APLS / IT Division

FY ’18 and FY ’19 Technology Plan

***Last Updated on July 17, 2018 by Jay W. Mims***
# Table of Contents

Executive Summary ........................................................................................................................................ 3

Replacement Plan ....................................................................................................................................... 5
  I. Plan Overview and Explanation ........................................................................................................... 5
  II. PC Refresh Plan ................................................................................................................................. 6
  III. Server Refresh Plan .......................................................................................................................... 11
  IV. Peripheral Refresh Plan .................................................................................................................... 13
  V. Inventory Management Plan ............................................................................................................. 16
  VI. Deployment Plan ............................................................................................................................... 17

Project Development Plan .......................................................................................................................... 18

SWOT Analysis ........................................................................................................................................ 19

Training Plan ........................................................................................................................................... 21

Security Analysis .................................................................................................................................... 23

Disaster Recovery Initial Discoveries ....................................................................................................... 26
APLS / IT Division - Executive Summary

APLS / IT Division works diligently to provide excellent service to the APLS employees agency wide. We provide services such as email, secure and managed storage of information, internet availability, desktop hardware/software support and telephone/video conferencing services to any and all APLS employees.

APLS / IT Division also provides assistance to local libraries in a variety of ways including web site development and maintenance, remote and on-site desktop hardware and software support and network assistance as needed.

The following summary is an attempt to provide a high-level look at the work of our division and whom are the expert knowledge owners and back-ups for each of the main responsibilities of the APLS / IT Division

Desktop Services – IT Helpdesk
The Division provides assistance to all APLS employees and local library employees that use a PC or MAC device each and every day. The work performed ranges from simple password resets to difficult data recovery efforts and many different needs in between. The Helpdesk has technicians available from 8:00 a.m. to 5:00 p.m. Monday through Friday to assist with these needs. Any APLS employee or local library employee can contact the IT Helpdesk at any time with any technical need.

*Expert Knowledge Owners:*
Eric Bair
Demetris Smith

*Back-Up Technicians:*
Bryan Harris
Matt Sponsler

Server Administration
The Division manages and maintains 14 or more servers used by APLS employees every day. This includes managing new user accounts and user home storage. Also included within these duties are maintaining the servers for Evergreen, File Maker and Secure Data Back Ups. There are several different on-going projects within this group.

*Expert Knowledge Owners:*
Bryan Harris – Server Maintenance, VM Ware, SAN
Trevor Johnson – Data Back Up and Restoration, VM Ware
Clyde Mills – Data Back Up and Restoration
Back-Up Technicians:
Matt Sponsler

Program Development and Maintenance
The Division has a large network of database applications and programs that are administered and maintained on a daily basis. Most applications are supported through the File Maker product and other sole source programs. Our team assists with data fixes, development of new applications and installation of new services both inside the APLS agency and as a service to the local libraries served by APLS.

Expert Knowledge Owners:
Clyde Mills – File Maker Design, Development and Maintenance, Web Site Development and Maintenance
Trevor Johnson – Evergreen Maintenance and Installation
Bryan Harris – Keystone / KLAS Maintenance

***Trevor and Clyde back up one another in these roles, Clyde also backs up Keystone***

Network, Data and Cyber Security Control
The Division maintains the security and integrity of the APLS data network and the Microsoft and Apple operating systems located within the network. They administer these duties via software and hardware installation and maintenance. Another key component of the security strategy of APLS involves the server maintenance duties mentioned above.

Expert Knowledge Owners:
Trevor Johnson – Switch Set Up and Maintenance
Matt Sponsler – Tenable, PWNY Administration and Maintenance
Bryan Harris – Symantec Administration and Maintenance

Back Up Technicians:
Trevor Johnson – Tenable, PWNY and Symantec
Matt Sponsler – Switch Set Up and Maintenance

Telephone and Video Conferencing Administration
The Division maintains a fully functioning Voice over IP telephony environment that provides all telephone and fax capabilities to the staff of APLS. This includes voice mail, intercom, and transfer features. The Division also provides to the APLS staff, local libraries, state agencies and possibly the public business sector Video Conferencing (VidCon) Services that include training space (owned by APLS and local libraries), operating hardware, program direction and technical support.

Expert Knowledge Owners: Back Up Technician:
Matt Sponsler Trevor Johnson
APLS / IT Division – Product Replacement Plan

I. Plan Overview and Explanation
II. PC Refresh Plan
III. Server Refresh Plan
IV. Peripheral Refresh Plan
V. Inventory Management Plan
VI. Deployment Plan

I. Plan Overview and Explanation
As an IT Department our goal is to provide the most optimal technological solutions for our clients. This goal will be carried out in three phases.

A. Hardware – end user computers, server a data storage hardware and peripheral hardware (scanners, printers, etc…)
B. Software – Microsoft office, FileMaker databases, web browser compatibility, etc...
C. Support – desk top level support for end users and maintenance of background hardware and software.

This product life cycle plan is being developed and implemented in order to best provide for all three facets of the IT Department operations goal. By ensuring that hardware is up to date with industry technology standards our customers are always capable of computing at a level that meets the expectations perceived by the marketing of the discipline from outside the agency.

Our goal with this plan is to provide hardware, software and support that is readily available, properly operational and capable of meeting the everyday needs of our client’s workloads.
II. PC Refresh Plan

The industry standard for PC replacement is generally considered to be between two and four years. Our desire is to create a plan that is economically acceptable for our department while also providing high standard operational computing devices for our departments users.

The Alabama Public Library Services currently owns and operates 30 Apple iMac devices, 15 Apple MacBook devices and 10 PC devices.

The Admin Division has 5 iMac devices and 1 Apple MacBook device.

The Business Office/Finance has 4 Apple iMac devices and 1 Apple MacBook device.

The Consultants Division has 6 Apple iMac Devices and 6 Apple MacBook devices.

The Reference Division has 6 Apple iMac devices and 1 Apple MacBook device.

The BPH Division has 9 Dell PC’s.

The Building/Maintenance Division has 3 iMac devices.

Finally, the IT Division has 6 Apple iMac devices, 6 Apple MacBook devices and 3 Dell PC’s in service for daily use/support.

In the future, our effort will be to replace pc’s/iMac’s/laptops/MacBook’s on a 4 to 6-year cycle depending upon funding and daily operability.

However, for this initial plan, we have analyzed our equipment and categorized equipment for replacement based on system resources and the user’s ability to properly function with given equipment. The mistake was made in the past to buy larger sums of equipment that weren’t high level enterprise machines. This has resulted in groups of equipment that although are very similar are not uniform. Our desire is to develop a specification list for each device based on current needs and trends toward near future needs and buy products for lifecycle replacement that are uniform in specifications if at all possible.
The following equipment has been analyzed and identified as **critical** need for replacement immediately.

**Admin Division...**

<table>
<thead>
<tr>
<th>Inventory Number</th>
<th>User</th>
<th>Hardware version</th>
<th>Date of Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS-000161</td>
<td>Nancy</td>
<td>iMac late 2013</td>
<td>12/29/14</td>
</tr>
<tr>
<td>LS-000110</td>
<td>Wanda*</td>
<td>iMac late 2013</td>
<td>12/23/14</td>
</tr>
</tbody>
</table>

**Finance Division / Business Office...**

<table>
<thead>
<tr>
<th>Inventory Number</th>
<th>User</th>
<th>Hardware version</th>
<th>Date of Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS-000001</td>
<td>Jeannie*</td>
<td>iMac late 2013</td>
<td>12/23/14</td>
</tr>
<tr>
<td>LS-000115</td>
<td>Carol*</td>
<td>iMac late 2013</td>
<td>12/23/14</td>
</tr>
<tr>
<td>LS-000122</td>
<td>Susan*</td>
<td>iMac late 2013</td>
<td>12/23/14</td>
</tr>
</tbody>
</table>

**Building / Maintenance Division...**

<table>
<thead>
<tr>
<th>Inventory Number</th>
<th>User</th>
<th>Hardware version</th>
<th>Date of Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS-000157</td>
<td>Kedia</td>
<td>iMac late 2013</td>
<td>12/23/14</td>
</tr>
</tbody>
</table>

***Workers with an asterisk * beside their name indicates a worker that has been identified as possibly needing a pc instead of an iMac due to job functions.***
The following equipment has been identified and identified as **significant** need for replacement immediately.

**Consultants Division...**

<table>
<thead>
<tr>
<th>Inventory Number</th>
<th>User</th>
<th>Hardware version</th>
<th>Date of Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS-000218</td>
<td>Rhonda</td>
<td>iMac late 2013</td>
<td>7/27/15</td>
</tr>
<tr>
<td>LS-000221</td>
<td>Alisa</td>
<td>iMac late 2013</td>
<td>7/27/15</td>
</tr>
<tr>
<td>LS-000227</td>
<td>Gail</td>
<td>iMac late 2013</td>
<td>7/27/15</td>
</tr>
<tr>
<td>LS-000224</td>
<td>Jim</td>
<td>iMac late 2013</td>
<td>12/23/14</td>
</tr>
<tr>
<td>LS-000232</td>
<td>Stephanie</td>
<td>iMac late 2013</td>
<td>8/21/14</td>
</tr>
</tbody>
</table>

**Reference Division...**

<table>
<thead>
<tr>
<th>Inventory Number</th>
<th>User</th>
<th>Hardware version</th>
<th>Date of Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS-000140</td>
<td>Melinda</td>
<td>iMac late 2013</td>
<td>7/27/15</td>
</tr>
<tr>
<td>LS-000141</td>
<td>Alex</td>
<td>iMac late 2013</td>
<td>7/27/15</td>
</tr>
</tbody>
</table>
The following equipment has been identified and identified as *moderate* need for replacement immediately.

### Admin Division...

<table>
<thead>
<tr>
<th>Inventory Number</th>
<th>User</th>
<th>Hardware version</th>
<th>Date of Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS-000126</td>
<td>Vanessa</td>
<td>iMac late 2013</td>
<td>8/21/14</td>
</tr>
<tr>
<td>LS-000133</td>
<td>Kelyn</td>
<td>iMac late 2013</td>
<td>8/21/14</td>
</tr>
</tbody>
</table>

### IT Division...

<table>
<thead>
<tr>
<th>Inventory Number</th>
<th>User</th>
<th>Hardware version</th>
<th>Date of Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS-000338</td>
<td>Bryan</td>
<td>iMac late 2013</td>
<td>8/21/14</td>
</tr>
<tr>
<td>LS-000309</td>
<td>Trevor</td>
<td>iMac late 2013</td>
<td>8/21/14</td>
</tr>
<tr>
<td>LS-000346</td>
<td>Leonard</td>
<td>iMac late 2013</td>
<td>8/21/14</td>
</tr>
</tbody>
</table>
III. Server Refresh Plan
The IT division manages and maintains several different servers locally. They are as follows:

1) Microsoft Windows Domain Controller – M/S Win Server 2012 (Dell PowerEdge R430)
2) Microsoft Windows File Server – M/S Win Server 2012 (Dell PowerEdge R530)
3) Virtual Server 1 – ESXi 6.0.0 U3a (Dell PowerEdge R630)
4) Virtual Server 2 – ESXi 6.0.0 U3a (Dell PowerEdge R630)
5) Virtual Server 3 – ESXi 6.0.0 U3a (Apple MacPro)
6) Virtual Server 4 – ESXi 6.0.0 U3a (Apple MacPro)
7) Apple Directory Server – Mac OSx 10.11.6 (Apple Mac Pro)
8) Bard Server – Mac OSx 10.11.6 (Apple Mac Mini)
9) APLS/CloudStore Server – Mac OSx 10.11.6 (Apple Mac Mini)
10) Barracuda BackUp/Redundancy Service
11) EMC SAN Device (Storage Area Network)
12) CISCO Legacy BackUp/Redundancy Service
13) ESXi – Virtual Server Hardware (Production)
14) ESXi – Virtual Server Hardware (Test)

The following equipment has been analyzed and identified as significant need for replacement within the next 18 months.

<table>
<thead>
<tr>
<th>Inventory Number</th>
<th>Function</th>
<th>Hardware</th>
<th>Date of Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS-000470</td>
<td>Virtual Server 3</td>
<td>Apple MacPro</td>
<td>9/10/12</td>
</tr>
<tr>
<td></td>
<td>Surveillance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LS-000068</td>
<td>Camera Server</td>
<td>Apple Mac Mini</td>
<td>5/15/12</td>
</tr>
</tbody>
</table>

The following equipment has been identified and identified as moderate need for replacement immediately.

<table>
<thead>
<tr>
<th>Inventory Number</th>
<th>Function</th>
<th>Hardware</th>
<th>Date of Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS-000468</td>
<td>Virtual Server 4</td>
<td>Apple MacPro</td>
<td>9/10/12</td>
</tr>
</tbody>
</table>

***APLS / IT Division plans to replace Virtual Server 3 in FY ‘19 and Virtual Server 4 in FY ‘20 if approved by Nancy Pack and funds are available/budgeted.***
Outside of the replacement efforts noted above APLS/IT will also be working to virtualize the following two servers and decommission the aging hardware currently used to host the programs.

<table>
<thead>
<tr>
<th>Inventory Number</th>
<th>Function</th>
<th>Hardware</th>
<th>Date of Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS-000424</td>
<td>Bard Server</td>
<td>Apple Mac Mini</td>
<td>9/10/12</td>
</tr>
<tr>
<td>LS-000425</td>
<td>CloudStore Server</td>
<td>Apple Mac Mini</td>
<td>9/10/12</td>
</tr>
</tbody>
</table>
IV. Peripheral Refresh Plan
The IT Division will institute a plan to replace peripheral devices upon failure, loss of proper function or loss of ability to meet current standards implemented by the technology of the department.

The Alabama Public Library Services currently owns and operates 9 Scanners, 15 Printers and 15 Secondary Monitors.

The Admin Division has 3 printers, 1 secondary monitor and 2 scanners.

The Business Office/Finance has 2 printers 2 secondary monitors and 3 scanners.

The Consultants Division has 2 secondary monitors and 1 scanner.

The Reference Division has 2 printers.

The BPH Division has 1 printer and 2 specialty printers.

The Building/Maintenance Division has 1 printer and 1 scanner.

Finally, the IT Division has 4 printers, 2 scanners, 7 secondary monitors and 1 specialty printer in service for daily use/support.

Scanners:
APLS has the following scanning devices.
1) Fujitsu Fi5530 Scanner – Clyde Mills
2) Fujitsu iX500 ScanSnap Scanner – Jeannie Price
3) Fujitsu iX500 ScanSnap Scanner – Trevor Johnson
4) Fujitsu iX500 ScanSnap Scanner – Carol Burchett
5) Fujitsu iX500 ScanSnap Scanner – Susan Jana
6) Fujitsu iX500 ScanSnap Scanner – Kelyn Ralya
7) Fujitsu iX500 ScanSnap Scanner – Nancy Pack
8) Fujitsu iX500 ScanSnap Scanner – Randy Garmon
9) Fujitsu iX500 ScanSnap Scanner – Stephanie Taylor
Printers:
APLS has the following printing devices.
1) Xerox 3600n – Storage
2) Xerox 3600n – Storage
3) HP 4250dTn – Vanessa Carr
4) HP M553n – IT Division
5) HP LaserJet – Rhonda Napier
6) HP M602x – Jeannie Price
7) HP M402dNe – Jeannie Price
8) HP M402dNe – Nancy Pack
9) HP M402dNe – Randy Garmon
10) HP Brother MFP – Trevor Johnson
11) Xerox Phaser 3320 – IT Division
12) Xerox Phaser 3320 – Keith Walker
13) Xerox Phaser 3600n – Storage
14) Xerox Phaser 3610 – Rhonda Napier
15) Xerox Phaser 3610 – Trevor Johnson
Monitors:
APLS has the following secondary monitors.
1) Apple Thunderbolt Display – Matt Sponsler
2) Apple Thunderbolt Display – Bryan Harris
3) Apple Thunderbolt Display – IT Division Vacant
4) Apple Thunderbolt Display – Storage
5) Apple Thunderbolt Display – Trevor Johnson
6) Apple Thunderbolt Display – Jay Mims
7) Apple Monitor – Clyde Mills
8) HP 27” Display – Matt Sponsler
9) HP 27” Display – Matt Sponsler
10) HP 19” Display – Matt Sponsler
11) HP 19” Display – Bryan Harris
12) HP 27” Display – Bryan Harris
13) Dell 24” Display – Bryan Harris (may be on inventory)
14) HP 27” Display – IT Division Vacant
15) HP 19” Display – IT Division Testing
16) HP 19” Display – IT Division Testing
17) HP 19” Display – IT Division Testing
18) HP 27” Display – Alisa McLeod
19) HP 27” Display – Jim Smith
20) HP 27” Display – Ryan Godfrey
21) Dell 19” Display – Carol Burchett
22) HP 27” Display – Clyde Mills
23) HP 19” Display – Trevor Johnson
24) Dell 24” Display – Trevor Johnson (may be on inventory)
25) HP 24” Display – Trevor Johnson
V. Inventory Management Plan
Of the equipment that we have identified as needing replaced immediately, there are several options for the surplusing of the equipment.

First, several of the laptops that have been identified as needing replaced can be sanitized and set up for use as part of our Disaster Recovery plan. These machines will be stored in the APLS IT cage and held for use in case of emergency.

Secondly, some of the items, although no longer optimal for APLS service, may very well be equipment our customers in the local libraries of Alabama could utilize for different IT needs. We will first create a list of equipment we can properly sanitize and set up for use by a local library. The libraries can claim these items on a first come first serve basis after the list is provided.

Finally, any equipment that cannot be repurposed to Disaster Recovery or local libraries will be prepared properly for surplus through the business office and taken to the sale lot.
VI. Deployment Plan

**Step 1**) Develop specifications for replacement items as needed and request quotes from proper vendors via state contracts.

**Step 2**) Upon receiving the quotes, place an order for equipment as approved by Director and Finance.

**Step 3**) Receive and Inventory equipment properly through the Business Office.

**Step 4**) Train all users who are going to receive new equipment on changes to platform, etc... to ensure that all users are as prepared as possible to receive new equipment.

**Step 5**) After the release of equipment to IT, we will develop and install all images necessary on computing devices and plan with necessary divisions to deploy the new equipment to recipients in a way to minimize downtime to our users and make the best use of the time of our IT staff.

**Step 6**) Gather all removed equipment and prep for the Inventory Management plan explained above.
APLS / IT Division – Project Development Objectives

As an IT Division one of the main focuses is to identify, research, assist and develop technological projects for the divisions of our agency. As technology changes the agencies needs for technology will change as well. The IT Division desires to be proactive in ensuring that technologies are available for our agency as operations change in the future.

FY ’18 and FY ’19 Projects Identified

<table>
<thead>
<tr>
<th>Project Name</th>
<th>IT Employees Involved</th>
<th>Project Start Date</th>
<th>Projected End Date</th>
<th>Technology to be Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>BARD Server Virtualization</td>
<td>Trevor Johnson, Bryan Harris</td>
<td>TBD</td>
<td>TBD</td>
<td>Virtual Server / SAN</td>
</tr>
<tr>
<td>CloudServe Virtualization</td>
<td>Trevor Johnson, Bryan Harris</td>
<td>7/9/18</td>
<td>11/5/18</td>
<td>Virtual Server / SAN</td>
</tr>
<tr>
<td>PC Refresh Plan (Phase 1)</td>
<td>Bryan Harris</td>
<td>6/27/18</td>
<td>11/2/18</td>
<td>Multiple Technology Platforms</td>
</tr>
<tr>
<td>Server Refresh Plan (Phase 1)</td>
<td>Bryan Harris</td>
<td>6/27/18</td>
<td>11/2/18</td>
<td>Multiple Technology Platforms</td>
</tr>
<tr>
<td>Document Imaging System</td>
<td>Clyde Mills, Trevor Johnson, Bryan Harris</td>
<td>5/14/18</td>
<td>TBD - Ongoing</td>
<td>Filemaker / Fujitsu ScanSnap Scanner / SAN</td>
</tr>
<tr>
<td>VoIP / VidCon Hardware Upgrade</td>
<td>Matt Sponsler</td>
<td>5/1/18</td>
<td>FY ’19 - TBD</td>
<td>CISCO / Multiple Vid/Con Hardwares</td>
</tr>
<tr>
<td>SysLog Server Install and Set Up</td>
<td>Trevor Johnson</td>
<td>TBD</td>
<td>TBD</td>
<td>Virtual Server / SysLog Software</td>
</tr>
<tr>
<td>Sharepoint Server and System Install</td>
<td>Bryan Harris, Trevor Johnson</td>
<td>5/1/18</td>
<td>10-31-18 - Ongoing</td>
<td>Virtual Server / Sharepoint Software</td>
</tr>
<tr>
<td>Agency Technology Training</td>
<td>Clyde Mills, Trevor Johnson, Matt Sponsler</td>
<td>5/16/18</td>
<td>Ongoing</td>
<td>M/S Office / SANS / etc...</td>
</tr>
<tr>
<td>KACE Update Server</td>
<td>Trevor Johnson, Bryan Harris</td>
<td>TBD</td>
<td>TBD</td>
<td>Virtual Server / M/S Server</td>
</tr>
</tbody>
</table>
# APLS / IT Division – SWOT Analysis

<table>
<thead>
<tr>
<th><strong>Strengths</strong></th>
<th><strong>Weaknesses</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Longevity / Tenured IT Staff</td>
<td>o Lack of Focus on Project Completions</td>
</tr>
<tr>
<td>✓ Broad Knowledge Base among IT Staff</td>
<td>o Lack of Standardization in Deployed Equipment</td>
</tr>
<tr>
<td>✓ Strong Team Work and Collaboration Willingness</td>
<td>o Lack of Reporting / Advanced Metrics on Division Work / Customer Needs</td>
</tr>
<tr>
<td>✓ Division wide desire to assist the agency and local libraries with the best service we can provide</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Opportunities</strong></th>
<th><strong>Threats</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>➢ Streamline Project Development/Management</td>
<td>❖ Cyber Security Awareness</td>
</tr>
<tr>
<td>➢ Create Added IT Value for Agency and Local Libraries through Training</td>
<td>❖ Disaster Recovery Readiness</td>
</tr>
<tr>
<td>➢ Develop New Applications for Agency Divisions to Assist the Promotion of Agency Objectives</td>
<td></td>
</tr>
</tbody>
</table>

### How to take full advantage of **Strengths**:
- Ensure that staff members are aware of their importance to the agency and developed professionally to encourage a continued course of longevity.
- Properly assess work to guarantee that staff members best skills are being utilized for the agencies overall objectives.
- Continue to develop projects that are inclusive of all staff so that the division is giving both the agency and the local libraries our best services and support.

### How to develop **Weaknesses** into **Strengths**:
- Develop a proper and structured helpdesk that works all Tier 1 support which will free up tenured and experienced staff to focus on the larger projects and efforts of the division.
- IT Director will properly plan and manage projects creating a focused environment for staff.
- Develop a grouping of IT Equipment that is used within the agency and that is promoted to local libraries for purchase so that standards are naturally implemented over time.
- IT Director will work with staff to develop a standard for ticketing and information input so that good information and data is being collected.
- IT Director will work with Program Development to create good reports.
How to cultivate **Opportunities**:

- IT Director will implement and teach a specific project planning management style which will develop a stronger culture of preparation and implementation.
- IT Director will work with Public Relations Officer to develop marketing tools to be used to promote both training opportunities and services provided by the division to the local libraries via the new APLS website, Quarterly Admin Meetings and via Brochures delivered by Consultants when traveling and visiting all libraries state wide.
- Meet with the different divisions of the agency on a quarterly basis to see what work they are doing and to learn of any new efforts they are wanting to implement. Then ask questions to see where and how the IT Division can possibly assist with these efforts.

How to minimize **Threats**:

- Develop written policies for all areas of IT Division security that identify the security provided, the on-going maintenance needed and the schedule for such maintenance.
- Subscribe to and actively read the best newsletters and security information provided within the industry.
- Develop a specified IT Security team that will meet bi-weekly to analyze security scans and determine points of vulnerability and plan to address vulnerabilities through Desktop Services, Server Administration or Program Maintenance.
- Develop a Disaster Recovery IT Plan that is feasible and actionable.
- Perform quarterly assessments and vulnerability drills to actively learn and strengthen the security of APLS technology and data.
**APLS / IT Division – Training Plan**

**Internal Training:**
APLS / IT Division is seeking to have each employee attend a training and/or conference each year that correlates to one of the Division’s 5 areas of discipline.

The areas of discipline are:
1) Desktop Services
2) Server Administration
3) Program Development and Maintenance
4) Network, Data and Cyber Security Control
5) Telephone and Video Conferencing Administration

Implementing a training plan will allow our IT Division team members to continue to grow their skills in specific areas as technology continues to advance which in turn will allow the division to provide services and support to both agency employees and the local libraries we work to consult and assist on a daily basis.

***Internal Training Plan Proposal for FY’18 and FY’19 on next page***

**Agency and Local Library Staff Training:**
APLS / IT Division is seeking to develop and implement technical training in the everyday technologies and programs that the staff of APLS and local libraries use on a daily basis. These trainings will be shaped to refresh employees who are well versed in the everyday technologies while also opening new knowledge avenues for employees who seek to grow their knowledge bases in regards to the everyday technologies that are implemented by APLS and local libraries.

Targeted areas of training are:
- Microsoft Excel (Beginner and Intermediate)
- Microsoft Word (Beginner and Intermediate)
- Microsoft Outlook (Overview)
- Microsoft PowerPoint (Beginner)
- FileMaker Basics (Overview)

These trainings will be 2 or 3 hour courses that will be made available on a quarterly basis based upon interest to all APLS staff.

We also hope to offer a specific course each quarter on the day of the APLS Admin meetings that will be available for local library staff attending the admin meeting to stay and take after lunch as appropriate.

**Security Training:**
APLS / IT Division plans to continue to test and prepare security training for all agency staff through the SANS training offering made available to us via OIT.
***APLS / IT Division Internal Training Plan Proposal***

Per CFO, Jeannie Price, APLS has the funds available for the FY ‘18 proposal. She also indicated that she could budget the FY ‘19 proposal if approved by agency director, Nancy Pack.

**FY ‘18**

<table>
<thead>
<tr>
<th>Name</th>
<th>Class</th>
<th>Discipline</th>
<th>Cost</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clyde Mills</td>
<td>Filemaker Conference</td>
<td>Program Dev. &amp; Maint.</td>
<td>$1,800.00</td>
<td>8/6 – 8/9</td>
</tr>
<tr>
<td>Matt Sponsler</td>
<td>Implementing Cisco VoIP and Video (pt. 1)</td>
<td>Tele. &amp; Video Con. Admin.</td>
<td>$3,795.00</td>
<td>6/25 – 6/29</td>
</tr>
<tr>
<td>Trevor Johnson</td>
<td>CompTia Advanced Security</td>
<td>Network, Data &amp; Cyber Security Control</td>
<td>$3,695.00</td>
<td>7/9 – 7/13</td>
</tr>
<tr>
<td>Bryan Harris</td>
<td>Planning and Administering SharePoint</td>
<td>Program Dev. &amp; Maint.</td>
<td>$2,351.00</td>
<td>As Requested (TBD)</td>
</tr>
<tr>
<td>Jay Mims</td>
<td>CompTia Security +</td>
<td>Netowrk, Data &amp; Cyber Security Control</td>
<td>$1,628.00</td>
<td>6/25 – 6/29</td>
</tr>
</tbody>
</table>

**FY ‘19**

<table>
<thead>
<tr>
<th>Name</th>
<th>Class</th>
<th>Discipline</th>
<th>Cost</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clyde Mills</td>
<td>Planning and Administering SharePoint</td>
<td>Program Dev. &amp; Maint.</td>
<td>$2,351.00</td>
<td>As Requested (TBD)</td>
</tr>
<tr>
<td>Matt Sponsler</td>
<td>Implementing Cisco VoIP and Video (pt. 2)</td>
<td>Tele. &amp; Video Con. Admin.</td>
<td>$3,795.00</td>
<td>TBD</td>
</tr>
<tr>
<td>Trevor Johnson</td>
<td>CCNA Collaboration eCamp</td>
<td>Network, Data &amp; Cyber Security Control</td>
<td>$2,150.00</td>
<td>TBD</td>
</tr>
<tr>
<td>Bryan Harris</td>
<td>CompTia Security +</td>
<td>Netowrk, Data &amp; Cyber Security Control</td>
<td>$1,628.00</td>
<td>TBD</td>
</tr>
<tr>
<td>Jay Mims</td>
<td>CompTia Advanced Security</td>
<td>Netowrk, Data &amp; Cyber Security Control</td>
<td>$1,628.00</td>
<td>TBD</td>
</tr>
</tbody>
</table>

***APLS / IT Division Director plans to have every IT Division employee attend training and attain the CompTia Security + certification by the end of FY ‘20***
Physical Security Assessment:

1) The agency does not employ a full-time security guard or security management team.
2) There are two non-secured entry points where public access is possible. They are the main floor entrance to the APLS facility and the lower floor entrance to the BPH offices. Both of these entry points are manned by front desk personnel and backups who provide a first level of security to entry ability. Both desks also have security escalation options to trigger a rapid public safety response.
3) The agency does implement a sign-in sheet protocol at the front doors.
4) The agency does have a security system that creates access control to all perimeter entry points except the two main entry points.
5) Access to the administration suite is not locked down and has 3 access points. They are through the business office, the main suite entry and the back-suite entry. All offices are lockable by key and are generally, at least half of the offices, occupied by staff including the ASA located in the common area during business hours.
6) Access to the consultants’ area does not appear to be lockable and is generally open to all individuals that walk by their main entrance. The area is at times sparsely populated by staff and is possible that no staff are in the area during the agencies business hours.
7) Access to the BPH beyond the front desk employee is not secured. The Director’s office is lockable by key but all other locations are open during the days operational hours. In general, there are employees in cubicles or open areas including the warehouse throughout the day.
8) The Main IT Office is locked by a card key access-controlled magnetically locked door and is only accessible by those who have the proper permissions.
9) The IT Server closet (FACP Room) is locked by security magnet lock and accessible by card key permissions only. The cages housing the servers are also locked by physical key and accessible only by those who hold a key.
10) The IT Warehouse closet which houses vacant equipment, the security access control system and several switches is locked behind both the Main IT Office card key magnetic lock and a second lock on the door to entry for the closet itself which is also a card key magnetic lock only accessible by those with permissions.
11) The secondary switch closet is locked by a magnet locked access-controlled door which is only accessible by individuals with proper access permissions. This room also houses HVAC/Mechanical equipment. The secondary door to this facility is magnetically access control locked and only accessible by those who have permissions to the room.
12) The administration wing switch closet is sitting behind two lockable doors that do not appear to ever be locked. Most of the time there is at least one employee between possible public access and the switch.

Physical Security Threats:

1) Free access to most of the building by individuals not approved for access.
2) Technology equipment not actively occupied is susceptible to being removed by possible perpetrators.
3) Admin switch complex possibly accessible to the public without having to circumvent locks.
Suggestions to Alleviate Threats:
1) Suggest that agency management implement a locked door policy on admin switch complex closet.
2) Suggest that agency management implement a card key access locked door policy for Admin and Consultant suite. Consultant suite is a more critical request.

Network Security Assessment:
1) APLS/IT Division implements two different network security scanning systems. The systems are:
   a. Tenable – scans all software across the network and analyzes the scans for out of date patches, out of date service packs and other vulnerabilities and reports the outcomes of the analysis to a large report.
   b. PWNIE – scans the wireless network for changes, vulnerabilities and threats and reports the outcomes of the analysis to a report.
2) APLS/IT Division firewall – CISCO Adaptive Security Appliance 508x
3) APLS/IT Division web filter – CISCO Web Security Appliance S390
4) Domain Administration via M/S Domain Controller and Apple Controller

Network Security Threats:
1) Possibilities are always available for hacking. APLS/IT Division is making great efforts to keep the network as impenetrable as possible however network breaches are not completely inevitable and always a possibility.

Suggestions to Alleviate Threats:
1) Prepare a security/disaster response plan to properly, step by step, deal with any breach that we may experience in the future.

Device Security Assessment:
1) As mentioned above, a large portion of IT equipment that possibly holds data are not in secured areas. This includes both desktop pc’s and laptops.
2) Laptops are possibly free floating in non-secured areas where unapproved visitors can see them and take them without being noticed.
3) Vacant equipment is properly stored behind dually locked and controlled entry doors.
4) All desktop and laptop pc’s are accessible via domain controlled log-in user names and/or administrator user names held by IT Staff only.
5) All desktop and laptop pc’s receive updates to patch security issues via dedicated WSUS and Apple Update Servers.
6) All desktop and laptop devices are scanned while on the network by the Symantec Protection software employed across our network of computing devices.

Device Security Threats:
1) The big threat is physical as mentioned above under the physical security assessment.
a. Laptops that are in non-secure areas could possibly be removed by individuals looking to steal equipment.
b. Desktops and Laptops could be “hacked” in unsecure areas where unwanted visitors looking to cause damage may have access.

**Analysis to Alleviate Threats:**

1) Implement physical policy to have all laptops in non-secure areas locked within desks at all times when not in use.
   a. Set up policy for bi-weekly system scan of all non-daily technology equipment (laptops).

**Develop a Security Team and Team Policies and Procedures:**

Security Team will consist of Director of IT, Security Officer and Security Technician who will meet bi-weekly to analyze security scans and discuss security issues and news. Security team will develop the procedures and policies for the implementation of up to date, technologically relevant security for the network of the agency. Team will develop and deliver quarterly security reports to the agency director for overview and information.

Security Team will then develop policies and procedures for password creation/change management, policy for development and testing environments used by agency IT division as well as for laptop/portable device use and other policy necessities as needed.
APLS / IT Division – Disaster Recovery Initial Discoveries

For the Agency:
Loss of File Server – Recovery available via backup storage appliance, will require hardware purchase?
  ➢ File Server can be set up for vital functions via VMware until new hardware can be procured.
  ➢ Procurement cost will be approximately $8,000.00.

Loss of SAN Data – Recovery available via backup storage appliance, will require hardware purchase?
  ➢ Agency will be down until new hardware is delivered and set up is complete.
    o The SAN is currently on a maintenance contract for next day resolution in case of issue.
  ➢ Procurement cost will be approximately $40,000.00.

Loss of Off-Site Data Storage Redundancy – Link would need to be recreated and repopulated with data from data storage device

Loss of Physical Agency Building – hardware purchase would be necessary for servers and local computing devices, data could be repopulated from data storage offsite redundancy

For the Local Library:
Loss of Evergreen Server – Recovery available via backup storage appliance, server may be set up via VMware until new hardware can be procured and setup locally for the library.

Loss of Physical Building – APLS / IT could assist with setting up a temporary location including provision of aged laptops and set up of a LAN temporarily for library computing necessities, would require ISP assistance and/or MiFi devices???

Loss of PC’s – APLS / IT could respond with aged laptops and set up a LAN temporarily for library computing necessities