CLYDESDALE HOUSING ASSOCIATION LIMITED

Policy:	Data Back Up Strategy
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.

1. Purpose

1.1 Clydesdale Housing Association (CHA) recognises the need to take regular backups of important data, and make sure that these backups are recent and can be restored. By doing this, CHA will ensure that the organisation can still function following the impact of flood, fire, physical damage or theft.

1.2 Furthermore, a good plan for backing-up data will help CHA recover more quickly from cyber-attacks such as ransomware attacks.

2. Backup Strategy

2.1 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.

2.2 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.

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

2.4 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.

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

2.6 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.

2.7 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;

2.8 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.

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

2.10 <u>On-Site Back-Up</u>:

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

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

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

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

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

2.11 Off-Site Back-Up:

2.11.1 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.

2.11.2 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. Data Recovery

3.1 CHA's IT Maintenance Contractor will lead any data recovery activity required and liaise with the CEO and CSO on an ongoing basis as systems become operational.

3.2 Priorities for bringing systems on-line will be as follows:

Priority 1:	Microsoft Outlook – email, calendar & contacts
Priority 2:	SDM Database – SQL Server (Z:)
Priority 3:	CHA (Q); Finance (X:); Technical Services (T:); Housing Management (W:)
Priority 4:	Management Team (U:); Corporate Services (R); Human Resources (V:)
Priority 5:	Integrator Database – SQL Server (Y:)
Priority 6:	Internet Access

3.3 CHA will ensure that an annual data recovery test exercise is carried out that includes establishing remote server access for a sample of staff Users. Results of this test will be evaluated and action taken to address any weaknesses in order to improve CHA's business continuity arrangements.

4. Data Retention

4.1 CHA's Privacy Policy includes a Data Retention Schedule which lists the type of data CHA will retain on record, how long the record will be maintained and when it will be destroyed.

5. Applicability

5.1 This policy is applicable to all CHA employees and all official corporate records.