

Data System Back-up and Recovery Testing

PROCEDURE – This information is reviewed and tested annually in January.

Backups

Data backups will occur on a daily basis with tape verification and rotation as follows:

1. Bootable backup:

- Frequency: Each time any updates or changes are made to the system
- Copies: Two
- Storage: IS Lockbox (on-site), designated off-site location
- **Testing 1/2010: Verified backups on site and in the off-site location for all servers (system state backups).**

2. Daily backup:

Database File

- Specifics: Production database and files (UNICARE) are backed up by SQL Server 2005 each night at 1:00 a.m. Two days are maintained on the SQL server to allow for fast recovery. These files are then backed up to the KMH tape and on-line backup device.
- Frequency: Daily 1:00 a.m.
- Copies: Two on the SQL Server, image of these sent to daily tape and on-line backup storage.
- Storage: IS Lockbox (tape - on-site), on-line digital backup in the Secure Server Room.
- **Testing 1/2010: Restored test database from the backup file of the live database. Connected to the database and verified functionality. Verified system state backup from on-line storage and copies in the off-site safe.**

System files

- Specifics: Copies of at least one Application Server, Terminal Server and Automation Manager systems are contained within the nightly backup for quick restoration should it be needed.
- Frequency: Daily 1:00 a.m.
- Storage: Along with main KMH backup system.
- **Testing 1/2010: Verified system state backup from on-line storage and copies in off-site safe.**

3. Situational backup:

- Prior to any major version upgrade to the system(s). These are kept at the designated off-site location until the next major event.

- **Testing: Verified last copy of ProFiler system performed after the version upgrade to 2009 on 11/6/2009.**

Rotation of backups:

1. Bootable backup:

- 1 copy of current in IS Lockbox (Previous version moved to off-site storage in lockbox)
- 1 copy of current and previous 2 at designated off-site location
- **Testing 1/2010: Verified copy of current system state in IS lockbox. Verified storage at off-site location.**

2. Daily backup:

- Non end-of period *(see below): IS Lockbox (re-using oldest tapes in rotation)
- Wednesday at designated off-site location
- End of month: Designated off-site location (keep a quarter's worth of monthly tapes – Jan-Mar, Apr-Jun, Jul-Sep, Oct-Dec – then place older tapes back into rotation).
- End of quarter: Designated off-site location (keep 4 quarter's worth – placing oldest tape back into daily rotation).
- End of year: Designated off-site location (keep all yearly tapes). This should be created when all processing is completed and books closed for the FY.

3. Situational backup:

- Keep current and one previous version at designated off-site location

Hard Copy Reports

- Should temporary manual operations be required, monthly reports (data as identified in the Disaster Recovery Plan) from the data system will be copied to a device (ZIP, Flash or CD).

System Restoration and Recovery

Critical Need

The following functions have been identified as critical:

1. Transfer of information to WA State. This includes new data as well as any researched and corrected data. Data is sent directly via the www.waproviderone.org site (logging into the PRSN domain – 1050210) or via the Provider One secure FTP site (sftp:waproviderone.org). Should the preferred secure VPN connection to MHD be unavailable for transfer (for more than 1 week), the following alternative methods shall be used (in order of preference):
 - Files (in approved format) will be transferred to an external device (such as flash or CD) and delivered to MHD in person.

- **Testing 1/2010: Tested creating files as sent to the state on password protected Flash Drive. Verified data readability successfully.**
2. Basic client information. This includes information such as scheduled appointments, client contact/ location information, caseload lists. Basic client data mentioned above will be downloaded monthly from ProFiler and written to a flash drive stored in an Excel format and stored at the off-site safe. This file can be loaded to any standard personal computer for access/printing.
 - PRSN eligibility data from the State on a weekly basis. The database (Access database) containing the eligibility information is backed up within the standard nightly backup at KMHS.
 - **Testing 1/2010: Files downloaded from ProFiler (Excel and MS Word formats) opened for readability successfully. Data restored from system backup. Successful opening and operation of restored database (MS Access).**
 3. Payroll, Accounts Receivable, Protective Payee and Accounts Payable at any PRSN agency that uses these features within CMHC. The items described below will be downloaded monthly in a text or delimited file and written to a flash drive stored in the fire-proof disaster plan box in IS Tech office (room 508). This would require, at a minimum, the following to allow these crucial business functions to be manually processed:
 - Payroll: Listing of staff pay scales, FTE, deductions (CMHC Report ACSTFALL) – weekly reports, saved off monthly
 - Accounts Receivable: Listing of client balances from each funding source (AR Aging Report from ProFiler)
 - Protective Payee: Listing of current balances and check details for current FY.
 - Accounts Payable: Listing of vendors and Journal Detail/General Ledger information for the current FY.

All other services could be deferred to the recovery stage.

 - **Testing 1/2010: Files downloaded from ProFiler (Excel and MS Word formats) opened for readability successfully. Data restored from system backup. Successful opening and operation of documents.**

Recovery

The main impacts of catastrophic loss of computer equipment or extended delays in resuming full processing capacity would be delays in financial and statistical procedures: reports and backlogs of client and activity information to be entered. This would not affect services to the public following an emergency, but could have effect to the provider financial stability and ability to determine impact.

1. The provider information systems would face difficulties in returning to full production in the face of backlogs, if the system were unavailable for more than one month, under normal circumstances. Staff shortage and unusual demand for services would make the need more critical. Business department needs would be given first priority if computer access were limited.

2. Finance could tolerate a 1-2 month delay, depending on the timing of checks to be processed.

Use of On-Line Terminals during and after a system failure or natural disaster

- Responsibilities

The most critical computer functions will be assigned to any terminals that remain on-line at KMHS.

- First Priority

1. Verify that the ProFiler and CMHC systems are still functioning safely, and will have a source of continuous power.
 - a. Physically inspect the computer room and status of UPS.
 - b. An Information Systems staff (usually the IS Director) at Kitsap Mental Health Services will determine if the computer must be shut down.
2. Verify that terminal locations function properly and the areas are safe to work in.

- **Testing 1/2010: Weekly testing continues of access to all servers from systems contained within the IS Computer Room. On-going access verified via the external VPN connections.**

- Second Priority

1. After critical needs are met, allocate existing terminal access for emergency use by Jefferson Mental Health, West End Outreach and/or Peninsula Community Mental Health Services at Kitsap Mental Health Services locations.
2. Information Services staff from Kitsap Mental Health Services will be assigned to assist each site staff at KMH locations as needed.

Use of a Portable Computer as a Terminal during and after a system failure or natural disaster

- Responsibilities

A portable PC may be assigned to replace or supplement office terminals. The portable PC must be equipped with a modem for dial-up connectivity or, preferably, high speed Internet to connect to the PRSN VPN system.

- First Priority

1. If the Information Services offices are inaccessible, but the ProFiler, CMHC systems and phone lines are working, assign at least one laptop to serve as a terminal in a remote location.
 - a. Set up laptop in location with electricity and a phone jack.
 - b. Secure Internet connection with the KMHS VPN client installed (IP 66.81.199.165 or <https://secure.kmhs.org>)

- Second Priority

1. After critical needs are met, allocate existing access to Jefferson Mental Health, West End Outreach and Peninsula Community Mental Health staff for maintaining data processing.

Connection to and use of a CMHC “HOT SITE” during and after a system failure or natural disaster

- Responsibilities

Critical services for clients must be maintained by extracting or entering data in the system. If the CMHC system is not running, an emergency backup may be run at another location. Potential hot sites would include CMHC Systems in Dublin, Ohio; Jet Computers in Olympia, Washington; and Spokane Mental Health in Spokane, Washington. There would be costs associated with this hot site usage that would require negotiation at the time of the need.

- First Priority

1. Data necessary for direct client services.

- a. Retrieve most recent CMHC backup tape from lock box in Room 508 (Note: If the hot site does not have BRU as a backup program, the weekly TAR backup will have to be used – or the BRU could be provided to the remote site for installation).
- b. If Room 508 (located at KMHS main campus) is inaccessible, retrieve most recent backup tape (BRU or TAR format) from the safe located at 900 Sheridan, Bremerton, Washington.
- c. Load /c1/RSN, /c0/MIS, /c2/FKS, /c3/PT, /c4/IMAGEFILE and /c5/PA at hot site.
- d. Depending on location, dial in or have staff at hot site log on and print reports designated in the Critical Need section of this document.

- Second Priority

If staff may sustain access to the hot site, the following functions may be run, depending on time and equipment available.

1. Additional lists of staff or client, inventory, or financial/statistical reports for urgent needs.
2. Data lookups or updates for service to existing clients.
3. New client registers and services.

Information Services Evacuation Plan During a Natural Disaster

The following actions should be taken by KMHS IS staff upon evacuation and/or other assigned disaster prep staff upon assignment:

Upon initial evacuation:

IS Staff from room 508 (located on KMHS main campus) will take contents of the lock box. This lock box is located in room 508, by door. This lock box contains:

1. Nightly backup tapes from the IBM and Windows servers

2. Agency master key
3. Safe combination (for safe located at Sheridan facility)
4. Up-to-date IS, Agency, Cell Phone and vendor POC listing
5. Recovery procedures (data/programs, etc)
6. IS inventory listing
 - **Testing 1/2010: Verified contents of the IS Lock Box.**

Upon re-entrance/secure actions:

1. The main computer systems (room 508 computer room, labeled in orange) will be powered off and CPUs removed.
2. The computer designated for the DBA (room 508, labeled in orange) will be powered off and the CPU removed.
3. If power is on and water is present in room 508 or computer room, power should be secured via the circuit breakers. Any circuit breaker work must be coordinated with KMHS Facilities staff.
4. The telephone system computer (phone equipment room, labeled in orange) will be powered off and the CPU removed.
 - If power is on and water is present in phone equipment room, power should be secured via the circuit breakers. Any circuit breaker work must be coordinated with KMHS Facilities staff.
5. The IS companion telephones (assigned to the Help Desk and Computer/Telecommunication Technicians) will be removed and offered to command post for assistance (local on-campus communications only).
6. Additional charged batteries (as many as available) and charger units for companion phones.
7. If additional threat, the safe located at 900 Sheridan (Bremerton, WA) should be removed from area as soon as possible. This safe contains:
 - a. Master copies of software.
 - b. Master and scheduled backup tapes
 - c. Up-to-date IS POC listing
 - d. Disaster Plan (data/programs, etc)
 - e. IS inventory listing (quarterly run)
 - f. Critical printouts (identified in plan)