Technology Plan

Clermont County Board of DD
Calendar Year 2019

Mission and Goals

The mission of the Information Technology (IT) Department of the Clermont County Board of DD (CCDD) is to enable, support and help our customers (the CCDD staff) make the most of information and technology so they can be the best at their jobs and deliver the CCDD mission. Annual input for technology needs and trends are collecting from stakeholders and committees on an ongoing basis. This input is analyzed and used to develop the technology plan.

2019 Goals

The goals of the IT Department are closely tied to the goals of the agency. The following goals have been defined for calendar year 2018:

Maintain or enhance the computing infrastructure that supports the technological needs of the CCDD.

Office 365

- Current Exchange server 2010 residing on an 8-9 year old physical server.
- Running Server 2008R2 end of support is one year away
- Moving to Office 365 where Email is hosted by Microsoft instead of locally
- More HIPAA compliant
- Will not lose access to Email in cases of natural disaster or Internet outage at Wildey
- DD users will always have the latest patched Office such as Word, Excel, Outlook
- Cost: Currently contacting resellers for pricing and installation. Estimate $5000 -$9000 including moving all DD Email to new platform

New Server

- Currently we have 2 Physical servers at Wildey besides our Exchange server that are using Server 2008R2 that are at end of life
- Need for larger capacity for growing needs such as adding consumer pictures to Gatekeeper as suggested from our last survey
- Gives more space for disaster recovery if one of the other physical servers goes down.
-

Replacing all windows 7 computers before end of life.

Services

The Information Technology Department of CCDD provides the following services to approximately 120 technology users:

1. Managing and maintaining the computing infrastructure
2. Includes servers, networking and connectivity, etc.
3. Includes monitoring for problems, malware/viruses, responsiveness, etc.
4. Email service and support
5. Telephone service and support
6. Website

Operations and Administration

Network/Server operations are maintained by the technology officer. We have two outside agencies that have familiarity with our systems and backup in case of emergency or if technology officer is not available.

Connectivity and Security

Information Technology provides local area network connectivity to CCDD staff at three sites. IT also provides remote access to mobile workers.

Clermont DD supports a user indicated Encryption system for sending E-mail using Barracuda encryption.

Each staff member is provided their own user ID and password to access the network. Their access rights to network resources as well as software applications are based on their job responsibilities. Requests to changes staff access rights must be submitted by a supervisor or director.

Email can be accessed remotely via an Internet connection using password-protected Outlook Web Access.

Agency policy dictates that user IDs and passwords are for their individual use and are not to be shared with anyone.

Internet connectivity is currently provided by Time Warner. We use standard firewall protection to protect against threats. All computers and servers have anti-virus protection.

Hardware

Hardware is maintained on an established schedule to reduce the possibility of hardware failures from interrupting board activities. Computers for staff are changed on a 3-7 year rotation depending on user processing requirements.

Software

The board has an established set of software that is utilized by staff based on their access rights. Standard software includes:

- MS Office 2010/2013 (Word, Excel, PowerPoint, etc.)
- Infallible Financial Software
- Gatekeeper – manages information on individuals we serve including waiver billing.

Access to software applications is granted based on a staff member's job responsibilities. Access rights are also fine tuned within the enterprise applications to ensure that staff only have access to data and functions that their role is authorized to have.

Backup and Recovery Policies

The IT department regularly conducts backups on all production systems. There are also recovery policies in place should a failure take place. Currently all backups are saved on a 4TB NAS system. We are in the process of moving our secondary NAS system at another building for remote backups. We tested User file recover earlier this year and test other server recovery each year.

Virus Protection

The agency utilizes industry standard software to provide virus protection to servers and staff PCs. Trend Micro Antivirus or Microsoft Security software is installed and regular updates.