Network Discovery and Security Report

Executive Summary

For

Montrose County School District

March 2021

Presented By:

sentinel CONSULTING
Creating Secure Environments

And

Chester Consulting Group

Contents

Executive Summary 3

Introduction 3

Why was this study necessary? 3

Collect Answers to the Following Operational Design Questions 3

Collect Answers to the Following Network Design and Layout Questions 3

Collect Answers to the Following Server Design and Layout Questions 3

Findings Related to the Servers, Workstations, End-users, and Help Desk Support 4

Findings Related to the Network and Communications Systems 6

Findings Related to the Operational Policies and Procedures 7

High Priority Policy Recommendations 8

Costs for Services 9

Total Cost for All Servers, Workstations, End-users, and Help Desk Support 9

Total Costs for All Network and Communications Systems Projects 12

Total Costs for All Operational Policies and Procedures Projects 13

Executive Summary

Introduction

The Montrose County School District (MCSD) engaged Chester Consulting Group (CCG), through our strategic partnership with Sentinel Consulting, the districts Security Consulting firm, to perform an overall assessment of the districts network. This assessment was conducted to identify deficiencies and vulnerabilities within the network and its support structure, ultimately resulting in the development of a plan to remediate critical deficiencies and vulnerabilities to stabilize the network. This being a critical first step in developing a long-term strategic technology plan for MCSD.

Why was this study necessary?

When we requested information on how the network was designed, built, and operated we were told that very little documentation existed. Therefore, Chester Consulting Group provided a team of consultants to gather information to provide an overview of the following:

Collect Answers to the Following Operational Design Questions

1. What practices are in place to guide the staff and employees on avoiding security problems?

Collect Answers to the Following Network Design and Layout Questions

1. How complex is the network?
2. What components were used to build the network?
3. How old are the components that are contained in the network?
4. How up to date are the software components that support the network?
5. What security measures are present and what additional measures are needed?
6. What are the most important things to correct on the network?

Collect Answers to the Following Server Design and Layout Questions

1. What kind of servers are there?
2. How many are there?
3. What are their functions?
4. What security measures are in place to protect them?
5. Who supports them?
6. How up to date are the servers and their software?

The result of this study provides input to developing a plan for:

1. Identifying security measures that must be implemented.
2. Selecting technology upgrades to improve network and server performance and security.
3. Planning critical IT Infrastructure clean-up and repair investments.

Findings Related to the Servers, Workstations, End-users, and Help Desk Support

The team investigated the systems and servers being operated by MCSD to provide IT services to the School District. These systems are the core components of the business operations and form the foundation of the learning environment. The findings are summarized below:

1. Servers are not managed by MCSD administrators or the current managed service provider. What is the reason behind this conclusion?

   ### Problems Detected

   a) The manufacturer's support contracts had lapsed on the servers that support the entire school district. Therefore, if hardware breaks MCSD has to use the more expensive route to replace broken parts and components if they fail. The warranty coverage should be renewed as soon as feasible.

   b) Software updates have not been performed on the servers since September 2019. The purpose of these software updates is to correct manufacturer defects and more importantly to eliminate security holes that can be exploited by hackers or malware. The lack of updates leaves the systems exposed and vulnerable to attack. These updates must be installed as soon as feasible.

   c) The servers are designed in a fashion that puts many critical functions on the same device. This exposes the District to a single point of failure that could impact the ability to serve the teaching environment. This also leaves the systems open to attack, if a hacker gets into this device there is nothing to stop them from accessing all of the critical systems. These systems should be rebuilt in the correct fashion to separate critical functions and services.

   d) The Microsoft and Apple security protocols that are built into the software and hardware are not being fully implemented. This has forced the District to develop its own version of these protocols, or not have them at all, which slows down implementation of new systems. We recommend migration to the standard security protocols provided by Microsoft and Apple.

   e) Data stored on the servers must be encrypted so that it is useless to unauthorized users.

2. End-users and their workstations are not managed by MCSD administrators or the current managed service provider. What is the reason behind this conclusion?

   ### Problems Detected

   a) End user computers have not been given the appropriate security software (anti-virus and other software to protect from hacking), is not installed. This leaves the computers, laptops, and tablets open to attack from malware and hackers. We recommend implementing these additional software packages as soon as possible.

   b) IT Policies and Procedures that should readily be available to offer guidance to the District's has not been developed or implemented. The protective guidance needed by the teachers, students, administrators, volunteers and vendors is not in the employee handbook or available to students on the website. Therefore, they are left without direction on how to protect themselves and the District's resources. We recommend developing and publishing these new policies as soon as possible.

   c) Data stored on PCs and laptops must be encrypted so it is useless to unauthorized users. We recommend turning on the vendor provided encryption tools.

d) Password and other security policies need to be updated to offer better protection. We recommend implementing more secure method of verification of end-user passwords, for example two-factor authentication.

3. The current help desk is not organized and setup to maximize service delivery. What is the reason behind this conclusion?

Problems Detected

a) Help Desk best practices are not being utilized to the maximum benefit to the District. This causes delays in support and loss of efficiency of staff resources. We recommend implementing better help desk procedures and practices and tools.

b) Help desk tools are generally owned by the managed service provider and charged back to the District. The loss of this vendor will also take away the tools the District needs to service the environment. We recommend the District begin to migrate off the service provider tools onto its MCSD support software tools.

c) Tools needed to set up a database of known problems and resolutions are not implemented, resulting in recurring problems and lack of root cause problem remediation. We recommend the District begin to use a tool that has the ability to create a database for tracking and identifying problems and their resolution.

d) The contract between the Managed Service Provider (MSP) and MCSD was not available. So, we had no way to determine the types and quality of services that the MCSD is committed to deliver. This would normally be spelled out in a service level agreement (SLA) portion of the contract. We recommend renegotiating or negotiating a contract that is flexible enough to include a SLA; while also allowing the existing IT department to bring as many services back into the District as possible.

Summary of Servers, Workstations, End-Users, and Help Desk Findings

We have provided MCSD’s IT leadership with a detailed report and plan of action to remediate all of the problems listed above and additional problems that were not mentioned in this summary report. We have provided a list of the priorities and projected cost for each repair or remediation activity.

Findings Related to the Network and Communications Systems

The team investigated the network and communications systems being operated by MCSD to support IT services to the School District. These systems are also part of the core components of the business operations and form the foundation of the learning environment. The findings are summarized below:

1. Network security is minimal and poorly implemented leaving large portions of the communications systems exposed to the potential of unauthorized access. We have provided a detailed report of all of these security issues and steps to remediate each problem area. We recommend implementing these recommendations as soon as feasible.
2. Administrative passwords allowing access to secure portions of the communications systems are not changed frequently or made to be significantly complex. This results in former employees with who may have older passwords to still have access to the communications equipment. We recommend employing a more complex password management system and more comprehensive policies governing how user passwords are created and managed as soon as feasible.
3. Software on the network components has not been kept up to date. Many systems are reaching end of life and end of sale, so they are no longer supported by the manufacturer. These components present the potential for hackers to exploit them or for uncorrected vendor software bugs to corrupt the operation of the network. We recommend replacing these components with new models as soon as feasible.
4. The overall design of the fiber optic network between the schools and the District Office is not optimum. It allows bottlenecks to occur which impacts the students and teacher's ability to conduct studies and educational functions. We recommend performing a true network design and replacing aging components. This can be done in conjunction with applying for E-Rate funding which will significantly reduce the cost of replacement components and upgrading bandwidth at the schools to eliminate bottlenecks.
5. The wireless network is poorly designed and installed. The end-users experience numerous problems while using the system. Security is non-existent on some portions of the network allowing vendors or students the potential to access sensitive systems which also have minimal security protection. We recommend a full redesign to improve the capabilities and protection systems of the wireless network as soon as feasible.
6. The current Managed Services Providers' contract does not encourage them to identify the source of problems and eliminate from the environment. We recommend bringing as many of the functions they perform in this contract back into MCSD.
7. Documentation of all of these systems is not available or not up to date. In order to provide the best support of the systems the support staff must have an accurate repository of how everything is built and connected together. We recommend having the vendor that redesigns the network provide the "as built" documentation to MCSD for their records and addition to a database for the Help Desk.

Summary of Network Communications System Findings

We have provided MCSD's IT leadership with a detailed report and plan of action to remediate all of the problems listed above and additional problems that were not mentioned in this summary report. We have provided them a list of the priorities and projected cost for each repair or remediation activity.

Findings Related to the Operational Policies and Procedures

The operational assessment focuses on the policies and procedures that are being followed by Montrose County School District (MCSD), to keep their information and systems secure and protect the privacy of the individual employees and students.

We were able to identify written IT policies found in the ***Student Use of Internet and Electronic Communication*** manual on page 106 of section entitled ***Selected Policies and Procedures for Parents, Students and Staff*** revised 2018. The list below is from that document and many of these policies are aimed at students, but also apply to staff. Here are the defined policies:

- Blocking or Filtering Obscene, Pornographic and Harmful Information
- No Expectation of Privacy
- Unauthorized and Unacceptable Uses
- Student Security on District Devices
- No Use of the Internet using an Administrator Account.
- Online Safety for Students
- Vandalism
- Unauthorized Content
- Assigning Student Projects and Monitoring Student Use
- Student Use is a Privilege
- School District Makes no Warranties.

While this is a great beginning, listed below are additional policies that need to be developed or strengthened to protect MCSD's staff and employee privacy and security. These should be implemented as soon as possible.

- Policies covering password usage, complexity, and management.
- Policies to setup Virtual Private Network (VPN) security for work from home executives, staff and vendors who need remote access to the school systems.
- Setup two-factor authentication for all VPN connections.
- Develop employee onboarding and off boarding procedures.
- Personal Information Stored in the Cloud Policy.
- Employee and Student Information security policy
- Remote access policy for staff and vendors
- Mobile device security policy for staff, students and vendors
- Security awareness and training policy
- Telecommuting/Work from home policy
- IT staff systems/data access policy
- BYOD (Bring Your Own Device) policy
- Home usage of MCSD-owned equipment policy
- Internet and email usage policy
- Acceptable Use policy
- Network Security policy
- Wireless Network and Guest Access policy
- Confidential Data policy
- Vendor Remote Access policy
- Vendor Management policy

High Priority Policy Recommendations

Due to the email breaches and other security problems associated with end user accounts, it is advised that the Montrose County School District reset all passwords, immediately. Additionally, all users should follow a 90-day policy requiring passwords to be changed. Passwords should be a minimum of 8 characters utilizing capital and lowercase letters, numerical values, and special characters. Passwords should not contain names or common phrases that can be easily determined.

Here are the recommended steps that must be completed to correct develop the policies and procedures:

1. Develop User and Password Management Best Practices and Policies
2. Create separate accounts for administrators to utilize.
3. Best practices recommend disabling user accounts for professionals who are no longer employed at Montrose County School District.
4. An onboard and offboarding strategy should be documented to ensure that user accounts are created and deactivated consistently. Also, users can be issued all security policies at time of hire.
5. Implement two-factor authentication for applications where possible.

The five steps above can also be performed in conjunction with the server and network cleanup projects discussed in the previous sections of this report.

Costs for Services

Total Cost for All Servers, Workstations, End-users, and Help Desk Support

Server Hardware Support Expired	Priority	Hardware			Software			Labor Hours			Grand Total
Replace Server Cluster	**1 = High**	**Unit Cost**	**Quantity**	**Subtotal**	**Unit Cost**	**Quantity**	**Subtotal**	**Unit Cost**	**Quantity**	**Subtotal**	
Dell EMC PowerEdge R640 - rack-mountable - Xeon Gold 5218 2.3 GHz - 64 GB	1	$7,089.99	4	$28,359.96				$100.00	80	$8,000.00	**$36,359.96**
Rack and Cable Servers	1							$100.00	8	$800.00	**$800.00**
Install & Configure Hypervisor	1							$100.00	8	$800.00	**$800.00**
Configure vSphere	1							$100.00	8	$800.00	**$800.00**
16 Gbps Memory DIMMs	1	$1,212.00	20	$24,240.00							**$24,240.00**
Install RAM	1							$100.00	16	$1,600.00	**$1,600.00**
Support License with VMWare	1				$1,367.99	2	$2,735.98				**$2,735.98**
Support Subscription Basic Technical Support for VMWare V-Sphere (Monthly Fee)	1				$279.99	4	$1,119.96				**$1,119.96**
Professional Services to Install and Configure the Cluster (One Time fee)	1							$150.00	150	$22,500.00	**$22,500.00**
Subtotal				**$ 52,599.96**			**$3,855.94**			**$34,500.00**	**$90,955.90**

	Priority	Hardware			Software			Labor Hours			Grand Total
	1 = High	**Unit Cost**	**Quantity**	**Subtotal**	**Unit Cost**	**Quantity**	**Subtotal**	**Unit Cost**	**Quantity**	**Subtotal**	
Microsoft ended support of Windows 7											
Lease Windows 10 upgrade	1				$11.00	1	$11.00	$100.00	2	$ 200.00	**$ 211.00**
The Microsoft Windows Server 2012 operating expires October 10, 2023.											
License Windows Server 2019	5				$809.99	3	$2,429.97	$100.00	6	$ 600.00	**$ 3,029.97**
Professinoal Services to Plan and Manage	1							$150.00	50	$ 7,500.00	**$ 7,500.00**
Subtotal				**$ -**			**$2,440.97**			**$ 8,300.00**	**$ 10,740.97**

	Priority	Hardware			Software			Labor Hours			Grand Total
	1 = High	**Unit Cost**	**Quantity**	**Subtotal**	**Unit Cost**	**Quantity**	**Subtotal**	**Unit Cost**	**Quantity**	**Subtotal**	
Critical Servers & Device Management											
Run software updates for end-user workstations (MAC OS and Windows). Need accurate inventory to forecast cost estimate. Labor estimate based on local resources performing this task. Approximately 1hr/device for patching	1							$100.00	100	$10,000.00	**$10,000.00**
Encrypt the hard drives of critical workstations and device in the MCSD domain.	1				$99.00	50	$4,950.00	$100.00	100	$10,000.00	**$14,950.00**
Implement Two-Factor Authentication Using Software Purchased in Network Report	1							$100.00	40	$4,000.00	**$4,000.00**
Professional Services	1							$150.00	40	$6,000.00	**$6,000.00**
Subtotal				**$ -**			**$4,950.00**			**$30,000.00**	**$34,950.00**

	Priority	Hardware			Software			Labor Hours			Grand Total
	1 = High	Unit Cost	Quantity	Subtotal	Unit Cost	Quantity	Subtotal	Unit Cost	Quantity	Subtotal	
Lack of Device Inventory											
Audit and document ALL MCSD devices. Create Inventory to document who has been assigned each physical asset. Labor estimate based on local resources performing this task.	1							$100.00	80.00	$8,000.00	**$8,000.00**
Backup all workstations and servers.	1							$100.00	80.00	$8,000.00	**$8,000.00**
Associate all assets with an individual user or department.	3							$100.00	80.00	$8,000.00	**$8,000.00**
Manage all Apple Devices utlizing JAMF (Need accurate inventory to forecast cost estimate) Labor estimate based on local resources performing this task. Unit cost reflects monthly recurring fees for 1130 devices. (Monthly Fee)	1							$100.00	80.00	$8,000.00	**$8,000.00**
Purchase subscription of Datto RMM. Unit cost reflects monthly recurring fees. 1130 devices. (Monthly Recurring Fee)	1				$600.00	12	$7,200.00				**$7,200.00**
Subtotal				**$ -**			**$7,200.00**			**$32,000.00**	**$39,200.00**

	Priority	Hardware			Software			Labor Hours			Grand Total
	1 = High	Unit Cost	Quantity	Subtotal	Unit Cost	Quantity	Subtotal	Unit Cost	Quantity	Subtotal	
Lack of Patch Management Strategy for Critical Servers and End-Point Devices											
Lack of Antivirus and Malware Protection on Critical Servers and Devices	2										**$0.00**
PC Matic Ransomeware. Approximately 1hr/device. Licenseing for 100 devices.	2				$1,000.00	1	$1,000.00	$100.00	10	$1,000.00	**$2,000.00**
Upgrades and Changes Not Managed	2										
PC Matic Patch Management. Approximately 1hr/device. Licensing for 100 devices.	2				$1,000.00	1	$1,000.00	$100.00	10	$1,000.00	**$2,000.00**
Inconsistent Device Naming Convention	2										**$0.00**
Professional Services Advising								$150.00	10	$1,500.00	**$1,500.00**
Subtotal				**$ -**			**$2,000.00**			**$3,500.00**	**$5,500.00**

	Priority	Hardware			Software			Labor Hours			Grand Total
	1 = High	Unit Cost	Quantity	Subtotal	Unit Cost	Quantity	Subtotal	Unit Cost	Quantity	Subtotal	
User Account Access and Security Groups											
Require all Faculty, Staff and Students to reset their passwords every 90 days.	1							$100.00	10.00	$1,000.00	**$1,000.00**
Separate faculty and staff administrative access. Employees should only use elevated privileges when required. Create a separate admin account for each user requiring elevated privileges.	1							$100.00	16.00	$1,600.00	**$1,600.00**
Implement Two-Factor Authentication	1										
Subtotal				**$ -**			**$ -**			**$2,600.00**	**$2,600.00**

	Priority	Hardware			Software			Labor Hours			Grand Total
	1 = High	Unit Cost	Quantity	Subtotal	Unit Cost	Quantity	Subtotal	Unit Cost	Quantity	Subtotal	
Auditing and Security Recommendations											
Problems with User Credentials Compromised								$100.00	10.00	$1,000.00	**$1,000.00**
Enable auditing using Microsoft Group Policy. Users requiring admin privileges should have a separate account that is used for adminstrative access only.	3							$100.00	1	$100.00	**$100.00**
Problems with Local Administrator Accounts								$100.00	4	$400.00	**$400.00**
Disable Local administrative accounts unless absolutely necessary. Disable Local a	2							$100.00	1	$100.00	**$100.00**
Secure Domain Controllers by Implementing Firewalls and Disable RDP	2									$0.00	**$0.00**
Professional Services advising and review								$150.00	10	$1,500.00	**$1,500.00**
Subtotal				$ -			$ -			**$3,100.00**	**$3,100.00**

	Priority	Hardware			Software			Labor Hours			Grand Total
	1 = High	Unit Cost	Quantity	Subtotal	Unit Cost	Quantity	Subtotal	Unit Cost	Quantity	Subtotal	
Issues with FSMO Role Placement											
Upgrade Domain Controllers											
Upgrade to Windows Server 2019. Primary Domain Controller, and AD	2							$100.00	4.00	$400.00	**$400.00**
Upgrade to Windows Server 2019. Secondary Domain Controller, and AD	2							$100.00	4.00	$400.00	**$400.00**
Upgrade to Windows Server 2019. Primary DNS/DHCP Server.	2							$100.00	2.00	$200.00	**$200.00**
Upgrade to Windows Server 2019. Secondary DNS/DHCP Server.	2							$100.00	2.00	$200.00	**$200.00**
Upgrade to Windows Server 2019. Webserver	2							$100.00	2.00	$200.00	**$200.00**
Upgrade to Windows Server 2019. RDP Server	2							$100.00	2.00	$200.00	**$200.00**
Professional Services Microsoft Best Practices	2							$150.00	75.00	$11,250.00	**$11,250.00**
Subtotal				$ -			$ -			**$12,850.00**	**$12,850.00**

	Priority	Hardware			Software			Labor Hours			Grand Total
	1 = High	Unit Cost	Quantity	Subtotal	Unit Cost	Quantity	Subtotal	Unit Cost	Quantity	Subtotal	
Properly Setup the Additional Domain Controllers and Support Servers											
Correct DNS Loopback IP Address on Server. Use DNS servers instead of loopback address.	1							$100.00	1	$100.00	**$ 100.00**
Subtotal				$ -			$ -			**$100.00**	**$100.00**
Total Estimate for Server Projects				**$52,599.96**			**$20,446.91**			**$126,950.00**	**$199,996.87**

Legend	
Monthly Fees	🟨
One Time Fees	🟩

Total Costs for All Network and Communications Systems Projects

Order In Report	All Recommended Network Remediation Tasks	Recommended Implementation Order	Estimated Labor Hours	Estimated Professional Services Cost			Estimated Hardware Cost		Estimated Software Cost		Professional Services, Hardware, and Software Total
				Bell Tech Pros or Other IT Vendor Fees	Amount Paid by E-Rate	Chester Consulting Fees	Amount Paid by MCSD	Amount Paid by E-Rate	Amount Paid by MCSD	Amount Paid by E-Rate	
1	Remove Primary Network Routing Functions from Firewall	1	120	$6,588.00	$15,372.00		$20,000.00		$0.00		$41,960.00
25	Firewall Acting as the Main Router	1	120	$6,588.00	$15,372.00		$30,000.00	$70,000.00	$0.00		$121,960.00
5	Minimize Use of Unencrypted Administrative Traffic	2	60	$10,980.00			$0.00		$0.00		$10,980.00
32	Unencrypted Administrative Traffic	2	60	$10,980.00			$0.00		$0.00		$10,980.00
7	Implement Two-Factor Authentication. $8 per month per user	3	60	$10,980.00			$0.00		$19,200.00		$30,180.00
41	Single Factor Authentication. $8 per month per user	3	60	$10,980.00			$0.00		$19,200.00		$30,180.00
4	Define A Network Security Model	4	80	$14,640.00			$0.00		$0.00		$14,640.00
31	Network Security Model	4	80	$14,640.00			$0.00		$0.00		$14,640.00
2	Implement Functional Segmentation of Traffic	5	240			$43,920.00	$0.00		$0.00		$43,920.00
27	Lack of Functional Segmentation of Traffic	5	240			$43,920.00	$0.00		$0.00		$43,920.00
8	Implement Stronger Credentials on BYOD Wireless Network Vulnerability	6	4	$732.00			$0.00		$0.00		$732.00
42	BYOD Wireless Network Vulnerability	6	4	$732.00			$0.00		$0.00		$732.00
6	Encrypt Wireless Networks	7	20	$3,660.00			$0.00		$0.00		$3,660.00
40	Wireless Network with no Encryption	7	20	$3,660.00			$0.00		$0.00		$3,660.00
3	Implement Quality of Service Priorities	8	80	$14,640.00			$0.00		$0.00		$14,640.00
29	Quality of Service Implementation	8	80	$14,640.00			$0.00		$0.00		$14,640.00
44	High Firewall CPU Utilization	9	120	$21,960.00			$0.00		$0.00		$21,960.00
47	Use of Reject in Filter Rules	10	16	$2,928.00			$0.00		$0.00		$2,928.00
48	Little Documentation on Requirements	11	240			$43,920.00	$0.00		$0.00		$43,920.00
49	Unneeded/Unused Definitions	12	240	$43,920.00			$0.00		$0.00		$43,920.00
45	Broad Network Source and Destinations Filter Rules	13	320			$58,560.00	$0.00		$0.00		$58,560.00
46	Lack Of Protocol Restrictions in Filter Rules	14	320			$58,560.00	$0.00		$0.00		$58,560.00
35	Use of Passwords Only	15	60	$10,980.00			$0.00		$0.00		$10,980.00
34	Trivial SNMP Community Strings	16	60	$10,980.00			$0.00		$0.00		$10,980.00
33	SNMP Filtering	17	60	$10,980.00			$0.00		$0.00		$10,980.00
39	Web Interface Enabled	18	60	$10,980.00			$0.00		$0.00		$10,980.00
37	Automatic Cisco IOS Image Verification not Enabled	19	60	$10,980.00			$0.00		$0.00		$10,980.00
38	Security Authentication Failure Rate Not Enabled	20	60	$10,980.00			$0.00		$0.00		$10,980.00
36	Local Authorization	21	80	$14,640.00			$0.00		$0.00		$14,640.00
20	Spanning-tree Path cost Method	22	60	$10,980.00			$0.00		$0.00		$10,980.00
19	Spanning-tree Priorities	23	60	$10,980.00			$0.00		$0.00		$10,980.00
22	Storm Control Not Enabled	24	60	$10,980.00			$0.00		$0.00		$10,980.00
23	Wireless Network Design	25	180			$32,940.00	$0.00		$5,000.00		$37,940.00
18	High CPU Utilization	26	120	$21,960.00			$0.00		$0.00		$21,960.00
17	High Number of Interface Errors	27	80	$14,640.00			$0.00		$0.00		$14,640.00
14	Log Sequence Numbers not Enabled	28	60	$10,980.00			$0.00		$0.00		$10,980.00
15	NAGLE Service is not Enabled	29	60	$10,980.00			$0.00		$0.00		$10,980.00
21	MAC Address Move Notification not Enabled	30	60	$10,980.00			$0.00		$0.00		$10,980.00
13	Device Operating System Versions	31	240	$43,920.00			$0.00		$0.00		$43,920.00
26	Static Routes	32	120			$21,960.00	$0.00		$0.00		$21,960.00
12	Device End-Of-Life and End-Of-Support Status	33	900	$49,410.00	$115,290.00		$360,000.00	$840,000.00	$0.00		$1,364,700.00
	Total for Recommended Network Remediation Projects		**5,024.00**	**$469,578.00**	**$146,034.00**	**$303,780.00**	**$410,000.00**	**$910,000.00**	**$43,400.00**	**$0.00**	**$2,282,792.00**

Legend	
Monthly Fees	🟨
One Time Fees	🟩
One Time Fees	🟦

Total Costs for All Operational Policies and Procedures Projects

	Priority	Hardware			Software			Labor Hours			Grand Total
	1 = High	Unit Cost	Quantity	Subtotal	Unit Cost	Quantity	Subtotal	Unit Cost	Quantity	Subtotal	
Develop Policies and Procedures											
Personal Information Stored in the Cloud Policy	1							150	8	$1,200.00	**$1,200.00**
Information security policy	1							150	8	$1,200.00	**$1,200.00**
Remote access policy	1							150	8	$1,200.00	**$1,200.00**
Mobile device security policy	1							150	8	$1,200.00	**$1,200.00**
Security awareness and training policy	1							150	8	$1,200.00	**$1,200.00**
Telecommuting/Work from home policy	1							150	8	$1,200.00	**$1,200.00**
BYOD (Bring Your Own Device) policy	1							150	8	$1,200.00	**$1,200.00**
Home usage of company-owned equipment policy	1							150	8	$1,200.00	**$1,200.00**
IT staff systems/data access policy	1							150	8	$1,200.00	**$1,200.00**
Internet and email usage policy	1							150	8	$1,200.00	**$1,200.00**
Acceptable Use policy	1							150	8	$1,200.00	**$1,200.00**
Network Security policy	1							150	8	$1,200.00	**$1,200.00**
Wireless Network and Guest Access policy	1							150	8	$1,200.00	**$1,200.00**
Confidential Data policy	1							150	8	$1,200.00	**$1,200.00**
Employee Off-boarding policy	1							150	8	$1,200.00	**$1,200.00**
Vendor Remote Access policy	1							150	8	$1,200.00	**$1,200.00**
Vendor Management policy	1							150	8	$1,200.00	**$1,200.00**
Totals							**$0.00**		**136**	**$7,200.00**	**$7,200.00**