All users are required to sign a compliance statement for access to district data and information systems. All users have a unique username and password.

Student Account Cashiers personnel are required to change their passwords quarterly. There will be no group, shared, or generic accounts and passwords.

Student Account Cashiers personnel are required to have fingerprinting on file with the district. Once an employee leaves the district, the account and passwords are immediately revoked.

All credit-card data printed on paper is protected against unauthorized access and securely stored. Credit-card data will be transported between campuses via armored transport or authorized personnel only. After six months, paper data will be destroyed via shredding before being disposed of or recycled.

If credit-card information is stored on network devices, the system will be encrypted. Credit-card data will only be stored as long as necessary to research chargebacks and process refunds. After 300 days, the account number will be truncated, and only the last four digits will be retained. The encryption keys will be renewed annually (see attached Cryptographic Key Management Procedures).

The district will remain in compliance with all PCIDSS (Payment Card Industry Data Security Standards) and contract with a compliance-validation service to satisfy these standards.

Refunds to credit cards will be processed back to the credit card used to pay fees. Exception requests must be made in person by presenting picture identification. A refund check can only be mailed to an address on file or picked up in person by showing picture identification.

Financial Aid may defer a tuition payment by adding the appropriate service indicator for the corresponding term.

EOPS emergency loan requests must be made in person at the EOPS office by presenting picture identification. The loan check can only be picked up in person by showing picture identification.

Effective Date:	2/16/10, 3/2/23
Periodic Review:	---
References:	Fair and Accurate Credit Transactions Act–15 U.S. Code §1681m (e)
CCLC Update:	#18, 2/11
Steering:	VPSS

Responsibility

The Registrar is responsible for accepting and responding to subpoenas, court orders, and requests involving release of records and personal information.

The Student Account Cashiers are responsible for developing procedures and standards regarding the processing, safeguarding, release, and disposal of bank and credit-card information acquired in person and physically stored, and the timing for disposal of online credit- card and checking information.

Academic Information Services (AIS) and the Student Account Cashiers are responsible for the encryption-upgrade process, quarterly password changes for specific positions, and retention of required data.

AIS will lead the quarterly network scan to comply with payment-card industry standards.

MiraCosta College recognizes its continuing obligation to protect the confidentiality and maintain the integrity of faculty, staff, and student information. The college will continue to provide administrative, technical, and physical safeguards to protect this information in the following ways:

1. Safeguard personal and confidential information regardless of format or medium.

2. Protect against anticipated threats to physical and technology-stored information.

3. Take all measures to prevent unauthorized use, access, or loss of stored data.

4. Ensure compliance with federal and state law, regulations, and district standards regarding information security and privacy.

5. Protect information that is acquired, transmitted, processed, transferred, and/or maintained by MiraCosta College.

Cryptographic Key Management Procedure

All keys used to encrypt credit-card data must be changed yearly and any time compromise of the key is suspected.

When keys are changed, the old keys must be revoked or expired.

All persons with custody of encryption keys must sign the encryption key custodian form. These forms will be scanned and kept on file in the \\in\ts\PCI folder on the MiraCosta College network.

SSL Web Server Keys (surf.miracosta.edu)

Keys must be renewed annually, and the old keys expired or allowed to expire. If the keys are replaced due to a suspected compromise, the old keys must be revoked.

To achieve separation of duties, one person must request the certificate through the vendor, and a second person must approve the request. The requester then replaces the existing certificate.

Credit-Card Vendor

Keys must be renewed annually, and the old keys expired or allowed to expire. If the keys are replaced due to a suspected compromise, the vendor must be contacted so the old keys can be revoked.

The credit-card vendor has key management procedures in place that must be followed to replace encryption keys on the PeopleSoft application servers and process schedulers annually.

Separation of duties is achieved by the vendor having separate keys to which MiraCosta does not have access.

PeopleSoft Credit Card Encryption

Keys must be renewed annually, and the old keys replaced. If the keys are replaced due to a suspected compromise, no additional steps must be taken because once the keys are replaced; the old keys can no longer be used.

Because the entire key must be used in clear text and is then readable in clear text via page access in PeopleSoft, separation of duties is achieved by the administrator granting the key custodian access to the pages and processes used to change the keys immediately prior to a key change, monitoring the processes during the key change, and revoking access after the key change is completed.

Encryption Key Custodian Form

I have read and understand the policies and procedures of MiraCosta College pertaining to cryptographic-key management, including the Enterprise Information Security Plan and the Cryptographic Key Management Procedure of MiraCosta College.

I agree to comply with the policies and procedures of MiraCosta College pertaining to cryptographic-key management, as well as any applicable laws.

I understand the responsibility that custody of the cryptographic keys carries and will take all reasonable precautions to prevent unauthorized disclosure of those keys and the data they encrypt.

I will promptly report to appropriate personnel any suspicious activity surrounding encryption keys in my custody, especially compromise or suspected compromise of those keys, or related files, passwords, or other security mechanisms associated with them.

Print:_____ Signed:_____

Date:_____