COUNTY OF YOLO

HEALTH AND HUMAN SERVICES AGENCY

POLICIES AND PROCEDURES

SECTION 5, CHAPTER 4, POLICY 005

DATA BACKUP AND PHYSICAL SAFEGUARDS

A. PURPOSE

To provide Yolo County Health and Human Services Agency (HHSA) Behavioral Health staff with information regarding periodic backup and storage of HHSA systems to ensure security and physical safeguards to protect against the loss, damage or destruction of data to include, but not limited to, PHI and PII. Additionally, to improve incident response during system failures, minimize service interruptions and support recovery of critical functionality after a disaster.

B. FORMS REQUIRED/ATTACHMENTS: N/A

C. DEFINITIONS:

1. **Workforce members:** Yolo County HHSA Behavioral Health Staff

2. **Portable Systems:** Laptops

D. POLICY

It is the policy of Yolo County HHSA Behavioral Health to maintain backup and storage plan for system server operating and application software and the file structure and contents of the related data files for the purposes or restoring the system and associated data, to include PHI and PII, in the event of failure of the system or its hardware or damage. At minimum, the backup schedule shall be completed weekly while offsite storage shall occur monthly.

E. PROCEDURES

1. Yolo County Information Technology Department shall be responsible for the following:

   a. Critical business information and critical software on HHSA computer systems must be periodically backed-up.

      i. Server and Network system backup processes must be performed with sufficient frequency to avoid loss of production data and to support documented contingency plans.

      ii. Portable Systems: Workforce members using portable computers are responsible for making backups of all critical information prior to taking out-oftown trips or expecting to do business where theft of the device is a possibility. These backups should be stored elsewhere than the portable computer's carrying case. This precaution supplements the periodic backups to network storage that must otherwise be made.

iii. Desktop Workstations: Critical data must be backed-up to removable media and/or to network storage periodically and at frequent enough intervals to minimize service dislocations due to restoring missing or compromised work data.

iv. Backup Media must be stored in a Secure Location when kept on site: The primary backup media storage site must be acceptably secure from unauthorized access, physical damage to the stored media, magnetic damage to the data on the media and unauthorized moving, copying or transmission of critical stored data. The default choice for this storage on a network File server for workstation data, and at the designated data center and offsite storage facility for production data.

b. Backup copies of critical business-related operating system information and production software must be stored in an environmentally-protected and access-controlled site which is a sufficient distance away from the originating facility to escape a local disaster.

i. A schedule of periodic update and/or replacement of media stored off-site shall be established, documented and followed.

ii. Procedures for routine transportation, storage and retrieval of offsite-stored media will be established and documented.

iii. Procedures for identification and authorization of designated personnel to access and retrieve offsite-stored media will be established and documented.

c. Accountability for Data Backup: All additions, relocations and changes to Backup Data and/or media will be documented in a way that preserves an audit trail of the content, transportation and location of the media and of the persons performing and responsible for approving modifications and relocations.

d. The responsible business-unit management for end-user applications and data shall be informed of the standard backup procedures and schedules for their systems.

e. Wherever possible and to the extent possible, backup processes shall be automated.

f. Media shall be stored in a cool, dry (temperature- and humidity-controlled, if possible), fire-resistant, access-controlled location.

g. Access to data-media storage sites will require, AT LEAST presentation of a workforce member photo identification to the person responsible for the media's physical security. Requiring possession and use of a magnetic or mechanical key or sign-in and escort by a person responsible for the media's security is preferred. Procedures for control and verification of access to storage sites shall be established and documented.

h. Backup devices and media shall be maintained in good working order.

    i. Tape and disk drives shall be monitored for mechanical or data transcription failure and repaired/replaced at the first sign of problems.

    ii. Backup and recovery software will be tested for proper performance and replaced/updated as required whenever evidence of software failure or inadequacy is exhibited.

    iii. Media (tape, disk or other) shall be monitored for mechanical or data transcription failure and replaced at the first sign of problems.

i. Copies of all critical data shall be securely transported to and stored at a secure offsite facility on a regular basis.

    i. The designated off-site facility is 120 W. Main Street (Data Center), 137 N. Cottonwood and 35 N. Cottonwood.

j. Accountability for Data Backup (NOTE: The requirements below apply to Enterprise or campus Data Center backup facilities, NOT individual workstations.)

    i. Backup device information to be documented includes:

        - Device inventory
        - Routine maintenance that affects backup device or media availability or reliability.
        - Addition, modification, replacement or removal of equipment, parts or components.
        - Identification of persons performing and/or approving the device changes.

    ii. Backup software information to be documented includes:

        - Inventory - including software name, version and patch-level.
        - History of addition, modification replacement or removal of backup system software.
        - Identification of persons performing and/or approving the software changes.

    iii. Backup media information to be documented includes:

        - Media inventory - date of purchase, media type and manufacturer
        - Date put into service, assigned data label and storage location
        - Verification/restore test dates, results and number of uses when tested
        - Date taken out of service and final disposition
        - Identification of persons performing and/or approving each media change

    iv. Backup procedure information to be documented includes:

- The systems and data backed up
- Schedule of regular backup to include start and end times
- Storage location of data
- Difficulties encountered during the procedures
- Authorized individuals performing the backup

v. Offsite backup storage procedure information includes:

- The data identification
- The identity of the authorized individuals pulling/replacing the media from/to storage

k. Audits shall test whether backup procedures are being followed, that backup media is properly stored, that documentation requirements are being met and that data can in fact be restored from backup media.

2. Yolo County HHSA Management shall establish guidelines and procedures for periodic audits of the Backup systems and procedures.

a. Audits shall test whether backup procedures are being followed, that backup media is properly stored and that data can, in fact, be restored from backup media.

b. Audits may be performed of the physical safety and security of both primary (on-site) and off-site storage locations.

c. Audits will also be performed of the documentation, logging and tracking controls of data transported or stored off-site.

3. Yolo County HHSA Information Security Officer or delegates shall be responsible for:

a. Advocating and supporting HHSA IT security needs, concerns and projects to Senior management.

b. Directing the development and promulgation of training and orientation materials to enable and encourage employee awareness of the security problems and issues involved in creating, storing and managing backups.

c. Performing the routine backup

d. Performing periodic collection and transfer of duplicates of backup data storage media to offsite storage and replacing returning media into onsite storage.

e. Routine and emergency maintenance of backup devices.

f. Maintaining documentation of backup media and equipment inventory, maintenance, storage, relocation and disposition.

g. Maintaining backup media storage facilities

4. Program Managers or their delegates shall ensure that storage of PHI/PII on desktop workstations should be discouraged and only allowed when there are compelling reasons and no viable alternatives. If such data is present in workstations; backups of data shall be made frequently and stored securely in a lockable drawer, cabinet, closet or similar container.

    a. In cases where restricted data/PHI/PII has to be stored on a desktop device, workstation security procedures shall be strictly followed and enforced.

    b. If technology to do so is available, restricted and critical data on desktop and portable devices must be encrypted.

    c. In cases for restricted data/PHI/PII has to be stored on a workstation or portable device, it shall be removed and securely disposed of as soon as the need for it ends.

    d. Backup or any form of copying and/or removal of data from desktop workstations will be supervised by authorized individuals.

5. Avatar Database Backup

    Conducting and maintaining AVATAR backups is a critical element to the operation of the Health and Human Services Agency (HHSA) to ensure the availability and protection of data. Backing up files help protect against accidental loss of data caused by users, database corruption, hardware failures, and natural disasters.

    Restoration of Avatar access is addressed in both HHSA and General Services-Information Technology (GSD-IT) Disaster Recovery (DR) Plan.

    The data availability and backup protocol for AVATAR databases includes:

    a. A shadow server housed at the Bauer Building to keep a duplicate copy of the database. The primary database sends a copy of the data to the shadow server as changes occur. In the event the primary database server fails, users can be routed to the shadow server.
    b. Backup protocols are scheduled as follows:
        i. Full AVATAR database backups are scheduled to run nightly. The AVATAR system administrator will verify the backup runs daily and determine issue if the backup fails to run as scheduled
        ii. An incremental backup of the server is scheduled to occur every day
        iii. A full server backup is scheduled to occur every Friday. These backups are stored on tapes and maintained as follows:
            1. Weekly tape backups are kept for 90 days
            2. Quarterly tape backups are kept for 1 year
    c. Weekly tapes are rotated weekly between 3 locations in Woodland and stored in locked cabinets in secured facilities to help ensure availability of backed up data if a building becomes inaccessible.

d. In the event of a natural disaster or hardware failure that damages the AVATAR application server, it is estimated full operations could be restored in 48 hours or less depending on the timeliness of the following events:
    i. Rebuild server
    ii. Netsmart to restore application
    iii. Restore databases from backup

Approved by:

Karen Lar

Karen Larsen, Director
Yolo County Health and Human Services Agency

12/5/17
Date