Document title: **AUC Backup Policy – October 2019**

Approval date: **October 2019**

Purpose of document: **This document is to illustrate the backup policy used at AUC for different systems upon agreement. It also includes details about how the backup is being taken, its schedule and the media used for that purpose. This policy is not fixed as it should be updated as backup internal procedures/ operations developed or changed**

Office/department responsible: **Office of Information Technology – University Technology Infrastructure**
Approved by: **Chief Technology Officer: Ms. Marwa Mansour**

Document classification level: **RESTRICTED to AUC community**

AUC backup policy

Policy Statement

To ensure users are aware of the backup policy used to govern the backup procedures and process for different applications on different systems.

Reason for Policy/Purpose

The purpose of this policy is to illustrate a string backup plan to cover different systems using standard procedures, which could be easily developed and enhanced.

Who Approved This Policy

Chief Technology Officer: Ms. Marwa Mansour
Date: 1st of October, 2019

Who Needs to Know This Policy

All systems and applications administrators in addition to the delegated admins, whose systems or application are being backed up.

Web Address for this Policy

https://documents.aucegypt.edu/Docs/Policies/AUC%20Backup%20Policy%20and%20Procedures.pdf

Contacts

Responsible University Official: Mr. Ibrahim Galal, Associate Director, Systems & SAN

Responsible University Office: University Technology Infrastructure (UTI)

If you have any questions on the policy or procedure for this policy, you may:

1. Call Ibrahim Galal Gaber at 26154830, or

2. Send an e-mail to Ibrahim.Galal@aucegypt.edu

Policy/Procedures

1. Introduction

AUC has many critical applications that should be backed up on different layers so that it can be used in all cases of restore.

2. Overview

Systems & SAN is responsible for ensuring that mission critical applications and data are well preserved and protected against loss and destruction. Adequate backups allow data recovery when information technology systems or information has been destroyed by system malfunction or by accidental/intentional action.

3. Scope

This policy applies to all systems residing at AUC and managed by Office of Information Technology.

4. Backup types and media

4.1. Disk Library Backup

- This type of backups can be taken through Network or Fiber connection.
- Full or Incremental backups can be taken and it is considered the first layer of backup.

4.2. Recover Point

The recover point is an appliance used to enable back-in-time replication between two sites, thus an online copy of SAN LUNs connected to critical applications' servers could be done to secure such data. This is implemented between AUC and Vodafone. This kind of backup is used for disaster recovery plan.

4.3. Tape Library

The Tape Library will enable us to take backups offsite campus; which is requested by audit in some sensitive application. In addition, this media and type of backup provides longer period of retention.

5. Backup Policy

5.1. General

- At least once a week all AUC critical systems and production data are fully backed up.
- Other less critical systems/applications are fully backed up once monthly.
- Backup of systems and data should take place at night away of the working hours.
- Appropriate backup methods (i.e., full, incremental, or differential) should be employed daily in accordance with the allotted backup window.
- Backup media must adhere to industry accepted backup technology standards, such as:
  - The media's read/write capacity shall be rapid enough to permit the backup to be completed during the allotted time (i.e., before the start of the next business day
  - The media's compressed capacity shall be large enough to hold the complete backup
  - The media should be readable after a minimum of 5 years in unattended storage.
  - Data compression algorithms may be used to minimize the volume of data on the backup medium. When compression is employed, the selected parameters and algorithms must be documented and observed during data restoration (decompression).

5.2. Backup Administrator Responsibilities

Backup administrator is responsible for the following

- Maintain backup media: check the storage for the backup whether it is disks or tapes.
- Storing the backup tapes
- Checking if the backup has been successfully taken.
- Troubleshooting and managing backup failure.
- Maintaining the backup log.

5.3. Verification of Backup Status

The designated member of staff must check the backup status on the system first thing every morning and report any failures to the direct supervisor.

The backup software has automatic verification, which checks data transfer, reports error if occur, immediately corrects those errors and verifies backup data store.

5.4. Backup Log

A Backup log could be automatically issued at any time by the backup software for reporting purposes, including status, which tapes are used and housekeeping of the backup system. Daily backup job sends mail notification in case of errors.

5.5. House-keeping of the Backup System

Regular maintenance of the backup device is carried out to ensure it is kept in good working order. Cleaning tapes are used in accordance with manufacturer's instructions. LTO tape drives should be cleaned monthly or more often if the cleaning light is illuminated.

5.6. Managing Backup Failure

In the event of an unsuccessful backup, an email should be sent by the backup application to the backup administrator. The staff responsible for checking the backup must immediately do the following:

1. Note any messages / information on the server monitor
2. Report the failure to the practice manager
3. Record the failure in the backup log and any actions taken as a result
4. If the backup fails repeatedly, it may be necessary to perform a manual backup. This takes time, and must be performed when all users are logged out.

5.7. Storage of Backup Tapes

- The backup tapes when removed from the tape library are stored securely in a locked fire-proof media case then is taken off-site by a specialized company; it is for now "EDS".
- At the same time, the tape deposited two weeks previously will be collected and returned to the tape library for reuse during the following week

5.8. Management of Tapes

Tapes are clearly labeled with a date plus name of client and used in strict rotation to ensure immediate identification of any problems with a specific tape.

6. Backup Strategy

6.1. Backup Information

The below form should be filled for every system/application to be backed up

Application	
Server Host Name	
Server IP Address	
Application Owner Name	
Application Owner Email	

6.2. Backup schedule

The following schedule lists each of the detailed backup procedures included in this backup and recovery plan. It also indicates the frequency and schedule for each backup and shows who is responsible for each backup.
Every System/application backup requirements information should be filled individually in the following table. Thus, the appropriate backup schedule and frequency will be followed and this differs from application to another.

Name/Id	Name or identifier associated with the backup procedure
File System Type	Name(s) of the file system(s) included in this backup
Operating System	Defines the operating system that holds the data
Level	Such as "Full" or "Incremental"
Frequency	Such as "Daily" or "Weekly" or "When modified"
Schedule	Such as "Last Friday of the month" or "Monday" or "As required"
Responsible	Organization or individual responsible for the Data that is backed up

6.3. Backup Procedures

The following report should include all backed up systems/applications in order to be able to track backup procedure executions.

Name/ID	Name or identifier associated with this backup procedure
Description /Purpose	Description or purpose of this backup, such as "Daily incremental backup of modified partitions"
File System(s) Flat Files Database	Name(s) of the file system(s) included in this backup
Level	Full Incremental Other (explain):
Frequency (Cycle)	Daily Weekdays Weekly Monthly Quarterly Annually When files are modified Other (explain):
Retention	_____ backup cycles (enter the number of cycles to retain) Forever Other (explain):
Storage Location/ID	Onsite Offsite Notes (describe storage identifier, storage location, storage vendor):
Backup Medium	Disk Library Other (describe):
Procedures	Detailed steps for executing the backup procedure, including login, file locations, executables to run, parameters to use, expected messages or results, verification of backup results

6.4. Backup Testing (drill)

After taking backup, we should arrange for backup drill that will indicate the backup success and estimate time taken for the recovery. Random restore for each backup type should be conducted every month or at least quarterly.
Drills must run using below process steps.

- Send mail to application owner.
- Restore date must be clear and known by application owner.
- Backup engineer restores the VM or database as per owner request.
- Application owner confirms restore status by mail.

7. Recovery or Restoration Strategy

Systems or data can be destroyed or corrupted in some cases due to errors, outages, or intentional disruptions. Sometimes only a specific file or file system must be recovered or restored from backups after an outage occur. Major outages or disruptions may require restoration of most or all of the files from backups. The following sections of this document describe procedures for both minor and major restorations of files from backups.

7.1. Recovery or Restoration of a particular file or file system

In most cases, if a particular file or file system is corrupted or destroyed, only that file or file system needs to be restored from the Recover Point or Disk Library backups.

7.2. Recovery or Restoration after a Major Outage

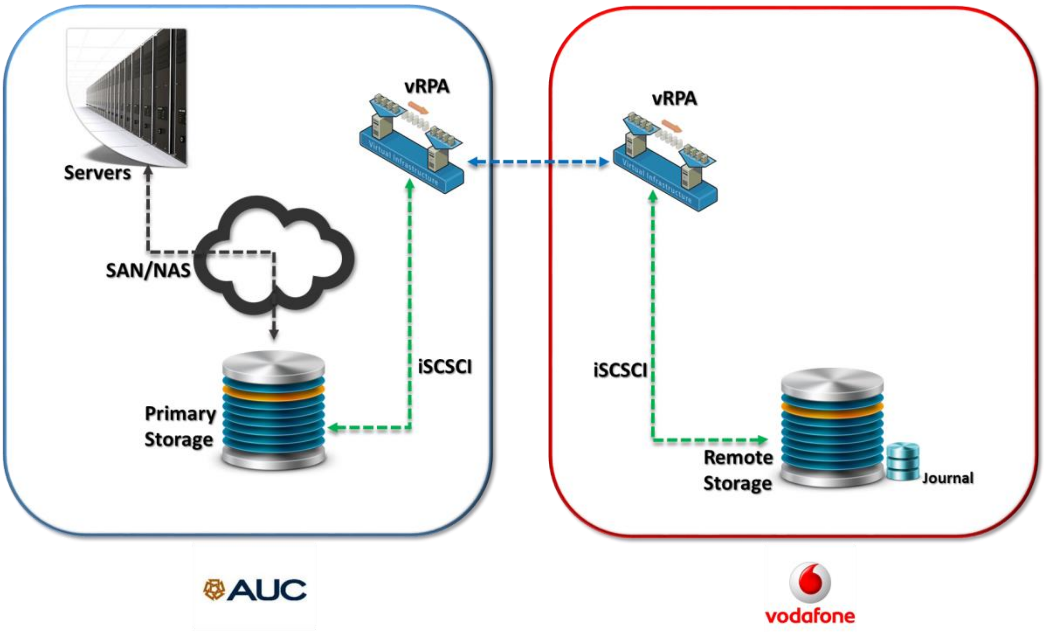
If a major outage, such an outage caused by a natural or manmade disaster occur, you may need to restore many or all of the files and file systems. Such major restorations requires proper timing and sequencing due to business priorities and file dependencies. This part is covered on the Disaster Recovery Plan for each application whether by using the Recover Point to switch to DR site or getting tapes from the offsite company to restore data from it.

7.3. AUC data storage disaster recovery site & data replication (AUC DR @ Vodafone).

For partial data disaster (data loss/corruption) on main site in any of the critical systems like:

- SAP (AUC Main ERP system running on MSSQL Database).
- Blackboard (AUC Learning Management System)
- Virtual systems “the critical VMS all over campus departments”

In such a case, any of these systems data could be restored back to a specific point in time using the Recover point appliance which provides a consistent data recovery.
For continuous data protection (CDP), failover and failback technologies are used to move the workload from the Main site (AUC) to the Backup site.
The following figure illustrates this link between AUC and Vodafone



A new disaster recovery infrastructure is being studied to move AUC DR to the cloud using Microsoft Azure or Amazon web services (AWS). This provides AUC with better cost effective disaster recovery plan for optimum sustainable operations.

Forms/Instructions

N/A

Related Information

N/A

Appendices *(optional)*

N/A

History/Revision Dates

Origination Date: January, 1, 2014
Last Amended Date: October, 1, 2019
Next Review Date: May, 4, 2020