



DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS

Program Statement

OPI: OMITS
Number: 2420.8
Date: December 15, 2003
Subject: Disaster Recovery Plan

1. **PURPOSE AND SCOPE.** This program statement governs routine backup and disaster recovery operations to ensure continuity of operations in the District of Columbia Department of Corrections (DOC). It applies to all critical DOC computing resources and data.
2. **PROGRAM OBJECTIVES.** The expected results of this program are:
 - a. Systems and applications software, files and data shall be backed up regularly to enable recovery in the event of disaster or other disruption of computing services.
 - b. Backup and recovery processes shall be 100% effective.
 - c. Continuity of operations shall be ensured by maintaining alternate processing sites and duplicating files, programs and documentation that shall be stored in secure premises outside of DOC computer rooms.
3. **DIRECTIVES AFFECTED**
 - a. **Directives Rescinded.** None
 - b. **Directives Referenced**
 - 1) PS 2000.2 "Retention and Disposal of Department Records", (2/26/01)
 - 2) PS 2420.2 "Information Security", (12/15/03)
4. **AUTHORITY**
 - a. D.C. Code Section §24-211.02 Powers: Promulgation of Rules
 - b. DOC Office of Management Information and Technology Services (OMITS) Disaster Recovery Plan

5. STANDARDS REFERENCED

- a. American Correctional Association (ACA) 2nd Edition Standards for Administration of Correctional Agencies: 2-CO-1F-01 and 2-CO-1F-06.
- b. American Correctional Association (ACA) 3rd Edition Standards for Adult Local Detention Facilities: 3-ALDF-1F-01 and 3-ALDF-1F-02.

6. RESPONSIBILITIES

- a. The Office of Management Information and Technology Services (OMITS) Administrator is responsible for oversight and enforcement of the Disaster Recovery Plan, and shall personally take charge of recovery operations in emergencies.
- b. OMITS technical staff (On-Call, System, Network, and Database Administrators) shall maintain and implement a multi-level Recovery Operations Plan and provide technical assistance in its application.
- c. DOC office chiefs shall coordinate with OMITS in all matters relating to backup and disaster recovery, and ensure that the procedures in this directive are followed.

7. REQUIREMENTS

a. Disaster Recovery Plan

- 1) The Disaster Recovery Operations Plan shall be used to avoid prolonged disruption of information service to users. This plan is "Agency Confidential", and contains procedures that will protect against the loss of automated data processing files, data in DOC's databases and servers, applications and systems software, systems documentation, and processing instructions.
- 2) OMITS shall review the operations plan and the set of materials kept for backup and recovery operations, at a minimum, every six months.
- 3) Detailed instructions for routine backup and disaster recovery shall be maintained in secure locations in computer rooms or off-site.

b. OMITS Director shall:

- 1) Ensure adequate OMITS staff are available for 24-hour/7-day coverage.
- 2) Ensure that OMITS "on-call" staff are trained and prepared to implement the DOC Disaster Recovery Plan and shall do so in the event of any emergency or disaster occurring during non-duty hours.

- 3) Provide an Emergency Contact List of OMITS staff that are authorized to grant access to the DOC Backup and Recovery Operational Plan.

c. **OMITS Technical Staff shall:**

- 1) Acquire and maintain, at a minimum, an inventory of spare parts to support any emergency, memory, monitors, Network Interface Cards, CD ROMs, floppy drives, and other components determined to be critical.
- 2) Acquire, install, and maintain the necessary software and equipment required to ensure DOC's readiness to implement backup and recovery procedures in the event of an emergency or disaster.
- 3) Maintain the on-line "backup" server for JACCS at a location other than at the DC Central Detention Facility (CDF). This backup server shall be used in the event of unforeseen emergencies or disasters.
- 4) Determine the requirements for backup for each organizational unit in coordination with the DOC office chiefs.
- 5) Develop and maintain DOC's multi-level Backup and Recovery Operations Plan to meet the requirements, and review this plan semi-annually (every 6 months). These reviews shall include review and evaluation of the set of materials kept for backup support. The following five (5) components shall be addressed in DOC's Backup and Recovery Operations Plan and as specific agenda items during plan reviews:
 - a) Processes and procedures used to copy, label, and store all data files, applications software, systems software, and plans of action. Reviews shall specifically include evaluation to ensure that copies are complete, accurate, and up-to-date.
 - b) Verification of the list of materials required and backup copies required. The list of materials required for backup shall be compared with actual copies of material presently available to ensure accountability for each item.
 - c) The schedule for creating copies of backup and recovery materials. Reviews shall examine schedules for creating backup copies and processes used for restoration of data and files. Thus, the reviews shall be conducted to ensure that users understand the processes and procedures and what baseline shall be restored under various emergencies. Copies stored "off-site" must be current to satisfy user-specified requirements.

- d) Environmental protection afforded backup and recovery copies must be commensurate with the level of sensitivity required for the data, applications, and materials being backed up.
 - e) The list of data, files, and systems requiring special backup procedures and controls to ensure it is up to date.
- 6) Test applications software developed in-house or commercial-off-the-shelf software (COTS) acquired to ensure they have backup and recovery utilities or support modules for automatic data backup at least once a week, that changes are updated at least daily, and that they are able to recover work-in-progress if the system fails in the middle of a transaction.
- 7) Ensure that applications support documentation includes, at minimum, the following:
- a) Provisions for on-line intervention, abort, and user communications;
 - b) Automatic and manual procedures to be followed for each potential trouble occurrence; and
 - c) A description of steps to be taken to restart the application after an abort or interruption of operation.

d. **DOC Office Chiefs shall:**

- 1) Provide to OMITS, and update as necessary, a listing of data, files, and systems requiring special backup procedures and controls;
- 2) Participate in semi-annual reviews of the Backup and Recovery Operations Plan in coordination with OMITS; and
- 3) Follow the DOC notification procedures in the event of an emergency or imminent threat to computing resources and data under their responsibility.

8. **ROUTINE BACKUP PROCEDURES.** OMITS Technical Staff shall:

- a. Maintain instructions for shutdown and startup of critical servers in the Computer Room. These procedures cover servers in the Computer Room, as well as network components across the wide-area network;
- b. Perform a local and remote backup each night on key servers;
- c. Store backup tapes for each week in the Computer Room;
- d. Conduct a daily review of backup logs to ensure successful backup operations were performed;

- e. On a weekly basis, ship the collection of tapes for the previous week to a different facility, as determined by Chief of Network Operations, for offsite storage;
- f. Each month collect tapes aged older than one month and retain for one year at a location set aside for monthly archives; and
- g. Each January 1, collect tapes aged older than one year and retain for three years at a location set aside for long term archives.

9. **DISASTER RECOVERY PROCEDURES**

a. **Requirements**

- 1) A 'disaster' is defined as physical damage, or a threat of physical damage, to be caused to critical computing resources such as fire, flood, or other causes, including a security breach or a power loss.
- 2) Detailed information on system configuration, passwords, and other information critical to accessing and starting up of the system shall be distributed to OMITS technical staff who shall maintain their copy off-site, secure and readily available in the event of a disaster.
- 3) Order of recovery shall be:
 - a) **Priority 1: Critical Services and Recovery Priorities**
 - (1) Secure and set up a location Network Room;
 - (2) Install the server LAN Hubs, routers, switches local to the room;
 - (3) Install the servers;
 - (4) Install or connect to the building/campus LAN Hubs, routers, etc.;
 - (5) Establish telephone services; and
 - (6) Install the Internet service Connections.
 - b) **Priority 2: Re-establishment of business systems**
 - (1) JACCS access;
 - (2) Accounting/Budget;
 - (3) Payroll; and
 - (4) Procurement.

- c) **Priority 3: All remaining services**
- 4) Priority order for processing in a 'degraded mode' shall be:
 - a) Interactive input of data;
 - b) Ad hoc query of databases; and
 - c) Standard reports generation.
- b. **Person discovering a disaster shall:** Notify the appropriate OMITS First Response Officer, who shall notify others, as appropriate. For situations during normal business hours, personal contact shall be made; for a disaster outside of normal business hours, contact (202) 538-2501. OMITS shall provide a sequenced list of First Response Officers and associated contact number(s) for insertion into the Administrative Duty Officers Book and the Facility Duty Officers Book.

OMITS First Response Officer shall:

- c.
 - 1) Ensure that all required notifications are completed;
 - 2) Implement the duties of the OMITS Administrator until relieved by the OMITS Director;
 - 3) Begin documenting the situation and events that have occurred;
 - 4) Check the "events" log; and
 - 5) Assist the System Administrator in diagnosing hardware and/or software problem(s) and with implementation of corrective actions.

OMITS Administrator shall:

- d.
 - 1) Notify and assemble the recovery staff;
 - 2) Review this recovery plan with the staff;
 - 3) Organize for damage assessment;
 - 4) Establish communications systems for the staff;
 - 5) Assign duties and responsibilities to the staff;
 - 6) Ensure that corrective actions are timely and appropriate;

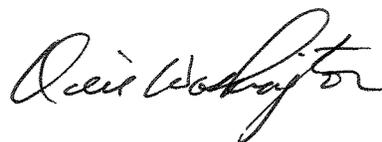
- 7) Inform the DOC Director in extreme cases of emergency, in the event of a security breach, unusual damages, or in the event of casualties;
- 8) Notify external agencies when appropriate;
- 9) Notify the appropriate vendors and service providers; and
- 10) Communicate status to executive staff as necessary.

e. **OMITS Recovery Staff shall:**

- 1) Review the detailed disaster plan retrieved from the designated off-site location;
- 2) Conduct a site survey of the affected area;
- 3) Develop a detailed action plan;
- 4) Inventory any salvageable or usable equipment;
- 5) Recover all salvageable hardware;
- 6) Service or refurbish equipment as necessary;
- 7) Re-establish services in their order of priority (1,2, 3); and
- 8) Document the recovery progress and maintain on file for periodic review of "lessons learned".

10. **TRAINING**

- a. A special training program in support of the DOC Backup and Recovery Operations Plan shall be developed by OMITS for use by DOC offices. Its focus shall be on end users and their roles and responsibilities for backing up their individual work, data, and documents.
- b. Supervisors of DOC offices shall use the OMITS training program to support backup and recovery training, to orientate and train new employees, and ensure that all employees fully understand their responsibilities related to the backup and recovery of DOC data, files, and documentation.



Odie Washington
Director