Blue Water Developmental Housing, Inc.

Technology and System Plan

2018 - 2019

Description

Blue Water Developmental Housing, Inc. (BWDH), CARF accredited, utilizes various forms of technology to implement and execute daily organizational functions. The technology used includes telephone systems, fax machines, and computers. It is the practice of the organization to implement and review a technology and system plan (TSP) annually for relevance and update as needed. Annually completing a TSP allows the organization to support *Information Management* and performance improvement activities for *Program/Service Delivery and Business Functions.*

Backup Policies What is our back up system?

A cloud based back up system, Storagecraft, which is a managed cloud storage for the organization. We also have a local backup system that includes volume shadow copy.

Assistive Technology

BWDH will use assistive technology as is necessary for staff to perform their work. Assistive technology devices that would be useful to consumers are used as necessary and available.

Disaster Recovery Preparedness

In the event of destruction of computers or the network, BWDH has a policy through Michigan Millers Mutual Insurance Company to replace equipment. BWDH will utilize Storagecraft, to replace all confidential information stored on the network including medical and personnel files. BWDH has an arrangement with Advanced Digital Solutions (ADS) to provide network maintenance services and would be available to help with any disaster recovery tasks.

Hardware

ACTION PLAN	TIME LINE	OUTCOMES
Inventory of all Technology	Every year	*BWDH Inventory 2019* (S:\Technology\Technology Inventory)
General Equipment:	Every 5 to 7 years	Equipment will be purchased and replaced within specified timelines.
Administrative Equipment:	Every 3 to 5 years	Equipment will be purchased and replace within specified timelines.

Software

ACTION PLAN	TIME LINE	OUTCOMES
Microsoft Office 2016	Every 3 years	Operating system purchased in November 2017 and installed on all desktops.
Microsoft Outlook 2016	Every 3 years	Internal email for all locations.
Sage	Every 3 years	Finance Department
Nova Time 4000 Starbox: Cincinnati Time Systems, Inc.	Every year	Utilized by the finance department to cover 500 employees. There is a software maintenance agreement with Cincinnati.
Paycor	Every 3 years	Applicant tracking, onboarding, payroll, learning management, benefit administration, and payroll is processed through Paycor
Quick Mar	As needed	Program utilized for online administration of medications.

Confidentiality and Security

Confidentiality and security will be assessed yearly by way of the HIPAA Security Assessment. Listed below are tools to prevent unauthorized access and virus protection for the organizations internal transactions and office systems.

ACTION PLAN	TIME LINE	OUTCOMES
Virus protection:	Every year	The organization purchased Symatec as its virus protection software in April 2017, replacing the recent virus protection software AVG. Symatec has been installed on all desktops
Firewall	Every year	Symatec has a built in Firewall and is being utilized in all desktops. The administration office utilizes Guard Firebox 330 for the server
Password Protection: Employees are prohibited from sharing their passwords with others. Sharing of passwords will lead to disciplinary action up to and including dismissal.	As needed	Each workstation with a computer is password protected and can be changed upon the request of the Executive Director. OASIS, an approved software for electronic transactions requires password change every 90 days when not in use.
Server Protection Server is located at BWDH administrative office.	Every 3 months	Access to server files, located in air-conditioned locked room, are given to administrative staff upon approval by the executive director.
Encryption of Email	Every year	BWDH has purchased an email encryption through Microsoft which allows any PHI and/or secured information sent via email by the administrative staff is encrypted, which will not allow any breach of information.