Alfaisal University

Policy Name:	Backup Management Policy

Version	**02**
Date Approved	
Effective Date	
Policy Owner	IT Services

Summary:

This policy defines the backup policy for servers within the University which are expected to have their data backed up. These mission critical applications are typically installed on servers but are not necessarily limited to servers. Servers are expected to be backed (e.g. File Server, Mail server, Application Servers and the Web Server).

Signature: ……..

Table of Contents

1. Introduction

This policy defines the backup policy for servers within the University which are expected to have their data backed up. The mission critical applications are typically installed on servers but are not necessarily limited to servers. Servers are expected to be backed (e.g. File Server, Mail server, Application Servers and the Web Server).

2. Purpose

This policy is designed to protect the business critical applications/data at Alfaisal University to ensure that it is not lost and could be recovered in the event of an equipment failure, intentional destruction of data or disaster.

3. Policy Scope

This policy applies to all the data and computer equipment owned, supplied or maintained by the University including servers, desktop computers, laptops and portable computers

4. Backup Management Policy

4.1. Policy Statements

4.1.1. The purpose of the systems backup is to provide a means to restore the integrity of the Computer Systems in the event of a hardware/software failure or physical disaster and provide a measure of protection against human error or the accidental deletion of important files. The systems backup will consist of regular, full and incremental backups.

4.1.2. This policy provides guidelines for establishing backup procedures. Exceptions to the standard procedure are permitted when justified. All exceptions must be fully documented. The standard procedure for systems backup is as follows:

a. Incremental backups will be performed daily (on all week days from Sun through Thu). Incremental backups will be retained for a week, at which time the media will be recycled.
b. A full systems backup will be performed weekly during Weekends. Weekly backups will be saved for a full month.
c. The last weekly backup of the month will be saved as a monthly backup on the first day of the month. The other weekly backup media will be recycled.
d. Monthly backups will be saved for one year, at which time the media will be recycled.
e. All off-site copies will be stored in a secure fireproof safe at a remote location.
f. All backup media that is not re-usable shall be thoroughly destroyed in an approved manner. Backup media that is used for other purposes shall be thoroughly erased.

4.2. Timing

Backups (Daily, Weekly & Monthly) are performed after the working hours on all days. Off-site copies are performed during the weekends.

4.3. Delegate & Custodian

The IT Director shall delegate a member of the IT department to perform regular backups and to be the custodian of all the records under his custody. The delegated person shall develop a procedure for testing backups along with the business owners of the applications and test the ability to restore data from backups on a periodic basis. Each data backup process should have at least one primary person-in-charge and a substitute.

4.4. Restoration of Data (Testing)

The restoration of data using data backups must be tested at irregular intervals, at least after every modification to the data backup procedure. It must be done at least once to ensure that complete data restoration is possible.

4.5. Documentation

Documentation is necessary for orderly and efficient data backup and restoration. The person-in-charge of data backup should fully document the following items for each generated data backup:

a. Business unit owners request for the required backup with details.
b. Date of data backup
c. Type of data backup (incremental, full)
d. Number of generations
e. Responsibility for data backup
f. Extent of data backup (files/directories)
g. Data media on which the operational data are stored
h. Data media on which the backup data are stored
i. Data backup hardware and software (with version number)
j. Data backup parameters (type of data backup etc.)
k. Storage location of backup copies

4.6. Offsite Location

The designated offsite location is KFF Head Office.

5. Business Owner Responsibilities

It is recommended that the designated administrators of each application perform a secondary backup for their data. Periodic restoration should be performed on the backed up data by running a test case to make sure data can be recovered since users may be relying on a file that has been corrupted in the back-up process.

6. Exemptions

Exception to or exemptions from any provision of this policy must be approved by the VPFA. Similarly, any questions about the contents of this policy, or the applicability of this policy to a particular situation should be referred to the IT Director.

7. Enforcement

Non-compliance with this policy could severely impact the operation of the institution by exposing the University to permanent loss of University data leading to loss of financial records, students' records, other records, research material. It may also expose the individual or the University to legal action.

8. Definitions

Backup	The saving of files onto offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
Restore	The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.
Full Backup	A Full Backup creates a copy of every file on a storage device. This is absolutely the most complete, comprehensive, and fool-proof type of backup. It is also the costliest in terms of effort, time and money output.
Incremental Backup	An Incremental Backup creates a copy of files that have changed (modified, added to, or created) since the last backup was performed. This method can be used in conjunction with full and partial backups to maximize protection and minimize cost.