must meet appropriate security requirements as well as storage standards established by the manufacturer of the backup media.

Procedure:

1. The Security Officer will be responsible for implementing this policy and will ensure that further responsibility is properly assigned for the proper management of data.
2. The [Company name] Security Officer or designee is responsible for completing the backups and for ensuring effective training of the workforce members assigned to complete backups, for management of the backup media and for performing periodic testing of restored media.
3. The Security Officer or designee shall maintain a record of movements of hardware and electronic media and any person responsible therefore.
4. Data Backup
    a. A backup, recovery and testing strategy should be determined based upon the [Company name] Risk Analysis strategy.
    b. [Company name] shall create a retrievable, exact copy of sensitive and regulated data before movement of equipment.
        i. In the event a system does not allow for an electronic backup, [Company name] will develop an alternative method to create a copy of the sensitive and regulated data contained on that system, or complete an analysis delineating alternate solutions for compliance (such as a printed copy).
    c. In order to protect the confidentiality, integrity, and availability of sensitive and regulated data, [Company name] completes backups every (day, week, month, etc.).
    d. [Company name] will perform a daily (at a minimum) backup of all systems that create, receive, maintain, or transmit sensitive and regulated data. While a vendor may specify or recommend a full back up, an incremental back up, or may not specify, the Security Officer will determine the frequency with which backups are performed, dependent upon the criticality rating of the system or data assigned by the "Application and Data Criticality Analysis" procedure.
    e. Data backup systems may be manual or automated.
        i. Automated systems electronically capture backup locations, date/time, etc.
        ii. If the process is manual, documentation of the backup should include:
            1. Site/location name
            2. Name of the system
            3. Type of data
            4. Date & time of backup
            5. Where backup stored (or to whom it was provided)
            6. Signature of individual that completed the back up

f. The data backup plan requires that all media used for backing up sensitive and regulated data is stored in a physically secure environment, such as a secure, off-site storage facility.
    iii. If backup media remains on-site, it must be in a physically secure location, different from the location of the computer systems it backed up in order to protect the backups from loss or damage.
g. If an off-site storage facility or backup service is used, a Business Associate Agreement must be used to ensure that the Business Associate will safeguard the sensitive and regulated data in an appropriate manner.
h. Stored data must be accessible and retrievable at all times and all data backups should be tested and data restored to ensure accuracy.
i. When reusable media are used as the backup media refer to the "Device, Media, and Paper Record Sanitization for Disposal or Reuse" policy.
j. Data Backups should be tested and data restored, to assure accuracy. Documentation of backup testing, or restore logs, should be maintained and should capture the date and time the data was restored. Operational procedures for backup, recovery, and testing should be documented and periodically reviewed.
k. Proper management of situations concerning data back-up/data recovery, such as emergencies or other occurrences, should be addressed in the Disaster Recovery Plans.
l. All data backups should be encrypted using FIPS-validated encryption.

5. Destruction
    a. [Company name] will determine a record retention policy and data backup retention schedule. This schedule should include a timeline for ultimate destruction (tapes maintained and destroyed) of storage media.
6. Media Movement
    a. It is not possible or economically practical to control all media that enter and leave an organization. [Company name] makes all reasonable and prudent efforts to control media entering and leaving the organization. Workforce members are trained to handle media with sensitive and regulated data in a manner which protects the confidentiality of the data contained on it. Media that contains sensitive or regulated data that is no longer useful or useable should be sanitized consistent with the "Device, Media, and Paper Record Sanitization for Disposal or Reuse" policy.
7. Documentation
    b. All documentation required by this policy will be maintained for a period of six years from the date of creation or the date when it was last in effect, whichever is later.

Violations:

1. Failure to back up a system in the absence of a system failure is a violation of this policy and may result in corrective disciplinary action, up to and including termination of employment.
2. Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment.
3. Violation of this policy and procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges.
4. Violation may also result in civil and criminal penalties to [Company name] as determined by federal and state laws and regulations related to loss of data.
5. Violation may also result in liability to [Company name] related to loss of data.

Attachments: None

Related Policies: None