


Backup & Disaster Recovery of On-site Data & Server Infrastructure

2022-2023

Person Responsible	S.Salami/B McDermott
Last Review Date:	Feb 2022
Next Review Date:	Jan 23
This policy is communicated by the following means:	Website/Staff shared area
Governor's Signature:	



St Aloysius'
College

Hornsey Lane,
Highgate,
London
N6 5LY





St Aloysius' College: Backup & Disaster Recovery of On-site Data & Server Infrastructure

Purpose and Scope of this Document

Purpose and Scope of this Document

This document aims to provide staff with details of the Backup and DR (Disaster Recovery) measures which are currently in place at the school. These measures have been designed, implemented and are continually supported by Islington Schools IT.

This document will also outline the pre-requisites and expected time scales involved in various data restoration and DR scenarios.

The processes and configurations described in this document will be reviewed every 6 months, at which time this document will be amended and reissued if necessary, to include any changes.

Brief Overview of Server Infrastructure

The school employs a physical server cluster comprising two physical servers.

A physical server cluster is a group of two or more servers which work together to achieve a common purpose. The purpose of the physical server cluster in this case is to provide a platform on which to host a number of additional Virtual Machine servers, or VM servers.

VM servers are instances of server operating systems which are not installed directly on the server hardware. They are instead installed in software, allowing us to provide multiple VM guest servers on a single physical host server. This approach to server provisioning has numerous benefits.

The VM servers in the school provide the day-to-day services with which end users interact, such as allowing users to logon to workstations, giving users access to files and folders, providing remote access and providing access to SIMS (amongst other background functions).

The physical server cluster also aims to provide HA (High Availability) of the VM servers which run within the cluster. This means that the cluster can tolerate a degree of physical component failure and even total loss of one physical server, with minimal downtime to the VMs running in the cluster.

HA provides fault tolerance of physical server infrastructure failure, it does not provide protection against individual VM server failure or



St Aloysius' College: Backup & Disaster Recovery of On-site Data & Server Infrastructure

data loss and/or corruption of data that resides within individual VM servers. Protection of the VM servers and their associated data is provided by Backup and DR software.

Clustered Server Infrastructure

The following table details all servers which constitute the main clustered server platform, along with their associated roles

Physical Server	Primary Role
STA-HOST-01	Hosts VM servers in a fault tolerant HA cluster
STA-HOST-02	Hosts VM servers in a fault tolerant HA cluster
VM Server	
STA-DC01 (Domain Controller)	Provides logon services and general user settings and configurations. Holds the Active Directory database of domain User and Computer information
STA-DC02 (Domain Controller)	Provides logon services and general user settings and configurations. Holds the Active Directory database of domain User and Computer information which is replicated from STA-DC01



St Aloysius' College: Backup & Disaster Recovery of On-site Data & Server Infrastructure

STA-FS01 (File Server)	Hosts all on-premises file data including individual user data and shared areas
STA-MIS01 (MIS Server)	Hosts the SIMS Management Information System database
STA-APPS01 (Application Server)	Hosts a number of networked curriculum applications
STA-PRN01 (Print Server)	Provides all print services including hosting the PaperCut Print Management System
STA-RDS01 (Remote Desktop Server)	Provides remote access to on-premises IT services
STA-SQL01 (MS SQL Database Server)	Hosts a number of SQL databases such as Door Entry System and Catering System



St Aloysius' College: Backup & Disaster Recovery of On-site Data & Server Infrastructure

Standalone Servers

The following table details additional servers which are physical in nature and exist outside the main clustered server platform for reasons of allowing independent access to, and operation of, backup and DR functions and data, regardless of the health of the main server cluster.

Physical Server	Primary Role
STA-BAK01 (Primary backup server)	Altaro VM Backup server (more on Altaro to follow). Responsible for backing up and restoring all Altaro operations. The primary on-site backup storage location is attached to this server
STA-BAK02 (Secondary backup server)	Backup location for Veeam backup software (more on Veeam to follow)



St Aloysius' College: Backup & Disaster Recovery of On-site Data & Server Infrastructure

Backup and DR Software

Backup and DR services are currently achieved using three separate and independent software solutions. All three solutions are in use simultaneously, all backing up data nightly. These are **Altaro VM Backup**, **Veeam Agent for Windows** and **RedStor Pro**, with Altaro VM Backup being the primary solution.

Backup Software Notifications

All backup software solutions have been configured to send email notifications to the Islington Schools IT helpdesk system on a nightly basis when backup operations are scheduled to run.

Notifications have been configured to log high priority incident tickets automatically on our helpdesk system when backup operation failures occur. This allows helpdesk staff to work on failed backup incidents as early as possible during working hours.

In addition to this, work routines are carried out each working day by the helpdesk staff to ensure that we are not only aware of any backup failures from the previous 24-hour period, but we are also aware of all successful backup operations. This means all scheduled backups can be accounted for and we are made aware of any scenarios at the earliest opportunity when a backup solution is offline or completely non-functional and therefore may be unable to send any backup notifications.

For Altaro VM Backup, the notifications make us aware of the operational status of the on and off-site backups independently.

Altaro VM Backup

Altaro backs up all VM servers entirely. It can be used in restoration scenarios where individual file/folder data restoration is required and also where complete VM server restoration is required.

Altaro has been configured to back-up both on-site and off-site backup data storage locations. In the event of a DR scenario where entire loss of the primary server infrastructure has occurred due to a local disaster at the school site, Altaro will be used in order to restore the data.



St Aloysius' College: Backup & Disaster Recovery of On-site Data & Server Infrastructure

The off-site backup location would ordinarily only be used for recovery purposes in a DR scenario where data from the on-site backup location has been lost.

Altaro off-site backups are sent to a partner school Beacon High at no cost to St Aloysius. Altaro off-site backups are fully encrypted meaning data could not feasibly be read even if the off-site backup medium were stolen from the off-site storage location.

Veeam Agent for Windows

Although all data is backed up by Altaro VM Backup, it is prudent, where possible, to back up mission critical data with supplementary solutions. Altaro utilises current data security best practices to make it very difficult for bad actors to affect the backed-up data. However, with constant and rapid developments **in IT systems**, it is not currently possible to predict data backup solutions will always be 100% unassailable. Therefore, we provide an additional backup copy of the mission critical file server data using an alternative system in addition to a different backup location, using Veeam Agent for Windows.

RedStor Pro

As with the provision of Veeam for file server data, we have configured the RedStor offering from LGfL to make an additional off-site backup copy of the school's mission critical SIMS data and databases (SIMS & FMS).

RedStor Pro is included at no extra charge with the schools LGfL internet connection subscription.

RedStor off-site backups are fully encrypted meaning data could not feasibly be read even if the off-site backup medium were stolen from the off-site storage location.



St Aloysius' College: Backup & Disaster Recovery of On-site Data & Server Infrastructure

The following table details the current configuration of each of the backup solutions in use.

	Data backed up	Backup Frequency	On-site backup medium & retention period	Off-site backup medium & retention period	Automated backed up data integrity health checks (checking for data restorability)
Altaro VM Backup	Entirety of all VM Servers	Nightly (once per 24 hours)	Fault tolerant disk storage* 1 year for File & MIS Servers, 90 days for all other VM servers	Fault tolerant disk storage* 1 year for File & MIS Servers, 90 days for all other VM servers	Twice weekly for both on-site and off-site backup copies
Veeam Agent	All mission critical file and folder data from STA-FS01 (main file server)	Nightly (once per 24 hours)	Fault tolerant disk storage* 180 days	n/a	Once per month



St Aloysius' College: Backup & Disaster Recovery of On-site Data & Server Infrastructure

RedStor Pro	All mission critical SIMS related data and databases from STA MIS01 (SIMS server)	Nightly (once per 24 hours)	n/a	Backed up to LGfL / Adept cloud 60 days **	Continually checked on LGfL storage platform
--------------------	---	-----------------------------	-----	---	--

* The backup storage location comprises an array of hard drives which can tolerate the loss of one drive without incurring data loss

** Backups are restorable in daily increments for the preceding 60 days. Beyond that, backups are restorable in monthly increments for a further 6 months

It is possible to extend the backup retention periods of both on-site and off-site backups if larger capacity storage is purchased.

Data Restoration and Disaster Recovery Scenarios

The following section will detail various scenarios and the time scales involved in recovery. A tolerance of $\pm 25\%$ should be applied to these figures to allow for indefinite environmental and workload conditions such as local and internet network utilisation, server resource utilisation and the nature of data to be transferred (smaller numbers of large files versus larger numbers of small files).

The figures presented here also assume that any potential data recovery environment will be the same as it was at time of testing i.e. local and internet network capabilities and server hardware (particularly server storage) are identical or closely matched.

Times presented here are measured from the onset of a technician working on the data restoration activity until all data is recovered and is again fully accessible as it was prior to the issue described in the scenario.

Although the onset of a data restoration activity would normally begin during working hours, recovery times are not limited to working hours only and do not pause outside of working hours. For example, if a recovery activity begins at 8am on Monday morning and has an expected



St Aloysius' College: Backup & Disaster Recovery of On-site Data & Server Infrastructure

time of 16 hours, this means we would expect the process to be complete by midnight later that Monday, not by the end of the working day on Tuesday.

Finally, times presented in this section are directly related to the size of the data at time of writing. If the amount of data stored grows over time, we should expect recovery times to grow accordingly.

Scenario 1. Files and folders are missing, corrupted, or otherwise unusable on STA-FS01 (file server) or STA-MIS01 (SIMS server)

Assumptions	Data to be recovered	Expected recovery time
Technician has gained precise knowledge of data to be recovered Data is recoverable from on-site backup location(s)	20GB of file server mixed data, mainly small files	2 hours 30 minutes
	100GB of file server mixed data, mainly small files	10 hours 30 minutes



St Aloysius' College: Backup & Disaster Recovery of On-site Data & Server Infrastructure

Scenario 2. Files and folders encrypted by ransomware

Assumptions	Data to be recovered	Expected recovery time
Data is recoverable from on-site backup location(s) using backup data that pre-dates encryption	20GB of file server mixed data, mainly small files	6 hours 20 minutes
	100GB of file server mixed data, mainly small files	15 hours 20 minutes
	100GB – 1TB of file server mixed data, mainly small files	24 – 48 hours
	1TB – 4TB of file server mixed data, mainly small files	48 - 96 hours



St Aloysius' College: Backup & Disaster Recovery of On-site Data & Server Infrastructure

Scenario 3. Whole VM Server needs to be restored from on-site backup location due to serious issue which is preventing normal operation of service and cannot be rectified (or cannot be rectified within a tolerable length of time)

Assumptions	VM Server to be recovered	Expected recovery time
Data is recoverable from on-site backup location(s)	STA-DC01 (Domain Controller)	50 minutes
	STA-DC02 (Domain Controller)	45 minutes
	STA-FS01 (File Server)	3 hours 25 minutes
	STA-MIS01 (MIS Server)	2 hours 35 minutes
	STA-APPS01 (Application Server)	3 hours 50 minutes



St Aloysius' College: Backup & Disaster Recovery of On-site Data & Server Infrastructure

	STA-PRN01 (Print Server)	2 hours 10 minutes
	STA-RDS01 (Remote Desktop Server)	1 hour 40 minutes
	STA-SQL01 (MS SQL Database Server)	1 hour 35 minutes



St Aloysius' College: Backup & Disaster Recovery of On-site Data & Server Infrastructure

Scenario 4. Whole VM Server needs to be restored from off-site backup location due to serious issue which is preventing normal operation of service and cannot be rectified (or cannot be rectified within a tolerable length of time) and recovery from on-site backup copy is not possible.

Assumptions	VM Server to be recovered	Expected recovery time
Data is not recoverable from onsite backup location(s) Data is recoverable from off-site backup location(s)	STA-DC01 (Domain Controller)	2 hours 30 minutes
	STA-DC02 (Domain Controller)	2 hours 15 minutes
	STA-FS01 (File Server)	11 hours 10 minutes
	STA-MIS01 (MIS Server)	8 hours 5 minutes
	STA-APPS01 (Application Server)	12 hours 10 minutes



St Aloysius' College: Backup & Disaster Recovery of On-site Data & Server Infrastructure

	STA-PRN01 (Print Server)	7 hours 20 minutes
	STA-RDS01 (Remote Desktop Server)	5 hours 15 minutes
	STA-SQL01 (MS SQL Database Server)	5 hours 10 minutes

Scenario 5. One or more SIMS databases have become corrupt or is otherwise unusable

Assumptions	Database	Expected recovery time
Database is recoverable from on-site backup location(s) SQL server is available to restore SIMS database to	SIMS	2 hours 10 minutes
	FMS	1 hour 55 minutes



St Aloysius' College: Backup & Disaster Recovery of On-site Data & Server Infrastructure

Scenario 6. One or more SIMS databases has become corrupt or is otherwise unusable and recovery from on-site backup is not possible

Assumptions	Database	Expected recovery time
Database is not recoverable from on-site backup location(s)	SIMS	2 hours 40 minutes
	FMS	2 hours 25 minutes
Database is recoverable from off-site backup location(s)		
SQL server is available to restore SIMS database to		



St Aloysius' College: Backup & Disaster Recovery of On-site Data & Server Infrastructure

Scenario 7. Disaster Recovery. Complete loss of on-premises server infrastructure

Recovery points are stages in the process to full recovery where varying aspects of IT services gradually become available.

Recovery Point A: Once this point has been reached, users will be able to log on and access personal and shared files and folder data. Users will also be able to log in to the system remotely.

Recovery Point B: Once this point has been reached, users will have access to everything made available from Recovery Point A with the addition of SIMS and FMS databases becoming available.

Recovery Point C: Once this point has been reached, users will have access to everything made available from Recovery Points A & B, with the addition of all remaining IT services.

Assumptions	Recovery Point	VM servers recovered	Expected recovery time
Server infrastructure is available to recover VM servers to * Data is not recoverable from on-site backup location(s) Data is recoverable from off-site backup location(s)	A	STA-DC01 (Domain Controller)	12 hours
		STA-FS01 (File Server)	
		STA-RDS01 (Remote Desktop Server)	



St Aloysius' College: Backup & Disaster Recovery of On-site Data & Server Infrastructure

	B	STA-MIS01 (MIS Server)	A + 8 hours 5 minutes
	C	STA-DC02 (Domain Controller)	A + B + 12 hours
		STA-APPS01 (Application Server)	
		STA-PRN01 (Print Server)	
		STA-SQL01 (MS SQL Database Server)	

*This could be replacement or temporary physical servers in primary site or temporary site, or recovering to cloud hosted virtual servers

Restoration Rehearsal

In addition to the automated backup data integrity checks, we manually rehearse backup restorations every 90 days. This allows us to become aware of any unlikely issues with data restorability which have not been brought to our attention by the automated checks.