

Attachment A

FISCAL AFFAIRS

DISASTER RECOVERY AND CONTINUITY PLAN

JULY 2006

TABLE OF CONTENTS

ACCOUNTS PAYABLE

Identification and Recovery	1
Manual Checks.....	2 - 3

BURSAR

Cash Control	4 - 5
Cash Receipt	5 - 6
Onestep Security and Backup	6 - 7

ONECARD

Summary	8
University Department Effected	8
Software Safeguards	8 - 9

PROCUREMENT

Purchasing.....	10
Asset Management.....	10 - 11

ACCOUNTS PAYABLE

Identification and Recovery

Summary

A process is required to insure the reliability and completeness of our financial data when business operations may be interrupted due to a system failure, natural disaster or some other catastrophic event. We have certain safeguards in place to minimize the negative effects of such an event:

- FMS financial data is housed with a third party vendor in Salt Lake City.
- A copy of the AP data is maintained on the Fiscal Affairs Data Warehouse.
- A weekly backup copy of AP data is stored in an off-campus facility.

Identification

In the event that the system becomes unavailable for query and data entry, invoices should be divided into the following categories:

- New/unprocessed invoices, kept in order of the date received
- Invoices received/unprocessed and sent out for department approval
- Voucher keyed, but there is no payment associated with the voucher
- Voucher keyed, but on hold (system or manual)

Unless data has been lost entirely, queries would be generated by the AP Supervisor to insure that all vouchers already in the system are identified and worked expeditiously. An open commitments report can also be generated to reconcile invoices in process to amounts paid and commitments outstanding. If necessary, requests can be made to vendors for copies of outstanding invoices, based upon the open commitment report.

Recovery

A number of scenarios may occur, but are basically reduced to two critical factors: 1) the electricity, internet or CMS is down or compromised; 2) the electricity, internet and CMS are operational, but one or both of our printers are not operational 3) data already entered into the system may have been lost.

In the first scenario, processing must be done on a totally manual basis; manual checks would need to be written as approved by the Manager, and the Procurement Card used whenever possible. When the system is once again available, all necessary data would be entered into the system, as prioritized by the Supervisor or Manager. In the second scenario, if one of the check printers is operational, check printing could be done at the viable location, with little disruption to normal business. If both printers are not operating, we could a) send the payment files to a sister campus for processing/printing if the problem is for an extended period, or b) could write manual checks as deemed appropriate by the Manager, if the problem is one of relatively short duration. In the third scenario, recovery would be attempted by accessing backup files. If backup files are not available, daily work would be reconstructed by gathering the paper and/or scanned documents from either our on-campus files or from the off-campus storage facility. Final approval of reconstructed data will be made by the AP Supervisor and the Manager.

Manual Checks

1. Policy

Manual checks are the exception to normal Accounts Payable processing. Because a check is produced outside the Accounts Payable system, it is necessary to adhere to strict controls regarding its processing in order to avoid errors, misuse or fraud. All manual checks must be approved by the Manager or Supervisor. Note that manual checks are different from NOW checks, which are generated in the AP system. In nearly all possible scenarios, if the internet is up and the CMS data center is operational, invoices could be processed, the pay cycle run and checks printed either on campus or at one of our sister campuses in another part of California. Manual checks are only authorized when 1) the FMS system is not available at all; 2) both printers have been damaged and have become unusable; and/or 3) when the electrical power supply is out, has not been restored, and necessity dictates that certain checks be generated and mailed.

Only certain designated AP Technicians have been given the authority to produce manual checks.

2. Overview

Manual check procedures are designed to insure that there are checks and balances in the process to prevent errors and fraud. In addition to maintaining the security of the check processing room, the Manual Check Log and manual check numbers are maintained in a safe in the Fiscal Services Unit. A backup printer is stored in Plan Operations, while an additional supply of checks and signature chip is stored in a safe in the Bursar's Office in the Student Services Building.

3. Pre-requisites

- Each request must contain all of the appropriate backup documentation required for a normal AP transaction.
- Documentation must contain all of the appropriate approval signatures required for a normal AP transaction; i.e., Dept Approver, P.I., ORSP, etc.
- Each request must be approved, prior to any processing step being taken, by the Accounts Payable Manager, the Accounts Payable Supervisor or the AVP for Fiscal Affairs.

4. Procedure

The following procedure applies to all manual check transactions.

1.	AP Tech	Receive invoice or other payment request
2.	AP Tech	Verify documentation is complete and appropriate to the transaction
3.	AP Tech	Verify request contains all appropriate approval signatures
4.	AP Tech	Obtain approval signature for manual check by one of the three authorized approvers within Fiscal Affairs
5.	AP Tech	Go to the Fiscal Services Unit (or SSB Bursar's Office) Obtain a manual

		check and the manual check log
6.	Fiscal Services	Select a check from the inventory listing
7.	Fiscal Services	Record check number to be used on the AP Manual Check Log
8.	Fiscal Services	Document authorization of the check number by initials and the date Authorized on the manual check inventory
9.	Fiscal Services	Disburse manual check and manual check log to the authorized AP Tech
10.	AP Tech	Complete appropriate fields of manual check log: - Processing date - Vendor ID - Complete chartfield string - Amount
11.	AP Tech	Process manual check
12.	AP Tech	Complete audit report
13.	AP Tech	Obtain authorized signature on the manual check
14.	AP Tech	Deliver manual check, along with all supporting documentation, audit report, batch sheet and manual check log to Governmental Accounting For auditing
15.	GA Auditor	Audit check and complete auditing section of the manual check log
16.	GA Auditor	Deliver manual check with supporting documents to Fiscal Services
17.	Fiscal Services	Verify the check number matches the number recorded on the manual check log
18.	AP Sup or Mgr	Review and approve the completed manual check, the back up documentation and the manual check log for accuracy
18.	Fiscal Services	Contact the appropriate person for check pickup or mail manual check, as appropriate, secure manual check log in sage; return backup documents to the AP Supervisor or Manager

5. Additional Security

The Accounts Payable Manager and the Accounts Payable Supervisor, in addition to approving the initiation of a manual check and the review of the check prior to disbursement, will conduct periodic audits to insure that all unused manual checks are maintained properly in both the Fiscal Services and the Bursar's Office (SSB) safe and that all check numbers have been appropriately accounted for. Documentation of periodic audits will be made on the Manual Check Log and will contain the date of the audit and the signatures of the Manager and Supervisor. Any irregularities noted will be documented directly on separate memorandum and will be followed up with appropriate staff and/or management.

BURSAR'S OFFICE

CASH CONTROL

System Down

Policy: All policies and procedures for cash control will be maintained.

Procedures:

1. Registers will be opened as usual.
2. If system becomes inoperative during processing:
 - a. Notify supervisor and other cashiers immediately. Supervisor must also advise other departments such as CEL, Housing, Rapid Copy, etc...
 - b. Maintain temporary receipts with copies of CashNet attached for a minimum of 90 days. After 90 days, archive the temporary receipts at the basement.
 - c. Supervisors will disburse temporary receipts for processing payments. Temporary receipts will serve as receipts for all transactions until system is operational. Each temporary receipt must be totally completed.
 - d. Always validate temporary receipt with date stamp (see 710.5.1). Receipt is not considered official without date stamp and cashier's signature or initials. After filling in necessary information, cashier will keep yellow copy of temporary receipt and give white copy to student.
 - e. Reopen under Core as soon as the system is operational. All Cashiers must process temporary receipt in Core system immediately. If there are more than 3 students per cashier waiting to be assisted, processing temporary receipts will be secondary.
 - f. All temporary receipts are to be given directly to your supervisor once they have been processed in the Core system. Temporary receipts must all be accounted for; including voided temporary receipts for auditing purposes.
 - g. Temporary receipts that will not be processed in the Core system until the following work day must be given to supervisor to be locked in the vault and processed immediately on the following work day.
3. Re-entry data must balance with total transaction count and transmitted data must equal the amount deposited.

4. For use when computer endorsement is unavailable or for multiple documents:
 - a. Cashier must initial, write type of payment (cash, check, etc.), full amount paid and transaction number if available.
 - b. If multiple documents, cashier should number 1 of 3, 2 of 3, etc.

CASH RECEIPTS

Summary

A process is required to insure the reliability and completeness of our financial data when business operations may be interrupted due to a system failure, natural disaster or some other catastrophic event. We have certain safeguards in place to minimize the effects of a possible negative event:

- Real-time postings of all cash receipts into ARM database
- System backup is performed nightly, weekly and monthly
- Off-site storage of the weekly back up tapes
- Daily back up tapes are kept in a safe located in another building – Students Services Bldg.
- Cash receipt tapes are stored at the basement

Identification

Should the system become unavailable for data entry, temporary receipts will be used (see Cash Control -> System Down)

For query, the users can log on onto ARM and view the students' payment activities. Should ARM be unavailable, a Fee Master File report can be used to verify payments. (Note: Fee Master Report is generated on a weekly and monthly basis.)

Unless data has been lost entirely, queries and reports would be used to insure that all payment transactions are in the system.

Recovery/Subsequent Data Entry

Several different scenarios may occur: 1) the system is unavailable for processing; 2) data already entered into the CashNet system may have been lost and not posted into ARM; and 3) data already entered into the CashNet system are not lost but may have not been posted into ARM.

In the first scenario, cash payment processing would require the use of temporary receipts and manually entered into the Core system when the system becomes available. In the second scenario, transactions will be entered into the Core system by using and verifying the transactions from the audit tape. These transactions are posted into ARM through an interface program. In the third scenario, recovery would be handled by the interface program written in Core.

ONESTEP SECURITY AND BACKUP

Physical Security:

The OneStep server (OS-Windows 2003, RDBMS-Oracle 9i) is located in an area where only authorized employees have access to. The server is key locked so only the server administrator and the Bursar have access to the hard drive or inside of the server. The server is attached to an uninterrupted power supply so in case of a power outage the server would have 20-30 minutes to shut down automatically.

DBA – The maintenance of the database resides in FABS (Fiscal Affairs Business Systems).

BackUP

Purpose: The need for and creation of daytime and end-of day backup files cannot be over emphasized. The backup files currently in place allow us to restore either the whole system or perhaps selected data files, to a specified 'end of the day' position.

Database: A program runs daily at 1 am which exports the entire database to another server.

System: Uses Veritas software to backup the entire system/hard drive to DLT tape.

Tape Cycle Method:

The backup strategy implemented is based on a ten-tape.

The method involves maintaining the entire system daily (Monday-Friday) and including the database. Every two weeks the daily tapes are recycled.

Daily BackUp tape is taken to the Bursar's satellite office at SSB and kept inside the vault. The Friday tape (weekly) for the database is forwarded to DoIT for off-site storage.

Test Procedures:

The Veritas software provides verification for a successful backup.

On a monthly basis, the FABS IT staff performs a test by restoring a portion of files on a test server to verify the completeness and accuracy of the backup.

Annually, a Full-Interruption Test is run (December break, Dec 26 – Dec 30), in which the server is shut down. The IT staff installs new or sometimes, spare hard drive on the server and restores all data and software from backup. After the restore is completed, a test to measure its success is performed. In cases of errors, problems are documented and resolved.

Recovering Data after System Corruption:

If any files/data is damaged and/or the system cannot boot, FABS IT staff performs a full or partial restore depending on the severity of the problem. The files or data are restored from the Veritas tape. Two things are required to perform this recovery:

- The backup tape(s) that contains the lost data
- Veritas recovery software

ONECARD OFFICE

Summary

A process is required to ensure that data is not lost for our OneCard Program in the case of any emergency. The functioning card system is needed to facilitate daily operations on sites in the University.

The servers are located in the Division of Information Technology (DoIT). They are maintained by the Data Base Administer and the Supervisor of the OneCard Office. All OneCard systems use mirrored disks to provide a back-up of data. DoIT does weekly maintenance on the system and back-up tapes are sent to an off site storage facility for emergency purposes.

The photo imaging hardware is located in the OneCard office and is maintained locally with assistance both form FABS and DoIT. Procedures for the backups for images should be completed by spring 2004. Currently they are saved on a CD, but we need to move images to a server.

The OneCard staff will need to determine the priorities of the departments that need to be back online with their readers. These priorities may be related to the time of the month and semester when the disaster occurs. Using the most recent backup will provide the University with a temporary solution to possible problems. All equipment will need to be evaluated to determine the extent of damage.

University departments effected:

Library

Readers attached to copy machines do not work in offline mode. For extended periods with no electricity the library copy readers will not be able to function until it is restored.

Housing & Residential Services

If there is no electricity, they will manually account for the meals as students enter dining services. If the NP processor is functioning transactions can be stored in the reader then uploaded later for reporting and processing. Vending would be affected by an electrical outage.

Centennial Village

Laundry and vending would be affected if there is a power outage.

Software Safeguards

SFSU employs Hewlett Packard's Disk Mirroring Utility. All system software (including operating system and vendor software) has a live mirror. This prevents system down time due to hard disk, disk controller, or disk interface cable failures.

In case of an emergency, the OneCard office would run a report of cardholders from the most recent backup and then a current report when the system comes online again. Comparisons would need to be made and decisions to correct data or re input lost cardholders and privileges.

Staff in the OneCard Office would be responsible for re-entering any lost data that is identified once an analysis has been done using existing reports and any information cardholders might bring to the attention of the staff. It is possible that some monetary transactions could be lost and we would need to validate those transactions against any receipts that cardholders had printed when making deposits via a Value Transfer Station or Web Deposit.

Point of Sale transactions are stored in the readers and when the system comes online end user would run a report of those transactions to balance against any records that are kept for student meal plans.

All other card readers do not operate in an online mode during regular processing and thus no transactions are held for future processing. These transactions would essentially be lost, but no data effecting cardholders would be affected.

PROCUREMENT

PURCHASING

Procedures in the event of a long-term loss of data processing capability

1. Campus users will be requested to limit purchase requests to emergency and urgent requirements to the greatest extent feasible.
2. Campus users will be instructed to make use of Procurement Cards to the greatest extent feasible and allowable.
3. Buyers will increase the use of their higher limit cards on behalf of end users, being sure to obtain all necessary account information to charge when the card statement comes in.
4. Campus users will submit hard copy requisitions for needed purchases. PO numbers will be manually assigned to each requisition from a sequential numbering sequence maintained in Purchasing. When data processing capability is restored, the issued orders will be input using a system generated number with a cross reference to the manual number allowing Accounts Payable to correctly match the invoice for payment.

ASSET MANAGEMENT

Procedures in the event of a long-term loss of data processing capability

1. Property Office staff will maintain hard copy paper records of asset acquisitions and retirements until data processing capability is restored.

Summary

A process is required to insure the reliability and completeness of our financial data when business operations may be interrupted due to a system failure, natural disaster or some other catastrophic event. We have certain safeguards in place to minimize the effects of a possible negative event:

- System backup is performed nightly, weekly and monthly
- A copy of procurement data is maintained on Fiscal Affairs Data Warehouse, both on-site and at CSULB
- Off-site storage of the weekly back up tapes
- Daily back up tapes are kept in a safe located in another building – Students Services Bldg.

Interim Operation

Should the system become unavailable for data entry, the following procedures will be implemented:

- Campus users will be requested to limit purchase requests to emergency and urgent requirements to the greatest extent feasible.
- Campus users will be instructed to make use of Procurement Cards to the greatest extent feasible and allowable.
- Buyers will increase the use of their higher limit cards on behalf of end users, being sure to obtain all necessary account information to charge when the card statement comes in.
- Campus users will submit hard copy requisitions for needed purchases. PO numbers will be manually assigned to each requisition from a sequential numbering sequence maintained in Purchasing.

Identification/Recovery

Once data processing capability is restored, the last we will determine the extent of lost data, if any. Because of data warehousing and the redundant backup safeguards, the worst case would be one day of lost data prior to the catastrophic event.

Using the best available combination of backup tapes, data warehouse reports, and paper records, purchasing data would be restored and/or re-keyed to bring update records to current status

When data processing capability is restored, all interim orders issued will be input using the system generated PO number with a cross reference to the PO number manually assigned during interim operation, allowing Accounts Payable to correctly match the invoice for payment.

Receiving information during the interim period would be manually tracked and input once data capability is restored. Any receiving data lost due to the catastrophic event that could not be recovered via electronic backup would need to be verified either through paper records in Receiving or through end user sign off on invoices prior to payment. In addition, all manually recorded asset acquisitions and retirements will be input into the AM module.

Note: P-Cards have the flexibility in their spending limits to be changed as needed to meet the campus needs.