PATHWAYS ABILITIES SOCIETY

POLICY: INFORMATION TECHNOLOGY STANDARDS AND GUIDELINES
Applies to: All Personnel, Volunteers and Persons Served

PREAMBLE

Most of Pathways Abilities Society's financial, administrative and personal data for the individuals served is accessible through the society network. As such, they are vulnerable to security breaches that may compromise confidential information and expose the Society to losses and other risks. As Pathways Abilities Society security is critical to the physical network, computer operating systems and application programs, each area offers its own set of security issues and risks.

Confidentiality, privacy, access, accountability, authentication, availability and information technology system and network maintenance are components of a comprehensive policy. This policy identifies key concerns and issues faced by the society at the application, host and network levels and strives for security of critical information and systems.

This policy compliments the Internet Usage policy and procedures.

POLICY

Confidentiality and Privacy

The society and all staff, volunteers and individuals receiving services are obligated to respect and protect confidential data. There are, however, technical and legal limitations on our ability to protect confidentiality. For legal purposes, electronic communications are no different than paper documents. Electronic communications are, however, more likely to leave a trail of inadvertent copies and more likely to be seen in the course of routine maintenance of computer systems.

Documents that contain personal information that are sent via email must be encrypted with a predetermined Pathways password.

The society permits incidental personal use of computers to staff, volunteers and individuals Pathways Abilities Society serves with preapproval from supervisory or management staff. No employee, volunteer or person receiving service should have any expectation of privacy as to his or her Internet or computer usage. The society has the right to examine computer records or monitor activities of individual computer users to protect the integrity or security of the computing resources or protect the society from liability, to investigate unusual or excessive activity, to investigate apparent violations of law or society policy, and as otherwise required by law. In limited circumstances, the society may be legally compelled to disclose information relating to business or personal use of the computer network to authorities or, in the context of litigation, to other third parties.

Personal Devices
Staff and individuals can use their own personal technology devices for work related documentation and activities with individuals. Network passwords are obtained from the management personnel. Employees choosing to use their devices will not be reimbursed for costs associated with operations unless pre-approved by management. Employees should not have any expectation of privacy while using his or her own personal device at work.

Staff are not permitted to take individual's pictures using their personal cellphones or of Pathways' documents without prior approval from their immediate supervisor or a manager.

The supervisor or manager will review the person's Community Support and Consent form and or consult with the person and or their substitute decision maker prior to taking any pictures using society cellphones.

Access
No one may access confidential records unless specifically authorized to do so. Even authorized individuals may use confidential records only for authorized purposes. This policy requires that staff, volunteers and persons receiving service of the society respect the privacy of others and their accounts, not access or intercept files or data of others without permission, and not use another's password or access files under false identity. Violators of any of these rules are subject to discipline consistent with the general disciplinary provisions.

Technology assets are housed in an appropriately secure physical location. Technology assets include servers, personal computers that house systems with controlled access (laptops are a category of special consideration), ports (active ports in public areas), open wireless sensing devices, modems and network components (cabling, electronics, etc.).

Laptops and IPads are either assigned to a specific person or are portable and used by different people in different areas at different times. Employees who have laptops assigned to them are responsible for their general care including storage and use in a secure location. Laptops available for use by all staff must be signed in and out.

Passwords help protect against misuse by seeking to restrict use of society systems and networks to authorized users. Each staff person is assigned a unique password or passwords that are to be protected by that individual and not shared with others. Volunteers and persons receiving service are not authorized to access the server without permission from management personnel.

Employees who create usernames and or passwords to internet sites to conduct society business notify the executive director or designate. He/she enters the information in either the Website Access information list in ShareVision or in the file Management/ Information Technology/ Pathways Login Password or in the file Executive Director/ Administration/ Security Information/ Computers/ Management Passwords.

Management personnel track general website access information in the Website Access Information list in ShareVision. This ensures continuity of society business. The

executive director tracks society staff usernames and passwords in the file Management/ Information Technology/ Pathways Login Password. The file is accessible only to management staff. The executive director tracks management's usernames and passwords in the file Executive Director/ Administration/ Security Information/ Computers/ Management Passwords. The file is accessible to the board president and executive director.

Management will ensure that controls are in place to avoid unauthorized intrusion of systems and networks and to detect efforts at such intrusion.

Only those authorized by the board of directors or management personnel can make changes to the society websites.
Pathways utilizes systems and services that enhance access options for the people we support. This includes SMARTboard technology for teaching sign language and local and provincial access agencies.

Accountability
Individual users are responsible for ensuring that others do not use their system privileges. In particular, users must take great care in protecting their usernames and passwords from eavesdropping or careless misplacement. Passwords are never to be 'loaned.' Individual users will be held responsible for any security violations associated with their usernames.

If staff, volunteers or persons receiving service believe a security incident has occurred, they will immediately notify management. Management assesses the potential implications of the incident, notifies Network Technology Services and takes any remedial and necessary action.

Before adding new software to society computers and networks, system defaults are carefully reviewed for potential security holes and passwords shipped with the software changed. Downloading software, particularly software that is not job-related or endorsed by management, may introduce security risks and is not permitted.

Authentication, Network Maintenance and Disaster Recovery
Network Authentication is required for all systems that send or receive sensitive data. ShareVision backs up the data daily. Backups of data is maintained in secure off site storage to guard against the impact of disasters. Select information stored on the Pathways ShareVision SharePoint system site is backed up quarterly, internally.

Virtual Data Corporation (VDC) maintains systems and networks on site or through remote maintenance and access support. They provide full daily offsite backups of all servers to a secondary secure data center that they own and keep eight weeks of retention in need of potential disaster recovery. Representatives of the company follow all society policies.

In the event of a power outage refer to the Power Outage policy and procedure. In the event of internet system shutdown, policies and procedures are accessed on flash drives at each service location. Individual's binders have hard copies of important individual information. The On-Call binder has basic society information to reference

and the executive director has an emergency folder with individual, staff and basic society information.

Annually in the month of October a continuity/disaster recovery test is completed.

Reporting Violations
All staff, volunteers and individuals receiving services using computers, networks, or applications systems are responsible for reporting any apparent violations of law, or society policy to management whenever such violations come to their attention.

Technology Plan
The society maintains an annual technology plan to ensure that Pathways Abilities society is keeping pace with the current technological needs of the Society.

Disposal of Hardware
Electronic devices including but not limited to computers, photocopy machines, and telephones will be disposed of as outlined in Pathways Abilities Society's Disposition of Inventory policy and procedures. Confidential information is completely removed from all systems with no ability to recover.

Effective/Revision Date	Board Approval	Date Approved
October 24, 2005		October 24, 2005
January 18, 2009		January 18, 2009
June 21, 2010		June 21, 2010
January 24, 2011		January 24, 2011
September 12, 2011		September 12, 2011
January 28, 2013		January 28, 2013
August 1, 2013		August 1, 2013
September 14, 2015		September 14, 2015
June 12, 2017		June 12, 2017
March 25, 2019		March 25, 2019
March 22, 2020		March 2, 2020