



DEPARTMENT OF THE AIR FORCE

HEADQUARTERS AIR FORCE SPACE COMMAND

MEMORANDUM FOR AFSPC CONS/CCs
SMC/PK

30 June 2004

FROM: HQ AFSPC/PK
150 Vandenberg St, STE 1105
Peterson AFB, CO 80914-4350

SUBJECT: Information Letter 2004-04 (Revision 1), Standard Procurement System (SPS) Data Back-up and Contingency Operations Plan (COOP)

1. This letter is directive in nature for all AFSPC contracting offices that use SPS. The changes in this letter are indicated by a line in the right hand margin. This letter supersedes Information Letter 2004-04 dated 9 Jan 2004.
2. In the event of a system failure or a catastrophic event the ability to recover SPS data is critical. The following procedures will ensure standardized back-up timeframes and will reduce downtime should you experience a system failure or catastrophic event.
3. A complete server backup will be performed daily. Each week the cumulative daily backups for the week will be stored at an off-site location to ensure recovery capability in the event of an emergency or disaster.
4. COOP plans will be developed at each location. Use the attached checklist as a guide in developing your COOP. Each plan will have as a minimum:
 - a. Primary and alternate site locations identified
 - b. The location of your off-site stored back-ups
 - c. A Memorandum of Agreement between your organization and both the primary and alternate sites outlining the level of support required to recover your location
5. For any questions, my POC is Mr. Rick Myers at DSN 692-5782 or e-mail at rick.myers@peterson.af.mil.

1 Atch
Emergency Readiness Checklist

A handwritten signature in black ink, appearing to read "Michael D. McAdams".

MICHAEL D. McADAMS
Asst. Chief, Contracting Division

EMERGENCY READINESS EVALUATION CHECKLIST

Site Information

Site Name:

Site Activity Code/DODAAC:

POC Name:

POC E-Mail Address:

POC Phone Number:

PART I -- SITE SPECIFIC COOP PREPARATIONS

Does your site have an established COOP?

Who at your site is familiar with the COOP process?

Name:

Commercial Phone Number:

Who is responsible for bringing your operations back online in case of disaster?

Name:

Commercial Phone Number:

Does the backup SA have experience bringing the server back online with assistance?

Name of Backup SA:

Commercial Phone Number:

Is the backup SA familiar with the hardware configuration at your site?

Does someone other than the SA know the System Administrator and Super User passwords for both PD² and Sybase? Is the Password maintained in a known location in the event those individuals with access are not available in an emergency?

Name:

Commercial Phone Number:

Have you identify a "sister" site within the USAF who would be able to assist with the restoration of your site's operations in case of disaster?

Name of site:

Is there someone at the "sister" site who could assist you if necessary?

Name:

Commercial Phone Number:

PART II -- SOFTWARE ACCESSIBILITY

Do you have all current installation CDs and instructions?

Are these CDs and instructions readily available?

PART III -- HARDWARE READINESS

Do you have an Uninterruptible Power Supply (UPS) for all servers?

How long can you maintain operations using only the UPS?

Do you have surge protectors for all client workstations?

Do you run a test to verify proper performance of hardware, software, and communication/telecommunications links?

Have you determined a schedule for interim restoration of service functions and processing of critical LAN applications?

PART IV -- BACKUPS

Are your database dump and backup processes automated?

Do you do daily dumps of your databases? If so, which databases are dumped daily?

Master
MODEL
SYBSECURITY
SYBSYSTEM PROCS
DBCCDB
Admin_DB
Production (SPS_FUIC_DB
SPSI (FUIC_SPSI_IDB)

Are daily dump files overwritten every night?

Do you have a week's worth of viable backups?

Are daily dumps archived?

Do you do weekly backups of the databases listed above?

Where are backups stored?

Does your site take Tape backups? If so, how often are these backups done?

What are the hardware specs of your Tape drive (Brand, Tape Size, Space available on tape)?

Is the entire Sybase directory copied to tape?

Are both .dmp and .dat files copied to tape?

Where are these Tape backups stored?

If tapes are stored at an outside source, how long would it take to retrieve these tapes in case of emergency?

Do you take Full File System backups or at least a backup of the entire Sybase Directory with an application other than Sybase?

In case of corruption, do you know how to stop the backup process from running, preventing a corrupted dump from overwriting a viable dump?

Are backup files maintained at a secondary site?

What is your current off-site storage rotation policy?

Are duplicate program files stored off-site?

AFCIS can ship a contingent server to a site. Is a backup service facility and/or backup LAN available to operate this contingent server?

Is the backup service facility or LAN in a different room or building than the primary facility or LAN?

Can the backup facility handle the current workload?

If no designated backup exists, is there access to another service facility, carrier, or LAN?

Is an implementation plan available for use of backup facility, carrier, or LAN?

Have formal contingency plans been developed for service facility or backup capability?

For a worst case scenario, do you have an SLA with the nearest other USAF base contracting office to load your database so you may continue operations?

PART V -- CONTINGENCY PROCEDURES

Has it been determined if manual processing of each critical service function or LAN application is feasible and necessary?

Are there formal, written manual operating procedures for each such critical service or LAN application?

Are there formal, written procedures for resuming operating services and LAN-based applications after manual processing?

Have all manual processing procedures been tested?

Have all procedures for resumption of operational services and LAN processing been tested?

PART VI -- RECOVERY PROCEDURES

Have disaster recovery teams been defined?

Does each recovery team have written responsibilities and procedures to follow?

Do recovery procedures cover retrieval of all necessary files documentation from the off-site vault?

Do recovery procedures cover the activation of a backup facility, carrier or LAN if necessary?

Do recovery procedures cover the transportation of personnel supplies to off-site alternatives, if necessary?

Do recovery procedures cover the establishment of necessary communications and telecommunications links?

Do recovery procedures cover copying backup files and programs to the backup alternative?

Do recovery procedures cover specific instructions for recovery of each service function and critical LAN application?

Do recovery procedures cover running a test to verify proper performance of hardware, software, and communications/telecommunications links?

Do recovery procedures determine a schedule for interim restoration of service?

Do recovery procedures return to normal operations and processing when the primary service facility or LAN is fully restored?

PART VII -- EVENT DETECTION

Are there specific procedures for responding to emergencies?

Are emergency procedures readily available in the service facility?

Do emergency procedures include actions that pertain specifically to the operational service or LAN data?

Do emergency procedures specify persons to be contacted and their alternates?

Are there procedures or guidelines for escalating problems or interruptions to disaster status?

PART VIII -- MANAGEMENT PROCEDURES

Is there one person with management responsibility for disaster recovery?

Is there a procedure for notifying the disaster management team?

Have specific locations been identified, either on-site and off-site (or both) to use as control centers for directing recovery operations?

Is there a procedure for conducting damage assessment?

Have the persons responsible for damage assessment been identified?

Is there a procedure for notifying the recovery LAN organization and mission-essential service users of steps to be taken?

PART IX -- INVENTORY

Is there a current inventory of each of the following resources:

Hardware
Communications and telecommunications components
Data entry devices, if required
Firmware
Software
Data
Supplies

PART X -- TRAINING

Is there a systematic program for training on the COOP?

Are records kept of which employees have received COOP training?

Is the training program revised based on the results of recovery tests?

Are service facility and LAN staff given cross-training?

Is the COOP used as the basis for training?

PART XI -- PREVENTIVE MAINTENANCE

Does your site have a test database?

Name of database

Are you expanding the size of this test database at the same rate at which you expand the PD² production database?

How often do you test your backups by loading them into the test database?

Where are your backup.log and Sybase error log located?

How often are your backup log and Sybase error logs examined for errors?

**Please provide ART with a copy of the backup.log and Sybase error log with two days worth of data*

How often do you run Database Consistency Checks (DBCCs)?

Do you run dbcc checkstorage daily?

Against which databases?

Do you run dbcc checkdb weekly?

Against which databases?

Do you run dbcc checkalloc weekly?

Against which databases?

Do you run dbcc check catalog weekly?

Against which databases?

Where are dbcc output files stored?

How often are dbcc output files checked for errors?

Do you regularly run "Update Statistics"? If so, how often?

Do you regularly monitor the space of your databases, and pre-emptively expand them before all users are locked out from lack of space?

Do you have your Security Model captured on Cognos Reports that can be used in case dumps are lost, or are not viable and a clean install is required?

Do you check your BrightStor logs daily?

PART XII --TESTING

Are there procedures for testing restoration of services using inhouse service or LAN facilities and off-site files or documentation?

Have recovery procedures been tested within the past year using inhouse facilities and off-site files and documentation?

Have recovery procedures been tested within the past year using backup facilities and offsite files and documentation?

PART XIII -- MAINTENANCE

Is there a procedure for initiating revisions to the COOP?

Are the results of testing reviewed for training implications?

Are the results of training reviewed for planning implications?