

CHARTING A COURSE TO EXCELLENCE



"Work Hard and Be Nice"

Saint Mary's County Public Schools

Information Technology Disaster Recovery Plan

SMCPS
IT Disaster Recovery Plan
Document Change Plan

Revision	Prepared Date	Approved Date	Changed by
Version 1.0	12/1/2007	12/31/2007	Van Sage
Version 1.1	04/1/2008	04/21/2008	William Caplins

Saint Mary’s County Public Schools
Information Technology (IT)
Disaster Recovery Plan

Table of Contents

1.0 Introduction	4
2.0 Objectives	4
3.0 Scope	4
4.0 Assumptions	5
5.0 Definitions	5
6.0 General Disaster Response and Recovery Guidelines.....	5
7.0 IT Risk Assessment	6
7.1 Level 1 Information Technology Services (ITS) building and Central Computer Room.....	6
7.2 Level 2 Network Infrastructure and Services	7
7.3 Level 2 Cable Plant.....	9
7.4 File and Print Service	10
7.5 Level 3 Student (eSchool) and Finance (eFinance) Services	11
7.6 Level 3 – Email services.....	12
7.7 Level 3 - Web Services	14
8.0 Maintenance of the IT Disaster recovery plan.....	15
Appendix A: IT Disaster Recovery Teams	16
Appendix B: SMCPS Campus Contact List	17
Appendix C: Vendor Contact List	17

1.0 Introduction

Saint Mary's County Public Schools (SMCPS) is a K thru 12 Maryland public school system. Over time, Information Technology (IT) services have become critical to performing the educational mission of the school system. As a result of this ever increasing reliance of technology, IT services require a comprehensive Disaster Recovery Plan to ensure these services can be re-established quickly and completely in the event of a disaster.

This plan summarizes the results of a comprehensive risk analysis conducted for all IT services, it provides general steps that will be taken in the event of a disaster to restore IT functions; and it provides recommendations for "hardening" of the IT infrastructure that require executive level management approval and additional funding to implement.

2.0 Objectives

The primary objective of this Disaster Recovery Plan is to help ensure educational business continuity by providing the ability to successfully recover computer services in the event of a disaster.

Specific goals of this plan relative to an emergency include:

- Detailing a general course of action to follow in the event of a disaster,
- Minimizing confusion, errors, and expense to the school system, and
- Implementing a quick and complete recovery of services.

Secondary objectives of this plan are:

- Reducing risks of loss of services,
- Providing ongoing protection of institutional assets, and
- Ensuring the continued viability of this plan.

3.0 Scope

This plan will only address the recovery of systems under the direct control of the IT Services Department that are considered critical for business continuity. Also, given the uncertain impact of a given incident or disaster, it is not the intent of this document to provide specific recovery instruction for every system. Rather, this document will outline a general recovery process which will lead to development of specific responses to any given incident or disaster.

Three levels of risk, based on severity to campus operations, have been identified. A Level 1 risk is associated with the Information Technology Services building and Central Computer Room, which houses the campus servers and routers and serves as the primary hub for campus electronic communications and connectivity. A Level 2 risk is associated with the campus network infrastructure. The final risk level, Level 3, is associated with risks specific to unique applications or functionality. Though risk at all levels must be addressed for disaster recovery purposes, Level 1 risks will be given increased priority over other levels. The same holds true for Level 2 versus Level 3 risks. The following major service areas are addressed in this plan.

- Level 1 – Information Technology Services Building and Central Computer Room
- Level 2 – Network Infrastructure and Services
- Level 2 – Cable Plant
- Level 3 – File and Print Services
- Level 3 – Email Services
- Level 3 – Web Services

Note: All systems that are both necessary for the daily operations of SMCPS and the responsibility of the Information Technology Services Department are maintained under service contracts with the appropriate equipment vendors.

4.0 Assumptions

This disaster recovery plan is based on the following assumptions:

- The safety of students, staff, and faculty is paramount; the safeguard of such will supersede concerns specific to hardware, software, and the recovery needs.
- Once an incident covered by this plan has been declared a disaster, the appropriate priority will be given to the recovery effort, and the resources and support required as outlined in this IT Disaster Recovery Plan will be made available.
- Depending on the severity of the disaster, other departments/divisions on campus may be required to modify their operations to accommodate changes in system performance, computer availability, and physical location until a full recovery has been completed. The Superintendent's cabinet will encourage departments to have contingency or business continuity plans for their operations, which include operating without IT systems for an extended period of time.

5.0 Definitions

The following definitions pertain to their use in this IT Disaster Recovery Plan:

- Campus: All buildings that comprise the SMCPSS school system.
- Backup/Recovery Tapes: Copies of all software and data located on the central servers, which are used to return the servers to the state of readiness and operation that existed shortly prior to the incident/disaster.
- Disaster: A significant or unusual incident that has long term implications to business continuity and the ongoing operations of SMCPSS.
- Incident: An event which impacts a specific IT service or server.
- Level 1 Risk: Risk associated with the most critical IT services/capabilities, based upon impact to the campus if the service or capability were lost.
- Level 2 Risk: Risk associated with critical IT services/capabilities, based upon impact to the campus if the service or capability were lost.
- Level 3 Risk: Risk associated with the loss of selected applications/functionality.

6.0 General Disaster Response and Recovery Guidelines

- In the event of a disaster, the Director of Technology will notify the three primary IT Disaster Recovery Teams: network, administrative, and repair (see Appendix A, IT Disaster Recovery Teams).
- Appropriate steps will be taken to safeguard personnel and minimize damage to related equipment and/or software.
- A damage assessment will be conducted by each team and recommendations made to the Director of Technology for recovery of impacted services.
- Individuals required to assist in recovery of these services will be identified. The Director of Technology will communicate this need to the superintendent and his cabinet (see Appendix B, SMCPSS Contact List).
- The campus will be informed as to IT system degradation and restrictions of IT usage and/or availability.
- The Director of Technology will develop an overall IT recovery plan and schedule, focusing on highest priorities of the campus infrastructure first, as defined by the superintendent's cabinet.
- Necessary software and hardware replacement will be coordinated with vendors and the SMCPSS purchasing office, as required (see Appendix C for vendor contact information).
- The Director of Technology will oversee the recovery of campus IT services based on established priorities.
- The Director of Technology will ensure the IT recovery efforts are properly coordinated with other campus recovery efforts.
- The Director of Technology will communicate recovery status updates to the Superintendent's School Support Team and campus at large.

- The Director of Technology will verify restoration of the IT infrastructure to pre disaster functionality.

7.0 IT Risk Assessment

7.1 Level 1 Information Technology Services (ITS) building and Central Computer Room

7.1.1 General

7.1.1.1 The ITS building is a one story, concrete, structure located at 22975 Colton Point Road, Bushwood MD 20618. The ITS staff, in its entirety, is housed in the facility on the 1st floor. The Central Computer Room is located on the 1st floor of the ITS facility. This room houses the main campus servers and routers. It is the location where all data and transmitted communications for Saint Mary's County Public Schools are redirected, combined, stored, and retrieved. There is no offsite backup facility currently identified, that could replace the functions of the Central Computer Room if it is rendered in operable by environmental or an accidental disaster.

7.1.2 Risk Assessment

7.1.2.1 Physical/Security Risks

- The ITS building can be accessed through four doors. All ITS employees have a master key, which can unlock all exterior and a majority of the interior doors.
- There are a large number of windows on the 1st floor of the building that are susceptible to breakage and possible unauthorized entry. Many of the windows have screws or bolts on the outside frames, allowing for potentially undetected intrusion into the building.
- There is a security alarm comprised of motion and IR sensors. A camera system is installed to record activities in the computer room and hallways. This alarm is monitored 24/7 and each employee has a unique access code to arm or disarm the system.
- Periodically, in the evening, officers from the Sheriff's Department will ensure that the building doors are secured and no suspicious vehicles are in the parking lot.
- Entrance to the Central Computer Room, located on the 1st floor is through a single, locked door; keyed with a unique key. The room is comprised of masonry and drywall walls with exterior windows.
- There is recorded video surveillance inside the computer room.

7.1.2.2 Environmental Risks

- Rain
 - The ITS building has a flat roof; the roof was replaced with new materials in 2007.
 - There are no environmental sensing devices installed in the computer room to detect water leakage.
- Flooding
 - Due to the building location and elevation there is a low risk of flooding.
- Fire
 - Though the building structure is concrete; it houses a large number of desktop computers, a paper storage area, individual cubicles which contain documents, books and equipment.
 - The computer room contains large quantities of equipment, but minimal combustibles such as papers or documents. Widespread fire is not likely; however, small, contained fires are possible in the wiring and equipment.
 - Within the computer room, the telecom wall is wood, plastic and PVC insulated wire. It is the most flammable part of the room.
 - Storage of combustibles (cardboard, paper, plastics, liquids) is not allowed in the computer room.
 - There is no fire detection system in the Central Computer Room.
- Extreme Temperatures
 - Externally mounted window A/C units provide cooling during the summer months.
 - Primary and supplemental air conditioners are available to cool the Central Computer Room. Neither system alone is capable of providing the necessary cooling for the room. All air conditioners will be generator powered when the building generator is installed.

- Central Computer Room air units do not have heaters however the computers produce heat, so the risk of too low a temperature is minimal.
- Natural Disasters (earthquakes, tornados, high winds, hurricanes)
 - The ITS building is a solidly constructed concrete structure which protects personnel and equipment from high winds and hurricanes.
 - Saint Mary's County does not have a history of major earthquakes or tornados.

7.1.2.3 Internal Systems Risk

- Power is provided to the ITS building from SMECO through the regular power grid. The building has 3 phase power utilizing transformers to provide power for the air conditioners and multiple electrical panels to provide power for equipment in the Central Computer Room.
- Standby power is currently not provided but a diesel generator for the building is in the FY 09 capital budget.
- Available Central Computer Room power is currently "maxed" out. Additional circuits must be freed up or installed to provide adequate power for additional server needs.
- Essential computers and equipment have battery UPS systems to maintain power for safe shutdown purposes only.

7.1.2.4 External Systems Risk

- Operation of the Central Computer Room is highly dependent upon the external campus cable plant which provides fiber and copper lines to carry data and telecommunication services.
- The cable plant was upgraded in FY2002 as part of the County Cable Franchise agreement.
- Utilities are pole mounted and susceptible to ice storms.

7.1.3 Recovery Planning

- Recovery decisions will be based on the extent of the damage to the ITS building and Central Computer Room. A Hot backup computing facility does not currently exist, so if the Central computer Room remains habitable, every effort will be made to re-establish service in the same area.
- If the Central Computer Room is not habitable, the training area that exists on the 1st floor of the Division of Supporting Services will be established as a backup computer facility. Adequate fiber, copper and power can be extended to the area in order to bring up services to the campus.
- If it appears recovery of individual services will take longer than a week to restore, on a selective basis, services will be evaluated for possible outsourcing to commercial organizations.

7.1.4 Preventative Measures

- 7.1.4.1 The current facility/room should be "hardened" to protect it from possible environmental or an accidental damage. The following recommendations are made to protect this significant resource:
 - Develop and document a "power" plan for the Central Computer Room as new generator is installed.
 - Add additional electrical power and circuits to accommodate near-term and future equipment needs.
 - Install generator power to ensure a seamless cutover, if and when there are power failures.

7.2 Level 2 Network Infrastructure and Services

7.2.1 General

- 7.2.1.1 Network services are provided via the wired and wireless network infrastructure. Network services include a wide variety of functions, such as network/file storage (including the associated backup), printing, routing, switching, DNS and DHCP services, web/internet services, bandwidth allocation and monitoring, firewalls, etc.
- 7.2.1.2 Network services are totally dependent on the campus cable plant and a wide variety of other commercial equipment including servers, switches, routers and wireless access points.

7.2.2 Risk Assessment

7.2.2.1 Physical/Security Risk

- With the exception of the cable plant infrastructure and switching electronics located in the campus wiring closets and individual building main distribution facilities (MDF), all other equipment supporting network services is located in the Central Computer Room located in the ITS building.

- Currently there is an offsite data storage capability at Moakley Street. Selected data is backed up to tape and stored offsite, data located on any disc backup system would be lost if the ITS computer room was rendered inoperable this is of medium concern.
 - Telephone and data switching electronics are located in main distribution facilities (MDFs) and/or wiring closets located in each of the major campus buildings.
 - Though each closet is locked, in many cases, particularly in the schools, these closets are also used for miscellaneous storage and are accessed by other than ITS personnel.
 - The risk for inadvertent damage and possible malicious damage is medium in these areas.
 - Many closet environments are excessively dusty/dirty and suffer from significant humidity and temperature fluctuations. This can cause a higher than normal network electronic failure rate and reduce the lifetime of the copper network and telephone termination/cablings.
 - Wiring closet security is of medium to high concern.
- 7.2.2.2 Environmental Risk
- Wiring closets/MDF's are generally not environmentally controlled and subject the equipment to varying humidity and temperature extremes and exposure to excessive dirt and dust. There is a risk of equipment and cabling failure because of the lack of a reasonable operating environment.
- 7.2.2.3 Internal Systems Risk
- Hardware or software failure impacting individual at remote location network services is a significant risk and would require significant cost to improve.
 - Most network services do not have redundant hardware or failover systems in place. There are numerous unique hardware items that represent potential single points of failure.
 - Equipment is used beyond its advertised /support life due to budgetary constraints. Failed equipment will be replaced by spare equipment obtained during equipment upgrade cycles.
 - Adequate training and career growth opportunities must be provided to maintain SMCPs current network technical staff.
 - Directory tree corruption could potentially require manual reinstallation of all network printer information for each individual device.
 - Wiring closet UPS systems are not tested and/or replaced unless budgetary means permits.
- 7.2.2.4 External system Risk
- Campus Internet connectivity is dependent upon a single T1 to Sailor and a single fiber optic line to Metrocast in Leonardtown. Both of these lines can be damaged, resulting in the loss of external campus connectivity.
 - There are currently no secondary (backup) data trunking pathways between campus buildings. If current cable plant pathways are damaged, network services will be impacted.
 - Hackers could attempt to launch denial of service attacks and/or attacks against network equipment and/or configuration files.
 - Hiring experienced technical staff is extremely difficult, given the institution's salary limitations and SMCPs location.
- 7.2.2.5 Recovery Planning
- Given the wide variety of potential problems that could impact network services, the following generic recovery planning steps will be utilized to identify and resolve network problems:
 - Assess which network service or services have been lost.
 - Notify the campus, by whatever means available, as to the service outage.
 - Troubleshoot to isolate the cause of the service outage – if necessary, contact the appropriate vendor for diagnostic support (see Appendix C for vendor contact information).
 - Once the problem is isolated, take appropriate action to restore the service(s).
 - In the event the service cannot be restored in a timely fashion, assess possible workarounds, including temporary outsourcing, if feasible.
 - Notify the campus as to the status of the affected service.
 - Notify the campus when the service becomes available.

7.2.2.6 Preventative Measures

- Maintenance agreements are maintained on all critical servers and systems to help mitigate the lack of redundancy and to ensure rapid vendor response to problems. See Attachment C for a listing of vendor contacts and Attachment D for a server inventory.
- Fund a network “refresh” program to replace aging network equipment on a regular basis.
- Ensure that annual vendor maintenance agreements are in place for all critical network systems.
- Maintain a pool of harvested, functional spares to provide replacement of failed, obsolete and un-repairable network switches.
- Develop a replacement plan for obsolete equipment.
- Procure backup hardware for critical, single point of failure systems.
- Develop a secondary campus core and switching /routing plant with redundant connection to major building wiring closets.
- Develop and implement a plan for offsite storage/backup of configuration files.
- Ensure that backup personnel are assigned for each critical network service.
- Build up and maintain a stock of wiring closet hardware.
- Improve and standardize backup power to switches located in wiring closets.
- Where possible, do not use wiring closets for storage purposes. Where not possible, build locked cages around wiring closet electronics.
- Standardize wiring closet access.
- Improve climate in wiring closets where there are significant temperature fluctuations.
- Adequate training and career growth opportunities must be provided to maintain SMCPs current technical staff.
- Offsite disk storage capability should be developed for all servers.
- Given the user requirement for 24/7 web services availability, establishing high availability redundancy for all web services should be budgeted for and implemented to minimize loss of services.

7.3 Level 2 Cable Plant

7.3.1 General

7.3.1.1 The cable plant is a complex integration of copper and fiber optics. The cable plant is, in essence, the nerve system for campus communications. The cable plant provides the connectivity and communication paths for campus network users.

7.3.1.2 The management focal point for the cable plant system is the 911 center in Leonardtown, from which point it branches out to all buildings that comprise our campus.

7.3.2 Risk Assessment

7.3.2.1 Physical/Security Risk

- The cable plant is subject to damage from vandalism and unintentional damage caused by construction projects. Unintentional damage is the most common physical/security risk to the cable plant.

7.3.2.2 Environmental Risk

- The cable plant is subject to the effects of extreme temperature ranges and moisture.
- Over time, environmental conditions such as temperature and moisture will affect the reliability and quality of the cable plant.

7.3.2.3 Internal System Risk

- The cable plant was designed and engineered to conform to the TIA/EIA industry standards to reduce the risk of installation damage and to ensure the required quality of service. Once installed, there is a minimal risk of component failure.
- The fiber optic portion of the cable plant is terminated at the 911 center in Leonardtown and a corresponding site.

7.3.2.4 External System Risk

- Fiber optic and copper pathways that comprise the SMCPs cable plant can be damaged. When this occurs, external network services will be impacted, until the service provider repairs its lines.

- Loss of service from external vendor will cause impact on services.

7.3.3 Recovery Planning

7.3.3.1 In most situations when a cable or fiber optic is damaged in a building, the repair can be effected by personnel on staff.

7.3.3.2 If damage occurs to inter-campus (WAN links) cables, the repairs have to be made by the service provider.

7.3.4 Preventative Measures

7.3.4.1 Current preventative measures include properly installing copper wire and fiber optics in the proper pathways and in accordance with TIA/EIA standards.

7.3.4.2 Periodical inspections of communication closets, pathways and vaults will help to eliminate potential problems.

7.3.4.3 Cable damage from construction equipment could be reduced if construction plans were routed through ITS for review and approval.

7.3.4.4 Controlled access to communication closets will reduce the probability of inadvertent storage related damage and damage from vandalism.

7.3.4.5 A reserve of emergency parts should be maintained to repair most anticipated types of damage.

7.4 File and Print Service

7.4.1 General

7.4.1.1 SMCPS uses Microsoft Windows Servers to provide campus file and print service. Windows file services provide campus computer users networked disk space to store files in personal home directories and collaborative group directories. Documents, spreadsheets, small databases, and other digital information and programs store and retrieve data from these servers.

7.4.1.2 The Windows printing services provide centrally managed print processing for campus printers.

7.4.1.3 The Windows servers are HP/Compaq or x86 hardware running Windows server 2000 or 2003

7.4.2 Risk Assessment

7.4.2.1 Physical/Security Risk

- At least one Windows server is located at each building and multiple servers are located at ITS Central Computer Room. Reference paragraph 7.1.2., Central Computer Room risk assessment, for a description of the physical, environmental, electrical, external and internal risks associated with this location.

7.4.2.2 Internal Risk Assessment

- SMCPS pays an annual maintenance licensing fee for all of the utilized Microsoft software products. In the event application software is lost due to equipment malfunctions, all required application and operating system software could be obtained from the vendor or via backup tapes or copied compact disks.
- All current production servers are covered under a basic HP/Compaq next day hardware warrantee. Access to this support is through HP at 800-474-6836.
- The most significant software-related risk is that associated with losing institutional data stored on Windows file servers. To mitigate this risk the following backup approach is currently in place to support Windows disaster recovery needs: 2 week retention of all data on backup media and Weekly backups of all data and system state.

7.4.2.3 External Risk Assessment

- Network connectivity is vital to the functionality of the Windows servers. Windows file and print services cannot operate without a functioning network.

7.4.2.4 Recovery Planning

- Assess which Windows service or services have been lost.
- Notify the campus or building as to the service outage.
- Troubleshoot and isolate the cause of the service outage – if necessary, contact the appropriate vendor for diagnostic support.
- Once the problem is isolated, take appropriate action to restore the service(s).
- In the event the service cannot be restored in a timely fashion, assess possible workarounds.

- Notify the campus or building as to the status of the affected service.
- Notify the campus or building when the service becomes available.

7.4.2.5 Preventative Measures

- Current preventative measures include:
 - Windows servers are replaced on a five-year life cycle to minimize problems associated with obsolescence and security.
 - Maintenance contracts are maintained on all Windows hardware during the operational life of the equipment.
 - Hardware and software patches and upgrades are installed on a regular basis.
 - Windows backup is performed on a regular basis.
- Future preventative measures include:
 - Review server clustering/high availability options to provide automatic failover and system redundancy in the event of hardware failure.
 - Develop a test environment to periodically restore and test backup's operational status.

7.5 Level 3 Student (eSchool) and Finance (eFinance) Services

7.5.1 General

- 7.5.1.1 The eSchool and eFinance systems provide SMCPs with administrative information such as system finances and student records; payroll and employee benefit information; and provide a framework for self service products that are available through the campus portal. This system serves almost all administrative staff on/off campus.
- 7.5.1.2 Integrated with eSchool is the data warehouse program Performance Matters, Café Enterprise food services application, Destiny library management application for all secondary schools and some elementary.
- 7.5.1.3 Both systems run on an HP/Compaq hardware platform, using Windows operating systems.

7.5.2 Risk Assessment

7.5.2.1 Physical/Security Risk

- All eSchool and eFinance servers are located in the ITS services central computing room. Reference paragraph 7.1.2., Central Computer Room risk assessment, for a description of the physical, environmental, electrical, external and internal risks associated with this location.

7.5.2.2 Internal System Risk

- The most significant software-related risk is that associated with losing institutional data stored in either SQL database. This risk has three components, which span both internal and external risks, including:
 - Internal database corruption which makes some or all of the data inaccessible
 - Unauthorized personnel access to either system through malicious intrusion/hacking
 - Unauthorized access to either system data through theft of data, such as theft of a laptop or desktop computer containing either systems data.
- eSchool and eFinance software and associated commercial software (Cognos Report Net, etc) as they are periodically updated, are all subject to software discrepancies, bugs and other associated problems.
- There are 13 operational servers consisting of 2 database servers, 4 web servers, 3 task servers, 2 reporting servers, 2 test environment servers. As with all computer systems, this hardware is susceptible to failure.
- Hiring experienced programmers and SQL experienced database administrators is extremely difficult, given the institution's salary limitations and SMCPs location.
- Adequate training and career growth opportunities must be provided to maintain SMCPs current programming and DBA staff.

7.5.2.3 External System Risk

- Network connectivity is vital to functionality of either system. Either system cannot operate without a functioning network.

- Unauthorized access to either data base via malicious hacking/intrusion to obtain sensitive personnel data is a minimum risk.
- Loss of data through laptop, desktop, or other theft is a significant risk.

7.5.2.4 Recovery Planning

- Assess which service or services have been lost.
- Notify the campus as to the service outage.
- Troubleshoot to isolate the cause of the service outage – if necessary, contact the appropriate vendor for diagnostic support, i.e. Pentamation for eSchool or eFinance software and HP/Compaq for the hardware.
- Once the problem is isolated, take appropriate actions to restore the service(s).
- In the event the service cannot be restored in a timely fashion, assess possible workarounds.
- Notify the campus as to the status of the affected service.
- Notify the campus when the service becomes available.

7.5.2.5 Preventative Measures

- To mitigate the risk of data loss, a new tape backup was purchased in FY2007 for both systems. The following backup approach is currently in-place to support either disaster recovery need:
 - Daily tape backups are created and archived onsite for 3 weeks.
 - Weekly backup tapes are retained offsite for 3 weeks.
 - Monthly backup tapes are retained on the 3rd week of each month and stored offsite for 2 months.
 - Periodically, the test database is restored using backup tapes to ensure the backup system is properly operating.
- SMCPs pays an annual maintenance fee for all of the utilized Pentamation software products and associated software products (Cognos, SQR, etc). As software bugs are identified, the appropriate vendor is notified. In the event application software is lost due to equipment malfunctions, all required application and operating system software could be obtained from the vendor or via backup tapes.
- Recognizing the importance of both systems to the institution redundant hardware should be budgeted for and acquired.
- SMCPs has maintenance contracts for both system servers with HP/Compaq. HP Service is handled primarily out of Greenbelt, Maryland. Current maintenance level for SMCPs is 4 hour onsite repair and a 3 year warranty, which entitles SMCPs to maintenance Monday through Friday between the hours of 7:30 am and 4:00 pm. Refer to Appendix B for HP/Compaq contact information.
- Provide adequate training and career growth opportunities to help maintain SMCPs current programming and DBA staff.

7.6 Level 3 – Email services

7.6.1 General

- 7.6.1.1 Email service includes email delivery, virus scanning, spam blocking and email storage. Currently, only Employees/Faculty/Staff are allowed to obtain an email account.

7.6.2 Risk Assessment

7.6.2.1 Physical/Security Risk

- If an attacker has physical access to the email servers, any and all other security measures can be bypassed.
- The campus email servers are located in the Central Computer Room. Reference paragraph 7.1.2., Central Computer Room risk assessment, for a description of the physical, environmental, electrical, external and internal risks associated with this location.

7.6.2.2 Internal System Risk

- Internal system risks include software viruses and spam spread either intentionally or unintentionally throughout the network; viruses in particular can render the network unusable

- Viruses: the vast majority of current viruses are transmitted via email. Viruses cause a reduction in productivity on workstations, and frequently require an ITS technician to clean or re-clone the computer.
- Incoming spam: some estimates place unwanted email (spam) at 90% of all email traffic. This has a significant impact on the user's productivity. Further, spam can introduce viruses and/or spyware onto a user's workstation.
- Outgoing spam: if the SMCPs network was to be used to relay spam out to the Internet, our systems will likely be blacklisted, preventing our users from sending legitimate messages to their contacts.
- Hardware failure: physical failure of the hardware in the server will cause downtime and may cause data corruption.
- Data compromise via web applications: there are a number of different kinds of attacks on web applications such as Outlook Web Access (OWA). They can allow an attacker to run programs on the server, masquerade as the user, etc.
- System level compromise via various running services ("Remote" Compromise): a flaw in any service running on a server could potentially be used to compromise the server by a remote attacker unless additional measures are taken.
- System level compromise by a local user ("Local" Compromise): local users are those users that actually have an account on the server. By necessity, they have additional rights above those given to an anonymous user.
- Accidental misconfiguration by an administrator: the system administrator, by necessity, has the ability to make drastic changes to server functionality. These changes can cause major problems to the functionality of the server, if not done properly. Should the administrator that made the change not be available to correct the problem, the alternate administrator can have difficulties determining what changes were made and how to restore previous functionality.
- Passwords passed in the clear; most email services transfer a user's password in clear text (via HTTP). This allows a malicious user to easily read the user's password and then masquerade as the user to send and receive messages as that user.

7.6.2.3 External System Risk

- Campus email services are dependent upon the network/cable plant for continued operation. This includes fiber connected to Metrocast and the T1 connected to Sailor.

7.6.3 Recovery Planning

7.6.3.1 General Recovery Steps

- Assess which network service or services have been lost.
- Notify the campus, by whatever means are available, as to the service outage.
- Troubleshoot to isolate the cause of the service outage.
- Once the problem is isolated, take appropriate action to restore the service(s).
- In the event the service cannot be restored in a timely fashion, assess possible workarounds, including temporary outsourcing, if feasible.
- Notify the campus as to the status of the affected service.
- Notify the campus when the service becomes available.
- In the case of a major virus infection, ensure that campus virus protection software is updated and establish an ITS disaster team to clean infected campus computers.
- Restore email system state and any possible data.
- For hardware failure, acquire replacement parts as needed from HP/Compaq. Refer to Appendix B for HP/Compaq contact information.
- In the case of malicious activity by a single user, disconnect the server from the network and determine the method of data corruption and the duration of inappropriate access. This may require the use of "clean room" techniques to ensure that SMCPs can prosecute, if desired. Secure the system as necessary, likely including a full system restore, followed by patching of the security flaw.

7.6.4 Preventative Measures

7.6.4.1 Current preventative measures include:

- Physical access to the server(s) -The door to the server room is kept locked.
- Viruses - SMCPSS uses Kaspersky Anti-Virus for mail servers on its email gateway. The virus definitions are updated every hour. Each workstation has Norman VirusScan installed and is set to automatically update.
- Incoming Spam - SMCPSS is using a Barracuda Spam Firewall 300 appliance as the email gateway to drop email delivery attempts from known spam/virus sources.
- Outgoing Spam - SMCPSS is currently only allowing email relaying from its own IP address blocks. This prevents a remote spammer from using SMCPSS mail servers directly. SMCPSS firewalls the campus workstations to prevent spammers from using them to send spam, using SMCPSS mail servers indirectly. Finally, SMCPSS is blocking directly, preventing them from being used to send spam through our mail servers.
- Passwords passed in the clear - Inform users on how to be aware of their actions

7.6.4.2 Future preventative measures

- Require users of standalone clients to use the encrypted protocols (HTTPS) instead of the unencrypted ones. This may break functionality with PDAs, as they tend to have extremely limited functionality.
- SMCPSS should be budgeting for a new Barracuda Spam firewall since the current one is three years of age.

7.7 Level 3 - Web Services

7.7.1 General

7.7.1.1 SMCPSS-WWW1.smcpss.org provides SMCPSS web presence.

7.7.1.2 SMCPSSIS1.smcpss.org, SMCPSSIS2.smcpss.org, and SMCPSSIS3.smcpss.org provide the eSchool and Home Access Center to staff and parents.

7.7.2 Risk Assessment

7.7.2.1 Internal System Risk

- Access to many online services rely on Active Directory which uses the SMCPSS.org domain. When a domain controller specified as a Global Catalog is unavailable, authentication to web services will become unavailable.
- Software bugs and hardware failure are the primary internal system risks to the web services area.

7.7.2.2 External System Risk

- Campus web services are dependent upon the network/cable plant for continued operation. This includes fiber connected to Metrocast and the T1 connected to Sailor.
- SMCPSS web services could be compromised by hackers via web application exploits.

7.7.3 Preventative Measures

7.7.3.1 Current preventative measures include:

- SMCPSS relies on onsite backups, error logs, and regular security updates.
- Regular server and software security patching is performed to minimize the risk for unauthorized intrusion/or exploitation.
- The main SMCPSS firewall is configured to block unnecessary external access to campus web servers.

7.7.3.2 Future preventative measures

- Offsite disk storage capability should be developed for all servers.
- Given the user requirement for 24/7 web services availability, establishing high availability redundancy for all web services should be budgeted for and implemented to minimize loss of services.

7.7.4 Recovery Plan

7.7.4.1 Recovery requires adapting to the specific disaster which has occurred. The following general recovery scenario is provided, which can be tailored, as necessary.

7.7.4.2 General Recovery Steps:

- Assess which network service or services have been lost.

- Notify the campus, by whatever means available, as to the service outage.
- Troubleshoot to isolate the cause of the service outage.
- Once the problem is isolated, take appropriate action to restore the service(s).
- In the event the service cannot be restored in a timely fashion, assess possible workarounds, including temporary outsourcing, if feasible.
- Notify the campus as to the status of the affected service.
- Notify the campus when the service becomes available.

8.0 Maintenance of the IT Disaster recovery plan

The effectiveness of this disaster recovery plan is impacted by changes in the environment that the plan was created to protect. Some major factors which will impact the plan are new equipment, changing software environment, staff and organizational changes, and new or changing applications.

Annually, the Director of Technology will ensure that the document is reviewed and updated (if required) by a team of ITS personnel. This review will include an assessment and update as needed.

Appendix A: IT Disaster Recovery Teams

Team	Members
Network	Director of Technology
	WAN Administrator(s)
	LAN Administrator(s)
	Web Master(s)
Administrative	Director of Technology
	Receptionist
	Secretary
Repair	Director of Technology
	Technology Specialist
	Helpdesk Manager
	Technicians

Appendix B: SMCPS Campus Contact List

Person Responsible	Who to Contact
Director of Technology	Superintendent of Schools
	Public Information Officer
	Director of Human Resources
	Chief Financial Officer
	Chief Operating Officer
	Chief Academic Officer
	Director of Professional Development
	Executive Director of Student Services
Technology Specialist	Helpdesk Manager
	School Principals
	School technology contacts
WAN Administrator	Director of Technology
	All other WAN Administrator(s)
	Technology Specialist
LAN Administrator	Director of Technology
	All other LAN Administrator(s)
	Technology Specialist

Appendix C: Vendor Contact List

Refer to the state Bid list