

YCCC Technology Master Plan

FY Years 17/18 through 21/22

Eric Bourque

Date: 2/13/18

Table of Contents

- [Section 1](#)
 - SWOT
- [Section 2](#)
 - Equipment Life Cycle
- [Section 3](#)
 - Software Life Cycle
- [Section 4](#)
 - Cloud Computing Cycle
- [Section 5](#)
 - Projects and Initiatives
- [Section 6](#)
 - SWOT Analysis Action Plan
- [Section 7](#)
 - Departmental Growth and Development
- [Appendix 1](#)
 - Condensed 5 Year Punch List
- [Appendix 2](#)
 - Break Down of Planned Equipment

Section 1

Strengths, Weaknesses, Opportunities, Threats (SWOT) for the YCCC computing Domain

The following is the result of an internal departmental SWOT analysis with departmental staff. Additionally we included internal review forms for PHI, HIPAA, and GLBA regulations due to recent changes in borrower regulations which impact data protection and privacy.

Strengths

1. Blackboard Learning Environment
2. Virtual Server Environment Infrastructure
3. Wifi Infrastructure
4. In house database management for student information system
5. Server monitoring system
6. Good communication with stake holder groups
7. Maintain expected network resource/services up times

Weaknesses

1. Lack of policy for incidents which cover unauthorized use, lost, theft, or other negative actives against or on the YCCC computer network. Including account locks and other desktop incidents.
2. Lack of defined criteria for people to be allowed access to Student Information system data. Policy exists, but not published where it is accessible to community.
3. Computer desktop time outs, password protected screen savers, and log offs are not being used.
4. Computer updates, while centrally managed, require manual intervention to apply which is not being done on a regular schedule.
5. No audit schedule for file level security settings to ensure user access is properly administered.
6. Do not have department specific security and procedures for institutional data.
7. Lack of design and development process for implementing organizational application changes, such as Email system, which also includes security considerations.
8. The IT department does not have a full inventory system which tracks the movement of equipment and software. It also only partially tracks signed out equipment and licenses shared with staff and faculty.
9. Lack of Protected Health Care Information (PHI) security procedures which control and detail who has access to potential health documentation (such as employee records).
10. No SSL for secure communication of data off campus.
11. Lack of a full body computer equipment inventory
12. Only partial functionality for users to change passwords while off campus

Opportunities

1. New building constructions
2. Funding through grants
3. Microsoft cloud platform

4. Potential Expansion of departmental staff
5. Training funding

Threats

1. Inability to terminate accounts for employees who no longer work here in a timely manner.
2. Passwords not forced to be change periodically
3. Network vulnerability scans are not being performed on servers or desktops
4. Users do not understand that transmitting sensitive student data via email is not permitted by the GLBA guidelines. Example is financial aid transmitting student social security numbers.
5. Staff are untrained at recognizing network vulnerabilities and threats as they pertain to data security.
6. Poor state of internal departmental documentation
7. Users who are fully online users cannot easily change their account passwords
8. Windows update services for desktop clients not fully functional
9. Anti-virus software is being phased out by US Dept of Homeland Security
10. Age of the campus email server software.
11. 5/7 of network switch stacks are so old they are no longer supported by Cisco and can only be purchased on the refurbished market.

Conclusion

Breaking down the categories in the internal SWOT a clear delineating line can be seen in the trends. The majority of Threats and Weaknesses involve policy and culture shifts within the department and the campus at large. While these require less monetary investment then infrastructure fixes, they do require time and consistency to implement and enforce. In contrast the majority of the Opportunities and Strengths reflect physical assets and infrastructure. This illustrates the recent investments and pushes in this area to improve existing systems. However to maintain these items as Strengths and Opportunities they must equally be maintained and shepherded in a forward direction through scheduled maintenance and resource allocation.

Section 2

Equipment Life Cycle within the YCCC Domain

Computer equipment on campus falls within three categories. Each category requires its own focused cycle and refresh plan in order to maintain levels of efficiency and cost.

1. Classroom/Instructional equipment
2. Office and Employee equipment
3. Server and Infrastructure equipment

Classroom/Instructional Equipment

All classrooms on the main campus have computers in them. They are however broken into two categories; dedicated computer labs and lecture rooms. A dedicated computer lab is defined as a classroom with computers available for each student to use independently. Dedicated computer labs on the main campus are made up of: B101, B104, B106, B208a, C112, C218, Openlab, Learning Lab, and the Library "Titanic" computer bank. Additionally the Sanford satellite site has one dedicated computer lab.

Most of the computer labs are used to meet specific course offerings and due to that require tailored specs. The tiers of software requirements can be grouped among the following machines on a scale of highest to least

1. Most resource intensive software labs
 - a. B104 for digital media
 - b. B106 for autocad
 - c. C218 for Programming
 - d. Sanford satellite lab for SolidWorks
 - e. Openlab which runs all of these programs.
2. Non-software intensive labs
 - a. B101 – Microsoft Office
 - b. B205 – Microsoft Office and Physics emulation software
 - c. B208a – Microsoft Office and VMWare Client
 - d. C112 – Microsoft Office and web based Accounting
 - e. D204 – Microsoft Office and math tutoring
 - f. Library Titanic – Microsoft Office

Lecture rooms are defined as rooms where only the instructor has a dedicated computer, students do not. Any classroom not identified as a computer lab falls in the category of a lecture room. Aside from this distinction all classrooms share some consistent technology features such as audio and projection.

Technology found in all classrooms includes at minimum:

- Instructor computer
- Projector
- Computer speakers

- Microsoft Office

Replacement Cycle for Computers

The rotation of computer equipment will be scheduled in the following order for each year. If multiple labs are replaced at once then the next following lab will be replaced in the subsequent year, maintaining the sequence.

1. C112 (21 units) & D204 (19 units)
2. Sanford Lab & B101
3. Openlab (17 units) & B205
4. B104 & Titanic (12 units + 2 for Library Front desk + 1 for Circulation)
5. B208a & Lecture (17 units)
6. B106 & C218

Outside of the classroom computer schedule, staff computers will be replaced through yearly review of the oldest computers on campus. Each year 20 new desktops will be purchased to earmark for staff machines. 15 of these computers will be deployed based on age of equipment. 5 will be kept on hand to use as rapid replacements for any computers which experience hardware failures. At the end of the year the remaining 5 computers will be added to the pool of new computers being distributed as staff upgrades.

Replacement cycle for Projectors

- 2nd floor B-wing (6 units)* and Main Building Conference Rooms (3 units)
- 1st Floor A & B wing projectors (7 units)
- 2nd Floor C-Wing (8 units)* and Sanford (1 unit)
- 1st Floor C-wing (7 units)
- Pratt & Wittney Building (8 units)

*Skip Projector in B208 on 2017 projector replacement pass, skip projector in C218 in 2019 pass

Computer Monitor Replacement Cycle

There is currently no standardize sizing of monitors on campus though all monitors have been migrated to LCD displays. Classroom monitors are spec'd based on instructor requirements and requests. Office monitor sizes are based upon availability at the time of replacement.

- Each fiscal period funding will be earmarked for 15 LCD monitors of the most common size on campus. Depending on pricing the next highest size (19" monitor in relation to a 17" monitor for example) will be considered as a point upgrade to.
- Specific classroom monitor sizes will be maintained. If they exceed the size of the 15 monitor replacement pool, then they will be purchased out of the replacement equipment fund (Line 7290)

Server Equipment Replacement Life Cycle

There are currently 8 physical servers on campus. The majority of our server environment, roughly 52 other servers, is virtualized in VMWare. Our remaining physical servers are:

- 4 servers which serve as physical hosts to the VMWare environment
- 2 Microsoft Active Directory Servers (AD and AD3)
- 1 server in Sanford operating as a print and network resource server
- 1 server as a security database server for the Pratt Building security system

The replacement cycle of the server hardware is heavily influenced by the VMWare system requirements due to how much of an impact the virtual environment has in our server infrastructure. In order to maintain key VMWare services such as VMotion and failover, all of the physical host hardware must be as similar as possible. Due to this the four servers must be replaced together. The remaining 4 physical servers can be replaced independently of one another.

- FY18/19 – Replace AD
- FY19/20 – Replace all VMWare physical host
- FY 20/21 – Replace AD3 and Sanford network resource server
- FY 21/22 – Replace security database server

Network Switch and Appliance Life Cycle

The campus includes 1 MDF closet and 4 IDF closets. Campus network topology includes a VPN tunnel for our 1 current satellite location which treats that data closet as one of the IDF locations. Likewise the Pratt building's IDF is connected via Fiber to the main building's MDF, treating that building as an extension of the main building's network. To further break down the MDF, it is comprised of two switch stacks. One being the main head switch stack acting as the gateway and a second larger switch stack which performs much in the same way as an IDF switch stack.

All IDF stacks include a split of PoE and non-PoE switches. Campus phones, wifi access points, and a handful of other devices are powered by PoE through these switch stacks. A failure here will disable any device attached to it as it will no longer receive power. The number of switches in each stack varies as not all available wall outlets are attached to live jacks. The current closet switch break downs are:

- A Wing MDF head switch stack – 2 non-PoE
- A Wing MDF non-head switch stack – 5 non-PoE and 2 PoE
- B Wing IDF switch stack – 4 non-PoE and 2 PoE
- C Wing IDF switch stack – 4 non-PoE and 1 PoE
- D Wing (Pratt Building) IDF switch stack – 2 non-PoE and 2 PoE
- Sanford IDF – 1 PoE

The majority of the campus switches are of a similar model. Due to this and the expense of replacing switches, when replaced all switches will be kept on hand to use as hot spares.

- FY 17/18 B Wing IDF
- FY 18/19 A Wing MDF non-head stack
- FY 19/20 C Wing IDF
- FY 20/21 Sanford IDF and A wing MDF Head

- FY 21/22 D Wing IDF

UPS Power Backup Maintenance

All MDF and IDF equipment is powered through APC UPS power management. We currently maintain two backup batteries as replacements for the UPS devices in place. The spare batteries are only for the most common UPS model however. Over the years older UPS models have been retired and we have not been able to maintain a unified type across all data closets. Due to this if a battery is not on hand to replace in a failed unit one will be ordered through operational equipment line 7290.

In the event of a UPS hardware failure there is currently sufficient power capacity in the local devices to accommodate the displaced equipment. UPS equipment replacement will be done on an equipment evaluation basis. Visual inspection of the equipment occurs fairly regularly and we are notified by an auidial alarm when a device has failed.

Misc Lab Equipment Replacement Cycle

Other equipment in labs such as, but not limited to; document cameras, speakers, slide progression clickers will be replaced on an as need basis. These pieces of equipment are considered consumable in regards to everyday use. Expansion and stock of these types of equipment however will be included in yearly budgets and planned for due to the cost associated with some pieces.

- At least 4 document cameras added to classroom environment yearly, or maintained in inventory as replacements
- At least 5 classroom speakers added to classroom environment yearly or maintained in inventory as replacements
- At least 6 classroom progression clickers maintained in inventory. These must be checked out and returned by those wishing to use them.
- At least 5 web cams maintained in inventory to be checked out by instructors for classroom use.
- At least 6 of the most common type of LCD projector bulbs in inventory at the start of the academic year

Section 3

Software Life Cycle within the YCCC Domain

Software on campus is currently divided into three categories: Student Information system and Server Based software, Classroom & Instructional Software, and Administrative software.

Student Information System and Server Based Software

The Jenzabar EX student information system version levels are highly influenced by Jenzabar's maintenance. At minimum the college will maintain the required version to receive technical support. Currently however there is discussion for converging the EX versions across all MCCS college campuses. At this point we will begin to perform upgrades in line with the MCCS schedule. Individual patching for the EX environment is performed in house and based on need/issue.

The operating servers are primarily at Server 2016 though there are instance of 2008 and 2012 still within the environment. The AD operating environment is currently set to 2008R2. Server upgrades to newer iterations will be done after evaluating the supported versions for the software they host.

Staff server based resources, such as PowerFaid, are upgraded per user request to maintain functionality and support levels.

Classroom & Instructional Software

Classroom computers are standardized on Windows 10 for both full labs and lecture rooms. Microsoft Office is installed on all computers. The standardized version of Office is established by the CIS program's curriculum for the version of Office being taught to students. All other classroom software is dictated by faculty department chairs. An email is sent to all chairs each spring prior to the semester end requesting software upgrade requests and/or new software needs.

Administrative Software

Staff computers are not currently unified across the version of Windows running on their desktops. Staff computers are split between Windows 7 and Windows 10. As computers are replaced users are upgraded to Windows 10 as a convergence target. No known Windows version specific software is currently running on staff computers, the primary challenge is the interruption to work caused by the upgrade.

There is also currently no standardized version of Microsoft Office on staff computers. Upgrades are currently done upon request from staff or when a replacement computer is deployed to the user.

Section 4

Cloud Computing Life Cycle and Integration

Microsoft Azure

YCCC is in a position to utilize cloud based services through Microsoft based on our current Campus License Agreement. The initial offer is a modest amount of space and resources meant to offer customers an inexpensive spring board into the service. Known as Azure, the target model for Microsoft is a back office integration/co-location of resources. There are several pros and cons to utilizing cloud based technology. Due to these YCCC will adopt a modest and paced migration into cloud so as to both leverage the strengths of the technology while mitigating our vulnerability to outages and data loss.

- Establish Azure account through Microsoft hosted solutions
- Create cloud based authentication server
 - a. All current external authentication services will be pointed to this new server
- Explore Cloud based Email services.
 - a. Currently known as Office 365

Meraki

Microsoft is not the only service provider offering cloud based solutions. Cisco systems has also deployed the Meraki platform for managing a wide array of network resources. Regardless of the vendor, YCCC will adopt the same measured approach to adoption with an eye to accentuating the pros while mitigating the cons.

- Migration of Wireless technology to Meraki Cloud management
- Evaluation and testing of Meraki security camera management through the cloud
 - a. Objective - is to unify the various security camera systems under one interface
 - b. Objective – To more easily provide access to first responders and external stake holders, regardless of the conditions here on campus.
- Evaluation and testing of Meraki Switch management through the cloud

Phone System

The migration of the on premise phone system to an MCCC Intranet model is close enough to a cloud based phone solution to include here. Overarching management and authority over this system is not yet established and will need to be addressed once deployment is complete. YCCC is scheduled to be the first site to receive the new phone system deployment during the Fall of 2017. Review, life cycle, and management of the overarching system has yet to be determined by the colleges involved in the project.

Independently of the MCCC, YCCC will take it upon themselves to evaluate the phone system after 5 years. The goal of this is to ensure that we do not find ourselves in a situation where we are

stuck with a failing or no longer supported system which becomes a burden to manage. If a group at the MCCS level is formed to perform periodic reviews then this information will be used in conjunction with the internal review of the phone system.

Section 5

New Projects and Initiatives outside the Three Life Cycles

Most of the projects which are undertaken are part of the yearly maintenance and upgrade plans for the previously identified areas. Projects listed here however do not neatly fit within the established categories.

- IT infrastructure for Sanford site (phases 2 and 3).
- Exploration of new cloud services which may benefit network survivability.
- Migration of licensing services which support SolidWorks and CamWorks PMT software to the Sanford site servers. This will localize license support to where it is most heavily used.
- Solution for Culinary lab classroom technology. They currently utilize tablet PCs which are wall mounted to connect to the projector and display content.
- Office 365 for email and data.
- Upgrade functional domain level to 2012

Section 6

SWOT Analysis Action Plan

The point of this section is to address the SWOT Analysis and propose focuses and plans for moving forward during the plan period to accentuate or mitigate identified points.

Strengths

1. Leveraging the hosted Blackboard Learn Environment reduces the support strain on the IT department while increasing availability and support resources to students and faculty. The IT department plans to continue utilizing this delivery service for our Distance Ed courses.
2. Our virtual server environment provides much flexibility and redundancy within the campuses server infrastructure. This continues to provide near 100% up time to internal network resources such as the Jenzabar student information system. Adhering to the planned hardware upgrade plan will help to ensure reliability in this area in the future.
3. The Cisco Meraki wireless cloud management system provides automatic updates and software maintenance to all campus wireless access points. This reduces the work load of campus IT staff while ensuring accessibility to campus users.
4. Through training and work load allocation we have managed to cultivate a person on staff so that they are now able to perform maintenance to our database and student information systems. Previously we had to rely upon external consultancy for these tasks. Having the ability in house to perform these tasks puts us in a stronger position of self-reliance for maintaining these mission critical systems. Maintaining this strength will include following through with departmental growth and development over the course of the 5 year plan, as outlined in Section 7.
5. All critically identified servers, switches, and network appliances are currently monitored under an external 3rd party monitoring service. This system both emails and sends a text alert to IT staff in the event of specified equipment thresholds, such as the equipment becoming unresponsive. The IT department intends to continue this service into the future.
6. Communication with stakeholders on campus is important to the IT department's success. We not only alert stake holders of issues but also attempt to explain them so that the community can understand better what is happening. We intend to continue this practice and hope to augment this strength with the campus wide security training initiatives.
7. In line with communicating with stakeholders, maintaining network resource and service up times is of importance to the department. While there must be down times for servicing equipment these must be effectively communicated. Similarly managing expectations with problem resolutions helps the department address day to day technology issues. The IT department intends to continue working with the goals of maintaining the highest technology availability for all stakeholders.

Weaknesses

1. Mitigation: The creation of a departmental internal policy which addresses the scope of these issues and outlines a best practice response. Research of this process for Fall 2017. Creation of policy for Spring 2018. Implementation of Policy Summer of 2018.

- a. Responsible: Paul A for research
 - b. Responsible: Eric B for creating and implementing the policy.
2. Mitigation: A policy exists for account data access, it just needs to be published within the portal where users can access it.
 - a. Target date for resolution: By end of semester 2017
 - b. Responsible: Eric B
3. Mitigation: Research how to implement these things via network policy rules. Prep them to be implemented along with the training session identified under Threat #4.
 - a. Assigned Task: Paul A to research implementation
 - b. Assigned Task: Brian implement based on what Paul Discovers.
 - c. Target date: Research completed by end of Fall 2017
 - d. Target date: Implementation by execution of training in Threat #4
4. Mitigation: While not ideal the current solution is working and able to update as needed. A more robust solution will be researched and implemented FY 18/19. The goal will be to create a more streamlined process with better centralized control.
5. Mitigation: TBA
6. Mitigation: TBA
7. Mitigation: The development of a strategic process which considers start, mid process, and end of IT related projects. Included is the concept of Threat Modeling for forecasting as many security issues as possible. Target date for development of this internal departmental procedure is FY 19/20.
8. Mitigation: The completion of the in house developed database driven inventory system. This database system was designed to include all of these functions. Was partially developed but due to resource constraints put on hold.
 - a. Responsibility: Brian H
 - b. Target Date: Spring 18
9. Mitigation: Related to weakness #5 and weakness #6. Resolution of those areas will include addressing and mitigating this weakness.
10. Mitigation: Resolution of this will be determined by the campus email system upgrades. Upon completion SSL implementation will be incorporated into the process.
 - a. Target completion date: Spring 18
 - b. Research: Eric B
 - c. Implementation: WGTech

Opportunities

1. The development of new physical campus resources, such as the expansion in Sanford, are opportunities to explore technology advances in small controlled environments. Through working with impacted users who are experts in their particular content areas we can provide more tailored solutions. Examples of this include the deployment of new projectors at the Sanford Precision Machining site where the projectors chosen were based upon faculty technical requests. Recognizing these opportunities improves stakeholder performance which in turn benefits the students.
2. Grants provide the department with an opportunity to augment its financial resources. These were used to provide funding for part of the Pratt & Whitney building's auditorium technology

for example. Due to the length of time required to apply and receive a grant, this opportunity may only be effective for longer ranged planned projects.

3. We are beginning to utilize the Microsoft cloud platform (Azure) for offsite authentication. The utilization of Azure is an opportunity for the college to move already web accessible resources into the cloud and shore up internal security. DMZ resources could potentially be moved into this environment if it proves effective much in the same way as Blackboard was moved off site to be hosted by Blackboard the company, freeing up YCCC's technical staff and resources.
4. The Potential Expansion of departmental staff is an opportunity for the college to expand both IT availability but to also further specialize roles. Much in the same way our current departmental strength has manifested by training a staff member to manage our Jenzabar dataset, more staff provide the opportunities for specializations in other areas. These staff members can either be hired with the skill sets or hired without them with the intent to train them along paths of their interest that benefit the college.
5. Departmental training budget does not have to be spent on just the department staff. This funding can also be extended to IT related campus wide training initiatives such as desktop security for campus staff.

Threats

1. Mitigation: is to work with HR to create a policy which addresses the time line for notification of employee termination. Outline the expectation of data saved, what data is removed (such as email accounts) and process for reclaiming college resources.
 - a. Target date for resolution is by end of Fall Semester 2017.
 - b. Task Assigned to: Paul A.
2. Mitigation: the creation of a policy which outlines expected password change schedule and complexity. Policy is to be posted within the campus portal which requires user authentication to view.
 - a. Target date for resolution is by end of Fall Semester 2017
 - b. Task Assigned to: Eric B.
3. Mitigation: for fiscal year fy17/18 research software solutions which will satisfy and address this vulnerability. Request budget allowance for FY 18/19 to purchase discovered solution.
 - a. Target Research FY 17/18 period
 - b. Request budgeting for FY 18/19 on solution
 - c. Research Task: Paul
 - d. Budgeting Task: Eric
4. Mitigation: Request training resources for desktop security to be presented campus wide. Using our new auditorium we have an opportunity to bring in external expertise to conduct in house training. Research solution services for this for Fall semester 2017. Target of presentation during Spring semester 2018.
 - a. Target Date for resolution: by end of Spring Semester 2018
 - b. Responsible: Eric B
5. Mitigation: same resolution as threat #4.

Section 7

Departmental Growth, Development, and External Support

Training, Conferences, and Skills

Yearly fiscal budgeting will allocate at minimum 1 technical course per staff member. The local training facility, VTEC, will be used for budgeting cost. Training courses will be on topics of interested to the employee but must be approved by the supervisor to ensure they are of benefit to the institution. Additionally a portion of the training budget may instead be used by departmental staff for reimbursement of degree program credits at other colleges, per the union benefits agreement.

There are two mandatory conferences for members of the departmental staff to attend each year. Both of the conferences are related to the campus student information system. The first being the Jenzabar hosted JAM yearly conference event. The second is the MCCS hosted internal event related to Jenzabar systems within the community college system. Other conferences aside from these will be evaluated upon request and funding.

JDQ and Classifications

- Reclassification of existing personnel during the FY 17/18 year

Personnel

- Hiring of new Tech staff
- Training or hiring of existing staff in the following areas:
 - DBA
 - Network Administrator

External Support

- WGTech contracted for 100 hours of unspecified support for FY 17/18 through FY 20/21
- Blackboard support for 24/7 distance ed delivery platform maintenance and troubleshooting

Appendix 1

Condensed 5 Year Punch List

*Objectives are derived from 2014 -2019 Strategic Plan Direction VI

FY 17/18 Objectives & Measures

- Maintaining operational effectiveness of technology (Action B)
 - Met life cycle requirements for Equipment and Software
- Provide survivable account access to offsite resources (Action F)
 - Establish external authentication server presence in the cloud
- Departmental Staff Resources (Action E)
 - Hiring a Tech
 - Training and Job reviews
- Deploy a new phone system
 - Successfully configure and install new phone equipment at all campus locations currently with a phone
- Address identified security issues in SWOT analysis (Action A)
 - Implemented policies earmarked for FY 17/18

FY 18/19 Objectives & Measures

- Maintaining operational effectiveness of technology (Action B)
 - Met life cycle requirements for Equipment and Software
- Expansion of technology at Sanford site (Action C)
 - Design, purchase, and deployed expanded technology resources at Sanford site
- Address identified security issues in SWOT analysis (Action A)
 - Implemented policies earmarked for FY 18/19
- Departmental Staff Resources (Action E)
 - Training and Job reviews
- Provide survivable account access to offsite resources (Action F)
 - Collaborate with the MCCS on anticipated cloud collaboration project to federate domains

FY 19/20 Objectives & Measures

- Maintaining operational effectiveness of technology (Action B)
 - Met life cycle requirements for Equipment and Software
- Address identified security issues in SWOT analysis (Action A & C)

- Implemented policies earmarked for FY 19/20
- Departmental Staff Resources (Action E)
 - Explore options for expanding/augmenting staff based on identified needs
 - Training and Job reviews
- Provide survivable account access to offsite resources (Action F)
 - Review of Cloud opportunities to find those that align with YCCC Mission

FY 20/21 Objectives & Measures

- Maintaining operational effectiveness of technology (Action B)
 - Met life cycle requirements for Equipment and Software
- Address identified security issues in SWOT analysis (Action A)
 - Assess implemented policies for continued viability
 - Develop plan to implement changes
 - Implement changes
- Provide survivable account access to offsite resources (Action F)
 - Review of Cloud opportunities to find those that align with YCCC Mission

FY 21/22 Objectives & Measures

- Maintaining operational effectiveness of technology (Action B)
 - Met life cycle requirements for Equipment and Software
 - 5 year review of the phone system
- Address identified security issues in SWOT analysis (Action A)
 - Assess implemented policies for continued viability
 - Develop plan to implement changes
 - Implement changes
- Provide survivable account access to offsite resources (Action F)
 - Review of Cloud opportunities to find those that align with YCCC Mission

Appendix 2

Breakdown of Planned Equipment

FY 17/18

- C112 (21 units) & D204 (19 units)
- 20 Staff Desktops
- 15 LCD Monitors
- Replace Production SAN Storage Environment
- B Wing IDF Switches
- 2nd floor B-wing (6 units)* and Main Building Conference Rooms (3 units) Projectors
- Misc consumable equipment
 - 4 document cameras to have in inventory
 - 5 classroom speakers to have in inventory
 - 6 classroom progression clickers to have in inventory
 - 5 web cams to have in inventory
 - 6 of the most common LCD projector bulbs in inventory

FY 18/19

- Sanford Lab & B101
- 20 Staff Desktops
- 15 LCD Monitors
- Replace AD Server
- A Wing MDF non-head stack Switches
- 1st Floor A & B wing projectors (7 units)
- Misc consumable equipment
 - 4 document cameras to have in inventory
 - 5 classroom speakers to have in inventory
 - 6 classroom progression clickers to have in inventory
 - 5 web cams to have in inventory
 - 6 of the most common LCD projector bulbs in inventory

FY 19/20

- Openlab (17 units) & B205
- 20 Staff Desktops
- 15 LCD Monitors
- Replace all VMWare physical host
- C Wing IDF Switches
- 2nd Floor C-Wing (8 units)* and Sanford (1 unit) Projectors
- Misc consumable equipment
 - 4 document cameras to have in inventory
 - 5 classroom speakers to have in inventory

- 6 classroom progression clickers to have in inventory
- 5 web cams to have in inventory
- 6 of the most common LCD projector bulbs in inventory

FY 20/21

- B104 & Titanic (12 units + 2 for Library Front desk + 1 for Circulation)
- 20 Staff Desktops
- 15 LCD Monitors
- Replace AD3 and Sanford network resource server
- Sanford IDF and A wing MDF Head Switches
- 1st Floor C-wing (7 units) projectors
- Misc consumable equipment
 - 4 document cameras to have in inventory
 - 5 classroom speakers to have in inventory
 - 6 classroom progression clickers to have in inventory
 - 5 web cams to have in inventory
 - 6 of the most common LCD projector bulbs in inventory

FY 21/22

- B208a & Lecture (17 units)
- 20 Staff Desktops
- 15 LCD Monitors
- Replace security database server
- D Wing IDF Switches
- Pratt & Whitney Building (8 units) Projectors
- Misc consumable equipment
 - 4 document cameras to have in inventory
 - 5 classroom speakers to have in inventory
 - 6 classroom progression clickers to have in inventory
 - 5 web cams to have in inventory
 - 6 of the most common LCD projector bulbs in inventory

Due to the volume of equipment, some replacements are scheduled outside the window of the 5 year plan. They are included below for completeness.

- B106 & C218 replaced in FY22/23