DATA BACKUP AND RECOVERY

POLICY

This policy is designed to ensure organizational data is stored in an on- and off-site location and can be easily found and recovered in the event of an equipment failure, intentional destruction of data, or disaster. This policy covers the infrastructure and procedures that are provided for organizational data backup and recovery. It is the responsibility of the Sherman Information Technology department to determine the backup schedule, recovery point objective, and retention per application. It is the responsibility of the Sherman Information Technology department to manage the data retention for their application(s). This policy does not cover data retention for compliance or legal purposes.

Definitions
For purposes of this policy and associated rules, the following words and phrases shall be defined as follows:

Backup – The saving of files onto disk, or other mass storage media for the purpose of preventing unplanned data loss in the event of equipment failure or destruction.

Application Owner – The user, department, or team that maintains or manages the application or data that is being backed up.

Data Retention – The saving of historic and/or inactive files on disk, or other mass storage media for the purpose of keeping it for compliance or legal reasons, for a defined period of time. *Data retention* is also subject to the litigation hold process as directed by legal and regulatory requirements.

Backup Retention – The time lapse between when a backup is created and when it is formatted to be destroyed or potentially reused. This can be considered the 'shelf-life' for the backup and is how long the backup will be kept before the images are expired. Backups will be saved onto disk, or in the cloud.

Data Recovery – The purpose of backing up data is to store a copy of the data in the event of a disaster where data is lost or corrupt. Data recovery is the act of restoring data from the backup in order to restore data to the desired point in time.

Recovery Point Objective (RPO) – is the maximum targeted period in which data might be lost from an IT service. The RPO is the age of files that must be recovered from backup storage for normal operations to resume. The RPO is expressed backward in time (that is, into the past) from the instant at which the failure occurs (e.g. a high transactional DB data is only good for 5 days. The RPO is 5 days ago or sooner).

Backup Software – The software used to manage the data backups and recovery (e.g. Veeam, Updraft).

DATA BACKUP AND RECOVERY

Rules, Procedures and Guidelines

A. The Sherman Information Technology department will be responsible for all aspects of backing up servers supported by Sherman Information Technology department. Test servers and Generic Operating Systems will not be backed up, unless requested by the server owner. Such backups include daily incremental, weekly, and full monthly backups as defined by service or application owner. This team will also be responsible for finding and restoring data when requested or required for Disaster Recovery purposes.

B. Procedures regarding offsite (cloud) backups
    1. Sherman Information Technology department is responsible for maintenance and support
    2. The following are backup schedule and *Backup retention* frequency:
        a. Daily backups
            i. Incremental and full backups will be kept on-site for 1 month
            ii. Full backups will be stored on- and off-site for 3 months
        b. Weekly Production Backups
            i. Full and incremental weekly backups will be stored on-site for 1 month
            ii. Full backups will be stored on- and off-site for 3 months
            iii. Occur as scheduled; 4 iterations per month
            iv. Duplicate copy of weekly backup will be stored securely off-site and retained for 3 months
        c. Monthly Production Backups
            i. Full and incremental backups will be stored on-site for 3 months
            ii. Full backups will be stored on- and off-site for 6 months
            iii. Monthly Vault Full backups to tape will be stored off-site for 3 months and on-site for the remainder of the year
        d. Non-production
            i. Non-production environments will be retained for 1 week
            ii. Will not be sent off-site
        e. Special Backup Requests (i.e. litigation, system upgrades, retirements etc.)
            i. Full backups may be sent off-site upon request
            ii. Copies may be set up for up to 6 months' retention or as required by law
            iii. Backup retention can be used as data retention
            iv. Backup retention special requests will require an IT manager approval

C. The following outlines Backup Software support – including policy configuration, restores, backups:

DATA BACKUP AND RECOVERY

1. It is the responsibility of the Sherman Information Technology department to make sure backups are running as scheduled
2. The Sherman Information Technology department will verify that backup jobs have completed successfully, and will contact employees if problems occur
3. Employees will open a service ticket with the Sherman Information Technology department when server problems occur and information technology team support is required
4. When a new server is added to the production environment, the administrator of the server will add the server to the backup system
5. The employee and Sherman Information Technology department will work together to find resolutions when problems occur
    a. It is the responsibility of the Sherman Information Technology department to install updates/upgrades of the backup software
    b. The Sherman Information Technology department will report any problems with the backup software to the customers. They will include:
        i. Troubleshooting steps taken; and
        ii. Any errors found
        iii. The Sherman Information Technology department is responsible to contact the vendor when necessary for troubleshooting. Troubleshooting these problems requires in-depth knowledge of operating systems and may require system reboot.
6. Regarding Data Restores:
    a. Restore requests will be submitted to the Sherman Information Technology department via Work Request
    b. Restores that require accessing off-site storage will be started within 72 hours
    c. All other restores will be started within 2 hours business hours
    d. Restores over weekends/holidays will be performed the following business day, unless an urgent/high ticket is submitted
7. The Sherman Information Technology department will be responsible for the following:
    a. Ordering backup media
    b. Checking backup reports to ensure that they were completed without errors
    c. Making sure offsite storage has the needed space available
    d. Updating clients/servers to current version after upgrades when feasible with assistance from the customer if necessary
    e. Managing relationships with storage vendors
    f. Maintaining storage arrays
    g. Executing this policy

8. The Sherman Information Technology department will **NOT** be responsible for the following:
    a. Troubleshooting and investigating what caused data loss or data corruption on client servers
    b. Lost production data as a result of end-user changes to an application or application data
    c. Lost data that falls outside of the backup windows outlined in this policy
    d. Rebooting or restarting clients/servers
    e. Making sure clients/servers have been entered into DNS properly
    f. Scheduling and testing of backups to ensure viability

Exceptions
There shall be no backups performed of the data stored on user devices, such as desktops, workstations, and/or laptops. Any exceptions to the data backup policy will require the explicit written approval of the director of information technology.

Restoration
Users who need files restored must submit a request to Sherman Information Technology department via a Work Request. They will need to include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

Exclusions or Special Circumstances
Exceptions to this Policy shall only be allowed if previously approved by the director of information technology and this approval is documented and verified.

Consequences
Use of College electronic information resources contrary to this policy or applicable federal, state or local law is prohibited and may subject the user to disciplinary action including, but not limited to, suspension of the user's access to the electronic information resources. Users also should be aware of other possible consequences under college policies and federal, state, or local laws, particularly those related to computer crime and copyright violation.