PATHWAYS ABILITIES SOCIETY

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

Effective/Revision Date:
October 24, 2005
March 29, 2006
September 29, 2006
February 6, 2007
May 5, 2008
June 21, 2010
February 1, 2011
June 6, 2011
September 12, 2011
May 2, 2012
August 23, 2012
February 12, 2013
August 1, 2013
April 2, 2014
April 15, 2014
May 25, 2015
September 14, 2015
July 4, 2016
March 25, 2019
March 2, 2020
April 6, 2020
June 24, 2020

General

1. All employees and volunteers using the Internet facilities of the agency are required to sign an Internet Usage Statement form upon hire and annually thereafter in January at their evaluation via ShareVision.

2. The executive director or designate issues personal user identification and passwords including the password to access wireless connections at Pathways facilities.

3. Employees who create usernames and/or passwords to internet sites to conduct society business notify the executive director or designate. They enter the information in 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.

4. Management personnel track general website access information in the Website Access Information list in ShareVision. 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.

5. Each employee, volunteer and individual receiving services using the internet facilities of the agency will identify themselves honestly, accurately and completely (including one's

agency affiliation and function where requested) when participating in chats or newsgroups or when setting up accounts on outside computer systems.

6. When downloading a file scan for viruses before accessing it.

7. When sending documents through email with personal information the document must be encrypted with the predetermined, Pathways approved password.

8. If an employee, volunteer or person served accidentally connects to a site that contains sexually explicit or offensive material, they must:
- Disconnect from that site immediately, regardless of whether that site was previously deemed acceptable by any screening or rating program.
- Report the incident to their immediate supervisor.

9. Employees must log off when not using a computer and at the end of the day and leave the computers on unless otherwise instructed not to.

10. An employee or volunteer wanting to use a computer and the Internet facilities for personal usage contacts their immediate supervisor and obtains approval.

11. An employee or volunteer wanting to use their own personal device at work obtains permission from their immediate supervisor or management personnel.

12. The executive director or designate is responsible for changing and updating usernames and passwords when required and when a person exits Pathways (refer to the Exiting Pathways policy and procedure).

11. A technology plan is developed annually in the month of April.

12. Portable laptop computers are signed-out for usage through the on-site supervisor or manager when being taken out of the building.

Computer Support

1. Virtual Data Corp (VDC) is our current technology provider. Standard support hours are Monday to Friday 8:00 am to 5:00 pm Central Time. Emergency support is available 24/7 365 days a year.

2. To ensure the quickest response times, please email support@virtualdata.com with the following information or call toll free 1-888-683-9543 (Press “2” for Support, after hours Support press “9”):
- Your name, company name, and contact telephone number.
- Description of the support issue.

Laptops and Mobile Devices Taking off Site

1. Staff requiring a laptop or mobile device to take off site or to borrow for internal use emails their immediate supervisor or manager for permission.

2. If the person is authorized to take the laptop out regularly, they complete the ShareVision list “Taking Computers Off Site” each time.

3. The supervisor or manager monitors the list and ensures the laptop or mobile device is returned.

4. Mobile devises and laptops issued to specific staff must be returned at the end of the employee's employment.

ShareVision

1. ShareVision servers are backed up by ShareVision daily.

2. The following ShareVision lists are backed up quarterly on September 30, December 31, March 31 and June 30 by the Activity Quality Assurance Manager (AQAM): Attendance, Bike Pick Ups, BikeWays, Goal Progress, Incidents, Individual Calendars, Individual Goals, Individual Information, Announcements, Volunteer Attendance Tracking, Notables, People, Organizations, Profiles, Service Referral Tracker, ISP (ISP and Personal Information Bank content types), Applications, and Pathways Service Announcements.

3. The AQAM exports the above lists to an Excel Spreadsheet, saves them on the server and copies them to an external storage device.

4. The AQAM archives the following lists annually in the month of January: Notables, Attendance and Agency Announcements.

5. The AQAM exports the above lists to an Excel Spreadsheet, saves them on the server and copies them to an external storage device.

6. The backup external storage device are kept in the safe at 123 Franklyn Road.

Technology Plan

1. The executive director in consultation with the leadership team develops a Technology Plan annually in the month of April and concludes the previous year's action plan.

2. Copies of the plan are given to the board of directors for approval.

3. The executive director develops, implements and monitors the Technology Action Plan and reports monthly on the plan's progress at the leadership meetings.

Disaster Recovery

1. Annually in the month of October the AQAM conducts a continuity/disaster recovery test. They document the results in the Emergency Response Drill ShareVision list.

2. In the event of a power outage refer to the Power Outage policy and procedure. Notify a manager or supervisor.

3. In the event of internet system shutdown, policies and procedures are to be accessed on flash drives at each service location. Individual's information is accessed via their binders.

4. Notify VDC.

5. Refer to the On-Call binder for basic society information.