State of Missouri
Offender Phones, Escalation Procedure

LAMINATED, FOR OFFICERS USE

THE FOLLOWING INFORMATION APPLIES TO INMATE PHONES ONLY

Priority Level 1:
(Repair will be made within 2 business days)

- **<u>One</u> of multiple inmate phones in a housing area not operational**

Priority Level 2:
(Repair will be made within 1 business day)

- **One intake phone not operational**
- **Multiple inmate phones in a housing area not Operational**

Priority Level 3:
(4 hour physical response and / or remote reset and repair)

- **One or more entire housing areas not operational**
- **Multiple intake phones not operational**
- **All inmate phones not operational**

IMMEDIATELY CALL PCS WITH DESCRIPTION OF PROBLEM AND PRIORITY LEVEL:

(800) 646-6283

(800-6-INMATE)

<u>DO NOT</u> DISTRIBUTE THE ABOVE NUMBER TO INMATES OR INMATE FAMILIES AND FRIENDS

INMATE FAMILIES WITH BLOCKED NUMBERS OR BILLING PROBLEMS SHOULD CALL: ***Monday through Friday, 8:00AM TO 5:00PM Pacific Time***

(888) 288-9879

State of Missouri

Facility Administration, Back-Up Contact Sheet

(To be used only if (800) 6-INMATE number should fail)

**** Please Keep This Sheet Private ****

These numbers are to be used by facility administration personnel only.

If the 800 number fails during normal business hours, please call Public Communications Services to report any problems with the Inmate Phone System.

PCS INMATE SERVICES:

818-898-3524

PCS OFFICE PHONE NUMBER:
(310) 231-1000

ERIC PETTERSEN, EXT. 3046
HELEN DOUGLAS, EXT. 3008

SOFT PLASTIC COVER, FOR OFFICERS IN CHARGE USE

If the 800 number fails after normal business hours, then call the following individuals to report the problem with the Inmate Phone System. Please allow fifteen minutes for individuals to respond before attempting to contact the next person on the list. Place calls in order listed below:

STAFF	CELL PHONE
ERIC PETTERSEN	**(310) 487-5297**
HELEN DOUGLAS	**(818) 523-5245**

INMATE FAMILIES WITH BLOCKED NUMBERS OR BILLING PROBLEMS SHOULD CALL: ***Monday through Friday, 8:00AM TO 5:00PM Pacific Time***

(888) 288-9879

NOTICE TO INMATES

***

AVISO PARA LOS DETENIDOS

LAMINATED, PLACED IN INMATE VIEW

PLEASE INFORM FRIENDS OR FAMILIES WITH BLOCKED NUMBERS OR BILLING PROBLEMS TO CALL:

***

POR FAVOR INFORMEN A LOS AMIGOS Y FAMILIARES CON PROBLEMAS CON SU CUENTA QUE LLAMEN A:

(888) 288-9879

Monday through Friday 8:00am to 5:00pm Pacific Time

UNBLOCKING	QUESTIONS ANSWERED
***	***
PARA QUITAR UN BLOQUEO	*PARA PREGUNTAS Y RESPUESTAS*

State of Missouri
INMATE PHONES
IN-HOUSE TROUBLE REPORT

TABLET FORM FOR OFFICERS USE

Facility Name: _____

Date Reported to PCS: _____ Time Reported to PCS: _____

Person Filing Report: _____

Person Reported to at PCS: _____

Location of Phone(s) Experiencing Trouble: _____

_____

Description of Trouble: _____

_____

PRIORITY LEVELS:	CHECK ONE:
Priority Level 1: ***(Repair will be made within 2 business days)*** • **<u>One</u> of multiple inmate phones in a housing area not operational**	
Priority Level 2: ***(Repair will be made within 1 business day)*** • **One intake phone not operational** • **Multiple inmate phones in a housing area not Operational**	
Priority Level 3: ***(4 hour physical response and/or remote reset and repair)*** • **One or more entire housing areas not operational** • **Multiple intake phones not operational** • **All inmate phones not operational**	

RESOLUTION:

Remote Fix (no signature needed)– PCS Rep Name: _____

Technician Needed on Site – Description of correction to trouble: _____

_____

_____

Date of Correction: _____ Time of Correction: _____

Technician Signature: _____

OFFENDER TELEPHONE SYSTEM
DISASTER RECOVERY PLAN (DRP)

TABLE OF CONTENTS

I. Administrative Information

The overall objectives of the Inmate Telephone System (ITS) Disaster Recovery Plan (DRP) are to protect public resources and employees, to safeguard the vital records of which the Department of Corrections (DOC) has become the custodian, and to guarantee the continued availability of essential Department of Correction services. The role of this Plan in these objectives is to document the disaster planning decisions and to design and implement a sufficient set of procedures for responding to a disaster that involves the central site and its services.

A disaster is defined as the occurrence of any event that causes a significant disruption in Department of Corrections capabilities and functions. The central theme of the Plan is to minimize the effect a disaster will have upon on-going operations. This Plan provides flexibility to respond to disasters of various magnitudes including the most severe disaster, destruction of the central site facility. Occurrences of a less severe nature are controlled at the appropriate management level as a part of the total Plan.

The basic approach, general assumptions, and sequence of events that need to be followed will be stated in the Plan. It will outline specific preparations prior to a disaster and emergency procedures immediately after a disaster. The Plan provides a roadmap from disaster to recovery. As it is implemented, executive staff may choose at any time to take detours for various management reasons. However, after the detour, staff will resume following the DRP as the main road to recovery. The Plan will be distributed to all key personnel, and they will receive periodic updates. The general approach is to make the plan as threat-independent as possible. This means that it should be functional regardless of what type of disaster occurs. In order to limit loss, the DRP will provide for the logical restoring of critical systems to contingent operation status within the acceptable outage period. The Plan also provides for full restoration of production operations at either the central site or an alternate location. By performing a business impact and risk analysis, the ITS can determine the potential dollar loss that will result from a major disaster.

For the recovery process to be effective, the DRP is organized around the team concept. Each team has specific duties and responsibilities once the decision is made to invoke the disaster recovery mode. The captains of each team and their alternates are key ITS personnel. The Plan contains the phone numbers of the team members and represents a dynamic process that is kept up-to-date through updates, testing, and reviews. As recommendations are completed or as new areas of concern are recognized, the Plan will be updated reflecting the current status.

Purpose

The purpose of this ITS DRP document is to provide a description of the steps to be taken in the event of a major disaster that affects the ITS central site. The ITS DRP identifies the computer and network resources that are critical to ITS operations, the information assets that are necessary for continuity of ITS services, and the plans for resuming operations following a disaster affecting the ITS Department of Corrections environment.

Assumptions

This Disaster Recovery Plan (DRP) is designed for the ITS Information Technology and (Department of Corrections) environment. The ITS and Department of Corrections environment consists of a small number of applications operated on central servers and resting upon a state-wide network.

- This DRP addresses disaster recovery operations for ITS central server operations only. The recovery plans for desktop computers, printers, and other Department of Corrections related office equipment can be added as an appendix.
- ITS can implement manual procedures or workarounds to allow for an acceptable system outage period of (to be determined) days.
- Documenting system-related manual procedures to be used by department staff during a system outage period or during a period of contingency operations is ITS' responsibility.
- Performing a full business impact and risk analysis is ITS' responsibility.
- Business continuity planning for the full range of ITS services is ITS' responsibility.
- Coordination with the ITS/County/State Emergency Operations Plans is ITS' responsibility.

DRP Responsibilities

The development, testing, maintenance, and implementation of the ITS Disaster Recovery Plan is the responsibility of the SBC ITS Project Manager. The ITS Disaster Recovery Plan will be reviewed annually and updated as required.

As the DRP is developed, it will be printed and distributed to applicable employees of all involved agencies and parties. After reviewing the document, employees generally tend to file it away with other work-related material. If a major disaster should ever occur, the data center could be totally destroyed along with copies of the DRP that were kept in desks and file cabinets. If the disaster occurred outside office hours, the key personnel would probably be at home.

To plan for various situations that could occur, copies of the DRP should be safeguarded both at the office and at the' residences of ITS key personnel and selected staff of the DOC as they may direct. An adequate number of copies should be maintained at the central site and at a minimum, additional copies should be located at the following locations:

- Central Server Room
- Offsite Storage
- Backup Site
- Department of Corrections Coordinator's Office
- Department of Corrections Coordinator's Home
- ITS Office

- ITS Site Administrator's Home and Office
- Other Key Employee's Offices
- Other Key Employee's Homes

The DRP is maintained in Microsoft word format and should be stored both on hard disk and on diskette. Each time the DRP is revised, diskette copies should be created, labeled, and stored onsite, offsite, and other key locations. Having paper and diskette copies of the Plan at various residences may be thought of as unnecessary and redundant since the diskettes are also stored offsite, but, should a disaster ever happen, time can be better utilized performing disaster recovery activities than in locating a PC, printing multiple sets of the plan, and collating the pages into usable documents for distribution.

Providing training required for the implementation of the ITS Disaster Recovery Plan is the responsibility of the Department of Corrections Director. The DRP training will be provided to ITS staff with the initial distribution of the plan in preparation for DRP testing. After the initial training, there will be periodic refresher training and training for new employees.

DRP Testing

The testing of the ITS Disaster Recovery Plan is recommended upon initial distribution and annually thereafter.

The objective of DRP testing is to evaluate whether plan and its individual procedures are capable of providing the desired level of support to the ITS core business processes. Testing will also validate whether a given procedure can be implemented within a specified time period, and will provide an opportunity to make necessary adjustments to the plan and to the environment within which the plan is tested. Finally, testing allows the opportunity for validation of the estimated cost of disaster recovery operations.

The guidelines for DRP testing include provisions for three levels of testing: review, desktop rehearsal, and simulation. Full system interruption testing of ITS systems is not contemplated due to its cost and the low probability.

DRP Review

The ITS DRP will undergo executive staff review, and each procedure will be subject to a workgroup level validation and review process.

At the workgroup level, managers and supervisory or technical staff participate in the validation of procedures that ensure that ITS core business processes will continue, to the extent possible, in the event of a disaster. The iterative nature of the procedure validation and review process ensures that optimum functionality and cost-beneficial alternatives are selected and documented. At each stage of review, the ability to provide acceptable levels of service delivery under various systems failure scenarios is considered.

On completion, overall disaster recovery procedures are reviewed by the disaster recovery planning team to see that all necessary elements are provided. These elements include, but are

not limited to, provisions for staff training, availability of supplies, availability of backup facilities, availability of procedures, and triggers for return to normal operations.

DRP Desktop Rehearsal

In a desktop rehearsal, the manager responsible for implementing a procedure will be advised of a hypothetical disaster situation. The manager, or his designee, will then use the plan to work out a response to the situation. The manager will answer questions that relate to the availability of trained staff, adequacy of the facilities, adequacy of the machines, and whether necessary forms and supplies are on hand. Adjustments will be made either to the procedures or to the particular environment during this phase should any part of the procedure fall short of its objective.

DRP Simulation

Simulation testing takes the desktop rehearsal a step further. Simulation testing involves both the manager and the staff who will be responsible for execution of recovery operations in a disaster situation. Procedures involving outside agencies, equipment suppliers, and third-party vendors will be executed up to the point where external resources are expended. (For example, a phone call may be placed to validate that the procedure identifies the correct emergency contact for ordering an external resource.) The simulation will stop short of actual interruption of the production system. The simulation will be thorough enough to assure that the manager and on-site personnel can handle the work, the necessary training has been carried out or scheduled, needed supplies are available, and that the facility can be adapted to the emergency. At this point, any inadequacy in the plan or the procedures will be remedied in advance of an actual disaster recovery situation.

II. Recovery Strategies

In preparing the ITS DRP, the following list of recovery strategies was identified:

- System Replacement – System Replacement provides for purchasing replacement components

  System Replacement is appropriate for Department of Corrections environment that can be restored within an acceptable outage period or when manual procedures can fill a gap in service.

- Cold Site – A cold site is an empty shell that is suitable for recovery operations. An empty shell is a computer room equipped with air conditioning, power supply, network wiring, and environmental controls for continued processing when equipment is shipped to the location. A cold site should be located near the sources of the required DRP resources.

- Warm Site – A warm site is a partially equipped backup site that provides a suitable environment and some of the equipment components necessary for recovery operations. The location of the warm site should also allow for rapid shipment of the additional equipment necessary to resume processing.

- Hot Site – A hot site is a fully equipped backup site provided by an outside vendor or as a second ITS controlled site. The hot site should have adequate equipment to support the level of service required for emergency processing during the disaster recovery period.

The ITS DRP will implement the System Replacement strategy. In addition, the plan will allow flexibility to respond to disasters of various magnitudes ranging from restoration of service following a partial interruption escalating to recovery from greater degrees of damage including destruction of the central site.

Backup Strategy

The ITS of ITS is committed to providing reliable and redundant backups of all system and user generated data on each of the systems, which it administers. The ITS has developed a Backup and Recovery Procedure that defines the standard operating procedures and detailed work instructions needed for performing periodic computer system backups to ensure applications software and ITS data are adequately preserved and protected from destruction. The Backup and Recovery Procedure also provides guidelines for users to ensure that data stored on individual personal computers is also protected.

The ITS' documented Backup and Recovery Procedure includes the following strategies to prepare for both random mechanical disk failures and large-scale natural disasters:

- Incremental backups are preformed on a daily basis (Monday – Friday) on all central servers and on all multi-user systems managed by the ITS Facilities Management Contractor.
- Full disk backups (image/archive) are performed on a weekly basis for all disks.
- Each employee is responsible for performing backup procedures for the employee's personal computer. The frequency of these backups, retention location, and the retention timeframes for each will be dependent on the criticality and volatility of the data residing on each personal computer.

III. Emergency Management

The Emergency Management Team is responsible for the initial response to the incident. This includes coordinating the initial response activities and using prudent office procedures to protect life and minimize property damage.

1. Assess the damage
2. Determine extent to which Department of Corrections Disaster Recovery Plan will be used
   - Minor Damage — Processing can be restarted in a short time with no special recall of personnel. Anticipated downtime is less than one day. Damage could be to hardware, software, mechanical equipment, electrical equipment, or the facility.
   - Major Damage — Selected teams will be called to direct restoration of normal operations at current site. Estimated downtime is two to six days. Major damage to hardware or facility.
   - Catastrophe — Damage is extensive. Restoration will take upwards of one week. Computer room or facility could be completely destroyed. All team leaders will be called to begin a total implementation of the Disaster Recovery Plan.

3. Notify ITS and DOC staff

   - Notify senior management
   - Notify line employees
   - Prepare regular status reports for senior management
   - Notify users of projected time for becoming operational

Following an emergency at the central office, ITS hub(s) or related computer center, the operational personnel on site will take the appropriate initial action and then contact a member of the Emergency Management Team starting with the first name on the list (Appendix A).

When a member is located, that member will contact the remaining members of the Emergency Management Team. The members will meet at or near the disaster to make a firsthand assessment of the damage. They will determine the action to take and will notify senior management.

If a determination is made to notify all other teams, the Emergency Management Team will phone the other teams using a predefined pyramid contact system. A brief message will be dictated over the phone and the called person will write down the message. At the end of the message, the called person will read back the message to verify that all critical information is stated. This same procedure will be used for all calls in the pyramid. It will ensure that all contacts have the same information.

Appendix A contains the names of all team members and their phone numbers.

IV. Contingency Operations

Contingency operations begin when the planned software, hardware, backup data files, and other resources are in place at the contingency operations site.

- Make arrangements with the telephone company and other vendors for delivery and installation of contingency operations equipment. Prior arrangements can be made to enable vendors to deliver the necessary equipment in a very short time.
- Conduct a series of diagnostic and continuity tests to ensure that hardware, communications equipment, and system software is operational.
- Retrieve backup application and data files from offsite storage.
- Install applications, rebuild databases, and check that critical applications are ready for contingency operations.

The next step is testing the essential functions of critical applications. Note that not all functions need to be tested, since contingency operations will support only the functions and applications necessary for continuity of ITS services during the disaster recovery period. An example might be the immediate recovery of "collect only" calling services while "pre-paid collect", "debit" or other end-user/customer services undergo a staged recovery to full operations.

The documentation in Appendices A, B, C, D, and E can be used by each team to keep track of the disaster recovery activities that will be performed simultaneously.

The Emergency Management Team will receive reports from each team to monitor progress and assess readiness for contingency operations.

V. Business Resumption Procedures

Now that the contingency operations site is providing critical Department of Corrections services, it is time to turn attention to rebuilding the permanent central site. Reconstruction plans should already have been in progress, but now it is time to devote more effort to this area. Reconstruction at the permanent facility may not require a totally new building but only repair of the existing facility. Once the permanent facility is ready for use, the hardware at the contingency operations site can be moved to the permanent facility.

VI. References

Appendix A1: Contact Lists

(ITS and DOC to provide contact names, addresses, phone numbers, email)

Emergency Management Team

This section includes the contact list for the Emergency Management Team. These contacts may be used during any problem including during disaster assessment.

Senior Management Team

This section includes the contact list for leadership personnel within, Public Communications Services, Inc., DOC and other senior managers who are responsible for communicating with department line staff.

Facilities Replacement Team

This section includes the contact list for the Facilities Replacement Team that is responsible for obtaining replacement equipment to be used for recovery operations, including testing that equipment and communications are ready for recovery operations.

Recovery Operations Team

This section includes the contact list for the Recovery Operations Team that is responsible for executing backup and recovery procedures, replacement system testing, system and application software installation, and contingency operations.

Appendix A2: Disaster Recovery Team Checklists

The checklists in Appendix A2 can be used by each team to keep track of the many disaster recovery activities that will be performed simultaneously.

State of Missouri
Department of Corrections

ITS

Disaster Recovery Checklist

EMERGENCY MANAGEMENT TEAM **Date: ____/____/_____**

Team Captain: _____

Alternate: _____

Timed Events	Assigned To	Begin Date Time	Complete DtTime
Coordinate initial response using office procedures to protect life and minimize property damage.			
Assess the damage.			
Notify senior management.			
Make decisions on implementation of Disaster Recovery Plan.			
Notify team captains and start recall process.			
Give formal notification for request to use backup facilities.			
Arrange for emergency funds to cover extra expenses.			
Establish a Control Center at or near original site and coordinate the recovery. Use the central telephone number or guard's phone as primary contact.			
Start Disaster Recovery Logs.			
Give senior management scheduled status updates.			
Review ITS policy, department budget, and cost-limit guidelines with other teams.			
Give users scheduled updates on status.			
Produce report on damages.			
Gather Disaster Recovery Logs from all teams. Produce daily status reports.			
Arrange for any additional professional help.			
Coordinate interviews to fill any vacancies.			
Keep status charts of recovery efforts.			

State of Missouri
Department of Corrections

ITS

Disaster Recovery Checklist

SENIOR MANAGEMENT TEAM **Date: ____/____/_____**

Team Captain: _____

Alternate: _____

Timed Events	Assigned To	Begin Date Time	Complete DtTime
Determine when backup site will be available.			
Arrange for setting up temporary office space.			
Deliver any needed furniture to the backup site.			
Notify employees of status and inform them when and where to report.			
Issue instructions for manual or contingency operations.			
Arrange transportation for materials, people, supplies, and equipment.			
Train employees who may be working outside their areas of responsibility.			
Provide administrative services.			
Serve as a clearinghouse for expediting payments.			
Facilitate support for all team leaders and staff.			
Establish internal mail delivery between locations.			
Maintain Disaster Recovery Log.			
Report status to Emergency Management Team.			

State of Missouri
Department of Corrections

ITS

Disaster Recovery Checklist

FACILITIES REPLACEMENT TEAM **Date: ____/____/_____**

Team Captain: _____

Alternate: _____

Timed Events	Assigned To	Begin Date Time	Complete DtTime
Determine when backup site will be available.			
Access damage to servicing Department of Corrections equipment.			
Identify equipment that can be repaired.			
Arrange for vendor field service repairs under warrantee or service contracts if possible.			
Identify necessary replacement equipment.			
Obtain necessary computer equipment from vendors.			
Arrange for delivery and installation of replacement equipment.			
Determine the damage to PCs, office equipment, printers, and other units; then schedule replacements.			
Review requirements and ensure availability of required power, hearing, telephone lines, and air-conditioning.			
Notify Recovery Operations Team when facilities are ready for backup recovery operations.			
Check operational status of equipment and communication lines using standard hardware and network diagnostic tests.			
Maintain Disaster Recovery Log.			
Report status to Emergency Management Team.			

State of Missouri
Department of Corrections

ITS

Disaster Recovery Checklist

RECOVERY OPERATIONS TEAM **Date: ____/____/_____**

Team Captain: _____

Alternate: _____

Timed Events	Assigned To	Begin Date Time	Complete DtTime
Obtain needed recovery tapes and documentation for use at backup site.			
Assess status of processing and point of recovery for the entire system and/or individual systems. Develop plan to restart operating schedule.			
Provide the operating systems as well as other control systems software.			
Provide application software and utilities.			
Restore application systems in priority sequence using backup tapes and verifying continuity.			
Restore the database from backup tapes using recovery documentation.			
Restore intermediate data to ensure current integrity.			
Perform tests and verify full restoration of applications and data.			
Ensure continuity by working with users.			
Establish contingency operations processing schedule.			
Maintain Disaster Recovery Log.			
Report status to Emergency Management Team.			

Appendix B: Hardware and Software Inventory

(PCS to insert hardware inventory upon final system design acceptance by the DOC)

(PCS to insert software inventory upon final system design acceptance by the DOC)

Appendix C: Network Diagram

(PCS to insert Network Diagram upon final system design acceptance by the DOC)

Appendix D: Backup and Recovery Procedure

The ITS Backup and Recovery Procedure is incorporated by reference. A copy of the Backup and Recovery Procedure will be distributed with this Disaster Recovery Plan upon final system design acceptance by the DOC for hardware, software, network and allied specifications.

Appendix E: Server Replacement Specifications

(PCS will copy and insert packing slip server specifications upon final system design acceptance by the DOC)

To facilitate ordering of replacement of servers, the specifications for the existing servers are provided. Replacement invoices should duplicate the existing servers as closely as possible, substituting current or equivalent models if necessary.

File Server

(PCS will insert specifications upon final system design acceptance by the DOC)

Application Server

(PCS will insert specifications upon final system design acceptance by the DOC)

Exchange Server

(PCS will insert specifications upon final system design acceptance by the DOC)

Jukebox Server

(PCS will insert specifications upon final system design acceptance by the DOC)

Backup Server

(PCS will insert specifications upon final system design acceptance by the DOC)

VAC
VALUE-ADDED
COMMUNICATIONS

Sample Reports

VAC Systems offer an extensive array of flexible reporting options to meet the needs of correctional facilities. These include: Maintenance Reports, Investigative Reports, and Financial Reports as described below:

1.1 Financial Reports

Financial Reports are most often used for systems that feature debit calling. Using the VAC administrative workstation VAC personnel, system administrators, and authorized facility staff are provided with the capability to generate, view and print the following Financial Reports:

- Call Refund Report
- Daily Call Charges
- Financial Transactions
- Inmate Deposit
- Inmate Reconciliation

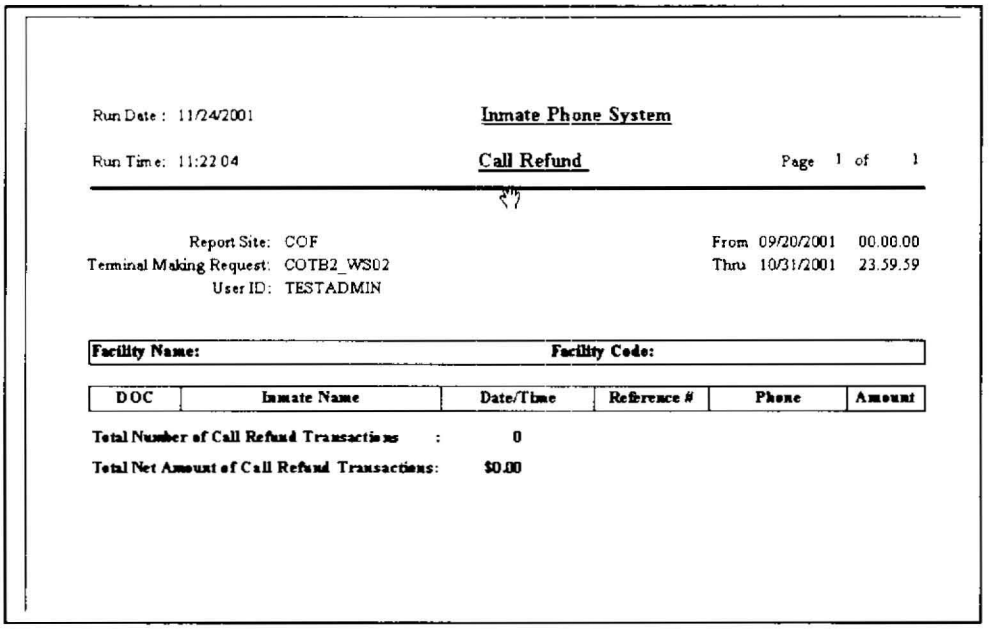
1.1.1 *Call Refund Report*

The *Call Refund Report* automatically generates when a user, with the appropriate authorization level, performs a Call Refund transaction. Call Refund generates and prints a summary transaction report. The Call Refund Report includes the following information:

- Inmate ID Number
- Inmate name
- Date & Time of Transaction
- Reference Number
- Dialed Digits
- Amount of Transaction
- Total Number of Call Refund Transactions
- Total Net Amount of Call Refund Transactions

VAC
VALUE-ADDED
COMMUNICATIONS

Sample Reports



Run Date : 11/24/2001 — Inmate Phone System

Run Time: 11:22:04 — Call Refund — Page 1 of 1

Report Site: COF — From 09/20/2001 00.00.00
Terminal Making Request: COTB2_WS02 — Thru 10/31/2001 23.59.59
User ID: TESTADMIN

Facility Name:	Facility Code:

DOC	Inmate Name	Date/Time	Reference #	Phone	Amount

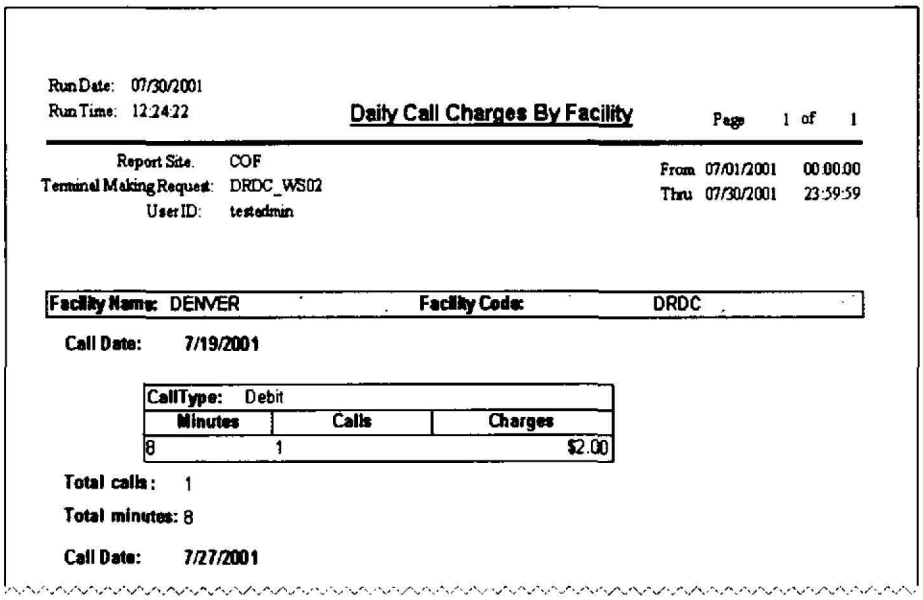
Total Number of Call Refund Transactions : 0

Total Net Amount of Call Refund Transactions: $0.00

1.1.2 *Daily Call Charges*

The *Daily Call Charges* report displays the total number of calls, duration, and charges for both Collect and Debit calls. The user determines the range of dates covered in the report. Grand totals are available at the bottom of the report. The Daily Call Charges report displays the following information for Debit and Collect calls:

- Call Date
- Call Type
- Minutes
- Calls
- Charges
- Total Calls
- Total Minutes



Run Date: 07/30/2001
Run Time: 12:24:22

Daily Call Charges By Facility

Page 1 of 1

Report Site: COF
Terminal Making Request: DRDC_WS02
User ID: testadmin

From 07/01/2001 00:00:00
Thru 07/30/2001 23:59:59

Facility Name: DENVER **Facility Code:** DRDC

Call Date: 7/19/2001

CallType: Debit

Minutes	Calls	Charges
8	1	$2.00

Total calls: 1

Total minutes: 8

Call Date: 7/27/2001

1.1.3 *Financial Transactions*

The *Financial Transactions* report provides a record for all inmates with a financial transaction during a specified period. The Financial Transactions report displays the following information:

- Inmate ID
- Inmate Name
- Date/Time of transaction
- Transaction Type
- Amount of transaction
- Reference Number
- Total Number of Financial Transactions for the Inmate

Run Date . 11/21/2001

Run Time 14:21:20 **Financial Transactions** Page 1 of

Report Site: COF
Terminal Making Request COTB2_WS02
User ID: TESTADMIN

From 10/25/2001 00:00:0
Thru 11/21/2001 23:59:

Facility Name: TEST BED 2 **Facility Code: COTB2**

Inmate DOC 00299-999 Inmate Name: LO, CO

Date/Time	Transaction Type	Amount	Reference #
10/25/2001 20:30:08	COLLECT CALL	$0.00	008DDA
10/25/2001 20:30:08	COLLECT CALL - INCOMPLETE	$0.00	008DDA
10/25/2001 20:30:49	DEBIT CALL	$0.00	008DDB
10/25/2001 20:30:49	DEBIT CALL - INCOMPLETE	$0.00	008DDB
10/25/2001 20:46:18	COLLECT CALL	$0.00	008DDC
10/25/2001 20:46:18	COLLECT CALL - INCOMPLETE	$0.00	008DDC
10/25/2001 20:46:35	DEBIT CALL	$1.00	008DDD
10/25/2001 20:46:35	DEBIT CALL - INCOMPLETE	$1.00	008DDD
10/25/2001 20:55:41	COLLECT CALL	$0.00	008DDE
10/25/2001 20:55:41	COLLECT CALL - INCOMPLETE	$0.00	008DDE

Total Number of Financial Transactions for the Inmate: 10

Total Number of Financial Transactions for the Facility: 10

1.1.4 *Inmate Deposit*

The *Inmate Deposit* report provides a record of all inmates with deposits during a specified period. The Inmate Deposit report displays the following information:

- Inmate Number
- Inmate Name
- DEP Date (deposit date)
- Deposit (deposit amount)
- Total Inmate Deposits For
- Total Amount (total amount of deposit)

Run Date: 09/22/2001
Run Time: 16:19:44

Inmate Deposits For: 2900
For Inmate: 111111

Report Site: COF
Terminal Making Request: QACOLO_WS01
User ID: TESTADMIN

From 09/06/2001 00:00:00
Thru 09/22/2001 23:59:59

Facility Name:	TEST BED 1	Facility Code:	TEST 1

DOC	INMATE NAME	DEP DATE	DEPOSIT
111111	SMITHERS,TOM,	09/12/2001	$2,500.00

Total Inmate Deposits For: 9/12/01 1 **Total Amount** $2,500.00

Facility Name:	TEST BED 1	Facility Code:	TEST 1

DOC	INMATE NAME	DEP DATE	DEPOSIT
111111	SMITHERS,TOM,	09/21/2001	$50.00

Total Inmate Deposits For: 9/21/01 1 **Total Amount** $50.00

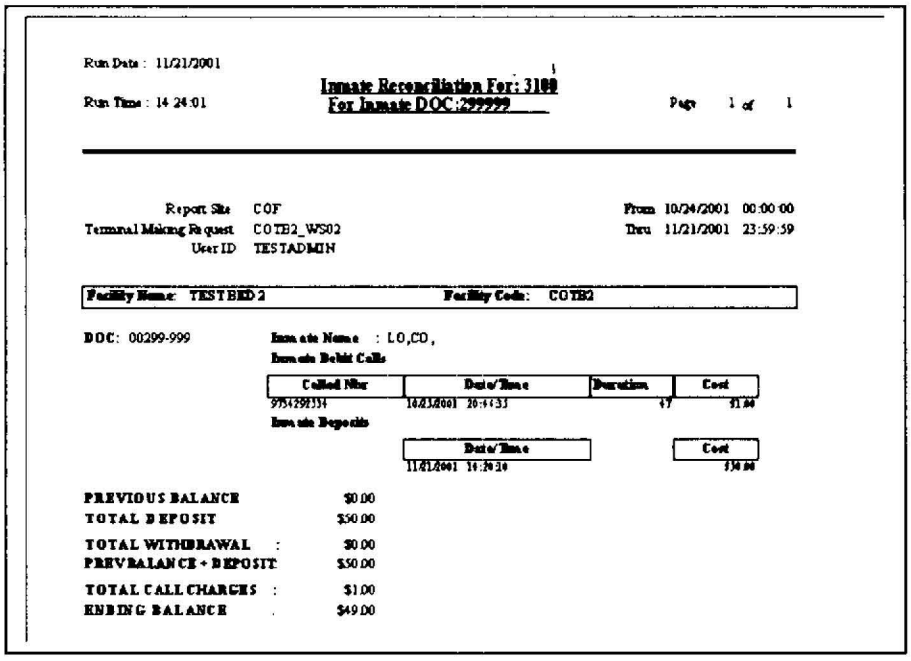
Facility Name:	TEST BED 1	Facility Code:	TEST 1

DOC	INMATE NAME	DEP DATE	DEPOSIT
111111	SMITHERS,TOM,	09/22/2001	$0.00
111111	SMITHERS,TOM,	09/22/2001	$5.00

1.1.5 *Inmate Reconciliation*

The *Inmate Reconciliation* report displays all financial activity associated with a particular inmate account for a specified time period. The Inmate Reconciliation report displays the following information:

- Inmate Number
- Inmate Name
- Inmate Debit Called Number
- Date/Time (of debit call)
- Duration
- Cost (deposits)
- Inmate Deposits
- Cost (withdrawals)
- Previous Balance
- Total deposits
- Previous Balance + Deposit
- Total Call Charges
- Ending Balance



Run Date : 11/21/2001
Run Time : 14:24:01

Inmate Reconciliation For: 3189
For Inmate DOC: 299999

Page 1 of 1

Report Site COF
Terminal Making Request COTB2_WS02
User ID TESTADMIN

From 10/24/2001 00:00:00
Thru 11/21/2001 23:59:59

Facility Name: TESTBED 2 Facility Code: COTB2

DOC: 00299-999 Inmate Name : LO,CO,

Inmate Debit Calls

Called Nbr	Date/Time	Duration	Cost
9754298334	10/23/2001 20:44:33	47	$1.00

Inmate Deposits

Date/Time	Cost
11/21/2001 16:20:20	$50.00

PREVIOUS BALANCE	$0.00
TOTAL DEPOSIT	$50.00
TOTAL WITHDRAWAL :	$0.00
PREVBALANCE + DEPOSIT	$50.00
TOTAL CALL CHARGES :	$1.00
ENDING BALANCE :	$49.00

1.2 Maintenance Reports

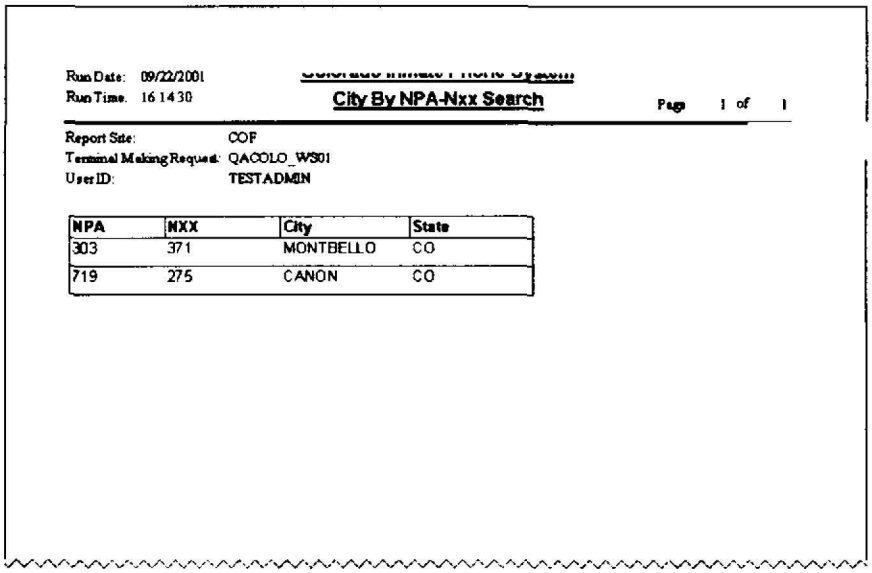
The following Maintenance Reports are available via the System workstation, or remote communications for authorized users:

- City by NPA-Nxx Search
- Local Exchanges
- Non Area Code/Exchange Attempts
- Percentage Grade of Blocking
- State by NPA Search

1.2.1 *City by NPA-Nxx Search*

The *City by NPA-Nxx Search* report provides the city and state for a particular NPA-Nxx. The City by NPA-Nxx Search report includes the following information:

- NPA
- Nxx
- City
- State



Run Date: 09/22/2001
Run Time: 16:14:30

City By NPA-Nxx Search

Page 1 of 1

Report Site: COF
Terminal Making Request: QACOLO_WS01
User ID: TESTADMIN

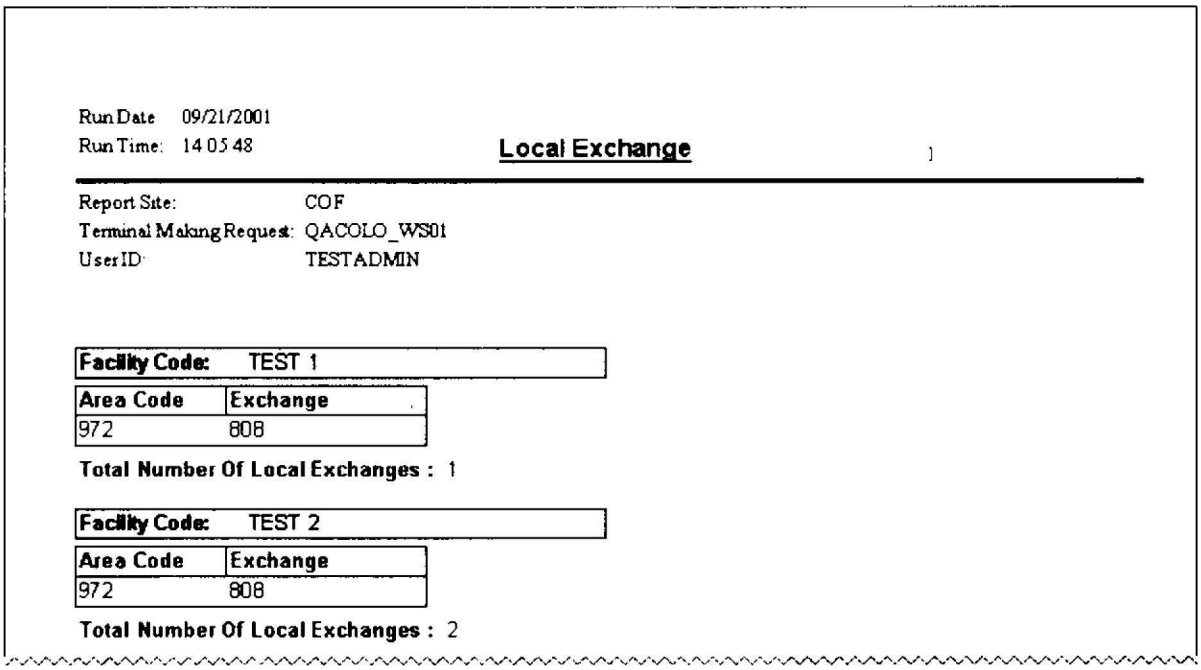
NPA	NXX	City	State
303	371	MONTBELLO	CO
719	275	CANON	CO

1.2.2 *Local Exchanges*

The *Local Exchanges* report provides a list of all area codes and exchanges, which are designated within the local calling area for the designated facility.

The Local Exchanges report contains the following:

- Facility Code
- Area Code
- Exchange associated with the area code
- Total Number of Local Exchanges



Run Date 09/21/2001
Run Time: 14 05 48

Local Exchange

Report Site: COF
Terminal Making Request: QACOLO_WS01
User ID: TESTADMIN

Facility Code:	TEST 1

Area Code	Exchange
972	808

Total Number Of Local Exchanges : 1

Facility Code:	TEST 2

Area Code	Exchange
972	808

Total Number Of Local Exchanges : 2

1.2.3 *Non Area Code/Exchange Attempts*

The *Non Area Code/Exchange Attempts* report lists call attempts to invalid area codes. The Non Area Code/Exchange Attempts report displays the following information:

- Facility Name
- Facility Code
- Inmate Number
- Inmate Name
- Date/Time of call attempt
- Dialed Digits
- Station
- Number of Calls Attempted with Invalid Area Code/Office

Run Date: 11/21/2001

Run Time: 14:27:30 **Non Area Code/Exchange Attempts** 1

Report Site: COF
Terminal Making Request: COTB2_WS02
User ID: TESTADMIN

From 09/21/2001 00:00:00
Thru 10/26/2001 23:59:59

Facility Name: **Facility Code:**

DOC	Inmate Name	Date/Time	Dialed Digits	Station

Number of Calls Attempted With Invalid Area Code/Office Code: 0

1.2.4 *Percentage Grade of Blocking*

The *Percentage Grade of Blocking* report provides phone information on a line-by-line basis for the percentage of calls blocked during specific hourly periods. The Percentage Grade of Blocking report displays the following information:

- Facility Name
- Facility Code
- Number of calls attempted
- Number of blocked by traffic
- Blocked Percentage
- Trunk Types

1.2.5 *State by NPA Search*

The *State by NPA Search* report allows the facility to locate the state for a particular NPA. The State by NPA Search report displays the following information:

- NPA
- State

Run Date 09/21/2001
Run Time: 14:17:56

State By NPA Search

Report Site: COF
Terminal Making Request: QACOLO_WS01
User ID: TESTADMIN

NPA	State
719	CO