Policy Title:		Backup and Restoration Policy	
	INFORMATION TECHNOLOGY SERVICES (ITS)	**Category**	Information Technology Services
		Administrative Policy #	
		Revision #	
		Review Frequency	As Needed – no less frequently than triennially
Administrative Division	Information Technology Services (ITS)	**Reviewed By**	Chief Information Officer
BOWC Approval		**Last Reviewed/Update Date**	
Implementation Date			

1. **OBJECTIVES**

    1.1. 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.

    1.2. 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 ITS team, it is the responsibility of the Application Owners to manage the data retention for their application(s).

2. **PURPOSE**

    2.1. The purpose of this policy is to document the ITS data backup and recovery procedures, protocols, and standards. This policy covers the data backup schedule, backup protocols, backup retention, and data recovery.

3. **DEFINITIONS**

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

    "Backup" means 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.

    "Backup Retention" means 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.

    "Backup Software" means the software used to manage the data backups and recovery.

    "Data Recovery" means 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.

    "Data Retention" means 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. ITS is not responsible for and does not manage Data Retention. Data Retention is determined and managed by Application Owners in conjunction with legal and regulatory requirements. Data retention is also subject to the litigation hold process as directed by Office of General Counsel.

"Recovery Point Objective (RPO)" means 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).

4. SCOPE

4.1. This policy is directed to the ITS staff who are accountable to ensure the plan is developed, tested and kept up-to-date. This policy assumes Application Owners will notify the ITS Team with the applications' recovery point objective (RPO), timing for when the backups should take place, and compliance requirements as they pertain to data backup and recovery.

4.2. This policy does not cover data retention for compliance or legal purposes.

5. RESPONSIBILITIES

5.1. **Chief Information Officer (CIO)**

5.1.1. The Chief Information Officer (CIO) is responsible for publishing this policy; communicating this policy to all employees; for review, approval and publishing of divisional standards; and updating this policy as necessary.

5.1.2. The CIO, or delegate, is responsible for interpreting and enforcing this policy.

5.2. **Application Owners**

5.2.1. Application owners are responsible for working with ITS to establish a backup and recovery strategy.

5.2.2. The application owner must provide ITS with information required to determine the appropriate recovery point objective (RPO), or acceptable data loss, which will dictate the backup type and frequency implemented by ITS.

5.2.3. The application owner must inform ITS of any compliance requirements for that data, as they pertain to backup and recovery.

5.3. **Management**

5.3.1. Management is responsible for monitoring work areas for compliance and addressing any incident(s) of noncompliance and alerting Human Resources when a violation has occurred.

6. POLICY

6.1. The ITS team will be responsible for all aspects of backing up servers supported by ITS. 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.

6.2. Procedures regarding Target Media (e.g. Tape, Disk, and Cloud).

    6.2.1. ITS team is responsible for performing backups and recoveries of systems they directly support.

    6.2.2. The following is a minimum backup schedule and retention frequency:

        6.2.2.1. Full backups will occur monthly.

        6.2.2.2. Incremental backups will occur daily.

        6.2.2.3. Minimum retention frequency is 4 weeks.

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

    6.3.1. The ITS Team will:

        6.3.1.1. Verify backups are running as scheduled. The ITS Team will review reports to ensure that backups were completed without errors.

        6.3.1.2. Verify that backup jobs have completed successfully, and will investigate if problems occur.

        6.3.1.3. Test system recovery processes at least once annually.

        6.3.1.4. Test each server's recovery at least once annually.

    6.3.2. Regarding data restores:

        6.3.2.1. Restore requests will be submitted to the ITS via a Service Desk Request.

        6.3.2.2. Restores will be started within 24 business hours.

        6.3.2.3. Restores over weekends/holidays will be performed the following business day, unless an urgent/high priority ticket is submitted.