# University of Saint Asterisk Cyber Defense Strategy Planning

***John Mettler***

***Marc Moran***

***Elijah Lasater***

***Phillip Longo***

Saint Leo University

April 2015

# Table of Contents

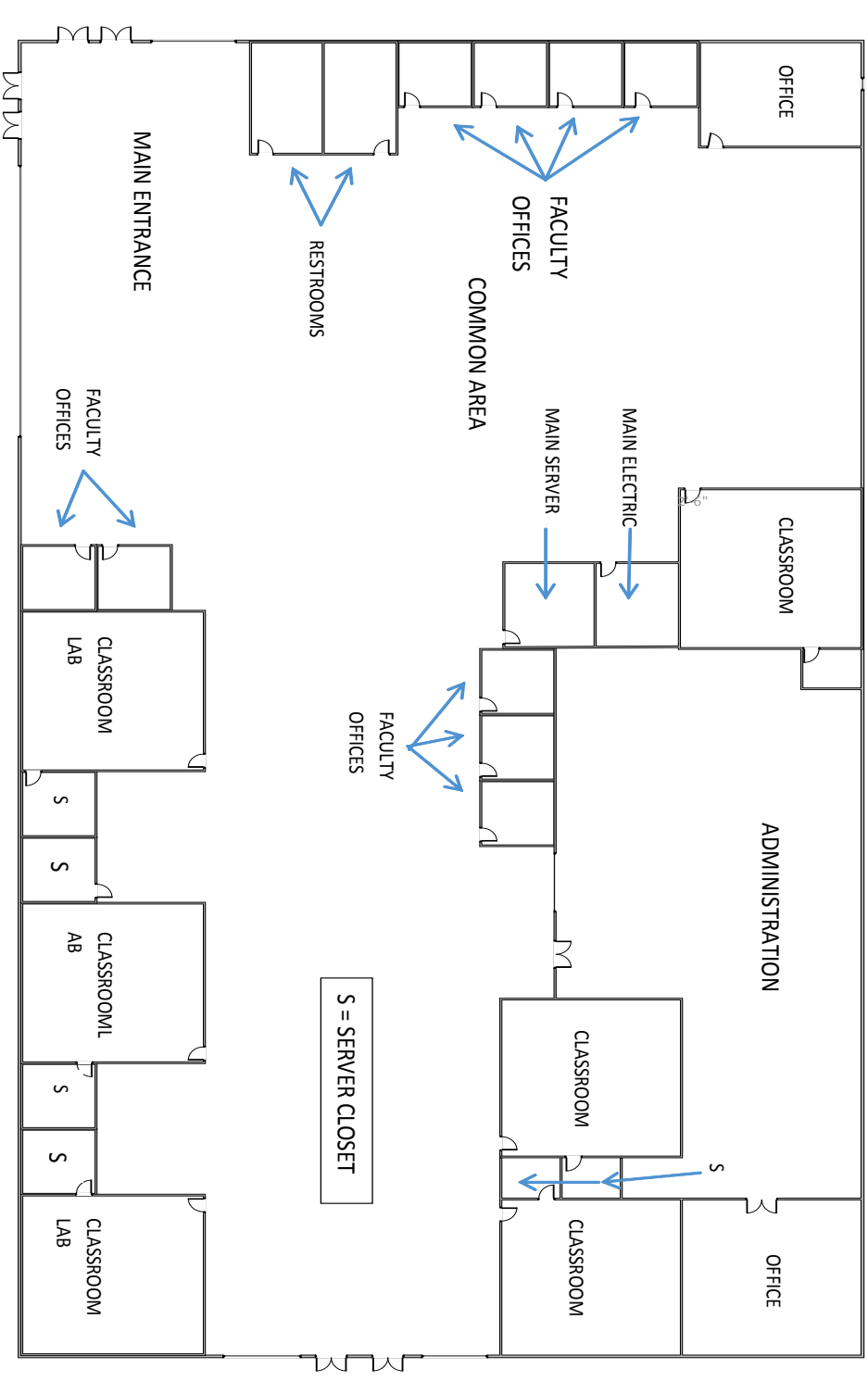
# Introduction

The purpose of this project was to allow us to have a chance to step into the shoes of defense planners for a building-wide network. This became a research project that allowed each of us to learn more about various parts of defending a building or work place and in the preparation and creation of a policy plan. By comparing the policies from professionals, ranging from important policy-defining companies like SANS to the individual policies of schools and businesses, a lot of information was gathered on how to create a proper and tight set of policies. This opportunity also gave us a chance to pool our knowledge together and teach each other all the important parts that made up our sections, expanding all of our knowledge on the subject four-fold. The importance of this project lies in that it helps prepare us for the future of working in a policy creation and computer defense setting.

# Executive Summary

We here at **DDISC**, or **Defense-Driven Information Security Consulting**, have been approached by the University of Saint Asterisk to create an overall assessment report and defense plan for the new computer lab building off campus. USA has provided information on the current set-up they have for their building and want to hear a proposal for new security measures and recommendations to better protect the labs. To help the university get a grasp of their situation and how to better prepare themselves for the future, we will be tackling four different sections: **Physical Environment, Network Infrastructure, Servers, and Workstations**. These will be accompanied with other policies, such as a Bring Your Own Device and Disaster Recovery policy. The first thing we will do in order to prepare the report is to do a current status report of what the USA already has in terms of security, equipment, and software, followed by suggestions for upgrades, recommended guidelines, and price details.

# Floor Plan




FACULTY OFFICES (9) MAIN SERVER ROOM (1) DEPARTMENT HEAD OFFICES (2)

CLASSROOMS WITH LAB (3) MAIN ELECTRIC ROOM (1)

CLASSROOMS UPGRADABLE (3) ADMINISTRAION AREA SAINT ASTERISK SATELLITE LOCATION

# Physical Environment

## Overview

The goal of DDISC is to ensure that the new St Asterisks satellite location is providing a Physical Environment suited for the optimal performance and security of all IT equipment. Physical Security is one the most overlooked elements in securing information. It is the responsibility of DDISC to make our clients aware of the latest methods and techniques being used to infiltrate the most secured organizations. Social engineering has been taken to the next level to gain physical access to secure facilities. Even though St Asterisks is not a high tech company with proprietary information, the same care should be taken as to not be victimized by attackers. Physical security breaches can result in more damage to an organization than say a worm attack. The areas that will be addressed by this section of the report are heating/cooling, humidity, physical space, physical security, fire suppression and the backup power supply. DDISC will also make recommendations to the Physical Security policy as it pertains to the new location.

## Current Specifications

DDISC was provided an as is blueprint that shows the state of the current facility. There is an existing main server location and electrical room located in the main common area. The Electrical room is connected to Florida Power for electric service and to Bright House Cable for ISP. Existing wire and cabling are to be utilized in efforts to control cost. There are nine offices that are to be utilized for faculty and two larger offices are to be used for administration. The existing administrative area will be utilized in the same manner. There are six classrooms total,

three will be used as computer labs. Each classroom has its own server room for a total of six. The following deficiencies should be addressed so all IT systems can run with maximum efficiency and security.

## Environmental Evaluation

### Temperature and Humidity Control

The main server room has server cabinets positioned directly on the floor. This minimizes the circulation of air within the room. Server cabinets have also been placed along the walls. This prevents proper air flow to those units. Further growth is anticipated as more computer labs will be brought online in the future. Though the current temperature in the room is suitable for operation, the current room configuration is inefficient and could cause loss of equipment. Temperature and humidity should be maintained within the manufacturer's parameters. We recommend that a raised floor system be installed and all server cabinets be relocated away from walls. Existing AC ducting should be rerouted to provide cold air flow through perforated tiles in the raised floor. A hot aisle / cold aisle approach will be utilized to provide proper cooling taking into account future growth. Hot aisle containment encloses and captures the hot exhaust and ducts it directly back to the computer room air conditioners. The cold air containment side provides the cooling. A $6500 capital investment, 24 hours labor at estimated rate of $126/hr. = $3024 to install raised floor, reconfigure server cabinet locations and air ducting. Extension of fiber and or copper wire is included.

### Environmental Alarming

There is no monitoring and alarming if the ambient temperature exceeds recommended thresholds. Proper monitoring and notification of temperature and humidity is vital to heading off

any potential emergency situations and protects the investment in IT equipment that could otherwise be lost. It is recommended that temperature and humidity alarms be implemented via the X310 Web-Enabled Programmable Controller. This is a cost effective device that is easily adaptable. It allows for continuous monitoring of all nine server rooms environments and provides an audible alarm as well as email and text message to the appropriate personnel. A $2895 capital investment, 9 hours labor at estimated rate of $135/hr. = $1215 to install monitoring unit and sensors in all nine server locations. Unit uses existing cabling.

## Maintenance

We also recommended that a comprehensive service plan that is specifically designed to provide preventive maintenance, reliable 24/7 emergency service and corrective measures to be taken be instituted. The Maintenance Service Plan should include:

- Development of an annual preventive maintenance schedule.
- Routine physical site inspections.
- Review of all service reports.
- UPS and battery maintenance / replacement.
- Power and data cabling physical inspection.
- Implementing a routine of inspecting all air ducts and cooling fans on servers for dust will ensure optimal cooling.
- Systematic vacuuming to remove dirt, dust and contaminates.
- Maintenance staff should be trained on the effects of rapidly dropping temperatures causing condensation within either the electric room or the main server room.
- Inspection of fire suppression and detection systems.

- Procedure for reporting findings.

## Physical Security Evaluation

### Physical Access

Currently, access to the entire facility relies on a mechanical lock and key method. There are inherent disadvantages to this system. The simple loss of a key can cost the organization tens of thousands of dollars for each occurrence. Currently all proposed faculty offices are accessed with same key. The two administrative offices also have a common key. There are also identical keys for the server rooms throughout the building. The master key provided to custodial staff allows access to every door in the facility with no way to track them. In general, there is a lack of accountability and an excess of accessibility. It is recommended that the Cisco Physical Access Control which includes the Physical Access Gateway and Physical Access Manager be implemented. The installation of card readers and electronic locks on all offices, classrooms, server rooms and main entrances will be required. Installation of CCTV cameras at each entrance of the facility is a necessity. This will provide the added security necessary in the absence of security guard.

The software component will be integrated with Microsoft Active Directory. It removes the redundancy of having two access data bases by allowing Active Directory to work in conjunction with the Cisco Physical Access Manager software. It eliminates the need to manually add and remove users from the system. This unit provides a centralized solution replacing traditional physical access controls. Traditional controls require expensive main control panels. Unlike physical access control solutions from door and camera vendors, the Cisco Physical Access

Control solution takes full advantage of IP network capabilities. Features of the Cisco Physical Access Control include:

- Each gateway controls up to two doors.
- Provides simplicity and ease of user management through Active Directory and existing HR databases.
- Any door in the facility can be locked down remotely to enhance campus security.
- Uses a power over Ethernet (PoE) switch.
- Let's you power badge readers and lock strikes with PoE.
- Ease of installation (single door can be fitted in 15 minutes)
- Allows you to add one or two doors at a time.
- Easily integrates with Cisco video surveillance manager.

Badge readers will be placed on all doors. Access to all computer rooms will be restricted to only those who maintain the servers or provided service to the infrastructure of the room. Access should be restricted to emergency access only on holidays. The cost of the above modifications is $50,000.

### Fire Suppression

Excessive heat is an unfortunate danger in a server room. It is a necessity to have a fire suppression system that is designed for computer rooms. Since the installation of halon systems and the refilling of halon tanks are now illegal in the United States, it is necessary to replace the current system. FM 200 is now the current standard replacement for halon. It can be dispersed in 10 seconds or less, and does not leave behind any residue. A typical clean agent system is comprised of storage components, distribution components, a control panel and early warning

detection and alarm devices. The system can act automatically, but also has a manual release located within the room. Fike's HFC – 227 clean agent fire suppression systems is a trusted name that provides versatility with cost effectiveness. The system, including all piping, tanks, controls and installation is estimated at $5500. We believe this system will provide an economical, environmentally acceptable fire prevention solution. We also recommend installing very early smoke detection apparatus (VESDA). Detection at the earliest possible time can prevent a fire from erupting and allow it to be extinguished before it can impact the overall operation of the facility. Due to the volume of air flow within the server room it is difficult for standard smoke detectors to operate efficiently in this environment. VESDA is a laser based detector that draws air in much like a vacuum. It sucks air in and samples the quality by passing it through a detection laser chamber. The VESDA VLF-250 detector is designed to protect rooms up to 2500 sq. ft. at $1600. Servicing of all fire suppression related systems should be addressed in the Maintenance Service Plan.

### Power Supply

The facility is reliant on an external provider for electricity. Every external provider will experience a service interruption at some point in time. The facilities location, Florida, makes this even more likely due to amount of lightning strikes each year. All IT equipment must be protected from power issues. Multi–mode UPS systems provide the optimal blend of both efficiency and protection. Under normal conditions, the system operates saving energy and money while also keeping voltages within safe tolerances and resolving common anomalies found in utility power. In facing power falls outside preset tolerance, the system automatically switches to double conversion mode, which completely isolates IT equipment from the incoming AC source. The AC input power fails UPS uses the battery to keep supportive loads up and

running. Multimode systems are designed to provide efficiency when input powers normal and deliver maximum levels of protection when it is not. We recommend installing (2) Tripp Lite SU30K3/3 UPS units at a cost of $24,000. Tripp Lite provides proprietary software called Power Alert Network Shutdown Agent that enables a systematic shutdown when specific power events occur. It “listens” to an SNMP-capable device on the local network that is directly connected to the UPS system, which allows the execution of a shutdown procedure when set parameters are not in line. Servicing of the UPS system should be addressed in the Maintenance Service Plan.

## Physical Environment Pricing

Here is the list of products recommended and the overall price for physical environment policy and security:

1. Modifications to server room to include raised floor, air conditioning modifications, labor and materials = $9,524
2. Temperature and humidity alarms and X310 controller = $4,110
3. Cisco Physical Access Control and all peripherals = $50,000
4. FM 200 fire suppression system = $5,500
5. VESDA smoke detection = $1600
6. (2) Tripp Lite SU30K3/3 UPS = $24,000

Total for modifications = $94,734.

# Server Use and Security

## Overview

Servers are the middle point between workstations and the rest of the system. It will be utilized to backup files, run webmail, and help in web searching. Servers need to have both hardware and software to run correctly. As many as one thousand users will be using the system, however not as many of these people will have direct access to the server systems. The important thing to do is to make sure that the location of the hardware is completely locked down, and that the server software has proper protocols to only allow those users that need access to have access.

## Current Specifications

Currently the school has seven spots for servers to be located, six of them in each classroom, and one in the server room. In the server room there are currently 4 servers that are being ran. The servers are running 4 differing environments including: File, Mail, Web, and Domain Control. The servers that currently being ran are Dell PowerEdge 2650, Dell PowerEdge 1850, and Dell PowerEdge 2950. The operating systems that are being ran on the servers are Windows 2008. These servers are currently equipped to the servers in classrooms which are equipped to the workstations.

## Server Management

The following sections details items that are required and/or recommended for servers belonging to USA, including server related devices, applications, and policies.

## Upgrades

The software that is being currently ran as server operating system is Windows 2008, which will soon become the next in line for End of Live (EOL). The mainstream support for Windows 2008 has since been discontinued. This means that there will not be any new advancements in the software. Microsoft will also not accept any new requests for updates in Windows 2008. Since Windows 2008 is almost a decade more vulnerabilities will become existent than the newer software. Newer Windows 2012 has greatly expanded upon Windows 2008 with new programs and/or enhanced programs which will help in setting up, utilizing, and maintaining the servers.

The current server set-up consists of discontinued hardware which consists of Dell PowerEdge 2650, Dell PowerEdge 1850, and Dell PowerEdge 2950. These servers will not be able to withstand the updated Windows 2012 since the Operating System needs to be run with 64 bit processors, which these servers do not have. Also the running of these servers will be more than getting a new all-in-one server that will help run the school. The server that will be running the school entirely will be Dell PowerEdge R920 Rack Server. This server has all the capabilities plus more than what those servers had. This one server has up to 6TB of memory which if broken down correctly to run mail, web, and domain environments, which were running on those other servers, will be running 3TB each. The current servers do not currently have 3TB of memory. The storage space on this server consists of 28TB of data, which will help in holding the data for web, mail, and domain controls. However the file environment will need to have its own appliance/server attachment. Though the storage space may seem to be a lot on the R920, for files that amount of storage will be quickly drained. The appliance/server attachment that will be needed for file storage will be Dell PowerVault NX3230. Since R920 will consists of networking ports, this appliance will be easily added to the server setup. NX3230 will contain

72TB of space, and memory space of up to 32GB of RAM. This appliance will also be part of the Network Attached Storage (NAS) which will be utilized by the R920 server to place files onto this appliance. Currently the pricing of R920 server on Dell's website is $9,699, and the NX3230 price is $2,779. All together the servers for the current set-up will be $12,478. In addition to the current set-up the school will also need servers per classroom which will help both in productivity in the classroom, as well as limiting bandwidth overload which will help lower any catastrophic events on the main server. The server per classroom will help in running of Smartboard technologies, also help in monitoring the student's workstations, and as well as give access to both professors and students to their own school accounts. This server will be directly connected to the main server, while it will also help monitor any incoming and outgoing traffic to the main server and classroom servers. PowerEdge T320 Tower Server will help in monitoring, and giving access to the main server. This server will offer 4GB of RAM, and 500GB of storage. This server will not need to utilize all of it RAM since all it will be doing is overseeing and pulling files from the main server. This server will cost $999 and all together this server hardware will cost $5,994 which will be getting the school 6, 1 for each classroom. All together for both the main servers, and classroom servers will cost $18,472.

### Security Control

Physical control is a major part when it comes to protecting servers. The rooms where the servers are located should be kept at a reasonable temperature and meet the Florida Building Code. The rooms should be locked up when not needed to be operated on physically. Keeping the room under certain conditions will need protocol of not allowing eating or drinking in the specific room. Cleaning of the rooms should occur periodically up to twice a week to minimize any dust going into the system. The door shall be closed upon entering the server room, which will

minimize any unauthorized people access while the room is being utilized. The door shall also not have a sign as to whether it is a server room, to minimize any changes to the server hardware. Only those that need access to the server rooms will be granted access with their identification tag. As to professors who need access to certain classroom servers, their access will be limited. The professors will only access the classroom servers at the scheduled times they have classes in the specific room. If they do need access to the specific room after class times, they must contact the information security office. Those that have access to the server rooms should have their identification tag on them at all times. The tag shall not be given to any other person, unless specified by information security office. Limiting the transfer of the identification tag will limit any unauthorized people access to the server rooms.

Software security is also a major part when it comes to protecting the server system. The main server will have great access to the outside world since it will handle any incoming or outgoing traffic with the web service environment. Protecting the main server should/and will be a key priority. The main server will be the brains of the satellite school. To protect the server, while following the same outline as physical, the server shall only grant access to those that need it. With Active Directory those that have granted access to the server room will also have high escalation access to the server software. Professors, and students will have lower access to the server. Active Directory will dictate as to where the users shall/shall not go on the server.

## Implementation

Virtual Machine software will be needed to run the differing environments on the server. Since there will only be one server hardware to run three differing environments, virtual machine will be running all these environments on that one machine. To help in installing virtual machine software, Windows 2012 comes pre-installed with Hypervisor, which is Microsoft owned virtual

machine software. There will be no need to purchase any software to run all these differing environments. The environments will include: Domain Control, Web, Files, and Email. Hypervisors will also come with virtual storage options, so adding any needed applications to these environments will be easy. Files can also be added with through the main machine and be utilized in the virtual machine. Hypervisor can also coordinate processes between differing users at one point in time to ensure that all the necessary resources are distributed. However since the file host will have its own hardware it will be utilizing the Windows 2012 software alone. The file host will be critical to running a school, since files is something that is needed for schools.

## Environments & Implementation

The server system will be utilizing multiple environments to run the system smoothly. These environments include: Email, Web, Domain Control, and Files. Three of these environments will be running on one single server which will be running in the Hypervisor software, virtual machine software. Of these four environments, Files will have its own server, utilizing the Network Attached Storage (NAS) network, which will be equipped to the main server. The File will have its own server due to the amount of storage that File servers will need to allocate.

**Email:** This domain will be necessary for outgoing/incoming emails to/from the server, and will also define what can be put in emails, and what cannot be put in emails. All emails must go through a scan prior to being sent to the recipients mailbox. A great tool that will monitor all incoming and outgoing emails is Paessler PRTG. Emails that may seem threatening to either the environment, or school must be placed in quarantine to ensure that the emails are not opened. Emails that are of such nature must pass proper protocols to ensure that they are not threatening, otherwise the emails recipient will not receive the email. To guarantee that the system is not threatened emails that do not pass proper protocols are saved in proper quarantine for future analysis. If an email passes the testing phase and is opened by a professor or administrator, they must alert the information security office immediately. This will minimize any more

risk that then what was put on either the server, or workstation. Outgoing emails will also be monitored to ensure that the sender is allowed to be sending on the email server. The only allowed users on the email server include administrators, and professors. The students will be receiving and utilizing the main campus email extension. The email server will be utilizing the IMAP protocol to ensure that all emails will be able to remain on the server, and be acquired from any location, at any time with proper user authentication.

**Web:** This domain will be necessary for outgoing/incoming traffic to/from the server. This environment will have to withstand attacks since this is the part of the system that regularly gets exploited. To help in lowering the exploitation use the rule of disabling all services, and applications, then re-enable only those that are necessary for web services. Also for confidential files be sure that the web environment will not have public access to these files. Utilizing the protocols SSL/TSL will be necessary for going into private and confidential web pages.

**Domain Control:** This domain will be necessary to ensure that the system, user information, and private information is kept safely in the servers. This will help in authentication processes to enter multiple server resources. A user may enter the differing server resources without having to enter the account information multiple times. This will minimize in allocating multiple login resources when an administrator needs to enter the other server resources. Minimizing the allocation will help in more throughput for other users in the server. This environment will be greatly integrated into Active Directory, which will be greatly utilized. It will allow only those that need/have access to the network, onto the network, otherwise it will disallow those users that are not allowed onto the system.

**Files:** This domain will be necessary for ensuring that only specific types of files will be stored, and being a backup location for the server domains. To maximize the amount of storage on the server there should only be specific types of file extensions stored on this server. Types of files that will be banned on the server include video, ISO, and RAR extensions. These types of file extensions can greatly take up space on the file server, and is not necessary for school activities. If for a reason that a professor needs to place

a video extension, or any file extension that is banned on the server, the professor should ask the server administrator to make an exception. Files that will be accepted on the server include Word, Excel, and PowerPoint extensions, this includes from Microsoft Office Suite, and any other productivity suites. This will ensure students, professors, and administrators will be able to store their necessary documents without any exceptions. Server domain settings will also be backed-up to this domain. The settings will be backed up on an hourly basis, with deletion of the past backed settings being deleted on a monthly basis. Including, if files do go unchanged for more than two years, the files are automatically removed from the server to make room for more files. The files should be deleted at the end of every school year prior to the school closing, with an email being sent out in the middle of the semester. The email should alert the students, professors, and administrators that the files that they may have on the school file server may be removed. This will allow those that have files on the server to be able to retrieve the files, and backup them up to their own local hard-drives.

### Monitoring

With Cisco Manager the access to the physical sever hardware will be kept. Cisco Manager will keep a log as to whom accessed the server rooms and at what time. The access will be directly linked to the identification tags that are needed to enter the server rooms. The Cisco Manager will also be equipped into Active Directory. The server settings will also be backed up periodically to confirm that any drastic changes to the server will be able to be recovered. This will make sure that downtime will be considerably lowered since the server could be automatically recovered without needing to bring the server down for a long period of time.

Cisco Manager and Active Directory will Track:

- Access to school building: After school hours if a professor, administrator, or student needs to access the school building they will be allowed to by using their identification tag.

- Access to server rooms: Only certain administrators and professors will be granted access to the server room. For professors they will only be able to access servers in their classrooms, at the time they are to teach.
- Access to offices: Only professors, administrators, and maintenance will have access to these specific rooms. The professors will only have access to their own offices, while administrators, and maintenance will be granted access to any offices.

Another tool that will be useful in monitoring the server that will work in conjunction with Active Directory will be Server & Application Monitor (SAM) by SolarWinds. This tool will help in monitoring and manage all the activities that the Active Directory is doing. This will help if for example a breach with a user account is occurring. If the program spots the activity it will send a flag to alert to let the server administrator know that a specific event is occurring. The program will also track the user throughput on the servers. If the server is having an excess amount of users at one point in time, the server administrators will be able to cancel sessions that are idle, to help recover more.

SAM and Active Directory Will Track

- Tracking of Email Environment
- Tracking of Web Environment
- Tracking Of Domain Control Environment
- Tracking of File Environment

## Server Use Pricing

1. 6 Classroom Servers (PowerEdge T320 Tower Server) = $999 per each or $5,499 altogether
2. 1 Dell PowerEdge R920 Rack Server = $9,699

3. 1 Dell PowerVault NX3230 = $2,779
4. Server & Application Monitor by SolarWinds = $15,195

Total = $33,667

# Network Use and Security

## Overview

The Network is what connects all of the devices at USA to each other (the intranet) and the internet (the external network). The network is also were the first line of defense for the devices on the network is located. The network supports up to 1000 thousand user at a time over three networks. These networks are wireless and wired. The networks are split up this way a network for students, another network for faculty and staff, and a third wireless only network for guests.

## Current Specifications

The current network consists of two Cisco routers model 7576 and four Cisco switches models 1500 and 1200. Through the use of vlans these devices support the following all three networks on the USA campus. The student network is primarily wireless with students able to connect their own devices there are also computers in the labs that are wired with CAT 5E to the student network.  The faculty/staff network allows professors to connect either wired in their office with CAT 5E or wirelessly throughout the building. There is also a computer at the podium of each class room that is connected to the faculty network.

## Network Management

*The following section details items that are required and/or recommended for networks belonging to USA, including network related devices.*

## Upgrades

All of USA's current network equipment is end of life (meaning it is no longer supported), so there are no more patches or software updates for this equipment. All of the current network equipment has to be replaced. It is recommended to replace the 7576 series routers with a ASR 1000 series router. I recommend you get two of the ASR 1004 model routers. This router comes with firewall protection and VPN support it will provide you with excellent network service plus it also has multiple ports for future growth. I found this router for the price of **$53,050.99.** The current 1500 and 1200 series switches are recommended to be replaced with four Cisco Catalyst 4500-X Series Switches. These switches cost $17,233.99 each they will provide the necessary ports for the current wired infrastructure plus provide room for future growth. There are higher performance switch that you could purchase but they are not recommended for your needs.

I am also recommending you purchase four of the Cisco MR34 these are wireless Access Points (AP) that are needed to support your current wireless networks. Based on the fact that the majority of your network traffic is wireless you need these high capacity and speed AP's, they come with built in firewall and antivirus scan. MR34 can be had a price of $1224.99 to $1709.00 each with anywhere from 3 to 10 years of license and support. The last Cisco product I am recommending that you purchase is a Cisco FirePOWER 8120 it is a Intrusion Prevention System (IPS) it costs **$56,413.99. This may seem like I am recommending a lot of Cisco products, the reason for this is if you get all of your security and networking components from the same company then you do not have to worry about compatibility issues and it makes it a lot easier for your networking and security team to manage.**

## Firewall

The firewall is the first and most important network defense device that is on your network. If it is properly configured and updated regularly the firewall can stop a lot of threats before they get into your network so picking the right firewall is very important. I recommend the Cisco ASA 5500-X Series firewall. With the Cisco ASA 5500-X Series firewall you get:

- Comprehensive Visibility and Control
    - Superior threat protection
    - Advanced malware protection
        - Real-time protection from malware and emerging threats
    - Greater automation to reduce cost and complexity

- Robust Multilayered Threat Protection
    - The industry's most deployed stateful firewall
    - Comprehensive range of next-generation network security services

- Feature and Capabilities
    - Granular visibility and control
    - Robust web security onsite or in the cloud
    - Industry-leading intrusion prevention system (IPS) to protect against known threats
    - Standalone appliances tailor-made small and midsize businesses Integration with other essential network security technologies
    - High availability for high-resiliency applications

## Intrusion Detection

Network based Intrusion Detection Systems are important part of network security. I have already recommended the Cisco FirePOWER 8120 as the IPS here are some of the capabilities that FirePOWER 8120 provides:

- Feature and Capabilities
    - Provides integrated real-time contextual awareness
    - Full-stack visibility
    - Intelligent security automation
    - Inspected throughput
    - Hardware acceleration technology
    - Reliable performance
    - Low total cost of ownership

## Attacks

There are many types of attacks that can threaten your network. In this section we will focus on threats that target the network not individuals or individual workstations. I cannot cover all of the network based attacks. I will focus on some of the most common types of network attacks and defensive measures against them.

**Port scanning** - an attack type where the attacker sends several requests to a range of ports to a targeted host in order to find out what ports are active and open - which allows him them to

exploit known service vulnerabilities related to specific ports. Symantec Endpoint Protection allows for port scan attack to be detected and blocked.

**Distributed Denial of Service Attack (DDoS Attack) -** occurs where multiple compromised or infected systems (botnet) flood a particular host with traffic simultaneously. The attack is designed to cause an interruption of services of a specific server by flooding it with large quantities of useless traffic. When the DDoS attack succeeds the server is not able to answer even to legitimate requests any more.

Here is an example of a DDoS attack, **ICMP flood attack (Ping Flood) -** the attack sends ICMP ping requests to the victim host without waiting for the answer in order to overload it with ICMP traffic to the point where the host cannot answer them anymore. Easiest way to protect against ICMP flood attacks is either to disable propagation of ICMP traffic sent to broadcast address on the router or disable ICMP traffic on the firewall level.

**Man-in-the-middle Attack** – this attack is a form of active monitoring or eavesdropping on victim's connections and communication between victim hosts. This form of attack includes interaction between both victim parties of the communication and the attacker - this is achieved by attacker intercepting all part of the communication, changing the content of it and sending back as legitimate replies. The both speaking parties are here not aware of the attacker presence and believing the replies they get are legitimate. For this attack to succeed the perpetrator must successfully impersonate at least one of the endpoints - this can be the case if there are no protocols in place that would secure mutual authentication or encryption during the communication process.

**Network sniffing (Packet sniffing)** - process of capturing the data packets travelling in the network. Network sniffing can be used by perpetrators to collect data sent over clear text that is easily readable with use of network sniffers. Best countermeasure against sniffing is the use of encrypted communication between the hosts.

## Network Use Pricing

The recommended upgrades for your network are:

1. Two ASR 1004 routers $53,050.99 x 2 = $106,101.98
2. Four Catalyst 4500-X switches $17,233.99 x 4 = $68,939.96
3. Four MR34 wireless AP's $1709.00 x 4 = $6,836.00
4. One IPS $56,413.99

This comes to a total of $238,291.93.

# Workstation Use and Security

## Overview

Workstations are the end-point terminals through which users can connect and use the university's network. These users include students, teachers, and administrators that work inside the building. With as many as 1000 users a day using these workstations, it is important to make sure that each terminal is protected from harm and that the information on the computers maintains its confidentiality and availability for those that it applies too.

## Current Specifications

At the time of this writing, the current USA building contains three classrooms with 32 workstation terminals for students and one workstation for the teacher, three classrooms with one workstation for the teacher, nine offices with one workstation for the teacher, one administration area with 10 workstations and two printers, and one office in the administration area with one workstation, for a total of 122 workstations. This comes up to 96 terminals for students, 15 for teachers, and 11 for administration. Each workstation in the building is a Dell OptiPlex 580 running Windows Vista, and is wired to a server in a nearby server room.

## Workstation Management

*The following section details items that are required and/or recommended for workstations belonging to USA, including workstation-related devices, applications, and policies.*

## Upgrades

Currently, USA classrooms and offices uses Dell OptiPlex 580 desktops with Windows Vista installed. The 580 model dates back to 2010, with a Athlon II X2 250 3 GHz processor, 2GB memory, and a 250GB hard drive. It maintains a RAM speed of 1.3 GHz and comes preloaded with Dell software such as Roxio Creator and Cyberlink PowderDVD, at a price of around $716. Luckily, Windows Vista still gets extended support from Microsoft, but unfortunately, that only lasts until 2017. Unfortunately again, you can no longer buy Windows 7 operating system from Microsoft, as it has been discontinued to make way for Windows 8.1 and 10. The only way to upgrade to Windows 7 is by purchasing it by OEM (original equipment manufacturer), meaning you would need to buy it by purchasing hardware with it already installed and cannot directly upgrade Vista to 7.

The money-saving option would be to not upgrade at all, as to avoid purchasing a large bulk of new desktop computers. With a lack of support on the horizon however, this is not a suitable option and the least safe one. The best thing to do is upgrade the current desktops to Dell OptiPlex 7020, a much more recent model that runs Windows 7 and come with two varieties: one that comes with DVD-ROM and one that comes with DVD+/-RW. The DVD-ROM desktop would be the 96 terminals for students so they can only read discs and not write, while the other 26 desktops would belong to the teachers and administration, allowing them to both read and write. The particular 7020 series model recommended for USA comes with an Intel® Core™ i3-4150 3.5 GHz processor, 4GB memory, and a 500GB hard drive. The RAM runs at 1.6 GHz, comes preloaded with the same software as the older model alongside Dell security tools, and, with the two models mentioned above, comes at a singular cost of $619-649 on its current discount, $927-941 otherwise. Combined with the price of 3 year warranty and Windows Office,

the 96 student workstations come up to $878.60 and 26 higher-up workstations at $979.32 each, for a total of $109, 807.92.

### Control

Password management will follow parts of the UTHSCSA (University of Texas Health Science Center at San Antonio) password standard, setting up rules for the creation and security of passwords, making sure user passwords are both safe and usable. A user will first be given a user name in the format of *firstname.lastname*, which will not be allowed to be changed. The original password given to a user will be the first letter of their first name, their last name, and their student id. Original passwords should be changed as soon as possible, as someone getting their hands on someone's idea would allow them to be hacked.

When creating a new password, users will be bound to a set of rules. Passwords will require a minimum of 8 characters, requiring at least one capital letter and one number. Recommendations of things to avoid when creating a new password include:

- Names of friends, family, pets, etc.
- Personal information, such as birthday, street name, mother's maiden name, etc.
- Word or number patterns, such as qwerty, 12345, etc.
- A single word preceded or followed by a number (i.e. password1 or 1password)

User passwords will be required to be changed every 60 days, users being warned a week beforehand to change them. Users are also unable to use the same password twice in a row, making sure the password is different than the last period. USA websites will allow a maximum of five log-in attempts before requiring a 5-minute wait on the used username.

Users will be responsible for the protection of their own passwords, so they should be informed of how to keep their information safe. Safety concerns that users should be cautious of include:

- Not writing down passwords on paper or electronic devices.
- Never tell your password to anyone, including administration. No one should ever ask for your password nor should you ever have a reason to tell it to someone.
- Attempt to use different passwords than ones you use on websites. Variety ensures it is harder for someone to get into all of your used sites and applications.
- Do not use the "Remember Password" option, unless using a personal computer or device that you are positive only you will use.
- Avoid others watching you enter your passwords.
- Make sure to be logged off your computer when you are away from it so as to avoid someone else getting onto it.
- If you suspect your account has been compromised, the incident should be reported to the information security office on campus and you should change your password immediately.

Shared resources between staff will follow a similar structure. If a resource is being placed into a service that allows it to be shared amongst several users, whether important or not, should be placed behind a password wall so unintended users do not gain access.

### Monitoring

In order to watch over and keep track of the use of system resources, performance, and activity, monitoring software will be used, preferably the software SpyAgent. This software can block and track online activities and more. SpyAgent creates detailed reports about all activities done

on the monitored computers. The recommended monitoring software can track things like web pages viewed, opened applications, and file paths traveled.

SpyAgent can block websites using keyword filtering and URL blocking, preventing users from visiting websites with content like pornography and gambling. Administration can also use the software to block users from opening up certain software applications, even going as far as stopping access to external media devices. Monitored computers can have times scheduled for when they can be used and when they can't.

Reporting features include remote reporting, allowing the delivering of logs through email, and USB retrieval, a quick gathering of reports from the monitored computer that allows for administration to review information at a later time. Log reports come with filtering functions that can sift data by attachments, keystrokes, usernames, and more. Built-in reports contains information on the most used application on the machine, searches performed, websites visited, users, and other activities performed. One of the most impressive features of SpyAgent is a snap-shooting feature that can take pictures of the monitored workstation's desktop at either customized intervals or when certain keywords are entered in, and then put them into categories.

Things that will be looked for and monitored will include but will not be limited to:

- Unexpected logins - A computer being accessed at a time it shouldn't, like during closing hours or when a staff member would not normally be in their office or possible warning signs of an attack. Workstations with more important information will be more closely watched for logins that should not be occurring, with SpyAgent's monitoring software being able to tell who is logging in or at least whose information is being used.

- System changes - New software being installed on a computer should be an instant flag, as all new programs to be installed on a workstation must be first approved and installed by computer administration.
- Changes to groups and accounts - only administration should be able to change group and account information, which must be approved beforehand.
- Prohibited applications - If an application has been blocked due to potential threats it may cause, this should raise a flag on getting the application removed from the computer.
- USB usage - USBs can be harmful due to potential viruses or other malware located on files in the storage media. By monitoring usage, if a virus is detected, it can be discovered if it came from a student or staff members removable media.
- Unusual behavior - Things like multiple failed attempts of logging into a workstation or account will raise a flag, as it could mean someone is trying to force their way into the system or an application.

The monitoring system should be watched closely and constantly for possible problems, possibly requiring a team to make sure nothing is going wrong. A team is better at catching suspicious activity on a workstation as it can cover more ground. At a price of $70, it's cheap while remaining effective.

### Patch Management

Patch management is designed to avoid vulnerabilities in devices through constant upkeep, helping to reduce money and time spent on fixing vulnerabilities and exploitation. Vulnerabilities are defined under four levels: low, moderate, important, and critical. Each level determines how likely a vulnerability is to be exploited and how dangerous it would be for the vulnerability to be exploited. Compliance levels, or percent of computers that have been

successfully patched, will be taken at the end of each patching session in order to see how many computers still need to be fixed. Workstations not in compliance will remain offline until proper patches are in place.

Patch management will be broken into various activities for different team members to achieve. Roles and their responsibilities include:

- Network Security Administrator
    - Responsible for tracking new vulnerabilities in important software and the associated patch compliance for computing and network devices. The administrator should also enable patch bulletins to inform other staff, reviewing the reports on successful patch compliance, and checking up when compliance is incorrect.
- Change Management Committee
    - Responsible for the approval of patch rollout schedule.
- Patch Testing Team
    - Responsible for testing new patches on most common workstation type used, both in fixing vulnerabilities and making sure there is no conflict with critical applications.
- IT Administrator
    - Responsible for patch testing, installing, and restart of assigned workstations and servers.

The testing process of the patch comes in two parts, the preparation and the testing. Preparation will involve knowing what the patch will impact when it is installed, possible conflicts between

the updated patch and software already on the machines, and figuring out what applications may be affected by system-level files being updated. This helps to reduce test cases needed before the patch is implemented. The testing phase can be composed of any of the following types of test cases:

- Installation Test - ensures the patch can install without errors
- Verification Test - checks that file associations possibly changed by the patch still work
- Execution Test - checks that keys and files created by the patch can be read when non-administrative users use the newly patched application
- Standard Test - checks that the patch does not hinder the ability for an application to run or to connect to a URL
- Rollback Test - making sure it is safe to uninstall the patch and still have everything running properly in case of a situation caused by the patch

The product recommended for patch management is the Desktop Central Enterprise Edition, coming in at $645. Desktop Central has many features including software deployment, operating system deployment, and mobile device management. The current program can be kept, as the current patch management program seems to be working fine, though an upgrade is recommended to go along with the new system.

### Application Management

All workstation applications are to be managed by the administrative team, making sure applications are secure, up to date, and have their vulnerabilities secured against threats. If a teacher or administrative staff requires a certain program installed on a workstation, they must request for the program to be evaluated before it can set up on the network. By preventing users

from downloading and installing their own software, we prevent them from opening up backdoors or from installing dangerous software that may affect the workstation or the network. The proper staff will ensure that the necessary program will cause no danger to the system and that it is safe to use before installing it on the workstations needed. Another point to evaluating the software is to ensure whatever necessary hardware is required is either already obtained or does not conflict with current specifications. The procedure for getting a program installed on workstations is listed below:

- Staff and faculty that wish to have software purchased and installed onto workstations for use on-campus are required to fill out a request form. The form will include information such as contact information, why the software is needed, and the cost.
- The form must be completed and then authorized by the appropriate administrative faculty member. Any information that is required to be shared with a third party must be handled with proper confidentiality so important information is not leaked out.
    - If a contract is required to use the application, contract must be approved and signed by the authorized university personnel.
- IT administrators will make sure that the application is possible in the current network and computer infrastructure. The request department will get a response issued to them on whether or not the request can be met. If it can't, possible alternate solutions may be provided.
- If it is determined that the request is viable, it is checked to see if it is also financially possible unless funds were allocated ahead of time. This process sets funding sources for the application request.

- Finally, the IT team will send a purchase order to the selected vendor and then implemented as requested by the original requestor.

The IT team will ensure that license agreements are met properly and documented accurately. Licensing agreements and schemes will be decided between these three options:

- Site License - allows the installation of a software on all campus-located workstations.
- Concurrent User License - allows the installation of a software on all campus-located workstations, with only a certain amount of users able to use the software at one time.
- Per-Seat License - allows a certain number of workstations to run the software.

All software items, such as licensing documents, program installation disks, and more, must stay in possession of the IT team at all times, only capable of being removed by a faculty member with express permission from a supervisor and an agreement with the CISO. By keeping them in one central location, everything needed by the software is easily available to IT members, can be stored safely without major risk of theft, and provides quick access to all materials in case of a licensing investigation.

Applications are subject to security assessments when certain criteria is met. The criteria that leads to a security assessment are as follows:

- New Application Release - assessment is done before being placed into the work/school environment
- Third Party Application Release - assessment is done and then fit to policy requirements
- Point Release - assessment is done based on risk of change in the application architecture of functionality.

- Patch Release - assessment is done based on risk of change in the application architecture of functionality.
- Emergency Release - emergency releases are special in that they can forego the security assessment until a proper assessment can be carried out. Only the CIO or equivalent can declare or designate an emergency release.

Types of assessments that may be required are the following:

- Full Assessment - comprised of multiple tests for every known application vulnerability using manual and automatic tools. The full assessment uses the manual tools to validate vulnerabilities and determine overall risk to the work/school environment of discovered vulnerabilities.
- Quick Assessment - consists of an automated scan of an application.
- Targeted Assessment - performed to ensure new application functionality and vulnerability remediation change.

Security issues discovered in the assessment are ranked and then mitigated based on the level of each threat. Validation testing is required to ensure that fixes and strategies worked as intended. Risk levels are based on OWASP Risk Rating Methodology:

- High Risk - risks ranked high are required to be dealt with immediately, whether by fix or by using mitigation strategies to ensure limited exposure to the system or network. High risk applications can be taken offline the instant that level of risk is discovered or can be denied release into the work/school environment.
- Medium Risk - risks ranked medium should be reviewed when possible to figure out mitigation strategies and when to deal with the risk. Medium risk applications may be

taken offline or denied release into the work/school environment if it creates too many issues and the amount of issues increase the risk to an unacceptable level.

- Low Risk- risks ranked low should be reviewed last to find out what is needed to fix the issue.

### Malware Management

All workstations connected to the school network must have the approved antivirus software installed on them, first of all. Recommended practices in order to reduce the threat of viruses to the system include:

- Keep the antivirus software updated as often as possible. This prevents newly found viruses from slipping through the cracks. This can be done on workstations via the IT team doing a system-wide update.
- Teachers, workers, and students must never open emails with attachments from unknown sources. These sorts of emails should be deleted as soon as possible, from the email system and from the computer.
- Never forward spam or chain emails to other teachers or workers. These likely contain some sort of malware on them and can be both dangerous and a nuisance to others.
- Make sure to scan removable devices from other users to ensure they do not carry viruses on them.
- If a lab test is going to be performed that could conflict with the antivirus software, the antivirus should be fun first to ensure that the machine is clean. After, the software can be uninstalled or turned off, the lab test done, and then the program must be reinstalled. Once done reinstalling, the antivirus must be run to ensure no problems were caused by the test.

The antivirus software I would recommend to use is Webroot SecureAnywhere AntiVirus. It is a small yet powerful program that takes up very few computer resources. Webroot contains a Realtime Shield, Web Shield, and a Firewall-like program that tracks connections and heightens detection levels when suspicious activity occurs. Webroot takes up little space because a local database isn't maintained and instead pulled from a cloud. This is the only problem with the antivirus, having a requirement of being online in order to scan for viruses. The cost of a yearly license is $39.99, with the cost of three licenses at a time is $49.99. With the amount of workstations required for the building, this should come up to $1,250 to cover all 122 workstations.

In case a piece of malware manages to infect a workstation, containment procedures must be taken to ensure the malware does not spread to other workstations or other networks. Some methods include disconnecting the workstation from the network to isolate it, but this doesn't necessarily protect workstations in the future. The malware could, for example, run so that it connects periodically, allowing it to try and reconnect to the network if it is not removed properly. There are several containment strategies that can be used:

- User Participation Containment
    - Workstation users should be informed and educated on how to identify possible infections and what to do if they notice such signs. This can include running a scan, disconnecting from the network, or calling the IT team for help.
    - There should be multiple ways to inform users of possible issues. Email is most efficient, but can be down if an issue is currently in process. Other ways can include signs and handouts.

    - Users are perhaps the biggest possible security risk to a network due to human error. In order to avoid this, users should be educated on how to avoid getting viruses, like avoiding unknown attachments or avoiding downloading from unofficial websites.

- Automated Detection Containment
    - Different types of detection include email filtering, antivirus, and intrusion prevention. Each one is a different method in blocking viruses, whether by detecting incoming wrongful connections, looking for already embedded malware, or blocking suspicious emails.
- Disablement Containment
    - Sometimes malware can effectively stop an application from working, so the application must be stopped to ensure malware doesn't spread from it or that the application does not harm the workstation or network by not working.
    - It is important not to disable to much however, as it can cause problems in the system. Enough of the application should be disable to stop spread but not enough that could halt functionality.

### Intrusion Detection

Host-based Intrusion Detection systems are important for monitoring a workstation for possible unlawful bypassing. Most HID systems can actively prevent malicious activity from a monitor-only mode, with the administrators able to define what counts as unusual activity to look for and check. The HID system should be managed from a single, central location.

For Intrusion Detection, I recommend the AlienVault Unified Security Management Standard Virtual Appliance for $10,200. The SVA is for mid-sized organizations and can monitor up to 150 assets. It provides five important security capabilities built into one console. These include:

- Asset Discovery
    - Active Network Scanning
    - Passive Network Monitoring
    - Asset Inventory
- Behavioral Monitoring
    - Log Collection
    - Netflow Analysis
    - Service Availability Monitoring
    - Full packet capture
- Vulnerability Assessment
    - Network Vulnerability Testing
    - Continuous Vulnerability Monitoring
- Security Intelligence
    - SIEM (Security Information and Event Management) Correlation
    - Incident Response
    - Reporting and Alarms
- Threat Detection
    - Network IDS
    - Host IDS
    - File Integrity Monitoring

## Workstation Pricing

Here is the list of products recommended and the overall price for workstation policy and security:

1. 122 Workstations = $109,808[1]
2. Spy Agent Monitoring Software = $70
3. Desktop Central Enterprise Edition = $645
4. Webroot SecureAnywhere AntiVirus = $1,250
5. AlienVault Unified Security Management Standard Virtual Appliance = $10,200

Altogether, this comes up to a price of around $121,973.

[1] Can likely be reduced in a bulk deal with Dell

# Bring Your Own Device

## Overview

We understand that keeping employees and students on only one type of device may be an unreasonable task in a school environment, especially with all the network capable devices people use these days. This section will list guidelines for the use of non-university owned devices.

## Scope

Students and employees will be allowed the use of their personal devices, such as their phones, tablets, and laptops. However, as employees will be dealing confidential information, they must sign an agreement stating which devices they will be bringing into the workplace and having the proper safety software to ensure the devices do not become infected.

## Bring Your Own Device Guideline

### Teachers and Employees

- Neither teachers or administration should use important school-related software on their personal devices when using an unprotected or public network.
- Employees are required to use the same antivirus as the university.
- Employees may not go to unsecure websites on their personal devices over the university network.
- Passwords cannot be placed into unencrypted files.

- When an employee is let go or goes on sabbatical, they must adhere to a wipe of sensitive university information from their personal devices.
- Employees must report suspicious or malicious activity on their personal devices to CISO or IT team.
- Do not keep university information on your personal device.
- The university will not take liability for the backup or loss of data from personal devices, and is the responsibility of the device owner to do so.
- Failure to comply with the above measures can lead to consequences from having their device rights revoked to being let go from the university.

### Students and Guests

- If it is discovered that you are using your personal device for an illegal application, such as illegal downloading or hacking, you can have your device banned from the network. Depending on the severity of the action, students and guests may also be subject to holding for police or required to pay a fine.

# Disaster Recovery

## Overview

The goal of DDISC is to provide additional recommendations to St Asterisk's disaster recovery plan as it pertains to the new remote location. The general recommendations will contribute to an effect response if a disaster were to occur at this location. This plan should be updated on a regular basis as changes to the IT environment are made.

## Plan Objective

DDISC approaches disaster recovery using a team concept. Each team will be tasked with specific duties and responsibilities. Due the small size of the IT department, staff will be assigned to multiple teams in accordance with their skill, availability and experience. It is also recommended that outside vendors be utilized to assist in the recovery. Cooperation with local authorities is essential. The most important function of the disaster recovery plan is to restore operations at a suitable location and resume normal operations.

## Disaster Recovery Teams

### Disaster Recovery Management Team

The overall coordination of the disaster recovery process will be the main purpose of this team. Other team leaders will report to this team during a disaster. General duties assigned to this team include:

- Assessment of damage

- Coordinate teams
- Approve actions that were not preplanned
- Give strategic direction

## Tech Support Team (Hardware, Software, Network, Operations)

### Hardware Team

The primary responsibilities of the Hardware Team are to provide technical expertise in the installation and configuration of all servers and workstations. Activities that this team will also conduct include:

- Determine extent of damage to all IT hardware
- Order appropriate equipment and supplies
- Set up new hardware
- Install all necessary software
- Restore Data
- Ensure that all data is backed up

### Software Team

The primary responsibilities of the Software Team are to maintain the system software at the predetermined alternate site and reconstruct the software upon return to the primary site. This team will provide technical support to the other teams. Additional activities to be performed by this team include:

- Test the hardware and software
- Work with appropriate vendors to assist in the recovery

- Verify systems perform as expected
- Reinstall and configure systems at the primary site

### Network Team

The primary responsibilities of the Network Team is to provide voice and data communications at the alternate location and restore voice and data communications at the primary site. Additional activities to be performed by this team include:

- Determine the requirements for voice and data communications
- Install new network including lines, routers, switches and other communication equipment
- Test network
- Operate backup network

### Operations Team

The primary responsibilities of the Operations Team include the daily operations of IT services and the management of all backups. In the event of a disaster, this team will provide the correct backups to the alternate site. Additional activities to be performed by this team include:

- Inventory and select the correct backups
- Assist all teams in the restoration of the IT environment at the alternate location
- Establish offsite storage at the alternate location
- Restore service at the primary location

## Disaster Recovery Plan Maintenance

It is important to remember that the disaster recovery plan is a “living” document. Failure to keep it current could result in a catastrophic failure when trying to recover in the event of a disaster. All changes to the plan should be documented and all copies of the plan be updated. An update log is recommended. Hardware, software and personnel changes that affect the plan should be updated as they occur.

# Overall Cost

The cost for each section is as follows:

1. Physical Environment: $94,734
2. Server Use Pricing: $33,667
3. Network Use Pricing: $238,292
4. Workstation Pricing: $121,973

The total cost for the entirety of the recommended purchases is $488,666.

# Conclusion

Each section provided their own blend of similar and unique challenges in attempting to create a series of plans. For the physical environment, the interconnected interface of all the different kinds of security devices provided a new look at how complicated letting only the proper people through can be. The server section involved the explanation of how everything in the building would connect to them. With a lack of server maintenance practice, this proved to be its own big challenge in researching how the servers worked and how they helped control everything. The biggest challenge for networking was how precise the network plan had to be to fit the setting. With so many devices for so many different types of connections or type of environments, finding the correct combination of devices for the fictional one-floor university building created many new research topics. Workstation policies have so many different guidelines that must be followed in order to secure the user end point, that each possible policy section could be their own paper. With so many different things to research, a wide net was cast in order to create a possible plan.

In the end, this research project provided each of us our own set of experiences and a unique fountain of knowledge for each of us to tap into. By pooling our information together, we each learned much more than what we would have learned working individually.