CLYDESDALE HOUSING ASSOCIATION LIMITED

Policy:	ICT Disaster Recovery Plan
Date:	28 April 2021
Lead Officer:	Chief Executive
Review Date:	April 2024
Regulatory Standard:	**Standard 4** The governing body bases its decisions on good quality information and advice and identifies and mitigates risks to the organisation’s purpose.
Regulatory Guidance:	4.3 The governing body identifies risks that might prevent it from achieving the RSL’s purpose and has effective strategies and systems for risk management and mitigation, internal control and audit.

Clydesdale Housing Association will provide this policy on request at no cost, in large print, in Braille, in audio or other non-written format, and in a variety of languages.

HAPPY TO TRANSLATE

1. Background

1.1 Clydesdale Housing Association (CHA) acknowledges the importance of its ICT systems in the day-to-day running of the business. CHA recognises the need for, and value of, a comprehensive ICT Disaster Recovery Plan which aims to minimise risk, service disruption, financial and reputational consequences should a disaster occur. CHA is therefore is committed to:

- Maintaining a comprehensive IT disaster recovery and business continuity plan.
- Conducting periodic and formal risk assessments to ensure business critical IT and data assets are safeguarded.
- Ensuring the disaster recovery and business continuity 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 disaster recovery and business continuity plan in a simulated environment to ensure that it can be implemented in emergency situations

2. Introduction

2.1 The ICT Disaster Recovery procedures are to be followed in the event of a disaster concerning the main computer systems at CHA. A disaster will be considered to be a disaster when users are unable to access the central servers and/or data is lost from business-critical systems.

2.2 A copy of these procedures will we accessible to all staff members in a secure online group area that will be available at all times (including in the event of a disaster). Any updates must be made to all copies. Additionally, the Associations’ IT Support Contractor, must receive a copy of the revised document if changes are made.

2.3 Responsibility for ensuring that these procedures are kept up to date and tested on a regular basis rests with the Chief Executive. The integrity of backups will be tested regularly by the IT Support Contractor.

3 Backup Procedures

3.1 CHA’s default position is for all data to be saved and stored on CHA’s network storage resources i.e., CHA’s system servers – to ensure data is backed up for security and business continuity purposes.

3.2 Given CHA’s enforcement of the principle of least privilege with Users, staff Users should save data in the most appropriate location on the CHA servers.

3.3 Staff Users are prohibited from saving data to local device storage drives, e.g., desktop computers and laptops.

3.4 Committee Users are permitted to save CHA data to local storage drives, although important corporate data must be saved in CHA’s network servers – such data should be shared with the Corporate Services Officer (CSO) for robust backing-up purposes.

3.5 All Users are prohibited from saving CHA data to personally owned devices.

3.6 Portable storage devices – the use of portable storage devices using USB ports is disabled in all CHA devices. The use of portable storage devices will only be permitted in exceptional circumstances, e.g., when connection to the network is unavailable and temporary use of such a storage drive is required to save data until it can be transferred to network storage facilities. When permitted, only CHA authorised portable storage devices can be used and these must always be scanned using anti-virus software and be encryption enabled.

3.7 Permission to use device USB memory drives must be obtained from the CEO, upon which a Ticket should be raised with CHA's IT Maintenance Contractor for this work to be actioned. Requests to the IT Maintenance Contractor will be rejected where proof of the CEO's authorisation is not provided.

3.8 Information must not be stored permanently on portable storage devices. Data being retained must be saved to CHA's system servers at the earliest opportunity and then deleted from the portable storage device.

3.9 CHA will run parallel on-site and off-site full server back-ups each working day in order to safeguard business continuity.

3.10 On-Site Back-Up:

3.10.1 The CSO oversees full on-site server back-ups at the end of each business day using external hard drive plug-ins.

3.10.2 Monday to Thursday, external back-up drives are overwritten every 7 days.

3.10.3 Weekly full on-site server back-ups are made each Friday. Weekly external back-up drives will be overwritten every 4 weeks.

3.10.4 The most recent successful external back-up drive will be stored off site for business continuity reasons.

3.10.5 CHA's IT Maintenance Contractor remotely monitors the success of back-ups each day and action is taken to address risk exposure as required.

3.10.6 If the backup fails the appropriate action will be taken by IT Maintenance Contractor to rectify the situation. CHA will be notified of instances where corrective action is taken.

3.11 Off-Site Back-Up:

3.11.1 CHA's IT Maintenance Contractor oversees off-site server back-ups to the cloud at the end of each business day. Daily off-site back-ups save incremental changes to data since the previous day.

3.11.2 CHA's IT Maintenance Contractor remotely monitors the success of back-ups each day and action is taken to address risk exposure as required.

3.11.3 If the backup fails the appropriate action will be taken by IT Maintenance Contractor to rectify the situation. CHA will be notified of instances where corrective action is taken.

3.12 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 CHA's secure servers to ensure they are safeguarded against loss or theft.

4 Disaster Recovery Procedures

4.1 In the event of a major computer disaster being discovered the following procedures detailed from 4.2 onwards should be followed in conjunction with the Disaster Recovery checklist in **Appendix A**. Examples of disasters are listed in **Appendix B**.

4.2 Immediately on the discovery of the disaster the following people must be notified:

- Chief Executive
- Management Team Members
- Corporate Services Officer
- IT Maintenance Contractor

4.3 Having assessed the seriousness of the disaster, the senior person present will contact other personnel as appropriate. Emergency contact details for contractors are included in **Appendix E**.

4.4 Responsibility for ensuring that the disaster recovery procedures are followed rests with the Chief Executive or in their absence, the senior staff member present.

4.5 In the event of a serious virus infection the Chief Executive will instruct all users to log out of all systems immediately. CHA will work with the IT Maintenance Contractor to ensure all PCs, Laptops and Servers are restored to last known good settings. If data is corrupt in any way a restore will then be taken from the most recent known good back-up.

4.6 If the situation is such that Police and/or Fire personnel are on site, then permission must be obtained from the appropriate authority before entering the site or touching any of the equipment.

4.7 In the event of CHA's offices or the hardware within it being a total loss, the Chief Executive will lead a team to work with the IT Maintenance Contractor to restore business-critical systems. Priority will be given to the servers necessary to reinstate SDM Housing Software and finance documentation/records with the integrity of the data checked before staff access is granted. The IT Maintenance Contractor will locate and set up alternative servers to restore business-critical systems.

4.8 If the premises are accessible and servers are intact and operational then connections to all devices and printers should be checked. Once this has been completed the servers should be switched on (if this is not already the case) and a check of the functionality of programs and data should be made. A fuller, more detailed check must be carried out at the earliest opportunity by all users.

4.9 No further updating of information is allowed until all users have confirmed that the data within SDM Housing Software, finance systems and other relevant systems is up to date.

4.10 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 Maintenance Contractor.

4.11 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.

4.12 Once the replacement host servers 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.

4.13 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.

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

4.15 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. Users must refer to the Password section of CHA's ICT Policy for further guidance on password standards.

4.16 As soon as the above procedures are completed and processing recommences, an insurance form must be completed, if appropriate, and submitted to CHA's Insurer.

4.17 Once normal business operations have been restored it will be necessary to return the responsibility for specific operations to the appropriate departmental managers. This process should be formalised using the form in **Appendix C** in order to ensure that all parties understand the change in overall responsibility from the Chief Executive in the role of business recovery process lead and the transition to business as-usual. It is assumed that departmental managers will be fully involved throughout the recovery, but in order for the recovery process to be fully effective, overall responsibility during the recovery period will sit with the Chief Executive.

4.18 These Disaster Recovery Procedures will be tested annually to ensure that they can be implemented in emergency situations. Testing will involve data recovery to a remote server, remote user connection to that server and time measurement for data/user recovery against the targets set out in section 5.5 of this document.

5 Risk Assessment

5.1 The risks outlined in 5.2 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

5.2 The Association has identified the following risks:

Risk	Probability	Impact	Total	Category
Complete loss of all systems & equipment	1	3	3	Low
Server Failure	2	3	6	Medium
Phone System Failure	1	3	3	Low
Website Failure	1	1	1	Low

5.3 The software/data risks outlined in 5.4 have been identified and categorised as follows:

Impact:

1 – Low	CHA can function without item longer term (>3 days)
2 – Medium	CHA can function without item medium term (up to 3 days)
3 – High	CHA cannot function without item

System:

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

Total: Impact x System
Category: 1-3 Low, 4-6 Medium, 7-9 High

5.4 The Association has identified the following risks:

System	Impact	System rating	Total	Category
MS Outlook: email, calendar & Contacts	3	3	9	High
Phone System	3	3	9	High
SDM Housing Software	2	3	6	Medium
Finance systems	2	3	6	Medium
Server Drives: CHA (Q); Finance (X:); Technical Services (T:); Housing Management (W:)	2	3	6	Medium
Server Drives: Management Team (U:); Corporate Services (R); Human Resources (V:)	1	3	3	Low
Integrator Database – SQL Server (Y:)	1	3	3	Low
Internet access	1	2	2	Low
Archive Documents	1	1	1	Low

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

Low: 5 working days
Medium: 3 working days
High: 2 working days if physical, 1 working day if software.

6 Checklists

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

7 Communications Plan

7.1 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	**Selected Staff member**
Staff Team	Depute Chief Executive
Customers	Depute Chief Executive
Suppliers	Technical Services Manager
Media	Chief Executive
Scottish Housing Regulator (SHR)	Chief Executive
Information Commissioners Office (ICO)	Corporate Services Officer

7.2 In the event of a disaster situation resulting in the loss or theft of personal and sensitive data the association must notify the ICO. Events notifiable to the ICO must also be considered notifiable to the SHR.

7.3 The following communication channels can be utilised to assist the communications plan. Instruction should be taken from the Depute Chief Executive 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	Corporate Services Officer
Social Media (cloud – always available)	Twitter and Facebook for text based situation updates.	Corporate Services Officer
Telephones (on premise, may not be available depending on disaster situation)	Two options can be implemented 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	Corporate Services Officer
SMS (cloud – always available)	Text customer base with situation updates	Depute Chief Executive
Email (cloud – always available)	Email suppliers with situation updates	Technical Services Manager

8 Monitoring and Review

8.1 Monitoring of the IT Disaster Recovery Plan will be undertaken by the Chief Executive. Reporting of any relevant incidents and annual testing results to the Audit & Risk Sub-Committee will occur as and when necessary. The report will include:

- A description of the emergency or incident
- Those people notified of the emergency
- Action taken by the Association
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Lessons learned

APPENDIX A: Disaster Recovery Checklist

	Procedure	Y/N	If N Action
1.	Have the following personnel been contacted? Chief Executive Depute Chief Executive Technical Services Manager Finance Manager Corporate Services Assistant Sabre Systems	Y/N **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.	If main office inaccessible, move server and notify all staff.	**Y/N**	
4.	Check equipment against IT asset list (Appendix D)	**Y/N**	
5.	Any missing/ damaged equipment? (If Yes attach list)	**Y/N**	
6.	Check if File Server operational? If YES proceed to ‘8’. If NO proceed to ‘9’.	**Y/N**	
7.	Onsite assistance sought from IT Support Partner for restoring from backup, etc. • SDM Housing Software Helpdesk contacted • Integrator Housing Solutions Helpdesk contacted	**Y/N** **Y/N**	
8.	Replacement server installed and tested?	**Y/N**	
9.	Check all connections to terminals & printers. If they are all operational switch on the Central Processor. **Do not input any new data at this stage.**	**Y/N**	
10.	Check set up of users and programs	**Y/N**	
11.	Identify the most recent backup and use to restore data	**Y/N**	
12.	Restore completed & checked	**Y/N**	

13.	Notify all users of the points that the system has been restored to i.e. date, time of last entries etc.	**Y/N**	
14.	Confirmation from all users that access levels and date is as it was before disaster	**Y/N**	
15.	**All** passwords changed and comply with password policy	**Y/N**	
16.	Double check the relevant check lists to ensure procedures completed	**Y/N**	
17.	Completed Insurance Form	**Y/N**	
18.	Submitted to Insurance Brokers	**Y/N**	
19.	Write report detailing the disaster event	**Y/N**	
20.	Report to Audit & Risk Sub-Committee and Management and Committee Date: Signed:	**Y/N**	

APPENDIX B: Examples of Disaster

Environmental Disasters
Flood
Snowstorm
Electrical storms
Fire
Subsidence and Landslides
Freezing Conditions
Contamination and Environmental Hazards
Pandemic/Work from Home

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
Cyber crime
Loss of records or data
IT system failure

APPENDIX C: Handover Form

<table>
<tr><th colspan="2">Handover of systems to department manager</th></tr>
<tr><td><b>Date of handover:</b></td><td></td></tr>
<tr><td colspan="2">I confirm that the work of the business recovery process has been completed in accordance with the disaster recovery plan and that normal business operations have been effectively restored.

<b>Chief Executive:</b>

<b>Signature:</b>

<b>Date:</b>

<b>Any relevant comments by the Chief Executive in connection with the return of business systems should be made here:</b></td></tr>
<tr><td colspan="2">I confirm that above business process is now acceptable for normal working conditions.

<b>Department Manager:</b>

<b>Signature:</b>

<b>Date:</b>

<b>Any relevant comments by the Department Manager in connection with the return of business systems should be made here:</b></td></tr>
</table>

APPENDIX D: IT Asset List

	Device	User	Location
1	HP Proliant DL20 Gen10 Rack Server Main File Server: Drive Drive Q (CHA; Drive R (Corporate Services); Drive S (Data Restore); Drive T (Technical Services); Drive U (Management Team); Drive V (Human Resources); Drive W (Housing Management); Drive X (Finance).	Server	Server cabinet
2	HPE DL360 Proliant Soluion Server 16GB 8 SQL Server: Drive Y (Integrator Database); Drive Z (SDM Database)	Server	Server cabinet
3	48 Port switch	Server	Server cabinet
4	Uninterrupted Power Supply x 2	Server	Server cabinet
5	Network Router	Server	Server cabinet
6	Ultima IEC 320 6 way PDU	Server	Server cabinet
7	Network Printer/Copier/Scanner		
8	Desktop Printer	CSO	
9	Desktop Printer		
10	Desktop Printer		
11	Desktop Scanner	CSO	
12	Desktop Scanner		
13	Desktop Scanner		
14	Desktop PC[1], 2 x Monitors, Keyboard, Mouse	CEO	CEO Desk
15	Desktop PC, 2 x 27inch Monitors, Keyboard, Mouse	DCE	DCE Desk
16	As above	TSM	TSM Desk
17	As above	FM	FM Desk
18	As above	CSO	CSO Desk
19	As above	HO	HM desk bank
20	As above	HO	HM desk bank
21	As above	HO	HM desk bank
22	As above	HO	HM desk bank
23	As above	HO	HM desk bank
24	As above	FA	HM desk bank
25	As above	TSO	TS desk bank
26	As above	TI	TS desk bank
27	As above	TSA	TS desk bank
28	As above	CSA	CSA desk
29	As above	CSA (Hub)	CSA (Hub) desk
30	As above	Multi-user	Reception desk

[1] Lenovo V530S -071CB Core i5, 8GB 256GB

31	Desktop PC, 1 x 27inch Monitor, Keyboard, Mouse	Multi-user	Hub Room 1
32	Desktop PC, 1 x 24inch Monitor, Keyboard, Mouse	Public	Reception area
33	As above	Public	Reception area
34	As above	Public	Reception area
35	HP Laptop, Mouse, Headset	CEO	Home
36	Lenovo Laptop, Mouse, Headset	DCE	Home
37	Lenovo Laptop, Mouse, Headset	TSM	Home
38	Lenovo Laptop, 24inch Monitor, Mouse, Headset	FM	Home
39	HP Laptop, Mouse, Headset	CSO - EM	Home
40	HP Laptop, Mouse, Headset	HO - JH	Home
41	Lenovo Laptop, Mouse, Headset	HO - IMcM	Home
42	Lenovo Laptop, Mouse, Headset	HO - LC	Home
43	Laptop, Mouse, Headset	HO - PMcM	Home
44	HP Laptop, Mouse, Headset	HO - CC	Home
45	Acer Laptop, 24 inch Monitor, Mouse, Headset	FA	Home
46	HP Laptop, Mouse, Headset	TSO	Home
47	HP Laptop, Mouse, Headset	TI	Home
48	Lenovo Laptop, Mouse, Headset	TSA- NMcL	Home
49	HP Laptop, Mouse, Headset	CSA	Home
50	Lenovo Laptop & Mouse	Hub users	
51	Lenovo Laptop & Mouse	Hub users	
52	65inch Smart TV	Reception	Reception area
53	65inch Smart TV	Hub users	Hub Room 3
54	75inch Smart TV	Hub users	Hub Room 3
55	65inch Smart TV	Staff users	Staff Breakout

APPENDIX E: Key Contact Details

Redacted for GDPR purposes.