Data Backup and Recovery Policy

I. Purpose and Scope

A. The purpose of this policy is to document the ITD-NBU data backup and recovery procedures, protocols, and standards. This policy covers the data backup schedule, backup protocols, *backup retention*, and data recovery. This policy does NOT cover *data retention* or compliance requirements.

B. This policy assumes Application Owners will notify the ITD - Hardware Platform Services Team, with the applications designated: recovery point objective (RPO), timing for when the backups should take place, and compliance requirements as they pertain to data backup and recovery.

C. The ITD team will only be responsible to manage the infrastructure, backup, and recovery of application data.

II. Definitions

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

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

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

3. *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. Data Retention is determined and managed by Application Owners (or Data Stewards) in conjunction with legal and regulatory requirements. *Data retention* is also subject to the litigation hold process as directed by Office of General Counsel.

4. *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 magnetic tape, disk, or in the cloud.

5. *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.

6. *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).

7. *Backup Software* – The software used to manage the data backups and recovery (e.g. Commvault, NetBackup Enterprise Server).

8. *ITD-NBU*– An internal team that handles the management of this policy, data backup, and recovery.

III. ITD Policy

A. 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.

B. This policy covers the infrastructure and procedures that are provided for organizational data backup and recovery. It is the responsibility of the Application Owners to determine the backup schedule, recovery point objective, and retention per application. Although they may seek guidance from the ITD-NBU team, it is the responsibility of the Application Owners to manage the data retention for their application(s). This policy does not cover data retention for compliance or legal purposes.

IV. Rules, Procedures, and Guidelines

Production Data Center (Downtown Data Center [DDC])

The following information outlines the policies with respect to data backup and restore.

A. ITD-NBU team will be responsible for all aspects of backing up servers supported by ITD-NBU. 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 Target Media (e.g. Tape, Disk, and Cloud)

1. ITD-NBU team 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
        iii. Tapes may be reused as they expire, if they are still viable
    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. Tapes may be reused as they expire, if they are still viable
        v. 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
        iv. Tapes may be reused as they expire if they are still viable
    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

iii. Backup retention can be used as data retention

iv. Backup retention special requests will require a written Service Level Agreement (SLA), presented to the university's Information Security Office (ISO) OR QUALITY SECTION.

v. A special request will need to be submitted through a ServiceNow IT General Request

vi. Operational-level agreement will be added to backup policy document

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

1. It is the responsibility of the ITD-NBU Team to make sure backups are running as scheduled
2. The ITD-NBU Team will verify that backup jobs have completed successfully and will contact USERS if problems occur.
3. USERS will open a service ticket with the ITD-NBU Team when server problems occur, and ITD-NBU team support is required
4. When a new server is added to the production environment, the administrator of the server will contact the ITD-NBU Team to have the server added to the backup system via ServiceNow Work Request
5. The customer and ITD-NBU Team will work together to find resolutions when problems occur

    a. It is the responsibility of the ITD-NBU team to install updates/upgrades of the backup software

    b. The ITD-NBU Team will report any problems with the backup software to the USERS. They will include:

        i. Troubleshooting steps taken; and

        ii. Any errors found

    c. The Hardware Platform Services Team 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 ITD-NBU Team via a ServiceNow Work Request
    b. Restores that require a tape from 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 ITD-NBU Team will be responsible for the following:
    a. Ordering backup media, cleaning tapes, and labels
    b. Checking backup reports to ensure that they were completed without errors
    c. Making sure the library has tape media available for backups and offsite storage
    d. Packing monthly tapes and sending them to the vault
    e. Updating clients/servers to current version after upgrades when feasible with assistance from the customer if necessary
    f. Managing relationships with storage vendors
    g. Maintaining storage arrays
    h. Executing this policy
8. The ITD-NBU Team 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 DNS properly
    f. Scheduling and testing of backups to ensure viability

Disaster Recovery Alternate Site

A. The policy for the disaster recovery alternative site will be the same as the production data center with the following exceptions:

Exceptions

A. 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 ITD-NBU.

Restoration

A. Users who need files restored must submit a 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.

Encryption

A. Backups shall be performed with at least 128-bit. Encryption keys are replicated from the Downtown Data Center to alternate site.