



## PENINSULA RSN

### MANAGEMENT INFORMATION SERVICES POLICIES AND PROCEDURES

**Policy Name:** DATA SYSTEM BACKUP AND RECOVERABILITY

**Policy Number:** 4.07

**Reference:** DSHS Contract

**Effective Date:** 4/2004

**Revision Date(s):** 9/2008

**Approved by:** PRSN Executive Board

#### CROSS REFERENCES

- Policy: Corrective Action Plans

#### PURPOSE

To ensure the Peninsula Regional Support Network (PRSN) data stored electronically is adequately backed up and plans in place to provide recoverability due to data corruption or a regional computer system failure.

#### Background

The Peninsula Regional Support Network contracts with Kitsap Mental Health Services (KMHS) to operate and maintain the data system used by all network contractors within the PRSN. The system uses CMHC/Netsmart software. All PRSN network providers are connected to the data system through either a VPN or a secure Point to Point T1 data connection, and are assigned a data base which is unique to each provider. KMHS is responsible for maintaining the network, importing required data from each provider's database into the unduplicated PRSN database, and transmitting required data to the Department of Social and Health Services Mental Health Division.

#### PROCEDURE

##### Preparedness

Because of the potential risk and ongoing vulnerability to loss of data, the KMHS Information Services Department has in place a backup and storage policy and procedure that is practiced every working day. These backup procedures would allow KMHS and the other network providers within the PRSN to retrieve critical information

necessary for the conduct of business functions on an immediate basis, and ultimately allow a full restoration of the data system given a catastrophic failure.

### 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

#### 2. Daily backup:

##### UNIX

- Frequency: Monday through Friday (backups actually run Tuesday through Saturday at 1 a.m.)
- Copies: One
- Storage: IS Lockbox (on-site)

#### 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.

### Rotation of backups:

#### 1. Bootable backup:

- 1 copy of current in IS Lockbox (destroy previous version in lockbox)
- 1 copy of previous 2 at designated off-site location

#### 2. Daily backup:

- Non end-of period \*(see below): Monday, Tuesday, Thursday, Friday in 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. Daily transfer of information to MHD/MAA. This includes new data as well as any researched and corrected data. MHD IP for file transfers: [ftp 147.56.37.121](ftp://147.56.37.121) is connected to using a secure VPN connection and is encrypted using SSH data transfer protocol. Should the preferred secure VPN connection to MHD be unavailable for transfer (for more than 3 working days), the following alternative methods shall be used (in order of preference):
  - Dial-up connection to MHD (with their approval) from any so equipped computer (with approved encryption protocols).
  - Secondary transmission method (dial-up) is tested and certified by MHD on an annual basis.
  - Files (in approved format) will be transferred to an external device (such as flash or CD) and delivered to MHD in person.
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 CMHC and written to a flash drive stored in the off-site safe. This file can be loaded to any standard personal computer for access/printing.
3. PRSN eligibility data from the State on a monthly basis. The database (master) containing the eligibility information will be downloaded monthly from CMHC and written to a flash drive stored in the off-site safe.
4. Payroll, Accounts Receivable, Protective Payee and Accounts Payable at any PRSN center 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 off-site safe. 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.
  - Accounts Receivable: Listing of client balances from each funding source.
  - 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.

### **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 Recovery Team (led by KMHS Information Services Director, staffed by KMHS Information Services staff as well as staff designated by provider agencies as needed) will ensure recovery within the priorities as listed below. In the event the KMHS Information Services Director is not available, the PRSN can delegate assignment, activities and leading of the Recovery Team as deemed necessary.

Emergency shutdown procedures are posted on the reverse of the entrance door to the KMHS Server Room (5455 Almira Drive NE – Bremerton, WA Room 509) along with contact phone numbers for Information Services staff (in order of priority).

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

- First Priority

1. Verify that the CMHC system is 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.

- 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 CMHC system 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. Use modem to dial into CMHC System (360-373-1928, 360-373-0979 or 360-373-0981) or have a secure Internet connection with the KMHS VPN client installed (IP 66.81.199.165)

- 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
7. Emergency shutdown procedures
8. Contact phone numbers for Information Services staff (in order of priority).

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 (CMHC latest releases, Acuprint, SolAce, BRU, Donor Perfect, Windows licensing and CD copies, and Backup Exec).
  - 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)

## **MONITORING**

This policy is mandated by contract.

1. This policy will be monitored by the PRSN by the following means:
  - Kitsap Mental Health Services and the PRSN will debrief any extended down-time and/or restoration action and resolve problems identified.
  - Annual EQRO audits and findings. The PRSN will follow-up with any assigned corrective action requirements.
  - Annual PRSN Subdelegation Review of the regional IS system
2. If KMHS performs below expected standards during any of the reviews listed above a Corrective Action will be required for PRSN approval. Reference PRSN Corrective Action Plan Policy
  - Because KMHS contractually provides the PIHP regional Information System, the PRSN has the ability to impose penalties, modify the Subdelegation contract, or decide to not continue to contract.