ICT Access Control

1. Background

Abbeyfield The Dales Ltd. (ATD) shall control access to its information to help ensure its confidentiality and integrity.

2. Objectives

ATD is committed to providing services that enhance the quality of life for older people and developing services that will meet the needs of future generations. This commitment is based on the Mission and Values of ATD. ATD will also comply with all relevant and current legislation.

The aim of this policy is to:

- Prevent unauthorised access to, or use of, ATD's information; and
- To ensure ATD's information security, confidentiality, integrity and availability to appropriate parties.

3. Scope

This policy covers all individuals working for ATD at all levels and grades, including senior managers, officers, directors, employees, volunteers, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff (collectively referred to as staff in this policy).

4. Policy

4.1. Definition – Access Control

Enforcement of specified authorisation rules based on a positive identification of users and the systems or data they are permitted to access.

4.2. Requirements for Regulating Access

- Each user shall be given access to IT resources based on position and department;
- User activity shall be monitored weekly and reviewed for unusual, unauthorised, or illegal activity;
- User access may be suspended for:
  1. Five (5) consecutive failed logon attempts, where accounts will be locked for a period of fifteen (15) minutes after which further attempts can be made; or
  2. Unauthorised or illegal activity.
- All users shall be made aware of the Information Security Policy.

4.3. Management of User Access

- IT will be notified of new starters and the level of access required based on position and department. The Director of Operational and Shared Services (DOSS) or the Business Support Manager (BSM) will be responsible for notifying IT of new starters.
- Once DOSS or BSM are notified of leavers, they will disable the account of the leaver immediately, and any associated emails redirected to a delegated user. Accounts for leavers will then be deleted thirty (30) days of leaving.
- Access to ATD information shall be granted on a need-to-know basis. Users shall be authorised according to minimum access requirements for their duties. Access may be

'read only', 'read/write', or 'full access' and users may or may not be given administrative privileges for their computers and for certain data.

- When a staff member changes role, in addition to advising IT of the relevant file system and application rights required, the manager must review the access rights from the previous role and advise IT what rights for applications and file system should be revoked.
- Contractor's accounts will be formally requested by e-mail detailing the reasons for the access and disabled when not required.
- Password control:
  1. Password must be six (6) characters or more in length.
  2. Default passwords must change upon initial login.
  3. Users shall change their passwords at least every ninety (90) days. If a user password has not been changed in that time, an account lockout will occur, and the user will have to contact the DOSS or BSM to reset the password.
  4. Passwords will not be used consecutively. There is a system in place to keep password history to prevent reuse for twenty-four (24) cycles.
  5. Users must not share their passwords with other staff.

4.4. User Responsibilities

- Users must secure their equipment by manually locking the PC screen if it is to be unattended for any length of time. Screen locks will automatically activate after 10 minutes of inactivity; and
- Users shall have direct access only to services and information that they have been specifically authorised to use. Unless expressly authorised, access to all resources and services is denied.

4.5. Operating Systems Access Control

- Access to operating systems shall be limited to trusted, authorised users i.e. IT support staff, contractors.

4.6. Asset Management

- All IT equipment will be purchased by the IT department this will include PC's, printers, fax machines etc;
- The DOSS will maintain an inventory of all ICT assets including software, hardware; this will include PC model/make, printers, fax machines etc; and
- Equipment will not be moved from one location to another or disposed of without written consent from the DOSS.

4.7. Server Room Access

- Access to the server room must be both controlled and restricted.
- Access control will be by numeric keypad lock.

4.8. Protection Against Malicious Software and Hacking

- All systems will be protected by a multi-level approach involving firewall, router configuration, e-mail scanning and virus protection on all workstations on the ATD network.

4.9. System Backup

System backups will be performed by the IT provider as detailed below:

- Daily during each evening an online and onsite backup of the system is made; and
- Backups of the system are kept for the 31 days.

4.10. Management of Network

- The configuration of critical routers, firewall and other network security devices will be the responsibility of, and maintained by, documented and kept securely by the IT provider;
- All Local Area Network (Lan) to Lan Virtual Private Networks (VPN's) are encrypted across all sites; and
- To comply with data protection and to prevent the loss of confidential information, data transfer to and from USB, CD and DVD drives is disabled on all machines within ATD. Requests to enable use of a USB or CD/DVD drive must be submitted to the DOSS.

4.11. Application Access Control

- Access to applications shall be limited to authorised users; and
- Access to applications shall be on a role-based requirement.

4.12. Monitoring System Access/Use/Errors

- Instances of access and use of any IT resources shall be automatically logged.
- IT periodically stores access control logs (as detailed below) and present a status report to the DOSS on request.
    1. Account logon events;
    2. Account management;
    3. Privilege Use; and
    4. System Events.

4.13. Phone Lines & Broadband

- All phone line requests and broadband connections for ATD must be raised with the DOSS.
- All phone bills must be submitted to the DOSS for payment. No phone bills may be paid at house/care home level.

4.14. Responsibilities

Users are responsible for knowing and following the policy.

IT Department (System Administrators) are responsible for:

- Review access requirements.
- Reviewing system logs.

5. Finance, Value for Money & Social Value

N/A

6. Supported Appendices

N/A

7. Linked Policies

Computer and Internet Usage (LG009P)
Data Protection (LG013P)
Information Security (LG023P)

8. Legislation/Regulation

N/A

9. Review

Every 3 years, subject to regulatory and legislative changes.

10. Procedure/Guidance

N/A