment card account numbers are properly secured and safeguarded.

(vi) Ensures accounts are properly reconciled with discrepancies immediately reported to Business Services. To maintain proper segregation of duties and minimize the risk of fraud, the individuals administering College financial systems may not be the same individual that initiates, authorizes and processes the transactions.

(e) Business Services

(i) Works with College department(s) to create and test payment card applications before implementation.

(ii) Works with external vendors to ensure compliance with College policies, practices and procedures for accepting and use of payment cards.

(iii) Verifies that payment card applications are PCI-DSS compliant and, if applicable, on the Payment Application Best Practice (PABP) list.

(f) Payment Card Processors

Responsible for reviewing, understanding and implementing the requirements set forth in applicable policy and this and other procedures.

(3) MAINTENANCE

(a) Annual review of applicable policy and procedures is required and revisions will be made as necessary, or at times of major change to the cardholder data environment or to update the PCI-DSS standards.

(b) All individuals accessing systems within the cardholder data environment are required to use their own uniquely assigned username and password. Sharing passwords or active sessions to any PCI system is strictly prohibited. See also Policy 15-01.

(c) The Information Technology (IT) department will maintain an inventory of all assigned credit card devices and other electronic payment systems in use in the College community.

(d) Any deployment, modification or removal of new or old products or technology for the use of processing credit card transactions must be reviewed, assessed and approved by IT.

(4) SERVICE PROVIDERS AND INCIDENT RESPONSE

(a) Use of third party service providers for the purpose of payment card processing must be reviewed and approved by the head of Business Services or designee and the head of IT.

(b) External service providers must be PCI-DSS compliant and provide current, certified proof of compliance upon request.

(c) A risk assessment is required for any new third party service providers responsible for possessing, storing or processing cardholder data on behalf of the College. At a minimum, members of the information security team and/or College counsel should be involved to adequately assess the service provider. The risk assessment should include a review of the service providers' policies demonstrating their commitment to comply with PCI DSS standards.

(d) The information security team and/or Computer Security Incident Response Team (CSIRT) will test the incident response plan and include reporting requirements in the event of a suspected incident or breach involving cardholder data. The incident response plan includes appropriate provisions for reporting and escalating incidents pertaining to the cardholder data environment and is the authoritative plan pertaining to this procedure and associated policy.

(5) FIREWALL

(a) The College will develop and implement formal, documented standards for its firewalls and routers. Such standards may include:

(i) A formal process for approving and testing network connections and changes to College firewall and router configurations.

(ii) A current network diagram that identifies connections between the College's cardholder data environment and other networks, including wireless networks.

(iii) A current diagram that shows College cardholder data flows across systems and networks; the diagram will be updated as needed

(iv) Requirements for a firewall at each internet connection and between any Demilitarized Zone (DMZ) and the College's internal network zone.

(v) Documentation and business justification for use of services, protocols and ports allowed by the College's firewalls and routers, including documentation of security features implemented for those protocols considered to be insecure (e.g., FTP, TELNET, POP3, IMAP, and SNMP V1 and V2).

(vi) A review of the College's firewall and router rule sets at least once every six (6) months.

(b) College firewall and router configurations will restrict connections between untrusted networks and any system components in the College's cardholder data environment. Such configurations will utilize best practices:

(i) Restrict inbound and outbound traffic necessary for the College's cardholder data environment and specifically deny all other traffic.

(ii) Configure perimeter firewalls between all wireless networks and the College's cardholder data environment to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the College's cardholder data environment.

(iii) Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols and ports.

(iv) Limit inbound internet traffic to IP addresses within the DMZ.

(v) Not allow direct connections inbound or outbound for traffic between the internet and College's cardholder data environment.

(vi) Implement anti-spoofing measures to detect and block forged source IP addresses from entering the College's network.

(vii) Restrict unauthorized outbound traffic from the College's cardholder data environment to the internet, unless there is a documented business need.

(viii) Implement a stateful inspection (i.e. dynamic packet filtering) firewall to allow only authorized connections into the College's network.

(ix) Not disclose private College IP addresses and other internal routing information to unauthorized parties (e.g., masquerading via implementation of Network Address Translation (NAT), proxies, etc.).

(x) Install personal host-based firewalls or equivalent software on any mobile device or computer containing, storing, accessing or transmitting College data over the internet. These firewalls will be configured to prevent unauthorized users from altering or disabling the firewall.

(6) PROTECTION OF STORED CARDHOLDER DATA

With the College implementing end-to-end encryption for the transmission of cardholder data, digital or "hard copy" cardholder data shall not be stored after authorization in the College's cardholder data environment. Where cardholder data is collected in a paper format, the following controls must be adhered to:

(a) Paper documents containing cardholder data must be redacted of sensitive authentication data (full track data, card validation code or value, and pin data) after the credit card has been authorized.

(b) All redacted paper documents shall be retained in accordance with the College's data/records retention standards.

(c) When the cardholder's Primary Account Number (PAN) is displayed, the PAN must be masked such that only the first six or last four digits are displayed. Only personnel with a legitimate business need has authorization to review the full PAN.

(d) Cardholder data should not be stored on servers, local hard drives or external media including "hard copy documents," floppy discs, CDs and thumb drives unless encrypted and otherwise in full compliance with PCI-DSS.

(7) ENCRYPTION OF TRANSMITTED CARDHOLDER DATA

(a) The College's cardholder data environment shall be isolated and segregated from the rest of the College network. Access to the College's cardholder data environment from unsecure networks, including any wireless technologies, is prohibited.

(b) Any transmission of cardholder data must be encrypted using strong cryptography and security protocols. The encryption standard shall be approved by IT.

(c) For any browser-based transactions of cardholder data, the system shall be configured to utilize secure HTTP (HTTPS), over Transport Layer Security (TLS) version 1.2 or greater, for encryption.

(d) Cardholder data shall not be sent unprotected via email, text message, instant messaging, chat or other communication protocols. Sending sensitive authentication data through these protocols, even with added encryption, is strongly discouraged.

(8) MALWARE PROTECTION

(a) The cardholder data environment must be configured and monitored accordingly to protect against malware infections.

(b) IT-approved antivirus software must be deployed, configured and activated on all workstations and servers within the cardholder data environment that is handling or processing cardholder data.

(c) All antivirus clients must be current (within three update revisions) with the latest definition updates and rulesets.

(d) The antivirus software must be configured to generate audit logs at the time of detection or quarantine of malware.

(e) The antivirus software must be capable of performing a periodic scan if initiated by a system administrator.

(f) Antivirus software must be configured so as to prevent other system users from disabling or altering the configuration settings.

(g) Any exceptions or exclusions that result in a temporary or permanent change to the antivirus software must be submitted to IT for review and implementation.

(9) SECURE SYSTEMS AND APPLICATIONS

(a) IT runs vulnerability scans of all systems within the cardholder data environment.

(b) All systems are patched with the latest security updates on a consistent basis. Systems that appear to be vulnerable to a threat and have a high likelihood of compromise may be blocked by IT from accessing the network, including the internet.

(10) LOGICAL ACCESS CONTROL MEASURE

(a) Access to the cardholder data environment is restricted to a "need to know" basis to authorized individuals only, based on role, job function and responsibility.

(b) Access rights to privileged cardholder information will be assigned to employees and, if applicable, contractors with the minimum access necessary to perform their job responsibilities.

(c) Individuals processing cardholder data must complete the appropriate PCI training courses offered by the College to understand the requirements of and compliance with the PCI-DSS standards. Such users must be authorized by a supervisor to complete the training in accordance with their job functions and responsibilities.

(d) Department personnel assigned to process payment card transactions must receive training on the process, policies and procedures in order to report and include those transactions in the College's financial systems.

(e) The Business Services area of the College will provide training to ensure employees accept and process payment cards in compliance with PCI-DSS standards.

(f) Users that do not require access to the cardholder data environment will not be provided access without proper authorization.

(g) Access to the cardholder data environment shall be reviewed and recertified to ensure authorizations are accurate and reflect current responsibilities.

(h) Administrators of College departments who need to accept payment cards and/or obtain a physical terminal to swipe, DIP, TAP or key transactions through a point of sale terminal must request approval from the head of Business Services or designee.

(i) Exceptions to this procedure may be granted only after a written request from the department has been reviewed and approved by the head of Business Services or designee.

(11) AUTHENTICATION TO SYSTEM COMPONENTS

(a) All individuals accessing the cardholder data environment must comply with the requirements set forth in College Policy 15-01 and all other applicable policies.

(b) The following controls and requirements apply to vendors and other third parties supporting and/or requiring access to the cardholder data environment:

(i) A uniquely-assigned account must be used to access the cardholder data environment.

(ii) The uniquely-assigned accounts must allow access to only the roles and modules required for purposes of support ("need to know" method).

(iii) Accounts must be recertified on an annual basis. Sign-off is required by the vendors' or third parties' sponsor in order to maintain access to the system.

(iv) A shared session should be used when a vendor or third party must connect to the cardholder data environment via remote access.

(12) PHYSICAL ACCESS CONTROL MEASURES

The following controls shall be adhered to in order to ensure adequate physical security of cardholder data:

(a) Network jacks and/or wireless access points located in public areas and areas accessible to visitors shall not provide access to the dedicated cardholder data environment Virtual Local Area Network (VLAN).

(b) Confidential data shall not be left in plain sight. Cardholder data stored in paper format must be labeled as confidential and securely kept and locked up when unattended.

(c) Workstations must be locked after no more than fifteen (15) minutes of inactivity when left unattended.

(d) An inventory of cardholder data must be maintained and includes the location of cardholder data in electronic and paper formats (i.e. specific storage closets, cabinets, servers, data centers, etc.).

(e) All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. Media must be destroyed using an approved technique (disintegrate, pulverize, melt, incinerate or shred) to ensure cardholder data is not recoverable.

(f) Devices that capture payment card data via direct physical interaction with the card (i.e. a card swipe, chip reader or TAP) must be protected from tampering or substitution.

(g) Card reading devices should be removed at the end of each business day and securely stored in a locked cabinet or office to protect against tampering or substitution when possible.

(i) Card reading devices that cannot be removed, disconnected and securely stored should be inspected for tampering or substitution at the start of each business day.

(ii) Card reading device inspections include:

1. Ensuring the manufacturer's name and model number are correct.

2. Validating the serial number against the department's inventory.

3. Confirming the manufacturer's security seals and labels are present with no signs of peeling or tampering.

4. Verifying the device's color and condition are as expected, with no additional marks or scratches around the seams, reader and/or window display.

(h) Individuals interacting with credit cards and card reading devices should be aware of and trained on the requirements set forth in this procedure to ensure devices have not been tampered with or substituted.

(13) MONITORING OF NETWORK RESOURCES

(a) All critical system and network components within the cardholder data environment will be configured to track and record audit logs linking individuals to actions. Logs should be forwarded to the IT event manager system to ensure logs are tracked, reviewed and monitored as well as stored in a secure location where they cannot be modified.

(b) Automated audit logs should include the following information in order to construct a timeline in the event of an incident or investigation:

(i) All individual user accesses to cardholder data, whether at the operating system or application level.

(ii) All actions taken by any individual with root or administrative privileges.

(iii) Access to all audit trails by any individual.

(iv) Individual or denied access attempts, such as failed or bad password.

(v) Use of and changes to authentication mechanisms, such as creating new accounts, elevating user privileges, etc.

(vi) Initialization, stopping or pausing of the audit logs.

(vii) Creation and deletion of system-level objects.

(c) All system components within the cardholder data environment should record the following information in the audit logs:

(i) User account or identification

(ii) Type of event

(iii) Date and time

(iv) Success or failure indication

(v) Origination of event

(vi) Identity or name of affected data, system component, or resource

(d) Errors, anomalies or suspicious entries are reviewed and escalated according to standard incident response processes and procedures. All audit log entries, specific to the cardholder data environment, shall be retained for at least one (1) year, with a minimum of three (3) months immediately available for analysis.

(14) SECURITY SYSTEM AND PROCESS TESTING

(a) System components, processes and applications shall be tested frequently to ensure security controls continue to reflect a changing environment.

(b) Vulnerability scans shall be run at least quarterly and after any significant change in the network which impacts the cardholder data environment.

(c) Internal quarterly vulnerability scanning must be performed by members of IT and repeated until all “high risk” vulnerabilities are resolved, remediated and/or exempted.

(d) External quarterly vulnerability scanning will be performed by an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC) and repeated until all “high-risk” vulnerabilities are resolved, remediated, and/or exempted.

(e) Changes to systems housing account information must only be performed when:

(i) Thorough testing has taken place to ensure adequacies of controls.

(ii) Functionality testing with module custodians and/or functional experts has taken place.

(iii) Change control processes have been followed.

(f) Internal and external penetration testing should be conducted every six (6) months and/or after any significant infrastructure or application upgrade or modification. Penetration testing shall include:

(i) Coverage of the entire cardholder data environment perimeter, critical systems and applications.

(ii) Testing from inside and outside the network.

(iii) Testing to validate all out-of-scope systems that are segmented from systems in the cardholder data environment.

(iv) Network-layer penetration tests including components that support network functions as well as operating systems.

(v) A review and consideration of threats and vulnerabilities experienced in the last 12 months.

(g) The cardholder data environment must be secured with intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network.

(15) Any actual or suspected breaches of this procedure or any of the PCI-DSS standards shall be reported immediately to the IT Support Center.