INTERMEDIATE SCHOOL DISTRICT 917
IN DAKOTA COUNTY

SCHOOL BOARD WORK SESSION **Tuesday, January 20, 2015**

AGENDA:

I. **Call to Order - Chair Lewis**

II. **Conduct Pledge of Allegiance - Chair Lewis**

III. **Goals Progress Review for 2014-2015 - All** 2

IV. **TIES Technology Report - Cory Langenfeld** 4

V. **Adjournment**

SCHOOL BOARD CALENDAR INFORMATION SCHOOL BOARD CALENDAR INFORMATION

February 3, 2015 - 5:00 PM, Regular School Board Meeting, 917 Board Room
February 16, 2015 - No school for staff or students - Presidents' Day
March 3, 2015 - 5:00 PM - Regular School Board Meeting, 917 Board Room

Administrative Operational Actions and Goals
2014-2015

1. Implement, evaluate, and refine the new educator development and evaluation process (EDEP) for Intermediate School District 917. (SD #3, #4)

2. Identify the additional direct and indirect costs of implementing the educator development and evaluation process (EDEP) compared to the direct and indirect costs prior to the 2014-2015 fiscal year. Develop a report of the increased expenses and prior expenses compared to the one year only revenue established in the 2014 legislative session. (SE #4)

3. Continue development and implementation of the DCALS/DCTC Transportation Academy in collaboration with the DCTC transportation department and MNSCU transportation director. (SD #2, #4)

4. Continue implementation and expansion of the DCALS Project Based Learning options to improve student motivation and credit completion. (SD #2)

5. Expand our involvement at DCALS with our local trades and apprenticeship training programs to increase student awareness of the career opportunities in the regional work force. (SD #2, #4)

6. Convene a study team to develop a proposal for a career academy model of programming that would integrate our alternative learning centers, our career and technical secondary education programs, and appropriate post-secondary programs at DCTC. (SD #4, #5)

7. Implement new requirements under the Affordable Care Act (ACA) to collect and report new payroll and insurance information. The ACA requires employers to count and report employee's hours on a continual basis to determine eligibility for an offer of insurance coverage. The ACA also mandates additional reporting requirements regarding benefits and employee status. We will be collaborating with the TIES consortium to select a software vendor to manage tracking of this new employee information. (SD #4)

8. Continue the implementation of the work plan for workers' compensation claims control and reduction of lost work time. Our current experience modification is 2.15 and our goal is to reduce it to below 2.0. The variables we work on are safety training for staff, support o staff who are injured and return to work plans which can improve recovery time and reduce district financial liabilities. (SD #4)

9. Develop a three-year plan of projected expenses and revenues for effective utilization of authorized uses of the increase in the levy authority for Safe Schools. (SD #4)

10. Continue to implement and evaluate the roles and responsibilities of behavior support staff, including licensed psychologist and board certified behavior analyst, across district programs to increase student academic engagement. (SD #2)

11. Explore and implement additional strategies to recruit and retain quality special education staff and support the lobbying efforts of the Intermediate School Districts, AMSD, MSBA, MASA, and MASE for legislation to create more flexible paths for alternative licensing procedures. (SD #5)

12. Research options for relocating programming from the Apple Valley Business Center to a facility with more appropriate space configurations and interior finishes to meet our programming needs. (SD #4, #5)

13. Conduct surveys of website users to gather input about their experience on the new website. Utilize the new feedback and the website user focus group input collected in the spring of 2014 to refine the new website features. (SD #1, #3)

14. Develop a marketing/communications action plan to enhance the regional awareness of student programs and opportunities at Intermediate School District 917. (SD #1)

Board Approved 9/2/14

TIES

Assessment Summary
For
Intermediate School District 917

November 17, 2014

Prepared by: TIES
Mark Gamelin
Larry Jacobs

Table of Contents

Charge

TIES Technical Services was engaged by Intermediate School District 917 to conduct assessments involving technology of existing equipment and procedures. This assessment will review ISD-917's existing technology and needs, and make recommendations regarding plans, processes, procedures, strategies and deployments, that allow ISD-917 to accomplish the goals of its strategic plans.

Executive Summary

Intermediate School District 917 (ISD917) has requested a technology audit from TIES. The purpose of the audit is to assess Intermediate School District 917 (ISD917)'s current technology and make related recommendations based on current IT best practices.

TIES completed a general technical audit for Intermediate School District 917 (ISD917). This executive summary outlines TIES recommendations according to industry standards and best practices. TIES is making the following recommendations:

1. Intermediate School District 917 needs to update their strategic technology plan every five years. (Process should start 3 years into the next plan.)
2. Conduct semi-annual meetings with districts that host sites to plan for new technology implementations.
3. Migrate physical Microsoft servers to a virtual environment.
4. Technology leadership needs to be enhanced through clear and frequent communications between the technical staff and administrators.
5. Set district-wide standards on which technologies are implemented; basing decisions on ongoing support costs, curriculum requirements and replacement costs.
6. Set Clear goals for District-wide technology leadership.
7. Include IT staff and curriculum staff in District Technology Mission goal discussions.
8. Implement district-wide resource and file sharing solution.
9. Update network infrastructure to support current and future network expansion.
10. Update and expand Wi-Fi, basing it more on density and less on partial coverage.
11. Implement an enterprise level network monitoring and firmware updating solution.
12. Implement an enterprise level management system to keep all computers in the District up to date.
13. Use industry certified professionals to implement new technology and train internal staff to manage new technologies.
14. Budget for adequate training for IT staff to manage new technologies.
15. Implement business continuity and disaster recovery strategies.
16. Budget replacement of technology based on the following schedule:
    a. Servers 5 years
    b. Workstations 5 years
    c. Network switches 5 years

   d. Phone system 10 years
   e. Wireless 3 years

17. Use helpdesk software metrics to generate reports to assess staff support levels and have regular meetings with admin staff to discuss reports.
18. Locate or develop technical champions or subject matter experts to find tools to create efficiencies and to get staff to follow the tech champions or subject matter experts' advice.
19. Implement end user training on district technologies.
20. Replace obsolete servers especially those out of warranty moving to a 5 year replacement cycle.
21. Replace equipment based on instructional goals, support requirements, and integration needs.
22. Platform decisions for computers for teachers and students should be determined by considering information systems requirements, curriculum needs and the total cost of ownership. Multi-platform computers may provide a solution where special needs exist.
23. Update and maintain an accurate inventory of **all** technology in the district.

Approach

1. TIES conducted an audit:
   a. General Technology Infrastructure– to examine Intermediate School District 917's (ISD917)'s technology infrastructure and recommend any upgrades or enhancements for effectiveness, responsiveness, robustness and security.
2. The TIES audit team conducted two interviews with Intermediate School District 917 (ISD917) staff to make recommendations on technology infrastructure enhancements.
3. The General Technology Infrastructure assessments were completed by the following content experts from TIES Technical Services Department: Mark Gamelin and Larry Jacobs.
4. Background details, findings and recommendations are assembled in this final report.

Technology of existing equipment and procedures Audit

Audit Deliverables

Summary of Existing Technology

Section 1.1.1: Hardware – Servers/Clients/Thin clients

- Findings:
  - Hardware inventory is verifiable.
  - Only new computers are under warranty coverage.
  - The district keeps old computers beyond their life span.
  - Some student desktops are locked down with Microsoft Active Directory Group Policies.
  - There is no server virtualization implemented.
  - The district has spam protection (Mail Foundry) and Web filtering using M8e6.
  - Employees work in sites that that are not connected to internal technical resources (file shares etc.).
  - Email resources are available remotely using Web access only.
  - None of server infrastructure is currently virtual or under warranty.
  - Some Windows XP workstations are still in use.
- Recommendations:

    - Keep all technology inventories current.
        - Manufacturer serial number and purchase costs.
        - Asset tagging.
        - Warranty.
        - Location tracking.
    - Consider purchase of desktop computer warranty matching the life cycle.
    - Enforce a replacement cycle based on warranties.
    - Consider leasing core technology hardware.
    - Keep hardware to a minimum variety of models.
    - Bind all MAC computers to Active Directory.
    - Set computer replacement life cycles to the following:
        - Servers 5 years.
        - Workstations 5 years.
        - Network switches and firewall 5 years.
        - Phone system 10 years.
    - Use an outside expert to install and configure a virtualization environment.
    - Use an outside expert to migrate all present network services into a virtual environment.
    - Remove all obsolete technologies from district use.
- Reasoning:
    - A verifiable hardware inventory allows for warranty and insurance tracking for loss recovery/replacement/support
    - Strict adherence to replacement life cycle lowers support costs, increases IT efficiencies, and reduces total power consumption.
    - Virtualizing the server environment allows less hardware to provide more capability and lowering the administration time and costs.
    - Virtualizing allows quick spin-up of a newly desired services.
    - Virtualizing allows for business continuity through the use of fast bare metal restores.
    - Microsoft has discontinued support of Windows XP. This creates a security vulnerability.
- Options:
    - VMware ESXi or Microsoft Hyper-V are server virtualization options.

Section 1.1.2: Printers/Fax

- Findings:
    - Loeffler has a printer / fax inventory.
    - Microsoft print server software running on a server.
    - Large multifunction printers are not under warranty.
    - Cory is responsible for larger printer maintenance.
    - Pam is responsible for maintenance of inkjets and smaller printers.
    - Loeffler is responsible for copier maintenance on a break fix basis.
    - Printing is not centralized is a big frustration.
    - Too many individual printers.
    - Fuser replacement are the most frequent service issues.
    - District printing consumables are managed by need.
- Recommendations:
    - Where ever possible move away from older and individual printers to a higher capacity multifunction network printing.
    - Work with current vendors to standardize and minimize printer models.
    - Assess Total cost of ownership when considering the purchase of a new printer models.
    - Verify that printers are physically labeled to reduce end user confusion.
- Reasoning:
    - Minimize the number of printer models to decrease IT support overhead and Total Cost of Ownership (TCO).
    - Higher capacity printers offer multi functions (scan to email or storage location, faxing, etc.) and do printing at a lower price per page as compared to individual class ink jet printers.
- Options:
    - Consider using printer support contracts.

Section 1.1.3: Software – OS/Applications/Licensing/SAM

- Findings:
  - The IT Staff believes software licensing is only accounted for on Microsoft products in the Microsoft portal.
  - The District uses the Microsoft Volume License Program.
  - There is an upgrade protection/software assurance contract on some software.
  - All non-Microsoft applications are purchased as needed.
  - Applications are installed manually one workstation at a time (sneaker-net).
  - Software includes:
    - Microsoft products.
    - Sophos Anti-Virus.
    - Apple iPad applications.
    - Special needs software.
- Recommendations:
  - Update the centralized repository for all software licenses and media and keep current.
  - Investigate the fiscal viability of a software upgrade protection program for all critical applications.
  - Create a Subject Matter Expert (SME) in the district staff for each critical application. package and provide additional up to date training for that person.
  - Minimize software versions for each application and operating system (OS).
  - Install Microsoft System Center Configuration Manager (SCCM):
    - Automate imaging of Windows desktops.
    - Automated application deployment to the Windows and MAC desktops.
    - Monitor software licensing compliance.
    - Automate Windows desktop updates and patches.
    - Remote management of desktops and users.
    - Windows Antivirus/malware monitoring and reporting.
  - Implement an iPad imaging solution.
- Reasoning:
  - Accurate and up to date software License documentation will verify software compliance.
  - Purchase of software assurance allows upgrading of all software to the same version across all workstations minimizing training and maintenance.
  - Create Subject Matter Experts (SMEs) in the district staff for each critical application package. E.g. train a person on Excel and they can share their knowledge among all staff by being the go-to person for advanced questions on Excel.
  - Standardizing on a single version of software minimizes conflict issues as discrepancies between versions will be minimized (e.g. a saved Word 2007 trying to be opened in Word 2000).
  - Maintaining software includes installing patches. This will minimize attack surface and data corruption exposure for safer computing.
  - SCCM provides an ability to
    - Centrally manage the software licensing compliance of the districts computers
    - Discover unknown software existence on computers within the district
    - Centrally manage the desktop experience for the end user
    - Enhances the security and compliance of the districts desktop computers
- Options:
  - Casper Suite an iPad management solution is a popular option.

Section 1.1.4: Business Applications

- Findings:n
  - TIES is the Student Information System (SIS).
  - Other TIES applications used include: iPlan, iContent, HR Pay, Finance and Parent Portal.
  - Sharp Schools is used for the districts New Web page.
  - Maintenance is in place for the business applications.
  - Remote access to file server based data is not available but desired.

- Recommendations:
  - Send district representatives to TIES for application training.
  - Keep critical business application maintenance contracts current.
  - Provide and schedule training for staff on remote data access.
  - Optional-Include Students to the remote data access method.
  - Consider implementing a Learning Management System (LMS) (example Moodle).
- Reasoning:
  - Training will benefit all staff.
  - With support in place staff can quickly call the manufacturer on issues they are experiencing.
  - Remote data access increases staff and productivity.
  - Student Remote data access can allow students to work from home or with any device, as well as utilizing a homework drop box system.
  - A LMS solution will allow access to classroom content from anywhere.
- Products:
  - A feature rich remote file access solution is HTTP Commander.
  - A feature rich LMS is Moodle.

Section 1.1.5: Network Infrastructure

- Findings:
  - Firewall is 9 years old
  - Most of the buildings are wired with Category 5e and some Category 6 network cables.
  - Mapping of the network drops is documented, but out of date.
  - There are some network ports open on switches.
  - The district is using Power over Ethernet (PoE) switches as needed.
  - Some wiring closets are connected back to the MDF via fiber.
  - Most of the district has 10/100 megabytes with some 1 gigabytes to the desktop.
  - Internet connectivity ranges from 1 Mb DSL to a maximum of 1000Mb fiber.
  - No centralized software is monitoring wireless network traffic.
  - There is no map of existing network.
  - Network Switches run until they fail.
  - Some IP phones run over the data network.
  - Network traffic is not monitored in any way.
- Recommendations:
  - Replace the nine year old firewall with current firewall technology.
  - Update network cabling documentation.
  - Replace old switches that are out of warranty with 1/10 gigabyte network connections where needed.
  - Conduct a bandwidth study of the current network's and Internet bandwidth capabilities to discover its ability to support new technologies. Review regularly.
  - Examine port usage and disconnect unneeded drops.
  - Add switch capacity where needed.
  - Add Power over Ethernet switches (POE) as needed to support future wireless and Voice over IP (VOIP) expansion.
  - Monitor and expand Guest wireless bandwidth as needed.
  - Document the network topology of all sites and buildings.
  - Bring in an outside expert to perform a wireless assessment and make recommendations to meet the district's density goals.
  - Bring in outside contractor to upgrade and optimize switch, router, vLAN, and firewall design and configurations.
  - Use an outside expert to implement an enterprise level network monitoring solution. This includes network diagrams and inventory of network hardware.
- Reasoning:
  - Some network infrastructure is out dated and will not support future network expansion.
  - Unused live network drops may pose a security threat.

- Current network monitoring is lacking the functionality to help troubleshoot network issues.

Section 1.1.6: Connectivity/Internet/E-mail

- Findings:
  - TIES is the current Internet provider for DCTC.
  - Connection speeds range from 1Mb DSL to 1000Mb fiber.
  - High speed Internet is critical and the District depends on its connectivity.
  - There are no service level agreements.
  - Static IP addresses are available from the ISP and the WAN IP is static.
  - The current version of Microsoft Exchange is 2010.
  - 350 staff use Outlook as a primary email platform.
  - The district uses Outlook and Outlook Web Access to receive email.
  - ISD917 does not allow Instant Messaging (IM) and/or don't use it for business.
  - Currently the district offers remote access to email via Outlook Web Access.
  - Most district staff would like to have remote access to their data on the servers.
  - Some district staff would like to use the full Outlook client for local archival purposes.
- Recommendations:
  - Upgrade Exchange 2010 to latest service pack and rollup update.
  - Consider other email options like Microsoft Officer 365.
  - Use industry expert outside vendor to facilitate migration to the new email system.
  - Consider implementing a remote file data share to provide access for all users.
  - Consider adding bandwidth to sites that have DSL.
- Reasoning:
  - Upgrading Microsoft Exchange 2010 to the latest version will allow for more feature options.
  - Microsoft Office 365 in hybrid mode will offer more options for mail and resource sharing.
  - Remote file access will enhance staff productivity and security.
    - Access to file shares from any device while at home or at a conference enhances staff productivity.
    - Carrying files on portable storage devices increases the possibility of lost data.
- Options:
  - On premise Microsoft Exchange with Outlook Anywhere.
  - Microsoft Office 365 hybrid.
  - Email/calendar – Smart phone access, tablet access, laptop access via a smart device gateway.
  - HttpCommander
  - SharePoint

Section 1.1.7: Wireless

- Findings:
  - Xirrus Access Points are in use.
  - Linksys small office / home office Access Points are in use.
  - The IT staff believes the wireless network is meeting their needs.
  - Staff has a low opinion on the wireless network capabilities and not meeting their needs.
    - Wireless times out and staff have to re-authenticate.
    - Staff complains about wireless dead spots.
  - There is no guest network access for wireless.
  - Wireless is protected with WPA-2 and WEP.
  - There is no single cell phone provider for the district.
  - Cell phone coverage in Dakota County Technical College (DCTC) is extremely limited.
  - Employees choose their own wireless devices.
  - There is no formal plan to implement BYOD or One to One initiative.
- Recommendations:

    - Update and expand Wi-Fi to base wireless on density and less on coverage especially in the district office and other high traffic areas.
    - Use an outside contractor to audit the building's existing wireless radio broadcast strengths (heat map).
    - Conduct a post wireless audit for all buildings.
    - Upgrade wireless design implementation based on audit discovery and density needs.
    - Monitor allocated wireless bandwidth utilization and adjust as needed.
    - Add a hidden guest wireless VLAN.
    - Consider a cell phone signal extender from a provider that enhances coverage.
        - FEMTOcell - A FEMTOcell allows one service provider to extend service coverage indoors or at the cell edge, especially where access would otherwise be limited or unavailable.
- Reasoning:
    - A wireless audit will provide a WAP location roadmap to meet density requirements.
    - A post wireless audit should always be done to ensure that wireless is working as predicted.
    - Due to the increasing number of Wi-Fi devices per person, a wireless density design will better meet the curriculum needs of the district.
    - A "Hiden PublicGuest" wireless allocated bandwidth to more effectively meet demand of non-district owned devices.
    - Extending the cell service coverage at DCTC will lead to better communication and productivity gains. (you may be able to negotiate with providers)

Section 1.1.8: Network Storage

- Findings:
    - The district has centralized and decentralized storage available through Microsoft Active Directory Domain file server.
    - Some computers in non DCTC sites cannot save to the file server in the Active Directory Domain.
    - Alliance and DCTC sites have access to file servers.
    - Staff has individual user accounts and files shares.
    - Students have shared accounts with shared file storage.
    - Staff also uses USB drives to save data to because they do not trust the network. (sneaker net)
    - The district does not use a Storage Area Network (SAN) to save data or run virtual servers.
    - The district is considering some type of Cloud Storage for easier document saving and sharing.
- Recommendations:
    - Consider implementing a remote file data share or Cloud system to provide access for all users.
    - Insure there is a section of the Acceptable Use Policy that addresses the use of moving data in and out of the district.
- Reasoning:
    - Remote file sharing for all platforms allows for secure data control and continuity.
    - Insure proper handling of confidential data is addressed by the District Acceptable Use Policy.

Section 1.1.9: Power

- Findings:
    - ISD 917 uses DCTC data center which has battery and generator capability. ISD 917 does not have control to test power for this facility.
    - Most site branches are inside host schools or independent buildings. Host schools including: Burnsville, Hastings, Lakeville, W. St. Paul, and Farmington schools, provide power failover. The independent sites have limited power failover except Alliance which has battery backup and no generator.

  - Only file servers are protected by Uninterruptible Power Supplies (UPSs).
  - UPS batteries are not tested and only replaced when they beep.
  - UPS connected file servers are set to use auto shutdown.
  - Power monitoring is not utilized.
  - The district UPS connected equipment cannot withstand a long term outage.

- Recommendations:
  - Document and chart current power outages.
  - Implement Uninterruptible Power Supplies (UPS) for all switches.
  - Test and document UPS systems on a regular basis as per manufacturer recommendations.
  - Verify auto shut down is implemented on all file servers.
  - Install UPS software to monitor power.
- Reasoning:
  - Inconsistent power leads to loss of productivity and data.
  - Inconsistent power is detrimental to technology hardware and software.
  - An UPS helps protect equipment from brown outs and power surges as well as outages.

Section 1.1.10: Telephony

- Findings:
  - The district receives 100-275 calls a day.
  - NEC is the telephone provider.
  - The district has 70 analog telephone lines.
  - The district has 30 digital telephone lines.
  - The district has 100 phones on site.
  - The district has 30+ mailbox accounts.
  - The district has 100 mb connections for the telephones
  - The district has issues with the phone system when there are power outages. They have lost the capability for 911 emergency calls.
  - The district owns its present telephone system.
  - The district does not have a WebEx type conferencing solution.
  - The district has 23 fax machines which includes one for each site.
  - The district has 7 receptionists for DCTC and one for each of the other sites or approximately 29 total.
  -
- Recommendations:
  - Budget phone system replacement cycle for 10 years
  - Verify that purchased telephone features are implemented and staff is trained to be productive with phone features.
- Reasoning:
  - Manufacturers recommended replacement cycle is 10 years.
  - Purchased features will lead to better staff productivity with training.

Review Technology Processes and Policies

Section 1.2.1: Technology Management

- Findings:
  - The district has a 5 year technology plan but was dated 2008-2011 and was reviewed in 2013.
  - Very limited cross training among IT staff.
  - Some IT staff can manage servers from outside the office.
  - When Cory is on vacation others do their best to fill in but he usually gets calls for help.
  - Users have admin rights to workstations. But are not supposed to install software or configure their district computers.
  - IT Staff vacation/absentee coverage is planned for.
  - Cory monitors the districts file servers and patches them.
  - The district uses Zendesk for help desk solution.
  - There is limited technology documentation.
  - IT staff adds students and staff to Active Directory.
  - The IT staff does not use an imaging software solution to setup and manage new workstations.
  - The IT staff manually installs applications on workstations.
  - District IT staff use group policies to manage the Windows desktops on a minimal basis.
- Recommendations:
  - Verify that the 5 year technology plan is up-to-date and its goals are being attained.
  - Cross train personnel on key functions
  - Document the IT issue contingency process for vacation coverage.
  - Document and securely house IT accounts and passwords for all district technology equipment.
  - Using outside experts to implement new technologies will expedite the installation and guarantee installation according to industry best practices.
  - Budget to use outside contractors to implement and train internal staff to manage new technologies.
  - Have quarterly meetings with administration to look at IT helpdesk support levels.
  - Create a written policy for technology management that is reviewed on an annual basis.
  - Budget and implement IT training for the support of new and existing technologies for all IT staff.
  - Reduce workstation setup time and ongoing management by implementing Microsoft Systems Center Configuration Manager (SCCM) imaging solution.
- Reasoning:
  - Technology goals should be measureable and IT staffing levels and efforts should be based on these goals.
  - Improved cross training minimizes outages when key personnel are out of office or unavailable.
  - Administration should have access to technology accounts and passwords in case of emergency.
  - Using industry experts will ease the burden on district IT staff and give them more time to support and maintain technologies.
  - A help desk solution allows monitoring and reviewing of helpdesk metrics. These metrics can generate reports that justify IT staffing levels.
  - The technology management policy defines the metrics to quantify technology achievements.
  - Training of IT staff leads to better support efficiencies.
  - Microsoft Systems Center Configuration Manager (SCCM) manages and deploys multiple versions of desktop operating systems, Antivirus, patching, applications, etc.

Section 1.2.2: Security

- Findings:
  - DCTC provides security for ISD917's main data center which has a locked door without an access record log.
  - There is not supposed to be critical data on staff notebooks or portable devices.
  - There is no single written security policy, there are pieces in multiple other policies.
  - Cory is the point of contact for district data security.
  - There has not been a security audit or network penetration test.
  - What type of security do you have for:
    - Network and Wireless Infrastructure = one admin account
    - Systems Infrastructure = Microsoft Active Directory accounts
    - Wireless Service Set IDentifier (SSID) = WEP and WPA2
  - There is no written password policy.
    - Passwords assigned by the IT staff.
    - Passwords are rarely changed. Once per year.
  - Terminated employee accounts are disabled.
  - There is no formal written process for a terminated employee.
  - Cameras are in place, but are dated.
- Recommendations:
  - Consider an annual security audit/penetration test to verify the districts data security preparedness.
  - Verify that staff is not saving sensitive data on portable devices.
  - If sensitive data is found on portable devices remove or encrypt as needed.
  - Create a district written security policy which includes a password provision.
  - Move away from shared administrative user security accounts.
  - Verify that existing video surveillance system covers critical IT areas.
  - Create a written process to deal with turnover or terminated employees.
- Reasoning:
  - Understanding security vulnerabilities will allow the district to proactively close these vulnerabilities and will lead to better security of confidential data.
  - Unsecured workstations holding sensitive data could be a security breech.
  - A district written security policy provides a formal understanding of security procedures that protect the district's IT assets.
  - A vulnerability test verifies that security best practices are being followed.
  - A shared administrative password makes tracking of changes difficult.
  - Video surveillance allows the tracking of critical IT access in case of malicious activity.

Section 1.2.3: Internet Usage

- Findings:
  - Yes, there is a written Internet acceptable use policy.
  - The Internet policy is reviewed every 2 years.
  - The district has an Internet Usage monitoring device in place.
  - High-volume access websites are blocked.
  - The district does consider the legal liability of not controlling Internet access.
- Recommendations:
  - Consider implementing a domain and wireless acceptable use splash screen for end user authentication.
  - Inclusion of the IT staff in the annual acceptable use policy review process will ensure the policy includes new and emerging technologies.
  - Review internet usage quarterly.
- Reasoning:
  - An acceptable use splash screen can help cover the district against litigation.
  - The IT staff can ensure that emerging technologies are included in the policy.

- A detailed description of the expectations of technology usage helps remove any ambiguities from the faculty, staff, and students.
- Internet usage reports will allow the district to monitor usage and limit non-educational high bandwidth sites resulting in more available bandwidth for educational sites.

Section 1.2.4: Spam/Spyware/AV

- Findings:
  - Sophos anti-virus / Mail Foundry anti-spam.
  - There is no written spam / malware policy.
  - IT Staff monitors that anti-virus / anti-spam.
  - Cory keeps the Microsoft Windows servers patched.
  - Spam is dealt with a multi-tiered approach
    - Mail Foundry Spam filtering
    - Spam Assassin Spam filtering
    - Outlook Spam filtering
  - There have been no major virus outbreaks.
  - The financial impact of malware is minimal.
- Recommendations:
  - Create and adopt a written anti-virus, anti-spam, and anti-malware policy.
  - Review new and upcoming (cost-effective) antivirus software solutions 6 months prior to contract expiration.
- Reasoning:
  - Features, capabilities, and pricing (competitive upgrade sales) change frequently. Verifying your present solution is the better choice.

Section 1.2.5: Backup

- Findings:
  - There is no written backup policy and it is not reviewed.
  - The recovery process has never been tested.
  - Only server data is backed up, anything on the desktop (non-redirected folders) is at risk for loss.
  - District IT feels they could perform Disaster Recovery process within a couple weeks but have not documented or tested Disaster Recovery.
  - Server backups cannot be recovered virtually if needed.
  - Backup uses a disk to tape (D2T) process.
  - The district is not using the most current version (Backup Exec version 10.x.x) of their backup software.
  - Cory is responsible for monitoring the backups.
  - Backups are not stored off-site.
  - Backup strategy is daily normal.
  - Size of current backup is 350 GB.
  - It is unknown how long the backup process takes.
  - The district uses folder redirection of the “my documents” directory to the file server for staff at DCTC and Alliance.
  - There is no bare metal restore capability for servers.

- Recommendations:
  - Create a written data archive and restore policy, and test this policy quarterly.
  - Create a written disaster/recovery plan and test it annually.
  - Verify that all needed data is backed according to backup schedule.
  - Verify that Active Directory System State is backed up and tested.
  - Move to an enterprise backup solution and keep current.
  - Consider budgeting for an off-site data recovery solution.
  - Review the backup process and ensure that it meets the recovery plan for data.
  - Verify that the district meets the Minnesota state guidelines for backup and archiving.
  - Verify the implementation of folder redirection of workstation data.

  - It is critical to have the ability to perform bare metal restores of servers within a short time period (4 hours or less).

- Reasoning:
  - Moving a copy of the backup data to an off-site location creates a replica that would be available in case of data center loss.
  - Folder redirection will verify that My Documents Folder user data is captured to server storage for backup purposes.
  - Most school districts have a virtual internal cloud running with fast bare metal restore capability. It is vital for the recovery of district resources.

Section 1.2.6: Proactive Maintenance and Monitoring

- Findings:
  - The IT team monitors the systems manually.
  - The IT team does not monitor the network.
  - Cory monitors the Internet bandwidth utilization TIES software.
  - The District does have a help desk ticketing system (ZenDesk).
- Recommendations:
  - Verify Internet Service Provider (ISP) monitors Internet connection for up time and bandwidth utilization.
  - The districts IT staff should periodically monitor the ISP's provided monitoring information.
  - Implement a monitoring solution that monitors systems. (Microsoft System Center Configuration Manager SCCM).
  - Implement a monitoring solution that monitors network traffic. (Solar Winds or Ridgeline for Extreme).
- Reasoning:
  - Verification that bandwidth is sufficient for technology needs.
  - Remember that a help desk ticketing solution provides metrics to track support needs and IT productivity and needs to be shared with district administration.
  - Monitoring systems and network hardware is vital to the health of both subsystems.
  - Document the history of all changes to district technology. Future change of vendor could be necessary and should be seamless.

Section 1.2.7: Patch Management

- Findings:
  - The Districts patching strategy is a manual process with each workstation set to auto update by the end user.
  - The IT department is responsible for the patching of desktop systems.
  - The District does not have a patch management policy.
  - Microsoft SCCM with WSUS is not used to keep all Windows desktop Operating systems patched.
  - Firewalls and routers have not been updated with the latest firmware by IT.
- Recommendations:
  - Create a policy to adopt firmware, BIOS, and OS updates for all network, computer, and printing hardware.
  - Use an outside expert to implement Microsoft SCCM according to industry best practices.
  - Verify automatic patching is configured on all workstations.
- Reasoning:
  - Using an outside expert to implement Microsoft SCCM which will expedite the installation and guarantee installation according to industry best practices.
  - Using an outside expert to train IT Staff on Microsoft SCCM will increase administration efficiencies of district wide hardware and software.
  - Inconsistent patches can open security holes.

Section 1.2.8: Data Storage

- Findings:
  - The District has no written data storage policy.
  - Staff are not limited for storage on servers.
  - Storage limits are never reviewed.
  - Staff has a need for remote access to their data.
- Recommendations:
  - Create a written policy for data storage.
  - Implement a policy to institute collaborative services on the network.
- Reasoning:
  - A written policy can outline data storage limits and restrictions on personal files saved.
  - Access to data via manual copying to thumb drives (sneaker-net) lowers productivity.
  - Sneaker-net can lead to inconsistent, lost data, malware, and data security breaches.
  - Lost or missing district owned portable media is a possible security breech.

Section 1.2.9: Mail Storage

- Findings:
  - Mail storage limits are set but flexible by need.
  - E-Mail is not archived.
- Recommendations:
  - Implement a policy that defines the handling of e-mail for all users, including mailbox limits.
  - Implement an e-mail retention policy that aligns with district policy.
- Reasoning:
  - Every school district entity should have a written email retention policy that is defined by local and state laws.
  - Have a discussion with your attorney to define your legal needs and publish these in an email policy.

Section 1.2.10: Access – VPN/RPC

- Findings:
  - There is no formal written policy
  - District staff has a desire for remote access to their data.
- Recommendations:
  - Create a written policy for all remote access users.
  - Train users how to use remote access.
- Reasoning:
  - A written policy helps ensure good security practices are followed.
  - Training end users on the use of remote access will enhance end user productivity.

Section 1.2.11: Training

- Findings:
  - Newly hired district staff receive informal training.
  - District IT believes staff training needs improvement.
  - District IT believes staff training could be augmented with a train the trainer program.
  - No written district staff training policy is in place.
  - Staff ask other staff members “How do I” questions.
  - IT Staff desires a larger training budget.
  - No written district IT staff training policy is in place.
- Recommendations:
  - Create a written policy that defines a budget for professional training and development for new technologies for all users.
  - IT Staff should attend manufacturer’s technology certification training.
- Reasoning:

- Written policy should set goals for staff training certification.
- With any new technology expansion, training applicable staff to use and administrate the new technologies is of benefit to Intermediate School District 917 (ISD917).
- Training should be based on learning and technical needs of staff.

Prioritize Project Road Map

1. Update and expand Wi-Fi and base wireless on density and less on coverage especially in the district office and other high traffic areas.
    a. Pricing on wireless would depend on the results of a wireless audit. This is recommended to assess coverage needs (Price about $700 per wireless Access Point depending on manufacturer plus labor and implementation)
2. Migrate physical Microsoft servers to a virtual environment.
    a. Server Hardware $22,000
    b. Storage Area Network (SAN) $34,000

    By adding 5 TB of storage to two server hosts could be an alternative to purchasing a SAN. (Some features would be limited without a SAN). $12,000 estimated

    c. Licensing for Windows Data Center 2012 R2 $ 2,500
        i. Hyper-V Included in NOS
        ii. **Optional:** VMware with VCenter 5.x $17,300
    d. Here is what is included in your existing Microsoft 2UJ-00012 OVS bundle:
        i. Desktop Bundle with Core CAL
        Windows Upgrade Rights
        Office Professional Plus
        Windows Server CAL
        Exchange Standard CAL
        SharePoint Standard CAL
        System Center Configuration Manager CML
        Lync Server Standard CAL
        Forefront Endpoint Protection
    e. Virtual project Labor Estimate $15,000
3. Implement district-wide resource and file sharing solution. $ 2,500
4. Implement business continuity and disaster recovery strategies. $15,000 (annually)
5. Implement System Center Computer Management. $10,000
6. Firewall replacement with redundant pairs $13,000
7. Replace old switches that are out of warranty with 1/10 gigabyte network connections where needed.
    a. ($3,000 to $4,000 per switch plus labor)