


Category	IT Infrastructure and Services	Policy Number	SUP-ITS-303	 جامعة زايد ZAYED UNIVERSITY
Classification	Public	Version	1.0	
Responsible Office	CAFO	Policy Owner	ITD Director	
Date Approved	28 January 2025	Effective Date	17 February 2025	
Date Last Reviewed	New Policy	Due Date for Next Review	28 January 2028	

POLICY

Data Backup and Recovery

1. Purpose

The purpose of this Data Backup and Recovery policy is to ensure that Zayed University conforms to a standard backup and recovery control process in line with international best practices.

2. Scope of Application

2.1 This policy applies to all Zayed University faculty, staff, and students. It also includes service providers and consultants, that house their hardware in the University Enterprise Datacenter.

2.2 This policy does not apply to applications or services hosted outside of the University Enterprise Datacenter, including in any cloud service.

3. Definitions

Backup	The saving of files onto magnetic tape, disk, or other mass storage media to prevent unplanned data loss in the event of equipment failure or destruction.
Backup Administrator	A backup administrator is an ITD staff member responsible for managing and maintaining an organization's backup and recovery infrastructure. This includes implementing backup policies and procedures, monitoring backup operations, performing data backups, and verifying that backups are properly stored and secured. The backup administrator may also be responsible for restoring data from backups in the event of data loss or system failure.
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 or disk.

Business Impact Analysis (“BIA”)	Predicts the consequences of a disruption to University operations, and gathers information needed to develop recovery strategies.
Business Service Owner	The user, department or team that is accountable for a specific service (Infrastructure, Application or Professional Service) within the University.
CAFO	University Chief Administration and Finance Officer
Data Recovery	The act of restoring data from the backup to the desired point in time.
IT Application Owner	The user, department, or team that maintains or manages the application or data that is being backed up.
ITD	University Information Technology Department
Recovery Point Objective (“RPO”)	The age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure.
TDRA	Telecommunications and Digital Government Regulatory Authority
University	Zayed University

4. Policy

Zayed University (“**University**”) maintains an extensive network infrastructure to support a wide variety of computing needs. The unprecedented growth in data volumes has necessitated an efficient approach to data backup and recovery. The aim of this policy is to ensure that the University conforms to a standard backup and recovery control process in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, and service efficiency. In addition, it seeks to define controls to enforce regular backups and support activities so that any risks associated to the management of data backups and recovery are mitigated.

5. Guiding Principles

5.1 Data Backup Standards

- 5.1.1 Data that is critical to the University must be defined by the Business Service Owner/IT Application Owner and must be backed up in the University’s onsite backup system.
- 5.1.2 Backup media will be stored in a secure, offsite location. Proper environmental controls, temperature, humidity and fire protection, shall be maintained at the storage location.
- 5.1.3 All backup jobs must be automatically verified by the backup software and reviewed on a weekly basis.
- 5.1.4 Restore capability must be verified by the Business Service Owner/IT Application Owner.
- 5.1.5 All the backup job status notifications must be emailed to the Backup Administrators or the Business Service Owner/IT Application Owner by the backup system, which are verified and filed.
- 5.1.6 All backup media that is not re-usable will be thoroughly destroyed in an approved manner that ensures that the data is not recoverable.

5.2 Backup Data Retention

- 5.2.1** Full backups must be performed weekly, monthly, and yearly with fixed backup retention periods.
- 5.2.2** Differential or incremental backups must be performed daily with a fixed backup retention period.
- 5.2.3** Daily, weekly, monthly, and yearly backup media must be reused once the backup retention period ends.
- 5.2.4** Backups will be kept on Tape media for the following durations.
 - Daily backups will be kept for 6 Months.
 - Weekly backups will be kept for 6 Months.
 - Monthly backups will be kept for 12 months.
 - Yearly backups will be kept for 5 Years.

5.3 Data Backup Selection

- 5.3.1** All data and software essential to the continued operation of the University, as well as all data that must be maintained for legislative purposes, must be backed up by system administrator.
- 5.3.2** All supporting material required to process the information must be backed up as well. This includes programs, control files, install files, and operating system software.
- 5.3.3** The Business Service Owner/IT Application Owner/Backup Administrators will determine what information must be backed up, and in what form.

5.4 Data Storage

- 5.4.1** Data backups must be stored in two (2) locations.
- 5.4.2** Minimum requirements are to store the monthly and yearly backup sets offsite.
- 5.4.3** Onsite data storage is storage with current data in machine-readable format to be used if operating data is lost, damaged or corrupted.
- 5.4.4** The offsite data storage provides additional protection against loss to the primary site and onsite data.
- 5.4.5** If high availability is required, additional backup copies may be securely stored in the proximity of the ITD system either within the datacenter or a secure vault.
- 5.4.6** The location used for storing data media offsite must be physically secure and safe.
- 5.4.7** If an offsite media set is required to perform a data restoration (restore), the data media must be returned to the offsite facility for the remainder of the applicable retention period.

5.5 Recovery Point Objective

- 5.5.1** The Recovery Point Objective (“**RPO**”) is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure.
- 5.5.2** RPO is expressed backward in time -- that is, into the past -- from the instant at which the failure occurs and can be specified in seconds, minutes, hours, or days.

5.5.3 The Business Service Owner must define and determine the criticality of business activities by using the Business Impact Analysis (“BIA”) tool.

5.6 Backup Schedule

5.6.1 Backup schedules must not interfere with the day-to-day operations of the university. This includes any end-of-day operations on the systems.

5.6.2 A longer backup window might be required, depending on the type of backup.

5.6.3 When the data in a system change frequently, backups need to be taken more frequently to ensure that data can be recovered in the event of a system failure.

5.6.4 Immediate full data backups are recommended when data is changed to a large extent, or the entire database needs to be made available at certain times. Regular, as well as event-dependent intervals need to be defined.

5.6.5 The Systems Development Manager determines the quantity of previous versions of operating systems and applications that must be retained at the Backup and Disaster Recovery location.

5.6.6 Annual, monthly, and weekly backups must be retained at the Backup and Disaster Recovery location. Weekly, monthly and annual backup media may be re-used to take new backups.

5.7 Backup Restoration

5.7.1 The Business Service Owner/IT Application Owner must prepare the server and application recovery documentation. Backup Administrators will prepare the data restore documentation.

5.7.2 All data restore requests must be formally submitted with complete details to the Backup Administrators through the ITD Service Desk.

5.7.3 The Business Service Owner/IT Application Owner must not attempt to initiate a restoration process from the client end without prior approval from the Backup Administrator.

5.7.4 Emergency restoration of any data must be formally approved by the ITD Director.

6. Related Policies and Laws

- SUP-ITS-10 Information Security
- Telecommunications and Digital Government Regulatory Authority (“TDRA”) Regulations for Information Technology Security in Federal Entities

7. Administration

This policy is administered by the ITD.

8. Revision History

Date	Revision	Ver.
17 February 2025	Chair of the Board’s Decision issued (PD#3 of 2025).	1.0
28 January 2025	Approved by the FAIAC.	
22 June 2023	Endorsed by the Executive Council	

6 July 2022	Endorsed by the CAFO Management Council.	
8 March 2022	Reviewed by IT consultant.	
28 April 2021	New policy reviewed by CAFO Management Council and endorsed for further approval.	