WILLIAMSBURGH
HOUSING ASSOCIATION LTD

I.T. DISASTER RECOVERY & INCIDENT POLICY
OCTOBER 2023

Revision History

Creation/Revised Date	Reviewer(s)	Review Date
October 2021	Corporate Services	
October 2022	Corporate Services	October 2023
October 2023	IT Manager	October 2025

CONTENTS

This policy should be read in conjunction with the Data Protection Policy, Appendix 3 (Information Security and Personal Data Breach Management Procedure) which specifically details procedures to handle personal data breaches.

1. POLICY STATEMENT

1.1 Williamsburgh Housing Association (WHA) recognises the need for, and value of, a comprehensive Disaster Recovery Plan which aims to minimise risk, service disruption, financial and reputational consequences should a disaster/major security incident occur.

WHA is committed to:

- Maintaining a comprehensive recovery plan.
- Ensuring any changes to procedures are adequately risk assessed (see section six)
- Ensuring the recovery plan covers all essential and critical infrastructure elements and data assets, systems and networks, in accordance with key business activities.
- Committing to periodic testing of the recovery plan in a simulated environment.

2. INTRODUCTION

2.1 These procedures are to be followed in the event of a disaster concerning WHA's office - in particular the IT computer systems and a serious security incidents (Cybercrime). An event will be considered to be a disaster when users are unable to access the office premises and/or central servers and/or data is lost from business-critical IT systems (see item 6.5).

Types of Disaster included but not restricted to:

Environmental Disasters
Flood / Snowstorm / Electrical storms / Fire /Subsidence and Landslides /Freezing Conditions.
Contamination and Environmental Hazards

Organised and / or Deliberate Disruption
Act of vandalism / Act of Sabotage / Theft / Arson

Loss of Utilities and Services
Electrical power failure

Equipment or System Failure
Internal power failure / Equipment failure (excluding IT hardware)

Serious Information Security Incidents
Cybercrime / Loss of records or data / IT system failure

Pandemics
Outbreak of infectious disease (resulting in office closure)

2.2 A copy of these procedures are to be held by the CEO, Head of Finance & Corporate Services and IT Manager. Any updates, including updates to contact names and numbers, must be made to all copies. Additionally WHA's IT Support Contractor must receive a copy of the revised document if changes are made.

3. NOTIFICATION OF A DISASTER SITUATION

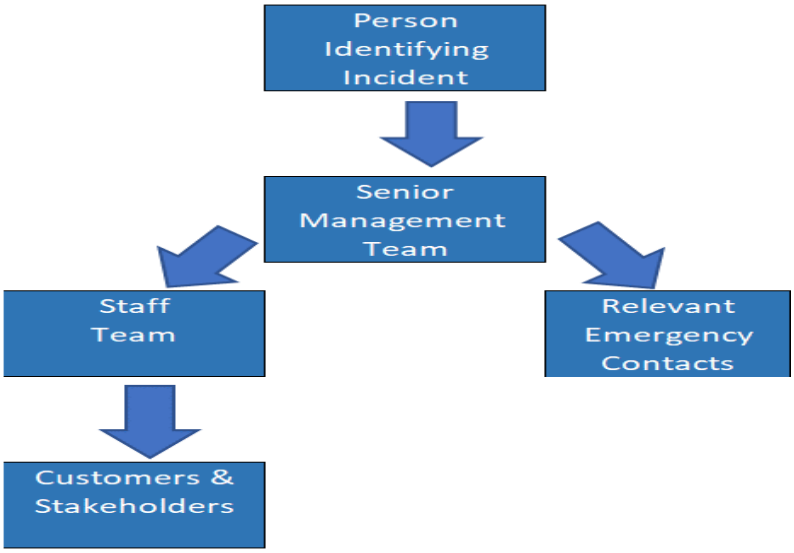
3.1 Listed below are the contact numbers for WHA's key personnel to be contacted should a disaster situation occur: -

Senior Management Team (SMT)		
Name	**Title**	**Contact number**
Jon Grant	Chief Executive Officer	
Lynne Ramsay	Head of Finance & Corporate Services	
Lesley Ferrie	Head of Housing Services	
Lisa Reynolds	Head of Property Services	
Graham Scott	Head of Development	

IT Team		
Name	**Title**	**Contact number**
John Kelly	IT Manager	
Roni Gallacher	IT Assistant	

Emergency Contacts		
Supplier	**Service Provision**	**Contact number(s)**
ChessICT	Current IT Support	03447 706000
Aareon	Housing Management System	01792 656699
NCS	Leased Line for Internet	03452 000012
NCS	Phone System	03452 000058

3.2 It is anticipated that the following notification tree will be utilised when reporting and communicating on a disaster event:-



3.3 For all data/information security incidents, the form at Appendix D should be used to report and document incident.

4. IT SYSTEM BACKUP PROCEDURES

4.1 Backup procedures are carried out at server level. The Servers are as follows:-

Main Servers					
Server Name	**Location**	**Manufacturer/ Model**	**Service Tag No**	**Warranty Status**	**Install Date**
WHA-APP-1 (Virtual)	Azure Cloud	N/A	N/A	N/A	November 2018
WHA-DC-3 (Virtual)	Azure Cloud	N/A	N/A	N/A	September 2023
WHA-DC-4 (Virtual)	Azure Cloud	N/A	N/A	N/A	September 2023
WHA-EXH-1 (Virtual)	Azure Cloud	N/A	N/A	N/A	January 2021
WHA-FP-1 (Virtual)	Azure Cloud	N/A	N/A	N/A	November 2018
WHA-SQL-1 (Virtual)	Azure Cloud	N/A	N/A	N/A	November 2018
WHA-REM-1 (Virtual)	Azure Cloud	N/A	N/A	N/A	November 2018
WHA-AVD-0 (Virtual)	Azure Cloud	N/A	N/A	N/A	August 2023
WHA-AVD-1 (Virtual)	Azure Cloud	N/A	N/A	N/A	August 2023
WHA-AVD-2 (Virtual)	Azure Cloud	N/A	N/A	N/A	August 2023
WHA-AVD-3 (Virtual)	Azure Cloud	N/A	N/A	N/A	August 2023
LepideDSP21-2 (Virtual)	Azure Cloud	N/A	N/A	N/A	August 2023
Tenable Core Live (Virtual)	Azure Cloud	N/A	N/A	N/A	August 2023

4.2 A backup of all virtual servers is carried out as outlined in the table below.

Server Name	**Main Role**	**Backup Policy**	**Backup Method**
WHA-APP-1 (Virtual)	Applications including Astrow and Locator Plus	Gold	Azure Backups
WHA-DC-3 (Virtual)	Domain Controller	Bronze	Azure Backups
WHA-DC-4 (Virtual)	Domain Controller	Bronze	Azure Backups
WHA-EXH-1 (Virtual)	Exchange Hybrid Server	Bronze	Azure Backups
WHA-FP-1 (Virtual)	File Server	Silver	Azure Backups
WHA-SQL-1 (Virtual)	Aareon Housing Management	Gold	Azure Backups

	System and Task Centre		
WHA-REM-1 (Virtual)	QL Contractor Server	Silver	Azure Backups
WHA-AVD-0 (Virtual)	Azure Virtual Desktop Host	Bronze	Azure Backups
WHA-AVD-1 (Virtual)	Azure Virtual Desktop Host	Bronze	Azure Backups
WHA-AVD-2 (Virtual)	Azure Virtual Desktop Host	Bronze	Azure Backups
WHA-AVD-3 (Virtual)	Azure Virtual Desktop Host	Bronze	Azure Backups
LepideDSP21-2 (Virtual)	Lepide Auditing Software Server	Bronze	Azure Backups
Tenable Core Live (Virtual)	Nessus Vulnerability Scan Server	Bronze	Azure Backups

4.3 Gold Back Up Policy (Azure default policies)

Backup frequency
Every 4 hours
Instant restore
Retain instant recovery snapshot(s) for 5 day(s)
Retention of daily backup point
Retain backup taken every day for 7 Day(s)
Retention of weekly backup point
Retain last backup taken every week on Sunday for 4 Week(s)
Retention of monthly backup point
Retain last backup taken every month on First Sunday for 12 Month(s)
Retention of yearly backup point *
Retain last backup taken every year in January on First Sunday for 7 Year(s)
** WHA set to 1 year for annual backup*

Silver Back Up Policy (Azure default policies)

Backup frequency
Every 4 hours
Instant restore
Retain instant recovery snapshot(s) for 5 day(s)
Retention of daily backup point
Retain backup taken every day for 7 Day(s)
Retention of weekly backup point
Retain last backup taken every week on Sunday for 4 Week(s)
Retention of monthly backup point
Retain last backup taken every month on First Sunday for 12 Month(s)
Retention of yearly backup point
Retain last backup taken every year in January on First Sunday for 1 Year(s)

Bronze Back Up Policy (Azure default policies)

Backup frequency
Every 4 hours
Instant restore
Retain instant recovery snapshot(s) for 5 day(s)
Retention of daily backup point
Retain backup taken every day for 7 Day(s)
Retention of weekly backup point
Retain last backup taken every week on Sunday for 4 Week(s)
Retention of monthly backup point
Retain last backup taken every month on First Sunday for 3 Month(s)

4.4 Backups in Azure are fully automated, and the system will email WHA IT Manager, IT Assistant and ChessICT if there are any backup failures or any attempts to manually delete backup data.

4.5 If the backup fails, the remote monitoring system will inform the IT Manager, IT Assistant and support company. The IT Manager will then take appropriate action to rectify the situation.

4.6 Any additional ad-hoc backup that may be required, e.g., prior to version upgrades etc should be suitably labelled and documented to represent the purpose of the backup. Any such ad-hoc backups are stored within Azure Recovery Services Vault to ensure they are safeguarded against loss or theft.

4.7 When Azure takes a backup it copies that backup to a Vault elsewhere in the Datacentre. Based on tests carried out on our largest server with 1TB of data we were able to restore this server in under 2 hours. In the unlikely event of a total failure of all servers the estimate recovery time is 8 hours.

4.8 One of the biggest risks to our data is Ransomware. By moving to Azure we have considerably reduced the risk should we need to recover from a Ransomware attack.

Azure has a number of protections against Ransomware.

- Recovery Service Vaults have no direct connection to the servers. Even if all servers were infected, they cannot influence the vault in any way.
- The only way to touch or attempt to delete backups would be in gaining control of an account with administrative access to the Azure Portal.
- To protect against Rogue Admins there is also a feature called soft delete where backups cannot be permanently deleted until a minimum period has passed since the initial deletion action. By default, Azure Backups have a soft-delete policy of 14 days.

4.9 In the event that there is an outage of Physical Hardware within the Microsoft Datacentre that houses our Virtual Machines, Microsoft guarantee availability between 95% and 99.9%.

5. IT DISASTER RECOVERY PROCEDURES

5.1 In the event of a major computer disaster being discovered the following procedures detailed from 5.2 onwards should be followed in conjunction with the DR checklist in Appendix A.

5.2 Immediately on the discovery of the disaster the following people must be notified using the appropriate contact numbers in section 3 if necessary.

– Head of Finance & Corporate Services
– Chief Executive Officer
– IT Manager
– IT Support Contractor

5.3 Having assessed the seriousness of the disaster, the senior person present will contact other personnel as appropriate. Emergency details for contractors are included in section 3.

5.4 Responsibility for ensuring that the disaster recovery procedures are followed rests with the Head of Finance & Corporate Services or in their absence the senior Manager present.

5.5 In the event of a serious virus or Ransomware infection the Head of Finance & Corporate Services or IT Manager will ask all users to log out of all systems immediately. The IT Manager, IT Assistant and IT Support Partner will then proceed to clean and disinfect all PCs and Servers. If data is corrupt in any way a restore will then be taken from the most recent known good back-up. IT Support Partner will assist in line with the current contract and anything over and above the current contract will be covered at the standard commercial rate.

5.6 If Police and/or Fire personnel are required to be on site, then permission must be obtained from the appropriate authority before entering the site or touching any of the equipment.

5.7 Once on site, all equipment within the office must be checked against the Asset Register contained in Appendix C. Any missing equipment must be listed. In the event of a serious virus or ransomware attack, all equipment affected must be identified, removed from the network and restore or replacement of equipment should be carried out depending on the nature and severity of the attack.

5.8 In the event of WHA's main offices, or the hardware within it, being a total loss, Business Continuity plans will be followed (see appendix B). The Head of Finance & Corporate Services , IT Manager and IT Assistant will work with the IT Support Partner to restore business critical systems. The IT Support Partner would assist in locating and setting up alternative equipment to restore business critical systems in line with the current five year support contract.

5.9 The phone system is hosted within WHA's office. If the phone system is unavailable the Head of Finance & Corporate Services will ensure that our website and social media platforms are updated with contact numbers until the phone system is reconnected. All staff would work from home until an operational office solution is achieved.

5.10 If the premises are accessible and equipment is intact and operational then connections to all clients and printers should be checked. Once this has been completed a check of the functionality of programs and connections to Azure Virtual Desktops should be made. A fuller more detailed check must be carried out at the earliest opportunity by all users.

5.11 No further updating of information is allowed until all users have confirmed that the data within the Aareon QL HMS and Finance system and other relevant systems is up to date.

5.12 If data is incorrect or has been corrupted in some way, then the most recent available backup is to be used to restore the system to that point. Assistance and procedures to restore from backup can be obtained through the IT Support Partner.

5.13 If this action is necessary then all users must be notified of the point that the system has been restored to at the earliest opportunity.

5.14 Once any replacement equipment and relevant software have been set up, all users must be notified of the point to which the backup relates e.g., date and time of last entries on the system, at the earliest possible opportunity.

5.15 Users must also be requested to confirm that the system is as expected, in particular reports such as trial balances etc and that they have access to the same programs and data that they had access to prior to the disaster.

5.16 No processing should be allowed until all such confirmations are completed.

5.17 As soon as the system is available for processing of data **all** passwords must be changed and the system will prompt all users for a new password.

5.18 In the event of a serious virus or ransomware attack, the insurance company must be notified to allow their cyber security procedures to be implemented. E.g. if required carry out forensic checks of equipment, liaise with police, advise on dealing with attackers etc.

5.19 As soon as the above procedures are completed and processing recommences, an insurance claim must be completed, if appropriate, and submitted to WHA's Insurance Brokers.

5.20 Once normal business operations have been restored the Head of Finance and Corporate Services or IT Manager will inform staff that all systems are in working order and staff can resume operations.

5.21 Where replacement hardware is required following a disaster e.g., replacement switches, workstations etc. there will be a lead time and costs from order to delivery that will impact the overall recovery time.

6. RISK ASSESSMENTS OF CRITICAL SYSTEMS

6.1 The risks outlined in 6.2 have been identified and categorised as follows:

Probability: 1 – Low
2 – Medium
3 – High

Impact: 1 – Low
2 – Medium
3 – High

Total: Probability x Impact

Category: 1-3 Low, 4-6 Medium, 7-9 High

6.2 The Association has identified the following risks:

Risk	Probability	Impact	Total	Category
Complete loss	1	3	3	Low
Server Failure	1	3	3	Low

6.3 The software/data risks outlined in 6.4 have been identified and categorised as follows:

6.4 **Impact**: 1 – Low Business can function without item longer term
2 – Medium Business can function without item medium term
3 – High Business cannot function without item

System rating 1 – Low Business can function with minimal disruption
2 – Medium System holds valuable but not essential data
3 – High Essential business system

Total: Impact x System rating

Category: 1-3 Low, 4-6 Medium, 7-9 High

6.5 The Association has identified the following risks:

System	Impact	System rating	Total	Category
Housing System	3	3	9	High
Finance System	3	3	9	High
Payroll/Sage	3	3	9	High
Email	2	2	4	Medium
Internet access	2	1	2	Low
Company file store	3	3	9	High
Time Management System	1	1	1	Low

6.6 The recovery time objective for each risk category is as follows:

Low: 10 working days
Medium: 5 working days
High: 3 working days if physical, 2 working days if software.

7. CHECKLISTS

7.1 A checklist to ensure all procedures have been followed is attached as Appendix A.

8. COMMUNICATIONS PLAN

8.1 It is very important during the disaster recovery and business recovery activities that all affected stakeholders are kept properly informed. The information given to all parties must be accurate and timely. In particular, any estimate of the timing to return to normal working operations should be announced with care. It is also very important that only authorised personnel deal with media queries and any potential regulatory notification.

Persons selected to communicate with stakeholders	
Stakeholders	**Name**
Staff Team	Senior Management Team
Committee	Chairperson and Members
Customers	Customer Services Team
Suppliers	Senior Management Team
Media	Chief Executive Officer
Scottish Housing Regulator (SHR)	Chief Executive/ Data Protection Manager (DPO)
Information Commissioners Office (ICO)	Data Protection Manager (DPO)
Insurance provider	Senior Management Team

8.2 In the event of a disaster situation resulting in the loss or theft of personal and sensitive data the association have 72 hours to notify the ICO. Appendix 3 of the Data Protection Policy details the procedure should personal data be breached.

8.3 The following communication channels can be utilised to assist the communications plan. Instruction should be taken from the CEO or Head of Finance &Corporate Services as to what information is released via each individual channel to ensure consistency of communications:-

Channel	Remit	Channel Manager
Website (cloud – always available)	Banner on homepage and latest news section for situation updates	Head of Finance & Corporate Services
Social Media (cloud – always available)	Twitter and Facebook for text based situation updates.	Head of Finance & Corporate Services
Telephones (on premise, may not be available depending on disaster situation)	Two options can be implemented via Telephone Provider depending on the disaster situation:- • Re-direct main number to a designated mobile phone. • Set phones to night service if not already on night service	Head of Property Services

9. MONITORING AND REVIEW

9.1 Monitoring of the Disaster Recovery Plan will be undertaken by the Head of Finance & Corporate Services.

Incident Reporting Forms (Appendix D) will be used to record the incident.

Once the incident is reported, the Senior Management Team, IT Manager, ChessICT Support and if required the DPO should be notified. Depending on the nature of the incident, a member of the Senior Management Team or IT Manager will manage the incident. The manager of the incident is then responsible for involving any or all persons deemed necessary for the incident and ensuring the process is followed correctly.

An incident log will be created, and the incident manager is responsible for creating the incident log and linking it to the WHA Incident Reporting Form to help track the incident.

The log will include:-

- A description of the emergency or incident
- Those people notified of the emergency (including dates and times)
- Action taken by members of the Management Team
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Assessment of the effectiveness of the Disaster Recovery Policy
- Lessons learned

9.2 The Disaster Recovery/Incident Response Policy will continue to be reviewed bi-annually.

APPENDIX A

Checklist – Disaster Recovery

	Procedure	**Y/N**	**If N Action**
1.	Have the following personnel been contacted? Head of Finance & Corporate Services Chief Executive Senior Management Team IT Support Partner IT Manager	 **Y/N** **Y/N** **Y/N** **Y/N** **Y/N**	
2.	In the event of structural damage or Police investigations permission must be granted to enter the building. Has permission been granted? Yes – Permission granted by:	 **Y/N**	
3	Depending on the nature of the incident follow the processes detailed in **Appendix B**	**Y/N**	
4.	Restore completed & checked	**Y/N**	
5.	Notify all users of the points that the system has been restored to i.e. date, time of last entries etc.	**Y/N**	
6.	Confirmation from all users that access levels and date is as it was before disaster	**Y/N**	
7.	All passwords changed	**Y/N**	
8.	Double check the relevant check lists to ensure procedures completed	**Y/N**	
9.	In the event of serious virus or ransomware contact cyber-Insurance company	**Y/N**	
10.	Complete insurance form and submit to broker	**Y/N**	
11.	Write report detailing the disaster event and submit to SMT	**Y/N**	

APPENDIX B

Disaster Recovery/Incident Repose Strategies

The overall DR strategy of WHA's server services are summarised in the table below and documented in more detail in the supporting sections.

Disaster Recovery Procedures

A disaster recovery event can be broken out into three phases, the response, the resumption, and the restoration. These phases are also managed in parallel with any corresponding business continuity procedures.

Response Phase: The immediate actions following a significant event.

- IT Manager contacted to assess impact on supported systems
- ChessICT contacted for any required input
- Decision made around recovery strategies to be taken based on symptoms
- Full recovery team identified

Resumption Phase: Activities necessary to resume services after team has been notified.

- Recovery procedures implemented
- Coordination with other departments executed as needed

Restoration Phase: Tasks taken to restore service to previous levels.

- Rollback procedures implemented
- Operations restored

Response Phase

The following are the activities, parties and items necessary for a DR response in this phase. Please note these procedures are the same regardless of the triggering event.

Response Phase Recovery Procedures – ALL DR Event Scenarios (A, B, and C, above)

Step	Owner	Components		If N Action
Identify issue, Designated Responsible Individual (IT Manager), contact ChessICT technical service desk	IT Manager	• Issue communicated to SMT • ChessICT notified • Identify priority of restore	**Y/N** **Y/N** **Y/N**	
Identify the team members needed for recovery	IT Manager	Selection of core team members required for restoration phase from among the following groups: • IT Manager • Technical resource from ChessICT	 **Y/N** **Y/N**	
Communicate the specific recovery roles and determine which recovery strategy will be pursued.	IT Manager	• Documentation / tracking of timelines and next decisions	**Y/N**	

Resumption Phase

During the resumption phase, the steps taken to enable recovery will vary based on the type of issue. The procedures for each recovery scenario are summarised below.

A. Virtual server failure

In the event of a single Azure virtual server encountering a failure the following steps would be taken to bring services back online.

Step	Owner	Components		If N Action
Identify failed server	ChessICT	• Restoration procedures identified.	**Y/N**	
Implement Instant Restore in Azure	ChessICT	• Ensure restored server is online. • Ensure data is current. • Ensure data can be accessed via Azure Virtual Desktop	**Y/N** **Y/N** **Y/N**	
Test Recovery	ChessICT	• Tests assigned and performed. • Results summarised and communicated to IT Manager	**Y/N** **Y/N**	

B. Complete Site loss

In the event of a complete site loss Business Continuity processes apply:

- Identify and secure temporary premises.
- Ensure internet access available at temporary premises (see 5.8)
- Follow Resumption phase B listed above.

C. Serious Virus or Ransomware

In the event of serious virus or Ransomware being discovered:

Step	Owner	Components		If N Action
Immediately disconnect the infected computers, laptops or tablets from all network connections whether wired,	IT Manager	• Ensure that WHA Staff are informed not to try to reconnect equipment.	**Y/N** **Y/N**	

Step	Owner	Components		If N Action
wireless or mobile phone based				
Turn off Wi-Fi, disable all core network connections (including switches) and disconnect from the Internet	IT Manager	• Restoration procedures identified.	**Y/N** **Y/N**	
Identify any data loss	IT Manager	• Data loss may have occurred due to encryption of files and folders • Recover data as required	**Y/N** **Y/N**	

Restoration Phase

During the restoration phase, the steps taken to enable recovery will vary based on the type of issue. The procedures for each recovery scenario are summarised below.

A. Virtual Server failure

Software fault

Step	Owner	Components		If N Action
Fault identified	ChessICT	Fault identified and resolution identified as fix or restore	**Y/N**	
Resolution executed	ChessICT	Identified resolution executed on server	**Y/N**	
Virtual Machine brought back into production	ChessICT	Server brought back online and verified as running	**Y/N**	
Reverse replica configuration	ChessICT	Active VM's on DR system replicated back to original Virtual Machine	**Y/N**	

B. Complete Site loss

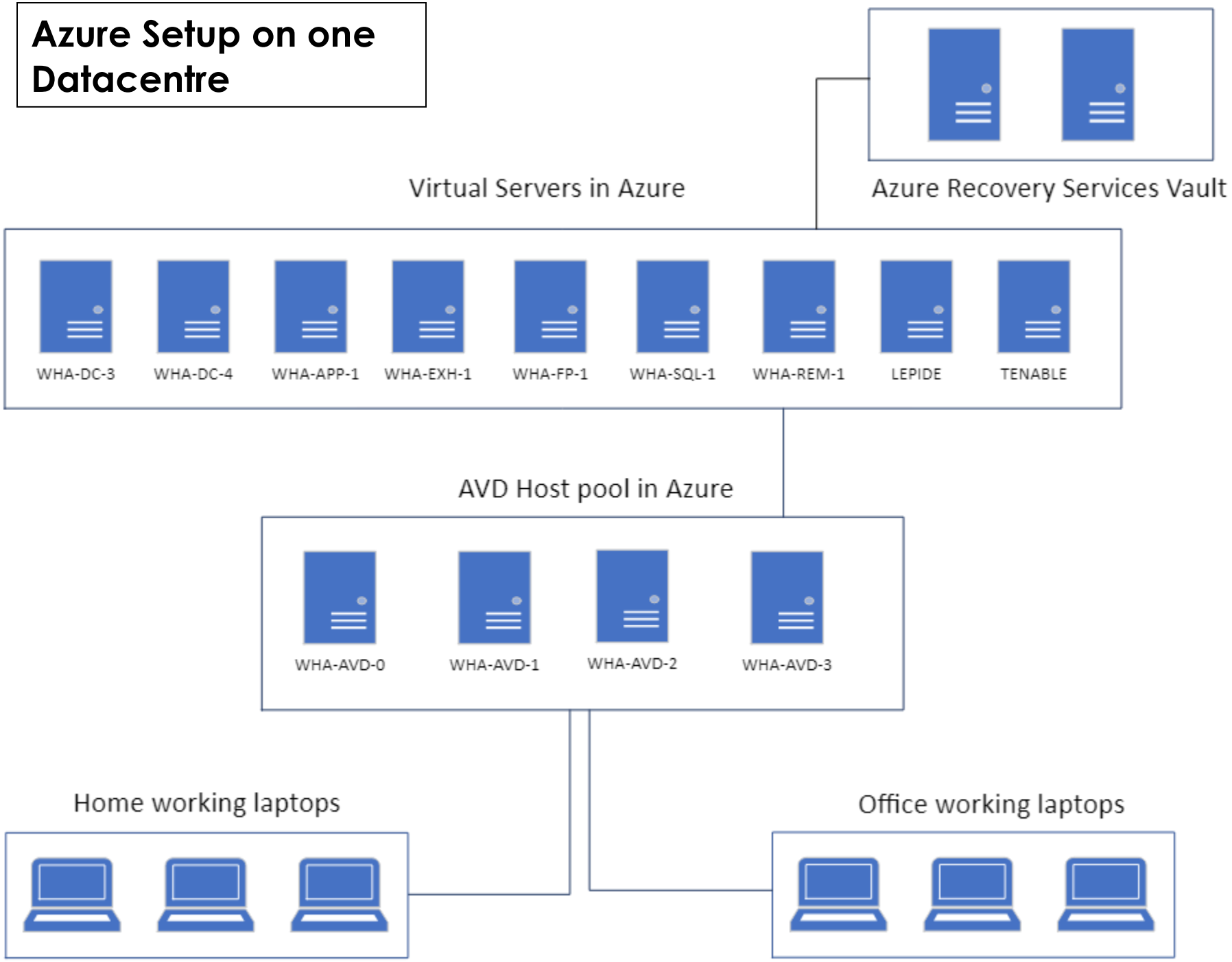
Step	Owner	Components		If N Action
Damaged equipment identified	IT Manager/ChessICT	Failed equipment identified and inventoried	**Y/N**	
Replacement specification created	IT Manager/ChessICT	Replacement equipment works specification generated	**Y/N**	
Sign off on replacement equipment and work	IT Manager	Williamsburgh to authorise work and parts	**Y/N**	
New Site Location Identified	CEO	Arrange to relocate to New Site Location or Home Working	**Y/N**	

Step	Owner	Components		If N Action
Replacement equipment ordered	IT Manager	Replacement equipment as per specification ordered	**Y/N**	
Configuration and rebuild of equipment	IT Manager/ChessICT	Configuration and rebuild of equipment in New Site Location/Home Working	**Y/N**	
Test equipment and connectivity at New Site to Azure Virtual Desktops	IT Manager/ChessICT	Replacement equipment	**Y/N**	

C. Serious Virus or Ransomware

Step	Owner	Components		If N Action
Infected equipment identified	IT Manager/ChessICT	Infected equipment identified and inventoried	**Y/N**	
Forensic analysis	Cyber Insurance	Investigation started to ascertain the source and extent of the infection	**Y/N**	
Safely wipe the infected devices and Operating System	IT Manager/ChessICT	Infected equipment	**Y/N**	
If it is considered infected equipment should be replaced, sign off on replacement equipment and work	IT Manager	Williamsburgh to authorise works and replacements Recover data as required	**Y/N**	
Restore from backups	IT Manager / ChessICT	• Verify that backups are free from malware or ransomware • Ensure that the back up and device connecting to are clean	**Y/N**	
Connect devices to a clean network	IT Manager / ChessICT	Download, install and update the Operating System and all other software	**Y/N**	
Anti-Virus check	IT Manager / ChessICT	Run antivirus software to ensure equipment is clean	**Y/N**	
Reconnect equipment to network	IT Manager/ChessICT	Monitor network traffic and run antivirus scans to identify if any infection remains	**Y/N**	

Azure Setup on one Datacentre



APPENDIX C

Asset Management Register

Asset Register 241022.xlsx

APPENDIX D

Incident Reporting Form

Adobe Acrobat Document