NWF Health Network
Policy & Procedure

Series:	900: Data Collection, Records and Reporting
Policy Name:	Information Systems Data Back-Up and Restoration
Policy Number:	911
Origination Date:	03/09/2009 **Revised:** Board Meeting of 02/22/2024
Regulation:	CFOP 50-17

Policy

The Information Technology (IT) department is responsible for managing all data backup and recovery activities for NWFHN. Certain departments, such as Finance and Accounting and Human Resources, are also responsible for providing the IT department with their requirements for data backup, protection and recovery. The IT department is also responsible for executing technology disaster recovery (DR) plans to ensure that data are backed up and securely stored, with the ability to quickly access and restore the data as quickly and securely as possible. The IT department is responsible for developing, executing and periodically testing procedures for data backup and recovery. The IT department also acknowledges it will comply with appropriate industry standards for data backup in its activities.

1. The company shall develop comprehensive data backup plans in accordance with good data backup and recovery management practices as defined by the above standards.
2. Data backup and recovery activities shall be performed as part of NWFHN's business continuity management system (BCMS) and technology disaster recovery (DR) plans, which administer and manage the overall technology data backup program, which includes:
    - Planning and design of data backup and recovery activities
    - Identification of data backup teams, defining their roles and responsibilities and ensuring they are properly trained and prepared to respond to an incident
    - Planning, design and documentation of data backup and recovery plans
    - Scheduling of updates to data backup and recovery business impact analyses
    - Scheduling of updates to data backup and recovery risk assessments
    - Planning and delivery of awareness and training activities for employees and data backup team members
    - Planning and design of incident response activities associated with data backup and recovery
    - Planning and execution of data backup and recovery plan exercises
    - Designing and implementing a data backup and recovery program/plan maintenance activity to ensure that plans are up to date and ready for use
    - Preparing for management review and auditing of data backup and recovery plan(s)
    - Planning and implementation of continuous improvement activities for the data backup and recovery program and plan(s).

3. A formal risk assessment (RA) and business impact analysis (BIA) shall be undertaken to determine the requirements for all data backup and recovery plans; RAs and BIAs shall be updated at least annually to ensure they are in alignment with NWFHN business and its technology requirements.
4. Strategies for responding to specific technology incidents, as defined in the BIA and RA, shall be identified and used when developing individual data backup and recovery plans
5. Data backup and recovery plans shall address the backup and recovery of critical technology elements, including systems, networks, databases and data, in accordance with key business activities.
6. Data backup and recovery plans shall be periodically tested in a suitable environment to ensure that the systems, networks, databases and other infrastructure elements can be recovered and returned to a business as usual (BAU) status in emergency situations and that NWFHN management and employees understand how the plans are to be executed as well as their roles and responsibilities.
7. All employees must be made aware of the data backup and recovery program and plans and their own roles and responsibilities during an incident.
8. Data backup and recovery plans and other documents are to be kept up to date and will reflect existing and changing circumstances.

Procedure

A. Workstations and End Users.

   1. All data used in conjunction with performing the duties of a position is the property of NWFHN and will be treated as a company owned resource.
   2. All data will be stored in a location approved by the NWFHN Network Administrator (NA).
   3. Permanent storage of data in any other location or on removable media, including, but not restricted to, Floppy disks, CD, Flash cards or Jump drives (also known as Thumb drives) is strictly prohibited.
   4. Removable storage devices may be used for temporary storage if such use is strictly time-limited and required to perform assigned job duties with prior approval from IT and an encrypted device.
   5. End user data will be stored on one (1) or more network servers. Workstations will not be periodically backed up since no user created data will be stored locally.

B. Servers.

   1. All user data on each NWFHN server will be backed up on a nightly basis to a separate physical disk or other media.
   2. Incremental backups will be stored in an off-site location for an indefinite period.

C. Restoration.

   1. To request a restoration of backed-up data, the end user will send an email request to IT@nwfhealth.org describing the extent of the loss and providing any details necessary for a successful restoration.

D. Data Backup and Recovery Specifications

   Following are specific data backup and recovery technical requirements:

   1. General

      a. Daily backups (full and/or incremental) retained for a period of 90 days.

   b. Weekly full backups retained for a period of 3 years.
   c. NWFHN IT Manager/Network Administrator is notified if a recurring problem with backup exists
   d. Weekly full backups of all servers will be created locally and uploaded to an offsite cloud location for a retention period of 3 years.
2. Backup Verification
   a. Snapshot logs will be reviewed for errors daily.
   b. Corrective actions will be taken when errors are identified.
   c. Random test restorations will be performed periodically to verify backup integrity.
3. Data Access, Security, Recovery and Restoration Procedures
   a. Restoration requests of accidentally deleted or corrupted information must be made through NWFHN IT Helpdesk.
   b. To request a restoration of backed-up data, the end user will send an email request to IT@nwfhealth.org describing the extent of the loss and providing any details necessary for a successful restoration.
4. Data Integrity
   a. Server backups are secured using Advanced Encryption 235-bit AES SSL encryption while transferring between computer and online storage. Once data has been synchronized with offsite location, it is re-encrypted using 256-bit AES and unique rotating keys for the best possible protection while in storage. Device Security: All access to data on Datto File Protection servers is protected via a unique key and validation of the device by the Datto Partner. After the initial authentication process, the File Protection agent uses encrypted session keys to ensure secure transmission of data between the device and the File Protection service.
5. Data Retention
   NWFHN Endpoint Backup for Servers backs up servers every hour, helping NWFHN IT to deliver on stringent RPO requirements. Endpoint Backup for Servers automatically runs a backup every hour on a 24/7 schedule Weekly full backups of all servers will be created locally and uploaded to an offsite cloud location for a retention period of 3 years.