CAMDEN COUNTY DEVELOPMENTAL DISABILITY RESOURCES

TECHNOLOGY PLAN

(Revised September 18th, 2017, August 13th, 2020)

This Technology Plan provides an overview of Camden County Developmental Disability Resources (CCDDR) information technology (IT) systems, security, confidentiality, and disaster recovery. CCDDR utilizes IT for a variety of reasons, including:

- To allow staff to adequately do their jobs
- To provide for informed decision-making both with regard to administrative as well as programmatic functions based upon analysis of available data
- To provide those served with quality services and supports

The following information summarizes CCDDR's Information Technology system, compliance with current regulations and guidelines, and action plan needed to enhance or improve CCDDR's current IT system and/or required for compliance issues. All IT needs identified in this plan shall be incorporated as budget items and/or otherwise approved by the Board of Directors in CCDDR's current year budget or proposed budget for future fiscal years.

Agency Hardware/Software/Network Systems

The status of CCDDR hardware and system software plays a vital role in allowing staff to properly complete their work. Systems in place must meet industry standards as well as standards specific to the work to be accomplished at CCDDR. In addition, computer systems play a role in assuring that all computer users have the capabilities to follow through on security and confidentiality procedures, as well as continual operation in case of theft or disaster.

Hardware

CCDDR currently has portable computer (laptop) systems in place for each employee; wireless multifunction printers and scanners with fax capability for each workstation, which are also portable if necessary; routers, cloud keys, network switches, wireless access points for the Targeted Case Management (TCM) and Administrative offices; remote access connectivity for each office network; docking stations at each workstation for ease of connection to CCDDR's network; and all related accessories for each system. All CCDDR computer systems are periodically updated to allow for compatibility with the most recent software programs for compliance with our current technology plan. Any computer system or device not meeting with current system minimal requirements may not be installed to the CCDDR network system.

Software

All networks, systems, and computers now have the most recent versions of the Windows operating systems, most recent security software available in the market, and the most recent firewalls available in the market. Main software programs utilized on all desktop systems include Microsoft Office, Adobe Acrobat, Foxit, Windows Media Player, and other ancillary programs. All hardware is less than 5 years old. Operating system software, office software, network software, and other office programs are up-to-date and meet current industry standards, including the most recent security and encryption capabilities. Any system that does not meet the minimal software requirements may not be installed.

Data Management Storage Systems

CCDDR no longer utilizes an on-site server. CCDDR's records are stored on web-based data storage systems (aka "cloud"). CCDDR currently utilizes Office 365, which accommodates CCDDR's email and internal data storage. Office 365 has separate storage options, capacities, and sections, depending on the information being stored. Access to data is based on designated levels of employee security and access. Permanent client files are stored in Office 365 with restricted access, while other sections of Office 365 contain working folders and files for employee use. A web-based accounting program (currently Quickbooks) is utilized for agency accounting purposes, and a web-based TCM program (currently SETWorks) is utilized for TCM services and client information pertaining to services provided and received as well as serving as the billing software for Medicaid claims.

CCDDR also utilizes a third-party data back-up system (currently Datto SaaS). A back-up system eliminates the loss of data/records or misfiling of data/records and emails.

IT Manager and Consultant

CCDDR utilizes a third-party IT manager/consultant (currently Corporate Business Systems, owned by Sumner One). The IT manager/consultant will ensure CCDDR's technology solutions continue to be modernized. The IT manager/consultant is also responsible for systems security, updates, and ongoing maintenance, which can predominantly be done remotely as long as the devices are connected to the internet.

Inventory

Inventory of all systems, with their current operating capacities, date of activation, and current authorized users are updated on a regular basis by the Compliance

Manager and IT Manager/Consultant. Any computer not included in the inventory list may not be installed on the CCDDR network/internet.

Security/Confidentiality

Security and confidentiality practices are the most important aspect of any organization working with sensitive, confidential information. CCDDR's current practices allow for complete protection of sensitive information from unauthorized outside and inside intrusion, as well as proper procedures for handling sensitive and private information electronically through such mediums as e-mail, network, or internet.

Password Security

All users have individual usernames and passwords that comply with industry standards and eliminate unauthorized access. All passwords must meet the following requirements:

- Not a word in the dictionary
- Are 9 or more characters in length
- Include a case sensitive character
- Include a number or character

Separate passwords are to be used for the accounting and TCM program systems.

Keeping or making hard copies of usernames and passwords for an extended period of time is prohibited. Employees are instructed to devote them solely to memory and not share them with unauthorized personnel. Passwords should be changed periodically. Temporary copies for general use should be destroyed after devoted to memory or the task completed. Passwords are not to be shared with other CCDDR staff, family members of staff, etc.

File & Network Security

CCDDR promotes flexibility and efficiency for staff to complete job assignments and meet the needs of the clients served; however, to prevent unauthorized access to confidential information and to protect the integrity of the data, the following must be adhered:

- All digital information, folders, and files are organized by staff and personal files/folders are only accessible by authorized users
- All files that need to be protected and are confidential must be stored on the data management storage systems or temporarily stored on devices issued to staff (laptops)

- Only the Executive Director, IT manager/consultant, or other staff authorized by the Executive Director have the proper security rights to administer the network
- All networks are username and password protected and can be accessed remotely by CCDDR staff
- Employees working remotely should save files directly to the data management storage systems or the devices (laptops) issued to them, immediately transferring and saving any data to the data management storage systems the next day in the office if there was no internet connection available at the time the data was created and/or saved
- No personal computers or other computers not owned or leased by CCDDR shall be used for conducting CCDDR business when protected or sensitive information is involved, which includes (but is not limited to) private or confidential client information, private or confidential employee information, private or confidential agency information, and the use of CCDDR's email system – the use of any personal computer or computer not owned by CCDDR must be approved by the Executive Director beforehand.
- No private or confidential information should be saved to an external drive or disk – information not private or confidential can be saved to external drives or disks owned by CCDDR, but this information must be also be saved to the data management storage systems or the devices (laptops) issued to them
- Private or confidential files submitted as attachments over the internet, names within the context of electronic transmissions, and other private of confidential information must be encrypted, either through CCDDR's email encryption or the State of Missouri encryption email system
- Settings on all devices issued to staff (laptops) will require re-entry of the username and password after 10 minutes of inactivity

Individual Firewalls

In addition to a Network firewall, firewalls are used on devices issued to staff (laptops) as an additional precaution.

Staff Requirements for Remote Use of the Online Programs and Data Management Storage Systems

The online programs and data management storage systems, including state-operated data management storage systems, are designed for user convenience and can be accessed from other computers via the internet. Nevertheless, security and confidentiality of client and other private information needs to be maintained. The following guidelines apply to all CCDDR employees when accessing the programs and data management storage systems remotely:

- Staff will only access the programs and systems from their assigned device (laptop) and not in the direct view of others, including (but not limited to) family members and friends – access from a public place or public connection is prohibited
- No family members, friends, etc. are authorized to view private or confidential information
- Only private, secured connections with the same or similar security features as CCDDR's connection can be used to access the programs and data storage systems remotely
- Passwords for accessing the system is not to be written on paper or recorded via any other method accessible to any individual at the employee's home or other remote location

Counter Intrusion & Virus protection

Measures to control unwanted intrusions from outside attacks, such as viruses and hackers, are a real threat; however, with simple preventive technologies, such as firewalls and security protection software, and with proper training, this type of threat can be controlled and eliminated.

Counter Intrusion

To prevent unauthorized access to confidential information and to protect the integrity of CCDDR's data, the following must be adhered:

- Firewalls and security protection software are to be maintained and updated as necessary
- Equipment and software should be replaced if they become obsolete, damaged/corrupted, or can no longer provide the proper security settings to meet the current and future protection for use

Virus Protection

A managed virus security application will be maintained at all times. Updates, scanning, and other functions are to be managed using virus protection utilities to ensure real time administration of virus program activities and scanning results.

The most recent and best software in the market is utilized within all CCDDR devices (laptops) and network systems. In addition to device (laptop) and file scanning, the current security software has the following capabilities:

- Automatic daily updates of new circulating viruses
- Network management capabilities
- Low system resource usage
- Remote management
- Spyware/malware detection

Theft and Disaster Recovery

Theft and disasters, such as fire, flood, and natural disasters, are unpredictable and can often result in complete destruction of a company's digital information. However, with proper preventive measures, these threats can be managed and data can be recovered in a timely manner. To prevent the loss of data and digital information, the following must be adhered:

- Complete backups of work related data that are stored on all CCDDR data management storage systems simultaneously and/or daily –multiple online servers are utilized via third parties and can retrieve information quickly and reliably
- In addition to the data management storage systems, each employee issued device (laptop) creates data back-ups saved by historical points of reference for quick, easy data restoration to ensure quick recovery of data and increase the chances of retrieving lost or misplaced data

Disaster Recovery

All devices attached to the network can be replaced and restored to their original state after replacement of the hardware due to volume licensing and current procedures. Volume licensing allows software property to be defined by codes and serial numbers, which are digitally stored and cannot be lost. Once the new hardware is replaced, the software can be reinstalled using current operational licenses or OEM system software that came with the system.

A stolen system is useless without the proper passwords; however, the hard drive is vulnerable to hacking. Saving all confidential or vital company data on the web-based data management storage systems will make them unavailable in a stolen computer.

Staff Training

For any technology plan to be fully effective, employees must understand and be trained to follow proper network user protocols. Efforts must be made to continuously offer training to keep CCDDR network users up to date and informed about the network and network regulations. The following are a few of the concepts and tasks all users should know and be trained to perform:

- Network
- Local drive vs. network drive
- Folder vs. file
- Saving documents to network drives
- Understand network security
- Username/password & user permission
- Shared folders

- Network groups vs. single users
- Administrator vs. standard user
- Software and hardware
- E-mail security etiquette & concepts
- Virus scanning
- Types of e-mail viruses and how they spread
- E-mail attachments
- Spyware and adware awareness
- Using links delivered through e-mail and the dangers involved
- Fishing and e-mail scams
- Virus protection
- Reporting errors
- Virus and worm types
- E-mail vs. browser viruses

Staff training on these subjects is to be provided by an IT professional, the Executive Director, and/or a designated CCDDR employee periodically.

Accessibility

CCDDR needs to identify technology that is accessible to both staff and persons served. Technology in the workplace can either create barriers to persons with various types of disabilities, or, alternatively, be a liberating force for persons with disabilities. This is true not only in terms of hardware and software utilized by CCDDR employees, but also the ability to access the CCDDR website and other media sites.

Assistive/accessible technology products are specialty products designed to provide additional accessibility to individuals who have physical or cognitive difficulties, impairments, and other disabilities. When selecting assistive technology products, it is critical to find products that are compatible with the computer operating system and programs on a specific computer.

Some of the ways that employees should be able to customize their computer system include:

- Change font size, color, and type of text on screen
- Adjust text and background colors
- Adjust sound options including the ability to get audio information visually (such as closed captioning or audio descriptions for multi-media) as well as aurally
- Adjust timings
- Eliminate or modify the rate of flashing or blinking
- Touch screen applications
- Customize toolbars for easy access to buttons used most often

- Adjust keyboard settings to compensate for impairments, such as hand tremors, or people who use select fingers, one hand, or no hands
- Operate a computer with a keyboard instead of a mouse
- Increase the visibility of the cursor
- Add assistive technology products for specific disabilities
- Use an alternative kind of mouse because of mobility impairments

In addition, CCDDR's technology ideally should provide ways for employees to:

- Easily access websites
- Use e-mail to collaborate and communicate
- Use a word processing system to collaborate
- Share documents
- Manage large amounts of data
- Sort and manage files and folders

Internet Services

Having a website and other media sites for the agency allows for better outreach services to be conducted by CCDDR and would spread the word about our agency and what we do to assist persons with developmental disabilities. CCDDR will either employ third-party professionals or appoint an employee to maintain and update its website and media sites to ensure ease of access, continual reference for pertinent information, news of changes, announcements, etc.

IT Support Services

CCDDR utilizes the services of an IT manager and consultant for its data management storage systems and IT networks. The manager/consultant is responsible for network administration and problem-solving/repair on an as-needed basis. CCDDR also utilizes the IT support services, which is part of its web-based TCM program, for TCM billing, logging, and other recordable TCM services, as well as utilizing its web-based accounting system support services. CCDDR has access to the Department of Mental Health database, which is managed by the Department of Mental Health. Access to the Missouri Department of Mental Health database is controlled and regulated by the Department of Mental Health.