

**CDS Family & Behavioral Health Services, Inc.**

**Information Technology Five Year Plan**

**FY 18-19 through FY 22-23**

Submitted to
Jim Pearce
Chief Executive Officer

Prepared by
Information Technology Team:

 Diana Sanchez Tracey Ousley Zach Toundas
 Comptroller Chief Operations Officer Systems Administrator

|  |
| --- |
| June 2019**Mission:*****“Strengthening Communities by Building Strong Families”*** |
|  | Geographical Area:Alachua, Baker, Bradford, Columbia, Dixie, Gilchrist, Hamilton, Lafayette, Levy, Madison, Putnam, Suwannee, and Union Counties |  |
|  | 1218 NW 6th StreetGAINESVILLE, FL 32601(352) –244-0628 |

This publication can be made available in multiple media formats upon request.

Table of Contents

[Introduction 1](#_Toc227006754)

[Executive Summary 1](#_Toc227006755)

[Assessment 2](#_Toc227006756)

[Hardware 2](#_Toc227006757)

[Current Hardware Resources & Description of Use 2](#_Toc227006758)

[Objectives 3](#_Toc227006759)

[Software 3](#_Toc227006760)

[Current Software Resources & Description of Use 3](#_Toc227006761)

[Objectives 4](#_Toc227006762)

[Assistive Technologies 4](#_Toc227006763)

[Objectives 4](#_Toc227006764)

[Network Infrastructure 5](#_Toc227006765)

[Description 5](#_Toc227006766)

[Objectives 5](#_Toc227006767)

[Internet & E-Mail 5](#_Toc227006768)

[Description of Use 5](#_Toc227006769)

[Objectives 5](#_Toc227006770)

[Websites 6](#_Toc227006771)

[Description of Use 6](#_Toc227006772)

[Objectives 6](#_Toc227006773)

[Security 6](#_Toc227006774)

[Description of Security Measures 6](#_Toc227006775)

[Objectives 7](#_Toc227006776)

[Virus Protection 7](#_Toc227006777)

[Description 7](#_Toc227006778)

[Objectives 7](#_Toc227006779)

[Confidentiality 8](#_Toc227006780)

[Description 8](#_Toc227006781)

[Objectives 8](#_Toc227006782)

[Data Back-ups 8](#_Toc227006783)

[Description 8](#_Toc227006784)

[Objectives 8](#_Toc227006785)

[Disaster Recovery 8](#_Toc227006786)

[Technology Plan Recommendations Details 9](#_Toc227006787)

[Categorically 9](#_Toc227006788)

[Chronologically 10](#_Toc227006789)

# Introduction

Communication is fundamental to our services and Information Technology Resources are a fundamental asset in facilitating communication. CDS’ Information Technology Five Year Plan is intended to document the status of the organization’s use of technology and to provide goals for improving technology for administration and program support for participant services.

# Executive Summary

CDS operates six sites over four counties, with over 80 desktops computers and laptops. Our main strengths are a centrally managed adaptable and reliable coordinated, information management system; strong security, confidentiality, redundancy, backup, and virus protection protocols; an intranet site which provides staff easy access to all agency policies, forms, reports, and other important information; compatible productivity software deployed throughout the agency; and in-house support and maintenance on all IT resources. Among the challenges to be addressed in this Plan are insufficient network speed, replacing old workstations, updating our operating system (Windows XP/7), replacing old phone systems and addressing the need for more capacity and security for our servers.

In order to foster a high level of productivity and user satisfaction throughout the agency, CDS maintains on ongoing schedule of evaluation, maintenance, upgrade, training, and tracking systems. The top priorities for FY 19-20 have been identified as:

1. A necessary upgrade of the networking infrastructure
2. Replacement of outdated computers
3. Maintenance of all ongoing systems

What follows is a detailed assessment of all IT resources, as well as objectives to be met over the next five years. These objectives are then summarized in the Technology Plan Implementation Details section of this plan first arranged categorically and then chronologically.

# Assessment

## Hardware

### Current Hardware Resources & Description of Use

CDS has moved away from accepting donations from other agencies’ discarded equipment based on the realization that technology is changing so rapidly these acquisitions were coming too dated to integrate into our current system. Instead CDS has created a budget to update our technology in phases upgrading approximately one third of our equipment annually. *Critical Servers:* Our Primary General Use Server was upgraded earlier this fiscal year to address the need for increased capabilities, power and to extend the life of the server. A Backup General Use Server was also purchased to host replicated information that is mission critical on our Fiscal and Windows Login Servers. Moving to a virtualized and redundant platform has also provided increased security through ransomware available through this format. Plans are under review to move the Backup General Use Server from the 1218 building to the Bivens location to decrease the likelihood of a physical mishap or natural disaster.

Another key improvement implemented this year was the addition of a secure file share server (TrueNas) which is highly redundant, adds increased ransomware protections and takes the load off the primary server for file storage. While the primary server supports administrative and group functions, TrueNas supports local individual and team based activities.

CDS plans to implement an emergency disk drive that can be removed by Data Systems staff, placed in a lock box and moved to a more secure location in the event of a hurricane or other natural disasters.

*Desktops:*  CDS provides Desktops to personnel whose responsibilities require and benefit from their use (40 currently in use).

*Laptops:* CDS provides laptops to personnel whose responsibilities require and benefit from their use, including remote work when required (40 currently in use).

*Networking equipment:* Modems are provided and maintained by Internet Service Providers. Following them are our physical firewalls (joined together between offices via a Site-to-Site VPN), and then our switches.

*Printers:* CDS continues to maintain a low reliance on single user printers in favor of larger printers that are networked at each site for individual users to access from their work stations. These printers are easier to maintain, more efficient and in the long run less expensive than single user machines. Additionally, these printers provide multipurpose functionality as scanners fax machines and file storage for documents. CDS intends to complete a vendor review during this 5 year plan to ensure our equipment is up to date, competitively priced and properly maintained. *Phone Systems:* CDS phone systems have finite capabilities and with the advent of new technology have become antiquated. In this Plan cycle, CDS will explore moving to a VOIP (Voice Over Internet Protocol) phone cloud hosted system. It is anticipated by doing so technical support will be more responsive and less expensive. We also anticipate cost savings in hardware and cost per minute usage.

*UPS:* All servers’ desktops, firewall, non-laser printers, and phone systems are protected by APC UPS’s with appropriate power levels. It is our plan to phase out UPS’s where not required.

*Video Surveillance Systems* Our three residential sites are equipped with Video Surveillance systems. All three systems are centrally accessible.

*Training:* Online new-hire orientation training, annual required training, new-systems training, and user-identified training is made available to CDS personnel. Personnel required to access outside data systems are required to maintain training for security clearances to ensure the security of data in those systems.

*Inventory:* A ‘living-document’ inventory is being implemented by the Systems Network Administrator.

*Maintenance:* The Systems Administrator/IT Specialist completes or coordinates periodic maintenance and troubleshooting for IT resources. Servers are purchased with 3 year next-day, on-site maintenance agreements. Desktops and laptops are purchased with a 2-year manufacturer service warranty. Maintenance contracts are in place with the phone systems’ vendor. Internet Service Providers maintain routers.

*Applicable Policies:* • P-1067 Hardware

 • P-1074 Software and Hardware Standards

 • P-1007 Personnel Responsibilities in the Use of Information

 Technology Resources

### Objectives

1. Evaluate need for replacement and upgrades of IT resources.
2. Evaluate useful life of critical servers, and replace as needed.
3. Add an emergency removable backup drive
4. Replace outdated desktops, laptops, and other IT equipment.
5. Update Video Surveillance Equipment at the shelters
6. Conduct periodic maintenance on all equipment.
7. Implement and maintain an up-to-date inventory system.
8. Acquire an Asset Management server to supplement our inventory and maintenance systems
9. Review and update policies on an annual basis, and as needed.
10. Upgrade network infrastructure.

Replace phone system

### Current Software Resources & Description of Use

*Accounting Software:* The Fiscal Department utilizes SAGE 2017 software to complete financial and administrative functions.

*Human Resources:* Employee Navigator Human Resources software is utilized by our full-time HR Specialist in addition to Excel spreadsheets and Access databases. These systems facilitate the tracking of approximately120 employees and the multiple requirements associated with Human Resources.

*Management Information Systems (MIS):* The Data Systems Department utilizes Network Management Information System (NETMIS) as maintained through the Florida Network: Runaway Homeless Youth Management Information System (RHYMIS) for federally funded runaway youth; Homeless Management Information System (HMIS) for services provided to the homeless population; Juvenile Justice Information System (JJIS) for all youth served through our Residential and Non-residential CINS/FINS services: Florida Safe Family Network (FSFN) for youth and young adults receiving Independent Living services, and PBPS to record substance abuse prevention services *Productivity Software:* In order to ensure compatibility with major funding sources and stakeholders CDS utilizes Windows based Microsoft Office software, provided via Microsoft’s 501c3 grant programs. Other software for project specific needs is also acquired and utilized as needed.

*Training:* Online new-hire orientation training, annual required training, new-systems training, and user-identified training is made available to CDS personnel.

*Inventory:* CDS maintains current licenses for all its software.

*Maintenance:* Support/service agreements are maintained for Fiscal software.

*Applicable Policies:* • P-1068 Software

 • P-1074 Software and Hardware Standards

 • P-1007 Personnel Responsibilities in the Use of Information

 Technology Resources

### Objectives

1. Budget for annual replacement and upgrades.
2. Evaluate useful life of critical software on an annual basis, and replace as needed.
3. Evaluate software version upgrade needs on an annual basis, and replace as needed.
4. Conduct periodic updates on all software.
5. Schedule and implement all necessary training for personnel who access online systems.
6. Implement and maintain an up-to-date software inventory system.
7. Review and update policies on an annual basis, or as needed.
8. Stay abreast of changes associated with external data systems and ensure that we effectively incorporate any updates into our data collection, entry and management processes.

## Assistive Technologies

In cases where an employee or participant may benefit from assistive technology that would increase or improve their functional capabilities CDS will attempt to accommodate this need if it is fiscally responsible and/or if the need can be resolved through an applicable referral.

### Objectives

1. Remain informed of changes in the requirements of Title III of the Americans with Disabilities Act.

## Network Infrastructure

### Description

*Wide Area Network (WAN):* CDS’s WAN connects programs at six (6) separate sites in three (3) counties, namely: Gainesville-Bivens, Gainesville-6th Street, Gainesville-IYPC, Lake City-IYPNW, Lake City-SNAP/FA, and Palatka-IYPE. Connectivity is attained through a secure virtual private network over the internet, secure virtual private network (VPN) tunneling technology over the internet. ISP provided cable internet connections are relatively stable with a few exceptions which we intend to address in this Plan

*Local Area Networks (LANs):* CDS maintains wired and wireless LANs throughout each of our buildings to facilitate communications and provide efficient and secure sharing of information.

*Maintenance:* The Systems Network Administrator.is responsible for the day to day operations and coordination of network troubleshooting. The DSM is responsible for setting-up and upgrading/changing CDS’s network infrastructure.

*Applicable Policies:* • None

### Objectives

1. Evaluate the efficacy of current network infrastructure and communications providers.
2. Implement a backup WAN connection via 4G failover modems.
3. Review and update policies on an annual basis, or as needed.

## Internet & E-Mail

### Description of Use

*Internet & E-Mail Access:* As Federal, State, local funding agencies and other stakeholder’s reliance on internet communications remain standard operating practice, CDS makes internet & e-mail access part of normal day-to-day operations. This access allows us to respond in a timely manner and to stay connected to required web-based reporting systems and resources. CDS attains Internet connectivity and e-mail services via Internet Service Providers.

*Applicable Policies:* • P-1075 E-Mail Systems

 • P-1007 Personnel Responsibilities in the Use of Information

 Technology Resources

### Objectives

1. Implement e-mail retention policies to prevent the accidental or intentional deletion of CDS-relevant e-mailed communications
2. Review and update policies on an annual basis, or as needed.

## Websites

### Description of Use

*cdsfl.org:* CDS maintains this website to communicate to the community at-large all essential aspects of the organization, with recent additions such as events and job opportunities. Our public website is currently hosted on the Wix.com platform. This platform performs the necessary security updates, facilitates payments and donations, greatly improves community engagement through video updates and community input via Facebook participation and responding to survey requests E-mail addresses are linked to this domain.

*cdsgvl.org:* CDS maintains this site as an Intranet, intended for the use of personnel and stakeholders. It contains CDS plans, reports, policies, forms, organizational information, and personnel information.

*Maintenance:* The Outreach Specialist is responsible for the day-to-day maintenance of CDS’s Website and the COO and Data Systems department for CDS’s Intranet. The COO must approve all critical content changes.

*Applicable Policies:* • P-1076 Websites

 • P-1010 Policy Review Process

### Objectives

1. Maintain CDS domain registration.
2. Maintain websites’ contents to be current.
3. Communicate website changes with personnel.
4. Review and update policies on an annual basis, or as needed.
5. Maintain a Facebook presence to enhance awareness and communication regarding program services.
6. Limit access to CDS intranet to CDS staff and other approved users.

## Security

### Description of Security Measures

*Network Security:* The agency-wide network is controlled by the Data Systems Department. It supplies on-line computer systems access and internet access. Network connectivity is essential to using current systems such as Office 365, NETMIS, PBPS, FSFN, JJIS, and HMIS.

*Equipment:* All servers have reliable redundant technologies built into them. VMs take snapshots daily (in-time checkpoints to which a VM can be ‘rolled back’ in the event of a major deletion/corruption) and are backed up weekly. All servers and high-value PCs are protected by a UPS with an approximate 15 minute runtime minimum. In the event of a power outage, work can be saved and the server can initiate a shutdown safely. Fax Machines are located in secure areas.

*Data Security:* All users of e-mail and other contractually required Management Information Systems (NETMIS, PBPS, JJIS, and HMIS) have unique personal identifier(s) and password(s) assigned. These are assigned and/or controlled by the security officer and his/her designee(s) and are confidential. Hardware firewalls (via SonicWALL) are configured to block all traffic by default except for predetermined traffic via an allow list. Sign-ins that originate from outside our controlled private LAN are monitored for sign of unauthorized access, such as successful logins from foreign IPs associated with VPN’s commonly used by malicious actors.

*Physical Security:* The Business Continuity Emergency Preparedness Plan, Preparation Plan (Phase 1) addresses security measures in this area.

*Training:* CDS’s Security Awareness Training program is maintained by the Data Systems department.

*Applicable Policies:* • P-1072 Security

 • P-1007 Personnel Responsibilities in the Use of Information

 Technology Resources

### Objectives

1. Evaluate the adequacy of security measures.
2. Review and update policies on an annual basis, or as needed.
3. Schedule and implement all necessary training.

## Malware/Phishing/Scam Protection

### Description

CDS follows protocols to minimize damage from malware, phishing attacks, and email impersonation scams. In addition to antivirus software and firewall equipment, staff are instructed and trained on preventive measures. Suspicious emails are reported, content from those emails are added to a filter, and an organization-wide scan is run to find other copies of the emails to be removed from users’ inboxes. Multi-factor Authentication is set up for high-value targets.

*Maintenance:* The Systems Network Administrator has day-to-day responsibility for data protection practices.

*Training:* New-hire orientation training, annual required training, new-systems training, and user-identified training is made available to CDS personnel.

*Applicable Policies:* • P-1066 Virus Protection

 • P-1074 Software and Hardware Standards

 • P-1007 Personnel Responsibilities in the Use of Information

 Technology Resources

### Objectives

1. Evaluate software version upgrade needs on an annual basis, and replace as needed.
2. Conduct timely updates of virus definitions.
3. Review and update policies on an annual basis, or as needed.
4. Review and update protection policies regarding email-vectored attacks.

## Confidentiality

### Description

CDS systems are designed to ensure that the confidentiality of its participants is not compromised by the use of Information Technology Resources. Access to all participant systems is maintained by Data Systems personnel, when not directly controlled by the respective system’s non-CDS administration, such as when a new staff member requires a DJJ password. All systems allow for several levels of access that control inquiry and update capabilities to what an employee has a need to know. Each user is assigned a unique user ID and password, and is granted a level of access commensurate to his/her responsibilities. Any locally-stored data is also controlled via specific file access rights and permissions on an individual basis.

All devices which reach end-of-life are securely purged of confidential and identifying information.

*Applicable Policies:* • P-1073 Confidentiality Standards

 • P-1072 Security

 • P-1007 Personnel Responsibilities in the Use of Information

 Technology Resources

### Objectives

1. Review and update policies on an annual basis, or as needed.

## Data Back-ups

### Description

Data back-ups are completed daily on CDS’s critical systems and on a scheduled basis on other important information.

*Maintenance:* The DSM has overall responsibility for back-up practices.

*Applicable Policies:* • P-1065 Backups

 • P-1074 Software and Hardware Standards

### Objectives

1. Conduct daily backups on critical systems
2. Review and update policies on an annual basis, or as needed.

## Disaster Recovery

Refer to CDS’s comprehensive Business Continuity Emergency Preparedness Plan, Phases 1 – 4.

Technology Plan Recommendations Details

## Categorically

| Category | Objectives | Responsibility | Implementation Schedule |
| --- | --- | --- | --- |
| Hardware | 1. Evaluate need for replacement and upgrades of IT resources.
 | COO,, DSM, Systems Administrator | Annually: Apr. – Jun. |
| 1. Evaluate useful life of critical servers and replace as needed.
 |  Systems Administrator | Apr. – Jun. 2021 |
|  |  |  |
| 1. Add backup domain controller server
 | COO, DSM | Completed January 2020 |
| 1. Replace outdated desktops, laptops, and other IT equipment.
 | DSM, Systems Administrator | Annually: Apr. – Jun. |
| 1. Replace Video Surveillance Equipment in the residential shelters.
 | COO, Coordinators | April 2018 |
| 1. Conduct periodic maintenance on all equipment.
 | Systems Administrator | On-going |
| 1. Maintain an up-to-date hardware inventory system.
 | Systems Administrator | On-going |
| 1. Review and update hardware policies on an annual basis and as needed.
 | COO, DSMSystems Administrator | Annually: Oct. – Dec. and as needed |
| 1. Upgrade network hardware
 | COO, DSM Systems Administrator | Annually: Apr. – Jun. |
| 1. Replace phone system
 | COO, DSMSystems Administrator | May – August. 2020 |
| Software | 1. Budget for replacement, upgrades and subscriptions for software.
 | COO, Comptroller, DSM Systems Administrator | Annually: Jul. – Sep. |
| 1. Evaluate useful life of critical software on an annual basis, and replace as needed.
 | DSM, Systems Administrator | Annually: Apr. – Jun. |
|  |  |  |
| 1. Conduct periodic updates on all software.
 | Systems Administrator | On-going |
| 1. Schedule and implement all necessary training for personnel who access online systems
 | DSM | On-going |
| 1. Maintain an up-to-date software inventory system.
 | Systems Administrator | On-going |
| 1. Review and update software policies on an annual basis, or as needed.
 | COO, DSMSystems Administrator | Annually: Oct. – Dec.and as needed |
|  |  |  |
| 1. Stay abreast of changes associated with external data systems and ensure that we effectively incorporate any updates into our data collection, entry and management processes.
 | DSM | Ongoing |
| Assistive Technologies | 1. Remain informed of changes in the requirements of title III of the Americans with Disabilities Act.
 | COO, DSM, Systems Administrator  | On-going and Annually: Apr. – Jun. |
| Network Infrastructure | 1. Evaluate the efficacy of network infrastructure and communications providers.
 | DSM Systems Administrator | Annually: Jan. – Mar. |
| 1. Identify and implement a connectivity failover
 |  Systems Administrator | January- March 2020 |
| 1. Review and update network policies on an annual basis, or as needed.
 | COO, DSM Systems Administrator | Annually: Oct. – Dec.and as needed |
| Internet & E-Mail | 1. Evaluate the adequacy ISP providers.
 | COO, DSM, Systems Administrator | Annually: Jan. – Mar. |
| 1. Review and update internet and e-mail policies on an annual basis, or as needed.
 | COO, DSM | Annually: Oct. – Dec.and as needed |
| Websites | 1. Maintain CDS domain registration.
 | Systems Administrator  | Ongoing |
| 1. Maintain websites’ contents to be current.
 | COO, Outreach Specialist | On-going |
| 1. Communicate website changes with personnel.
 | EMT | On-going |
| 1. Review and update website policies on an annual basis, or as needed.
 | COO, DSM | Annually: Oct. – Dec.and as needed |
| 1. Limit access to CDS intranet to CDS staff and other approved users.
 | DSM | Under review by management and Systems Administrator  |
| Security | 1. Evaluate the adequacy of security measures.
 | DSM, EMT, Systems Administrator | Annually: Apr. – Jun. |
| 1. Review and update security policies on an annual basis, or as needed.
 | COO, DSM, Systems Administrator  | Annually: Oct. – Dec.and as needed |
| 1. Schedule and implement all necessary security training.
 | DSM, Data Systems Staff, HR Specialist | On-going |
| Virus Protection | 1. Evaluate software version upgrade needs on an annual basis, and replace as needed.
 | DSM, Systems Administrator | Annually: Apr. – Jun. |
| 1. Conduct timely updates on virus definitions.
 | Systems Administrator | Weekly |
| 1. Review and update virus protection policies on an annual basis, or as needed.
 | COO, DSM Systems Administrator | Annually: Oct. – Dec.and as needed |
| Confidentiality | 1. Review and update confidentiality policies on an annual basis, or as needed.
 | COO, DSM,  | Annually: Oct. – Dec.and as needed |
| Data Backups | 1. Conduct daily backups on critical systems
 | Comptroller, DSMSystems Administrator | Daily |
| 1. Develop and maintain a backup schedule
 | Systems Administrator | On-going |
| 1. Review and update data backup policies on an annual basis, or as needed.
 | COO, DSM, Systems Administrator | Annually: Oct. – Dec.and as needed |