St. Lawrence – Lewis BOCES

Risk and Security Management
Business Continuity/Disaster Recovery Plan
For Technological Systems

SLL BOCES Technology Disaster Recovery Plan

Planning Policy Statement:

This Disaster Recovery Plan document addresses all aspects of day-to-day operations to ensure reliability of mission critical and other technology systems, in accordance with the Board Policy #5260, Personal use of Computerized Information Resources and Board Policy #6214, Student Use of Computerized Information Resources.
Mission critical functions include those involving personnel, student, and financial records. This plan will be reviewed/updated yearly by the Director of Financial Affairs, Director of Instruction and Staff Development, in coordination with the technology staff.

The geographic location of the BOCES buildings provides various options for storage and recovery. In the event of an emergency in one location, systems may be moved, or recovered at our DR Site located in another area of the county.

Plan Logistics:

The Technology Disaster Recovery Plan will be kept on file with the District Superintendent, Director of Financial Affairs at the Educational Services Center and the Director of Instruction and Staff Development at the ESC, 40 West Main Street, Canton. Additionally, the general information is available on the SLLBOCES web page and the confidential copy is kept with the technical staff in an encrypted format at the DR site.

Table of Contents

Technology System Stakeholders

System	Location(s)	Internal Stakeholders	External Stakeholders For districts ustilizing SLLBOCES services see Appendix D
Application/Databases Ie: BOE Website, Helpdesk, Online training Server	Educational Services Center (ESC)	All BOCES employees.	Administrators, teachers, staff, and students in participating districts in multiple BOCES.
DNS – Active Directory	ESC	All BOCES employees and students.	Districts using Hosted Server Service
Email Files (Microsoft Exchange)	ESC	All BOCES employees and students.	Not Applicable
Personnel Files and Data (Win-Cap Web)	ESC	BOCES EER staff.	Not Applicable
HR-Records Server	ESC	All BOCES employees.	Employees from participating component districts.
Financial Program Files and Data SLLBOCES(Win-Cap)	ESC	All BOCES employees.	Not Applicable
Financial Program CBO (Win-Cap)	ESC	BOCES Shared Business Office employees	Districts using Shared Business Office
Individual User files for all BOCES sites	ESC	All BOCES employees.	Not Applicable
OPALS Library Automation	ESC	BOCES teachers and students.	Teachers and students from 18 SLLBOCES districts.
Video Streaming Server	ESC	BOCES teachers and students.	Teachers and students from participating districts in multiple BOCES.
Self- Funded Health/ Workers' Compensation Insurance (WLT)	ESC	All BOCES employees.	Employees from participating component districts.
Voice Over Internet Protocol Telephony	ESC, Northwest Tech (VoIP failover site)	All BOCES employees and students.	All component districts, parents and community at-large, Districts using Hosted Phone Service
Wi-Fi Controller	ESC	All BOCES employees and students.	Districts using Hosted Wi-Fi Service
Web-services	Housed-offsite w/ School Fusion	All BOCES employees.	School district personnel, parents and community will maintain connection

St. Lawrence-Lewis BOCES Educational Services
Data Center

The St. Lawrence-Lewis BOCES Educational Services Data Center performs numerous mission critical functions for the BOCES and the 18 component districts. The Educational Services Data Center houses the BOCES financial, personnel and health insurance systems. All operations serviced from within the data center are mission critical or respected as such. Each of these systems is backed up, protected and/or replicated at BOCES DR site.

The main programs and services to be addressed in this plan are:

- Win-Cap – Financial Software (BOCES and CBO for Districts)
- Human Resources Software (Win-Cap Web)
- Human Resources Software (Electronic Records Management)
- BOCES Email Server
- BOCES Application Server (BOE Website, Help Desk, Online training)
- BOCES VoIP Call Manager /Hosted VoIP Services
- BOCES Active Directory Services/User Authentication Server
- Hosted District Servers
- Host Wi-Fi Services
- Healthcare Administration Services
- Distance Learning Services
- Library Resource Center Services
- Central WAN Hub for all 18 districts and BOCES sites

Network Diagram – Reviewed and updated yearly. This document will aid in disaster recovery. (Appendix A)

Backup Operations

Overview:

- Server backups occur nightly to a network drive. When this process is completed the files are offloaded to a tape backup using Symantec Backup Exec Software. This software is also used for recovery of data from the tapes.
- Backup tapes are placed on rotation to ensure data is maintained daily, monthly, and yearly. At all times a minimum of two weeks' worth of tapes are available in addition to monthly and yearly tapes.
- Next business day maintenance contracts are purchased for all mission-critical network equipment including servers, switches, and routers.

Daily Storage Process:

- Each day, the previous night's tapes are removed, labeled Monday-Friday with a date as well as information of what the tape contains. The sets of tapes are placed into a secure case with shock, thermal & water resistance to meet specifications.

Monthly Storage Process:

- At the end of each month, tapes are transported to the Seaway Technical Center in Norwood, are labeled as "Monthly Backup" with a date and information located on the tapes. These tapes are flagged for monthly storage in a secure fire proof safe in the locked server room. (Access to the safe is limited to IT Supervisor and IT staff responsible for backups). These tapes are reused at 6 months of age.

Yearly Storage Process:

- At the end of the close of each fiscal year, tapes are transported to the Seaway Technical Center in Norwood, are labeled as "Yearly Backup" with a date and information located on the tapes. These tapes are flagged for yearly storage in a secure fire proof safe in the locked server room. (Access to the safe is limited to IT Supervisor and IT staff responsible for backups). These tapes are not reused.

Storage of Offsite Mission Critical Media

Storage cases arrive at the Seaway Technical Center via the LRC van delivery system.

Monthly and yearly storage cases are transferred to a secure storage room and safe at the Seaway Technical Center. Monthly and yearly tapes a into a fireproof safe for longer term storage. Tapes are maintained for a period of six months and then returned to their originating sites. Tapes are also stored annually and are maintained for ten years. For all transactions into or out of the safe a Safe Activity Log is maintained. This log is located on the front of the safe and includes a record of each object removed, object inserted along with the time and initials of the person performing the transaction.

> *It is important to note that keys for the tape travel cases are located only at the originating site and Seaway. The van driver does not have access to the keys.

Data Recovery Testing Process:

- Backups will be tested a minimum of every 60 days, using a backup server to verify the tapes/backup reliability (Appendix B).
- Tape drives will be maintained by IT staff based on the manufacturer's recommendations for number of writes, cleaning the drives, etc.
- Unusable (damaged tapes) will be magnetically erased and physically destroyed.

Backup Recovery:

- BOCES will maintain a backup server locally, for data and application restoration in the event of a server crash. The DR site will contain hardware and application software compatible with the production server for recovery and continued backups of mission-critical operations, in the event the DR site becomes the production site.

Backup Components:

The data center utilizes virtualization. The virtual machines are backed up either as the entire virtual machine or the data only on each machine depending on each servers needs. Priority servers are backed up both ways and/or participate in the real time replication with the DR site.

SLLBOCES Virtual Servers	DR-site replicate	Backup mode: VM /Data/Both
SLL-APP-MP = FileMaker Pro	no	BOTH
SLL-APP-PM = Print Manager	no	VM
SLL-APP-Shared = WSUS, NTP, ccproxy (?)	no	VM
SLL-APP-TMS = Telepresence Media (DL)	no	VM
SLL-APP-WEB = Various Web Pages	no	Data
Backup Exec: network backups, VOIP backups	no	Data
SLL-CBOWincap = CBO wincap (for districts)	Yes	BOTH
SLL-DC1 = AD, GP, DHCP, DNS	Yes	VM
SLL-DC2 = File Server (Admin, BOCES, DL, ESC, NWT, SLLINS, Students, SWT, SWY)	Yes	Data
SLL-DC3 = File Server (User data-faculty/student documents and desktops)	Yes	Data
SLL-EX-2013 = Exchange	Yes	Both
SLL-LRCMedia	No	Both
SLL-LRCVideo	No	VM
SLL-Signage = Carousel/tightrope	No	VM
SLL-Systems = Archived servers – flat data	no	VM
SLL-VMAS = DL services	No	VM
SLL-Insurances	Yes	Data
SLL-Wincap	Yes	BOTH
VSphere (one at Live site and DR site)	NO	VM
SLL-Records	Yes	Data
Brasher & Hammond Info-Matic servers	Yes	Both
SLL-Helpdesk	no	Both
SLL-LinuxWeb	no	Both
SLL-Opals	Yes	Both
All 22 hosted district AD and File servers	Yes	DC1s -VM DC2s -Data

Physical servers: Firewall logging server, VoIP servers, some DL servers/appliances, Video Surveillance system.

Disaster Recovery Site

SLLBOCES DR site is located at the Massena School Central Administration Building 84 Nightingale Ave Massena, NY 13662. This site is intended as a continuous data replication site, staged for use as a failover site to restore IT services in the event of a disaster for the BOCES and 18 component districts.

Disaster Defined As:

- One or more vital systems are non-functional
- The building is not available for an extended period of time but all systems are functional within it
- The building is available but all systems are non-functional
- The building and all systems are non-functional
- Events that may result in a disaster – Fire, Flood, Power Outage, Virus, Data Corruption

Disaster Declaration:

- Identification
- Assessment
- Declaration
- Activation of DR Site

Communication:

- Employees
- Clients and Districts
- Vendors – Verizon/WLT/IBM/HP/VMWare/Annese
- Authorities (If Needed)

Responsible Disaster Recovery Team (see appendix c)

- Craig Lalonde - IT Supervisor
- Network - Lori Remington– Information Systems Coordinator
- Servers - Brian Remington & Quincy Wood
- Help Desk – Jay Hebert
- Onsite contact at remote DR location- Mike Allen

Recovery Facilities:

- Redundant Servers and Data Storage
    - IBM H22 Blade Center and Sans units
- Redundant Network components
- Office Space with 24 X 7 Access
- Voice and Internet connectivity

Maintenance and Support of DR Site components:

- IBM
  Monday – Friday 5 X 7
  Phone 800-426-7378

- Zerto Replication Software
  Zerto 24 X 7 Phone and E-Mail support, 1 response
  www.zerto.com
  Phone 617-993-6331

- VMWare
  Monday –Friday 5 X 7 or per case for off-hour support
  Phone 877-486-9273

Testing of DR Site Practices and Viability

- Off Line
- Simulated cutover – This will be performed twice yearly. May also include Migrating workload(s) to a remote datacenter.

In the Event of an Emergency for any of the IT services referenced here with-in should follow this procedure unless otherwise indicated.

- The IT Supervisor, Supervisor of IT, and department Director will be notified that an emergency has occurred (e.g. the district office has burned).

- The IT Supervisor (or designee if unavailable) will immediately contact department directors and employees (any IT support staff, server and network technicians) crucial to the restoration process. A contact list (see Appendix C) will be maintained to ensure timely communication.

- Determination will be made as to the to activate the DR site located at Massena School Admin Building, or which systems, services or data will need to be restored. (See appendix E)

- The IT Supervisor will assess the situation and determine next steps which might include, but not be limited to:
  - Contacting the Northeastern Regional Information Center
  - Contacting the Development Authority of the North Country
  - Obtaining most recent backups from the Seaway Technical Center
  - Individual or all servers may be made active from the DR site

- Restoration of Applications and Data will be completed in the following order:
  - Network communication services – DHCP/DNS for inbound/outbound support from vendors and supporting service providers such as DANC and the NERIC to recognize/route traffic to/from the new live DR site (if necessary).
  - Financial System to include accounting, billing, payroll, and human resources.
  - Health Insurance services
  - Wincap BOCES and CBO
  - Email for communications
  - Communications for the serviced districts
  - LRC services and DL services
  - Individual user files for SLLBOCES and districts
  - Electronic Management Data (HR Laserfiche)
  - Web-server/databases

Healthcare Administration Services

The Healthcare Administration Offices in the ESC, houses the St. Lawrence-Lewis Counties School District Employees Medical Plan. This self-funded insurance agency serves 18 component districts and the St. Lawrence-Lewis BOCES. All operations within this program are mission critical and serviced from a single SLL-Insurance server. The main components of the Health Care Administrative system are:

- Health Insurance
- Enrollment in the Pro-Act Prescription Drug Plan
- Administration of Flex Plan
- Worker's Compensation
- COBRA Coverage

In the event of an emergency the recovery plan would follow the outline depicted on page 11 with support as needed from the specific vendors or supportive organizations listed below:

Eagle Datagistics
19321 US-19 North, Suite 404
Clearwater FL 33764
727- 535-3592

WLT Software
2410 Northside Drive
Clearwater, FL 33761
727-442-9296

Payroll, Accounting and HR Services

The Educational Services Center houses the St. Lawrence-Lewis Counties payroll and accounting services for the BOCES and several 18 component school districts.
All operations within this program are mission critical serviced from three servers, the SLL-Wincap server, the CBO-Wincap server and the SLL-Records server (Laserfiche). The key components addressed in the plan are:

- Payroll and Account services
- Employee records for HR needs
- Wincap client for treasure and clerks
- Wincap client for all SLLBOCES administrators for employee attendance, order approval
- Wincap-Web for BOCES and District employees self-service

In the event of an emergency the recovery plan would follow the outline depicted on page 11 with support as needed from the specific vendors or supportive organizations listed below:

Wincap Contact Information:

Win-Cap Harris School Solutions
Ron Bombard
1 Winners Circle Suite 220
Albany NY, 12205 518-435-0500 x137

Laserfiche Contact Information:

Andy Squires
Consultative Solutions Technician, General Code
Content Management Solutions
Help Desk: 855.436.5500
781 Elmgrove Road | Rochester, NY 14624
cms.generalcode.com

BOCES Email Services

The Educational Services Center houses the St. Lawrence-Lewis BOCES Exchange email server.

In the event of an emergency the recovery plan would follow the outline depicted on page 11, with support as needed from Microsoft.

BOCES Application Server

The Educational Services Center houses the St. Lawrence-Lewis BOCES Application server for various systems such as helpdesk, Employee-staff RTK training, BOE communications etc.

In the event of an emergency the recovery plan would follow the outline depicted on page 11, with support from internal technicians.

BOCES VoIP Hosted Services

The Educational Services Center houses the St. Lawrence-Lewis BOCES VoIP Cluster for the SLLBOCES Sites and various School Districts (see appendix D). Each BOCES site and hosted district is equipped with failover equipment that will provide basic phone services independently until the VoIP system is restored.

In the event of an emergency the recovery plan would follow the outline depicted on page 11, with support from internal technicians and as needed from the specific vendors or supportive organizations listed below:

Annese & Associates, Inc.

518-309-6393 direct

518-371-9000 office

Hosted District Servers

The Educational Services Center houses active directory and file servers for several of the 18 component school districts as noted in appendix D. All operations within this program are critical services for the school. Each school has 2-3 servers.
The key components addressed in the plan are:

- Active Directory services
- Teacher and student files

In the event of an emergency the recovery plan would follow the outline depicted on page 11 with support from internal technicians.
See appendix C for network and server technician list.

BOCES Wi-Fi Hosted Services

The Educational Services Center houses the St. Lawrence-Lewis BOCES Wireless LAN controller for the SLLBOCES Sites and various School Districts (see appendix D). An redundant controller is maintained/stored at the DR site in the event the primary ESC unit failed or was inaccessible.

In the event of an emergency the recovery plan would follow the outline depicted on page 11, with support from internal technicians and as needed from the specific vendors or supportive organizations listed below:

Annese & Associates, Inc.
518-309-6393 direct
518-371-9000 office

BOCES WAN Hub Services

The Educational Services Data Center acts as a WAN Hub for the BOCES sites as well as all 18 component districts (see appendix D). Redundant equipment is maintained/stored at the DR site in the event the primary ESC unit failed or was inaccessible. These units are on maintenance agreements for four hour replacement from the vendor also.

In the event of an emergency the recovery plan would follow the outline depicted on page 11, with support from internal technicians and as needed from the specific vendors or supportive organizations listed below:

Annese & Associates, Inc.
518-309-6393 direct
518-371-9000 office

DANC
STEVE SMITHERS
(315) 661-3200

Distance Learning Services

The BOCES maintains is own onsite DL/conferencing service providing Distance Learning services to various schools around the county. SLLBOCES also subscribes to cloud based DL/conferencing systems. Although these services are not mission critical, the instructional programs in many of the eighteen component districts, depend greatly upon access to these collaborative resources.

In the event of an emergency the DL Classrooms at many of the 18 schools could be connected into one of the SLLBOCES cloud subscriptions (WebEx or Zoom) or be connected via the NERIC DL service until services and/or hardware units could be restored/replaced.
Additional consult and support from specific vendors or supportive organizations as listed below

- Steve Fenton
  SLL BOCES DL coordinator
  Educational Services Center
  40 West Main St
  Canton NY
  315-323-1848 (cell)

- One-Vision Solutions
  Matthew Meyer
  Project Manager
  Office: 972-580-8347
  Mobile: 214-457-2727

Learning Resources Center Services

The Learning Resources Center (LRC) houses a large collection of physical and electronic resources. Additionally, the library automation server for all of the component districts resides in the datacenter. Although these services are not mission critical, the instructional programs within the eighteen component districts, depend greatly upon access to these electronic resources.

The LRC services addressed in the plan are:
Library Automation (OPALS) , Video/Media Server , SNAP

In the event of an emergency the recovery plan would follow the outline depicted on page 11.

- Contacting

TekData(SeriesM/Snap)
Gene Lefare
Dan Marsh
Scott Zievterra
1-847-367-8800

Biblio Fiche MediaFlex CERF
Dan Weeks dan@bibliofiche.com
Harry Chan harry@bibliofiche.com
877-331-1022

PowerMediaPlus
1-800-323-9084

United Streaming Discovery Education
Kristen Olsen Kristen_Olson@discovery.com
301-272-2757

Career and Technical Education Centers

The BOCES has three Career and Technical Education (CTE) centers located in Fowler (Southwest Tech, SWT), Norwood (Seaway Area Tech, SATC), and Ogdensburg (Northwest Tech, NWT). The SLLBOCES Adult Education program also has satellite sites in various areas in the county.

In the event of an emergency at the BOCES datacenter the computers and user files could be unavailable until the servers/services were restored. The tech centers are equipped with failover systems for phone services for reliable communication in the event of disrupted ESC services.

Xenegrade and School Tool are the student information systems used by the CTE centers. All student information is housed off-site at the NERIC in Albany or with Xenegrade. These services would only be affected from a network outage. They are not housed with SLLBOCES but at remote provider sites.

School Tool Contact:

Lisa Grant
40 West Main Street
Canton N.Y. 13617
(315)386-4504 X 10141

Xenegrade support services provided by :

Xenegrade Support <support@xenegrade.com>

Preventative Practices

Proactive Intrusion Detection/Prevention Plan (Sabotage – Hacking)

- Firewall - A CISCO firewall is maintained at each SLLBOCES site and school district that assists in the prevention of intrusion by unauthorized users.
- The IT Supervisor and designee will receive emails indicating all intrusion attempts.
- In the event that an intrusion is detected the firewall will take corrective action (e.g. shutdown a port or shutdown a service).
- An investigation process will be enacted when system access is obtained by an intruder.
- A system log on the fileserver will track user access and will be used if an investigation is necessary.
- The investigation process will also include authorities as indicated by the level of intrusion. (e.g. local employee vs. international relaying)

System Security – Password Policies

- Administrative passwords for technology systems will only be available to the IT Supervisor and technology staff *directly* responsible for support of said systems. (In the event that technology staff *directly* responsible for systems change, then the passwords are immediately changed as well). .
- User passwords are setup by the technology staff member(s) *directly* responsible for the system.
- Password Complexity requirements
  - ❖ Passwords are automated to be reset every 365 days
  - ❖ Passwords must be 8 characters or more containing 3 of the 4 parameters
    - Uppercase and lowercase letters and a special character and/or number
    - Password may not contain or be too similar to the username

Employee Awareness of an individual's computing safety and security practices

Periodically awareness emails are distributed to all staff discussing:

- spotting phishing emails
- suspicious web sites.
- Phishing phone calls/scams
- Suspicious Cell phone and mobile device apps
- IT staff is continually updated on safe/security-conscientious technician practices

Preventative Maintenance

- Software upgrades: both OS and applications (Java, Adobe reader, etc.)
- Firewall (CISCO-ASA) – A new firewall is installed that will allow the BOCES to prevent intrusion by unauthorized users – Updated as new releases from vendor are available
- CISCO Firepower IPS/Management Center
- Maintain Anti-Virus (Microsoft Windows Defender) – All workstations and fileservers have anti-virus software installed with the most updated virus signatures to ensure that the machines are protected from attack.
- Any (hardware/software) maintenance contracts
- UPS (Uninterruptible Power Supply)

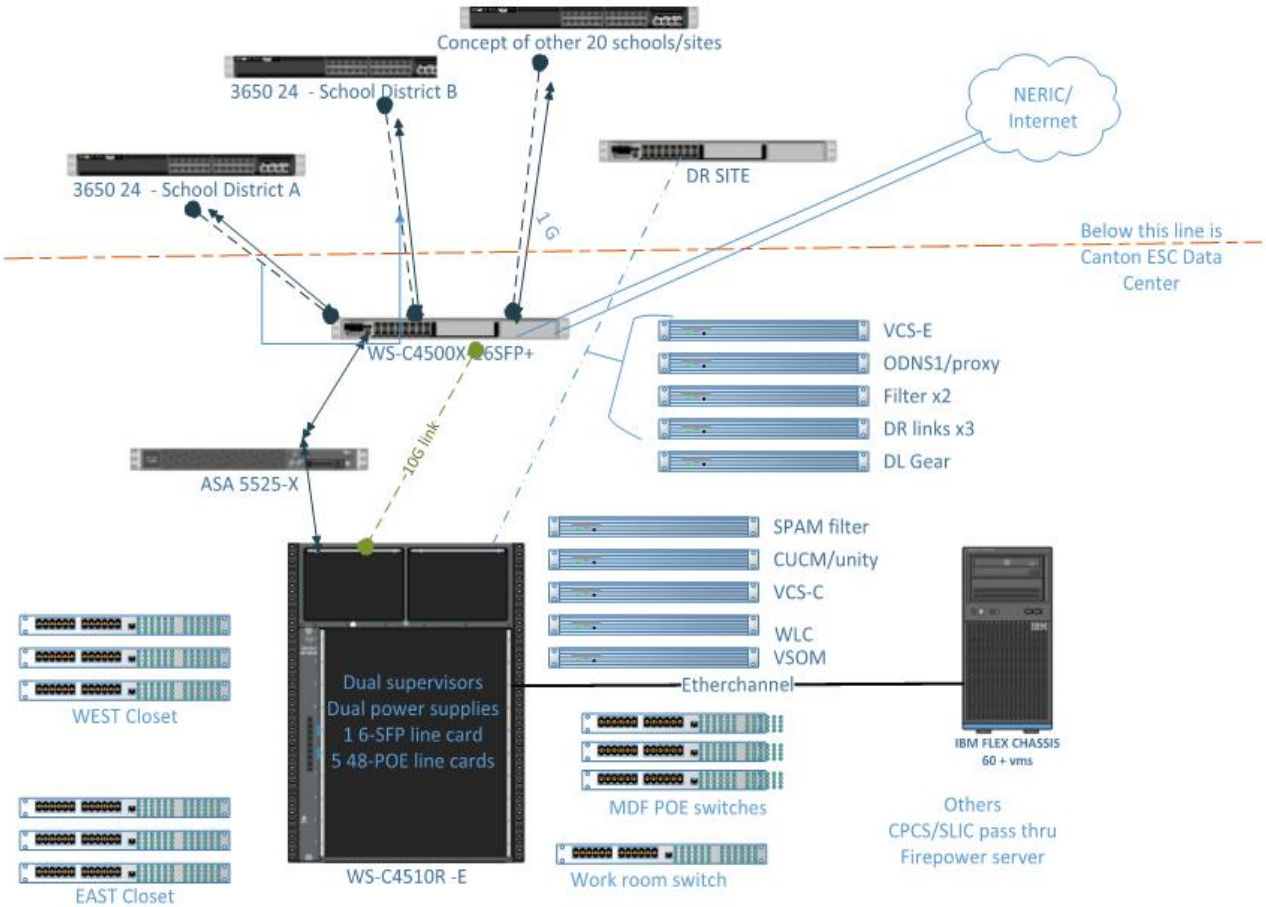
Software Availability and Inventory:

- Software such as the server operating systems, financial software and human resources software is available and will be secured from the vendors' websites to ensure currency in the event these resources would be needed in a disaster.
- A software inventory is maintained electronically along with licensing information.

Appendix A - Network Diagrams

This network diagram is a conceptual overview.
The detailed technical diagrams are available to
authorized personnel and organizations only.

The SLLBOCES Data Center Servers a WAN hub for most of the 18 school districts and the SLLBOCES sites, built on 1 Gig point-to-point connections in conjunction with DANC. Each site has 2 routing paths one for DL and VOIP traffic, the other for general internet and server traffic.



Appendix B1 – Tape Recovery Testing Record

Date	Media Tested	Files Tested	Results	Signature
10/7/2016	Feb 2016 6 month Tape 1	Restored a file from Wincap CBO server	Success	LR JH

Appendix B2 – DR site failover testing Record

Date	Server/Service Failed over	Results	Signature
8/2016	Test vm	success	QW/LR

Appendix C - Emergency Contacts

Home and cell numbers listed below are ONLY to be used in the event of an emergency, (these are not available on public website).

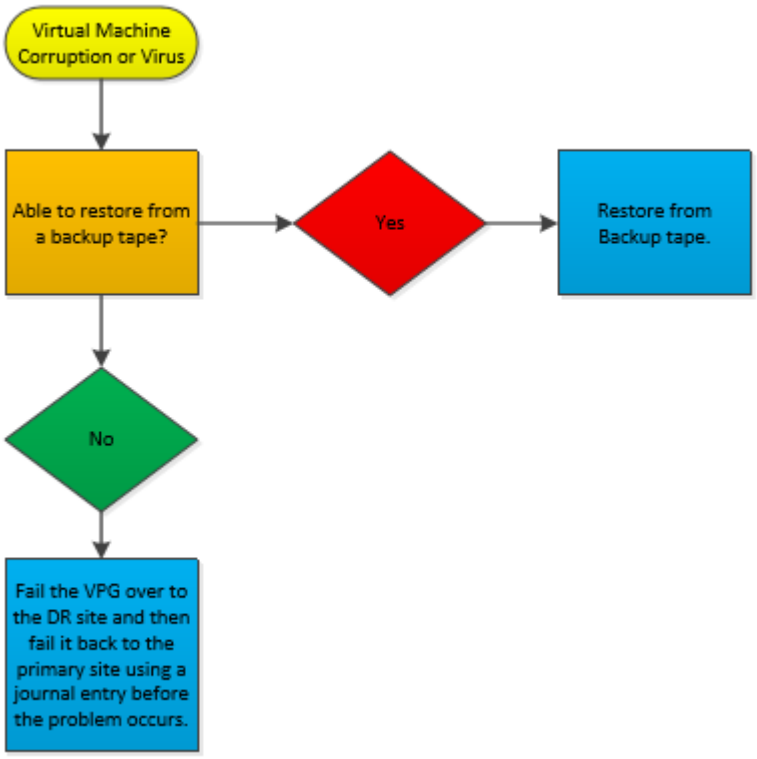
First	Last	Position	Work
Craig	Lalonde	Informational Technology Supervisor	386-4504 x10154
Thomas	Burns	District Superintendent/Executive Officer	386-4504
Jennifer	French	Senior Supervisor of School Improvement	386-2226 x15107
Burke	Ron	Assistant Superintendent for Instruction	386-2226 x15101
Kevin	Perretta	Supervisor of Buildings and Grounds	713-5327
Lori	Remington	Information Services Coordinator	386-4504 x10170
Nicole	Ashley	Director of Financial Affairs	386-4504 x10168
Rafael	Olazagasti	Director of Human Resources and Labor Relations/General Counsel	386-4504 x10129
Nicole	Ashley	Director of Financial Affairs	386-4504 x10172
Renee	Langtry-Green	Director of Special Education	386-4504 x 10155
Jayne	Carbone	Healthcare Administrator	379-3000
Kelly	Wilson	Director of Library Services	386-4504x202
Jane	Akins	Program Director Technical Centers	353-6693 x20221

Appendix D – Districts Utilizing SLLBOCES Hosted or Shared Services

SITE/District	Hosted Servers	Hosted WIFI	Hosted Phones	DL Services	Wincap
ESC	Yes	Yes	Yes	Yes	BOCES
NWT	Yes	Yes	Yes	Yes	BOCES
SWT	Yes	Yes	Yes	Yes	BOCES
Seaway	Yes	Yes	Yes	Yes	BOCES
P-Tech	Yes	Yes	Yes	Yes	n/a
35Glenn/MAC	Yes	Yes	Yes		n/a
Brasher	Yes		Yes		CBO
Clifton-Fine	Yes			Yes	CBO
Edwards-Knox	Yes	Yes	Yes		CBO
Hammond	Yes	Yes	Yes	Yes	
Harrisville	Yes	Yes		Yes	CBO
Hermon-DeKalb	Yes	Yes		Yes	
Heuvelton	Yes		Yes	Yes	CBO
Lisbon	Yes			Yes	
Morristown	Yes	Yes	Yes	Yes	CBO
Ogdensburg	Yes			Yes	CBO
Parishville-Hopkinton	Yes	Yes			CBO
Potsdam	NERIC Supported IT				
Madrid	NERIC Supported IT			Yes	
Gouverneur	NERIC supported IT			Yes	
Canton	Independent IT	using hosted Wi-Fi		-	
Massena	Independent IT			-	
Colton-Pierrepoint	Independent IT			-	
Norwood-Norfolk	Independent IT			Yes	

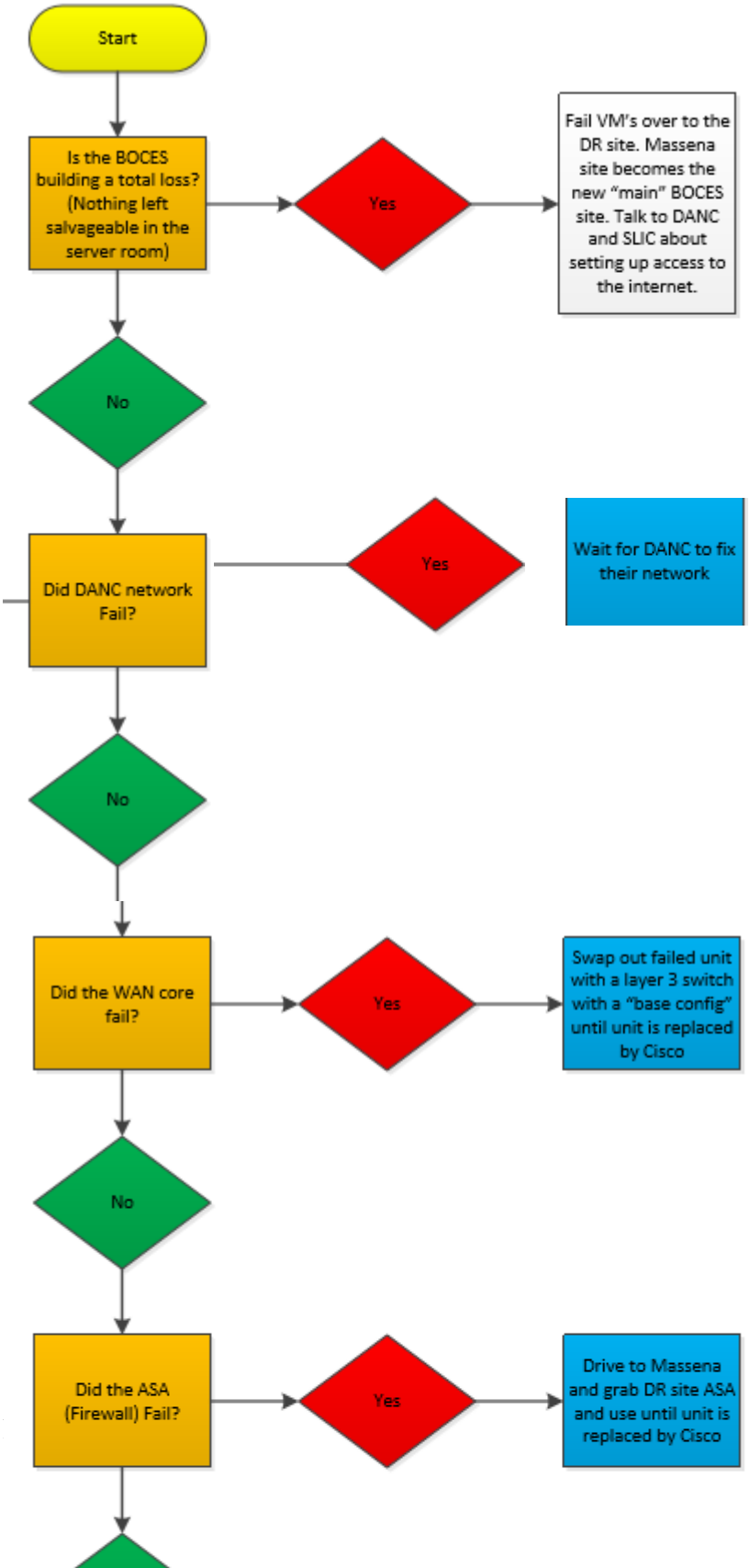
Pathway to Recovery

Virus or Data Corruption restoration flow.



Pathway to Recovery

Physical or environmental damage restoration flow.



Updated Fall 2016


No
Did the IBM Chassis Fail?
Yes
If chassis is a total failure (irrecoverable), fail over to the DR site. Craig's call on how long to wait before we failover.
No
Did the SANS unit fail?
Yes
Fail over to the DR site. Craig's call on how long to wait before we fail over.
No
Go back to start
For These 2 options, we can set up EIGRP for the DR site, Renumber the DR site core switch to 8.1, add a new default route back to BOCES so the internet is accessible, and add vlan 600 to the DR core. So the DR site will contain all of the VMs, but internet traffic will still be routed through the BOCES building. The main BOCES site will have to have vlan 10 clients moved to vlan 16.