GFM Backup Policy

Policy Updated By	Latest Publish Date	Monitoring Cycle
IT Security Manager	January 2023	Annually

Schedule for Development / Monitoring / Review

This policy was approved by the Governing Body on:	January 2023
The implementation of this policy will be monitored by the:	**Principal and Senior Leadership Team**
The Policy will be reviewed annually, or more regularly in the light of any significant new developments. The next anticipated review date will be:	**January 2024**
Should serious incidents take place, the following external persons/agencies should be informed:	**Akram Tarik (Principal) and in his absence (Vice Principal)**

POL/IT/0022: Back-up Policy

Policy Title:	GEMS Education MENASA ICT – Back-up Policy
Policy Number:	POL/IT/0022
Version:	1.0
Effective date:	27 January 2023
Scheduled review date:	26 January 2024
Policy approver:	Chief Disruption Officer
Policy owner:	ICT
Policy reviewer:	IT Security Manager
Relevant related policies:	• Refer Section 12
Other relevant documents:	• None

Vision
'At GFM we empower students to have the heart to celebrate uniqueness and the mind to be innovative, creative problem solvers, bringing a positive change to the world in which we live.'

Page 1 of 9

GFM Backup Policy

Table of Contents

1. Policy Statement

GEMS Education servers, device configurations and data critical to business functions stored on shared drives shall be backed up periodically to prevent disruptions resulting from system failures or corruption of data.

2. Purpose

The purpose of this policy is to ensure that GEMS Education critical information is backedup on regular basis to prevent loss of data.

3. Scope

- All critical IT assets owned by GEMS Education ICT Department at Datacentre;

Vision
'At GFM we empower students to have the heart to celebrate uniqueness and the mind to be innovative, creative problem solvers, bringing a positive change to the world in which we live.'

GFM Backup Policy

- All critical information stored on GEMS Education server platforms in the Datacentre;
- Backup administrators, application owners, application administrators, server administrators and network administrators of GEMS Education – ICT Department.

4. Responsibilities

Activities	Information Security Team	IT Manager	VP - Technology	ICT/ Backup Administrator	Application / System Owner
Backup Requirement Identification	-	C, I	I	R, C, I	A, R
Backup request / modification approval	-	C, I	A, R	I	R
Schedule and monitor Backup	-	R, C, I	A	R	C, I
Onsite/Offsite Storage	-	I	A	R	C, I

Activities	Information Security Team	IT Manager	VP - Technology	ICT/ Backup Administrator	Application / System Owner
Recovery Testing	I	C, I	A	R	C, I
Status Report	I	C, I	A	R	C, I

Vision
'At GFM we empower students to have the heart to celebrate uniqueness and the mind to be innovative, creative problem solvers, bringing a positive change to the world in which we live.'

GFM Backup Policy

Term Used	Definition
R-Responsible	Person who performs the activity or does the work.
A- Accountable	Person who ultimately answerable and has yes/no/power.
C- Consulted	Person that needs to feedback and contribute to the activity.
I- Informed	Person that needs to know the decision or action.

5. Process – Backup management

5.1   IT manager shall be responsible for ensuring successful implementation of backup and restoration processes.

5.2   The key stages of Data Backup and Recovery procedure are as follows:
- Backup Scheduling;
- Backup Monitoring;
- Security of Backup;

- Recovery Testing.

Signed...................................... Date..... March 2023

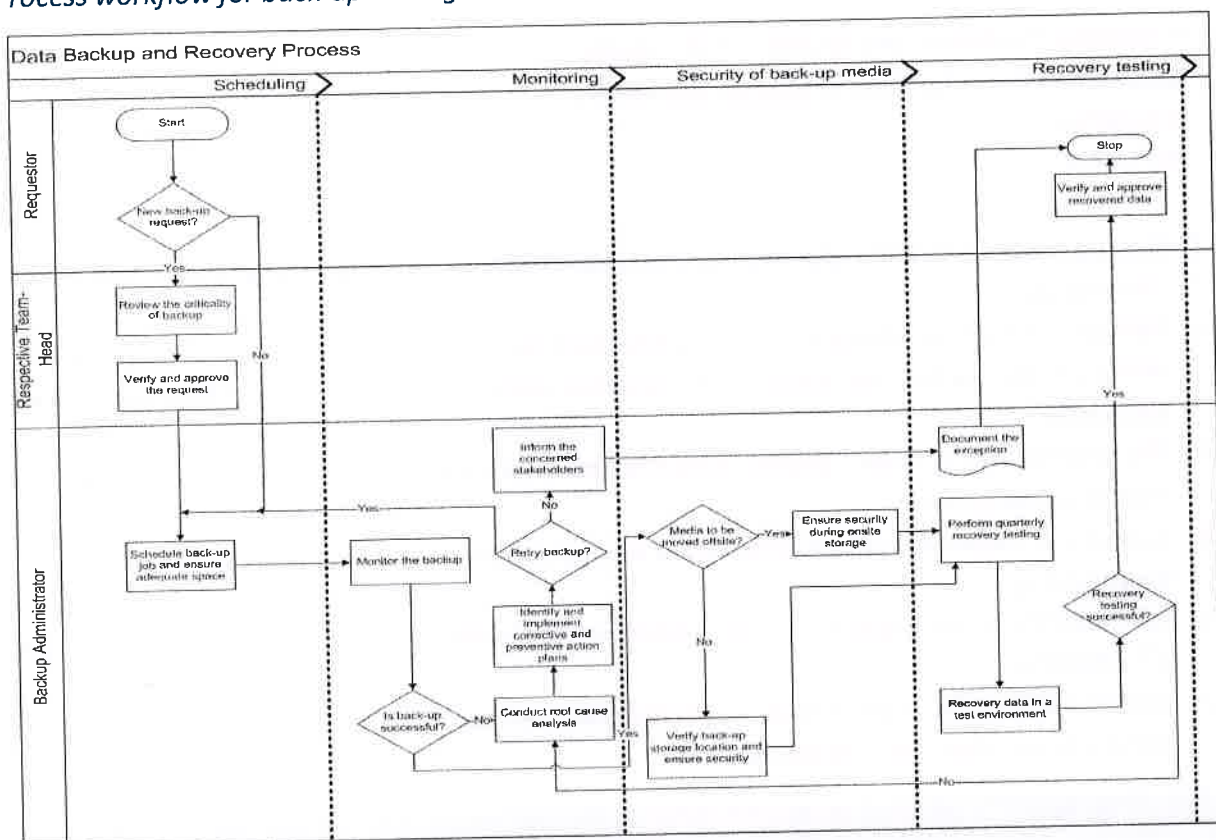**Principal/CEO**

Policy review date: January 2024

Vision
'At GFM we empower students to have the heart to celebrate uniqueness and the mind to be innovative, creative problem solvers, bringing a positive change to the world in which we live.'

Page **4** of **9**

Mission Statement:
Creating tomorrow's successful and
caring citizens today.

GFM Backup Policy

Process workflow for back-up management

Data Backup and Recovery Process

6. Back-up Scheduling

6.1   Scheduling of Backup

Vision
*'At GFM we empower students to have the heart to celebrate uniqueness and the mind to be
innovative, creative problem solvers, bringing a positive change to the world in which we live.'*

Mission Statement:
Creating tomorrow's successful and
caring citizens today.

GFM Backup Policy

6.1.1 Servers, device configurations and
data critical to business functions
stored on shared drives shall be backed up regularly;

6.1.2 System or Business owners shall be responsible to define the following in the backup requests to ICT through helpdesk:

- IP Address, Hostname and location of the server;
- Requested Files or location of data on the server;
- Frequency;
- Start Date.

6.1.3 Backup requests shall be approved by the Head of department requesting backup and the VP Technology;

6.1.4 Backup / ICT administrators shall schedule backup jobs in accordance with the frequency defined in the backup requests or in the documented Recovery Point Objective after relevant approvals;

6.1.5 The distribution of daily, weekly, monthly and yearly backups shall be maintainedby the backup administrator;

6.1.6 Backup / ICT administrator shall schedule backup jobs during off-peak business hours.

6.2 Rescheduling

6.2.1 Rescheduling of backup jobs shall be treated as new backup requests and registered through ICT helpdesk;

6.2.2 Backup / ICT administrators shall reschedule backup jobs in accordance with the re-defined requirements after relevant approvals.

7. Backup Monitoring

7.1 Logs for the success / failure of backup / restore shall be maintained based onfollowing parameters.

- Job ID;

Vision
'At GFM we empower students to have the heart to celebrate uniqueness and the mind to be innovative, creative problem solvers, bringing a positive change to the world in which we live.'

Page **6** of **9**

Mission Statement:
Creating tomorrow's successful and
caring citizens today.

GFM Backup Policy

- Type;
- Status;
- Job Policy/ Schedule;
- System details;
- Start Time;
- Storage Unit; and

- End Time.

7.2 Backup / ICT administrators shall perform the root cause analysis for consecutivefailed backup jobs;

7.3 Corrective and preventive actions shall be applied for the failed job;

7.4 Backup / ICT administrator shall notify the concerned stakeholders about the rootcause of back up failure, and action plans.

8. Status Report

8.1 Backup / ICT administrators shall generate following reports (not limited to):
- Number of instances of failed backup jobs;
- Number of instances of successful of backup jobs;
- Storage capacity utilization.

9. Security of Backup Media

9.1 Onsite / Offsite Storage:

9.1.1 Backup shall be encrypted;

9.1.2 Backup / ICT administrator shall be responsible for the physical security of thebackup media;

9.2 Backup tapes / media shall be disposed in accordance with the Asset and Mediadisposal policy;

9.3 Backup media movement (Applicable only if back up media is moved)

9.3.1 Backup / ICT administrator shall:
- Maintain logs on movement of backup media to offsite storage location;
- Ensure tamper proof box is utilized for transfer of backup media;
- Conduct

Vision

'At GFM we empower students to have the heart to celebrate uniqueness and the mind to be innovative, creative problem solvers, bringing a positive change to the world in which we live.'

Mission Statement:
Creating tomorrow's successful and
caring citizens today.

GFM Backup Policy

periodic audits of the offsite
storage location of backup
media toensure back up media are stored in a secure manner.

10.Recovery Testing

10.1   As a minimum baseline, samples of backup media for all information processingsystems shall be tested for successful recovery on a quarterly basis;

10.2   System owner shall raise a request for specific recovery testing requirements, ifrequired, through helpdesk;

10.3   Backup / ICT administrators shall conduct the recovery test in a testenvironment;

10.4   Successful recovery of the backup shall be confirmed by the system / Applicationowner.

11.Policy Compliance

11.1   Compliance measurement

11.1.1 Information security team shall be responsible to monitor compliance with thispolicy;

11.1.2 ICT team shall perform an independent review on the back-up and recoverytesting processes on a periodic basis.

11.2   Exceptions

11.2.1 Exceptions to this policy shall be documented. Exception shall include
- Justification,
- Impact / risk resulting and
- Approval from information security team, business/ application owner and VP

- Technology;

12.Related Standards, Policies and Processes

- Information

GFM Backup Policy

security policy
- Change management policy
- Asset classification, labelling and handling policy
- Asset and Media disposal policy