St. Lawrence – Lewis BOCES

Risk Management – Business Continuity/Disaster Recovery Plan
For Technological Systems

This plan was adopted by the St. Lawrence-Lewis Board of Education
During their January 15, 2009 Regular Meeting
Revised January 2015

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. 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, with representation by technology and financial staff members.

The geographic location of BOCES buildings provides tremendous 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, copies will be given to all people who have the potential to be contacted in the event of an emergency (See Appendix C).

Table of Contents

Technology System Stakeholders

System	Location(s)	Internal Stakeholders	External Stakeholders
Application/Databases (BOE Website, Cooperative Purchasing, Help Desk, Online training) Server	Educational Services Center	All BOCES employees.	Administrators, teachers, staff, and students in participating districts in multiple BOCES.
DNS – Active Directory	All BOCES Locations	All BOCES employees.	Not Applicable
Email Files (Microsoft Exchange)	Educational Services Center	All BOCES employees.	Not Applicable
Financial Program Files and Data SLLBOCES(Win-Cap)	Educational Services Center	All BOCES employees.	Not Applicable
Financial Program CBO (Win-Cap)	Educational Services Center	BOCES Shared Business Office employees	Districts using Shared Business Office
Individual Office User Files	All BOCES Locations	All BOCES employees.	Not Applicable
OPALS Library Automation	Learning Resources Center	BOCES teachers and students.	Teachers and students from 18 SLLBOCES districts.
Personnel Files and Data (Win-Cap Web)	Educational Services Center	BOCES EER staff.	Not Applicable
Self- Funded Health/ Workers' Compensation Insurance (WLT)	Educational Services Center	All BOCES employees.	Employees from participating component districts.
Video Streaming Server	Learning Resources Center	BOCES teachers and students.	Teachers and students from participating districts in multiple BOCES.
Voice Over Internet Protocol Telephony	Educational Services Center, Northwest Tech, Seaway Area Tech	All BOCES employees and students.	All component districts, parents and community at-large.
Web-server	Housed offsite	All BOCES employees.	School district personnel, parents and community will lose access to

St. Lawrence-Lewis BOCES Educational Services Center

The St. Lawrence-Lewis BOCES Educational Services Center performs numerous mission critical functions for the BOCES and the 18 component districts. The Educational Services Center houses the BOCES financial and personnel systems. Additionally, the Educational Services Center contains the main computing center for the BOCES. All operations within this program are mission critical. The main programs to be addressed in the plan are:

- Win-Cap – Financial Software
- Human Resources Software (Win-Cap Web)
- BOCES Email Server
- BOCES Application Server (BOE Website, Cooperative Purchasing, Help Desk, Online training)
- BOCES VoIP Call Manager
- BOCES User Authentication Server
- Hosted Server
- Hosted VoIP
- Host WiFi
- Healthcare Administration

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

System Security – Passwords

- 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). In addition, passwords will be changed on a periodic basis.
- User passwords are setup by the technology staff member(s) *directly* responsible for the system.

Preventative Maintenance

- Software upgrades (OS application)
- Firewall (CISCO-ASA) – A new firewall is installed that will allow the BOCES to prevent intrusion by unauthorized users.
- Maintain Anti-Virus (Norton/MS Forefront) – 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)

Intrusion Detection Plan (Sabotage – Hacking)

- Firewall (CISCO) – A firewall is installed that will allow the BOCES to prevent intrusion by unauthorized users.
- 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). In addition, passwords will be changed on a periodic basis.
- User passwords are setup by the technology staff member(s) *directly* responsible for the system.
- 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)

Disaster Recovery Plan - Backup Recovery (Applications/Data)

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. The case is transported to the Learning Resources Center at 7229 State Highway 56, Norwood NY via the BOCES Van Delivery Service for overnight offsite storage.
- Each day, sets of tapes, from two days prior, are returned from the Learning Resources Center in Norwood and stored on-site 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).

Monthly Storage Process:

- At the end of each month, tapes are transported to the Learning Resources 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).

Yearly Storage Process:

- At the end of the close of each fiscal year, tapes are transported to the Learning Resources 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).

Data Recovery Testing Process:

- Backups will be tested a minimum of twice a year, approximately every six months, 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.
- 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 off-site server will contain hardware and application software compatible with the production server for recovery and continued mission-critical operations.

Software Inventory:

- Software such as the financial software and human resources software is available on and will be secured from the vendors' websites to ensure currency.
- Software (e.g. server operating system, backup/restore) duplicated and housed off-site at the Learning Resources Center (LRC) at the Seaway Campus in Norwood. Software such as financial and human resources software that may be obtained from the vendor website is also backed up and stored at the LRC.
- A software inventory is maintained electronically along with licensing information.

Backup Contents

- Financial Program Files and Data (Win-Cap)
- Individual Office User Files
- Email Files (Microsoft Exchange)
- Web-server/ Databases
- DNS – Active Directory
- Instructional Content Management Files (Moodle)

In the Event of an Emergency

- 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 employees (webmaster, financial package support technician, and server support technician) crucial to the restoration process. A contact list (see Appendix C) will be maintained to ensure timely communication.
- 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
  - Contacting technicians responsible for various BOCES locations
  - Obtaining most recent backups from the Learning Resources Center
- Restoration of Applications and Data will be completed in the following order:
  - Financial System to include accounting, billing, payroll, and human resources. Restoration will also include client workstation configuration of telnet client and routing changes may occur at DANC and the NERIC to recognize the new location of the financial server (if necessary).
  - Email for communications
  - Individual user files
  - Web-server/databases

Healthcare Administration

The Healthcare Administration Offices 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. The main programs to be addressed in the plan are:

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

Network Diagram – Reviewed and updated yearly. This document will serve in disaster recovery. Copy of diagram may be found under Appendix A.

System Security – Passwords

- Administrative passwords for technology systems will only be available to the IT Supervisor, the Healthcare Administrator/designee, and the technology staff member *directly* responsible for support of said systems. (In the event that the technology staff *directly* responsible for systems changes, then the passwords are immediately changed as well). In addition, passwords will be changed on a periodic basis.
- User passwords are setup by the technology staff member *directly* responsible for the system.

Preventative Maintenance

- Software upgrades (OS application)
- Firewall (CISCO-ASA) – A new firewall is installed that will allow the BOCES to prevent intrusion by unauthorized users.
- Maintain Anti-Virus (Norton/MS Forfront) – All workstations and fileservers have anti-virus software installed with the most updated virus signatures to ensure that the machines are protected from attack.
- All (hardware/software) maintenance contracts are purchased and up-to-date
- UPS (Uninterruptible Power Supply) connected to all servers and network components

Intrusion Detection Plan (Sabotage – Hacking)

- Firewall (CISCO) – A firewall is installed that will allow the BOCES to prevent intrusion by unauthorized users.
- Administrative passwords for technology systems will only be available to the IT Supervisor, Healthcare Administrator/designee, 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). In addition, passwords will be changed on a periodic basis.
- User passwords are setup by the technology staff member(s) directly responsible for the system.
- The firewall contains statistics indicating suspicious activity.
- An investigation process will be enacted if system access is obtained by an intruder.
- Although limited, 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)

Disaster Recovery Plan - Backup Recovery (Applications/Data)

Overview:

- Server backups occur nightly directly to tape backup. 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.
- Additionally, an off-site backup is planned to begin later in the spring, that will allow weekly backups of data to a server at the BOCES District Office.
- Eagle Software Company of Florida (877-807-4730) verifies and certifies that the Healthcare Records database is running at optimal performance. Maintenance is performed monthly when the database is pulled back to the Eagle corporate office, to optimize the performance of the system.
- 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 tape(s) is removed, labeled Monday-Friday with a date as well as information of what the tape contains. The tape(s) is placed into a secure case with shock, thermal & water resistance to meet specifications. The case is transported daily to the BOCES District Office.
- Each day, sets of tapes, from two days prior, are returned from the BOCES District Office and stored on-site in a secure fire proof safe. (Access to the safe is limited to IT Supervisor, IT staff responsible for backups, and the Healthcare Administrator).

Monthly Storage Process:

- At the end of each month, tapes are transported to the BOCES District Office in Canton, and 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).
- Eagle Software Company of Florida verifies that data stored on the Healthcare server are not corrupt.

Yearly Storage Process:

- At the end of the close of each fiscal year, tapes are transported to the BOCES District Office in Canton, and 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).

Data Recovery Testing Process:

- Backup data will be verified a minimum of twice a year, approximately every six months to verify the tapes/backup reliability (Appendix B).
- Tape drives will be maintained by IT staff based on the manufacturer's recommendations.
- 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 off-site server will contain hardware and application software compatible with the production server for recovery and continued mission-critical operations.
- An offsite server is available in the event of a site catastrophe on which the Eagle software company will rebuild and restore all software as part of their maintenance agreement using backup files.

Software Inventory:

- WLT and Oracle software is available on and will be secured from the vendors' websites to ensure currency.
- Software (e.g. server operating system, backup/restore) duplicated and housed off-site at the BOCES District Office in Canton.
- A software inventory is maintained electronically along with licensing information.

Backup Contents

- WLT Software
- Oracle Software
- Healthcare, Worker's Compensation, COBRA Insurance, Pro-Act Prescription Drug Plan and Flex Plan data are all found within the Oracle Database

In the Event of an Emergency

- The IT Supervisor, Supervisor of IT, and department Director will be notified that an emergency has occurred.
- The IT Supervisor (or designee if unavailable) will immediately contact employees (webmaster, financial package support technician, and server support technician) crucial to the restoration process. A contact list (see Appendix C) will be maintained to ensure timely communication.
- 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
  - Contacting technicians responsible for various BOCES locations
  - Obtaining most recent backups from the BOCES District Office
  - Contacting Eagle Software Company of Florida
  - Contacting WLT Software Company of Florida
- Restoration of Applications and Data will be completed in the following order:
  - Restoration of Healthcare Server and Databases
  - Restoration of client workstations
  - Restoration of user data (e.g. memos, letters)

- Contact Information:

Eagle Software
19321 US-19 North, Suite 404
Clearwater FL 33764

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

Washington Education Building

The Washington School building houses the St. Lawrence-Lewis BOCES Print Shop.

Other BOCES Services, housed at Washington School, that are not addressed in this plan include:

- ❖ Print Shop – Billing (this system will be backed up at the BOCES Educational Services Center)

Network Diagram – Reviewed and updated yearly. This document will serve in disaster recovery. Copy of diagram may be found under Appendix A,

System Security – Passwords

- Administrative passwords for technology systems will only be available to the IT Supervisor, the Director of Financial Affairs/designee, and the technology staff member *directly* responsible for support of said systems. (In the event that the technology staff *directly* responsible for systems changes, then the passwords are immediately changed as well). In addition, passwords will be changed on a periodic basis.
- User passwords are setup by the technology staff member *directly* responsible for the system.

Preventative Maintenance

- Software upgrades (OS application) are completed by the Director of Finance/designee. If the system is upgraded the IT Supervisor or technology staff member *directly* responsible for support of said systems will upgrade software applications.
- Firewall (CISCO-ASA) – A new firewall is installed that will allow the BOCES to prevent intrusion by unauthorized users. The IT Supervisor and designee will receive emails indicating all intrusion attempts.
- Maintain Anti-Virus (Norton) – All workstations and fileservers have anti-virus software installed with the most updated virus signatures to ensure that the machines are protected from attack.
- All (hardware/software) maintenance contracts are purchased and up-to-date.
- UPS (Uninterruptible Power Supply) connected to all servers and network components.

Intrusion Prevention Plan (Sabotage – Hacking)

- Firewall (CISCO) – A firewall is installed that will allow the BOCES to prevent intrusion by unauthorized users.
- Administrative passwords for technology systems will only be available to the IT Supervisor, Director of Financial Affairs/designee, 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). In addition, passwords will be changed on a periodic basis.
- User passwords are setup by the technology staff member(s) *directly* responsible for the system.
- The firewall contains statistics indicating suspicious activity. These reports will be reviewed periodically and upon awareness of suspicious activity statistics will be closely monitored.
- An investigation process will be enacted if system access is obtained by an intruder.
- Although limited, 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)

Disaster Recovery Plan - Backup Recovery (Applications/Data)

Overview:

- System backups occur nightly directly to tape backup. This software is also used for recovery of data from these tapes.
- Backup tapes are placed on rotation to ensure data is maintained daily (incremental), weekly (data and library files), monthly, and yearly (by fiscal and calendar year). At all times a minimum of one week worth of daily tapes are available in addition to weekly (four weeks maintained), and yearly (maintained five years) tapes.
- Additionally, an off-site backup is planned to begin later in the summer 2013 that will allow weekly backups of data to a server at the BOCES District Office.
- 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 tape(s) is removed, labeled Monday-Friday with a date as well as information of what the tape contains. The tape(s) is placed into a secure case with shock, thermal & water resistance to meet specifications. The case is transported daily to the BOCES District Office.
- Each day, sets of tapes, from one week prior, are returned from the BOCES District Office and stored on-site in a secure fire proof safe. (Access to the safe is limited to IT Supervisor, IT staff responsible for backups, and the Director of Financial Affairs).

Weekly Storage Process:

- At the end of each week, tapes are transported to the BOCES District Office in Canton, and are labeled as "Weekly Backup" with a date and information located on the tapes. These tapes are flagged for weekly 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).

Yearly Storage Process:

- At the end of the close of each fiscal year and calendar year, tapes are transported to the BOCES District Office in Canton, and are labeled as "Yearly (fiscal or calendar year) 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).

Data Recovery Testing Process:

- Backup data will be verified a minimum of twice a year, approximately every six months to verify the tapes/backup reliability (Appendix B).
- Tape drives will be maintained by IT staff based on the manufacturer's recommendations.
- Unusable (damaged tapes) will be magnetically erased and physically destroyed.

Backup Recovery:

- A second server will be built (Winter/Spring 2013) as a backup server on site for data and application restoration in the event of a server crash. The backup server will contain hardware and application software compatible with the production server for recovery and continued mission-critical operations.

Software Inventory:

Backup Contents

- Print Shop Database and libraries

In the Event of an Emergency

- The IT Supervisor, Supervisor of IT, and department Director will be notified that an emergency has occurred (e.g. the Washington Educational Building has burned).
- The IT Supervisor (or designee if unavailable) will immediately contact employees (financial package support technician and server support technician) crucial to the restoration process. A contact list (see Appendix C) will be maintained to ensure timely communication.
- 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
  - Contacting technicians responsible for various BOCES locations(Appendix C)
  - Obtaining most recent backups from the BOCES District Office
  - Contacting Capital Computer Associates Corporation (WINCAP Software)
- Restoration of Applications and Data will be completed in the following order:
  - Restoration of client workstations
  - Restoration of user data (e.g. memos, letters)
- Contact Information:

Learning Resources Center

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 on this site. Although these services are not mission critical, the instructional programs within the eighteen component districts, depend greatly upon access to these electronic resources.

The main programs to be addressed in the plan are:

- Library Automation
- Video/Media Server
- Tekdata

The main process to be addressed in the plan is:

- Storage of long-term, electronic backups from other BOCES locations in fire-proof safe

Network Diagram – Reviewed and updated yearly. This document will serve in disaster recovery. Copy of diagram may be found under Appendix A.

System Security – Passwords

- Administrative passwords for technology systems will only be available to the IT Supervisor, the Supervisor of the Learning Resources Center, and the technology staff member(s) *directly* responsible for support of said systems. (In the event that the technology staff *directly* responsible for systems changes, then the passwords are immediately changed as well). In addition, passwords will be changed on a periodic basis.
- User passwords are setup by the technology staff member(s) *directly* responsible for the system.

Preventative Maintenance

- Software upgrades (OS application)
- Firewall (CISCO) – A new firewall is installed that will allow the BOCES to prevent intrusion by unauthorized users for the entire Seaway Campus.
- Maintain Anti-Virus (Norton) – All workstations and fileservers have anti-virus software installed with the most updated virus signatures to ensure that the machines are protected from attack.
- All (hardware/software) maintenance contracts are purchased and up-to-date.
- UPS (Uninterruptible Power Supply) connected to all servers and network components.

Intrusion Prevention Plan (Sabotage – Hacking)

- Firewall (CISCO) – A firewall is installed that will allow the BOCES to prevent intrusion by unauthorized users.
- Administrative passwords for technology systems will only be available to the IT Supervisor, Learning Resources Center Supervisor/designee, 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). In addition, passwords will be changed on a periodic basis.
- User passwords are setup by the technology staff member(s) *directly* responsible for the system.
- The firewall contains statistics indicating suspicious activity. These reports will be reviewed periodically and upon awareness of suspicious activity statistics will be closely monitored.
- An investigation process will be enacted if system access is obtained by an intruder.
- Although limited, 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)

Disaster Recovery Plan - Backup Recovery (Applications/Data)

Overview:

- Server backups occur nightly directly to tape/removable hard drive backup. This software is also used for recovery of data from the tapes/ hard drives.
- Backup tapes/hard drives 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.
- Contracts are established with , OPALS, Tekdata and Mandarin.

Daily/Weekly Storage Process:

- Each day, the previous night's tape(s) is removed, labeled Monday-Friday with a date as well as information of what the tape contains. Every Tuesday, the tapes/ hard drives are placed into a secure case with shock, thermal & water resistance to meet specifications. The case is transported weekly to the BOCES District Office.
- Each week backup tapes/hard drives, from the week prior, are returned from the BOCES District Office and stored on-site in a secure fire proof safe. (Access to the safe is limited to IT Supervisor, IT staff responsible for backups, and the Supervisor of the LRC).

Monthly Storage Process:

- At the end of each month, tapes are transported to the BOCES District Office in Canton, and 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).

Yearly Storage Process:

- At the end of the close of each fiscal year, tapes are transported to the BOCES District Office in Canton, and 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).

Data Recovery Testing Process:

- Backup data will be verified a minimum of twice a year, approximately every six months to verify the tapes/backup reliability (Appendix B).
- Tape drives will be maintained by IT staff based on the manufacturer's recommendations.
- Unusable (damaged tapes) will be magnetically erased and physically destroyed.

Backup Recovery:

- Tekdata – Contact Tekdata to restore files.
- OPALS - Contact MediaFlex to restore files.
- Mandarin - Contact Mandarin to restore files.
- Windows Server User Files – restore to local server if available or to server housed at Educational Services Center if necessary.

Software Inventory:

- Tekdata, OPALS, Mandarin software is available on and will be secured from the vendors' websites to ensure currency.
- Software (e.g. server operating system, backup/restore) duplicated and housed off-site at the Old LRC building Via Tape Backup.
- A software inventory is maintained electronically along with licensing information.

Backup Contents:

- Tekdata database, user, and booking information
- OPALS database – library holdings and circulation information
- Mandarin database - Union Catalog

Storage of Offsite Mission Critical Media

Storage cases arrive at the Old LRC building via the LRC van delivery system.

Storage cases* are taken from the LRC van to the secure room(Old Server room) and kept in the transport cases as a daily function. Once a month the tapes are placed 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 the LRC. The van driver does not have access to the keys.

In the Event of an Emergency

- The IT Supervisor, Supervisor of IT, and department Director will be notified that an emergency has occurred (e.g. the Learning Resources Center has burned).
- The IT Supervisor (or designee if unavailable) will immediately contact employees (server support technicians) crucial to the restoration process. A contact list (see Appendix C) will be maintained to ensure timely communication.
- 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 technicians responsible for various BOCES locations(Appendix C)
  - Obtaining most recent backups from the BOCES District Office
  - 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

    Mandarin
    (800) 426-7477 Toll-free
    (561) 995-4010 Local

    Dell Support
    800-915-3355

    PowerMediaPlus
    1-800-323-9084

    United Streaming Discovery Education
    Kristen Olsen Kristen_Olson@discovery.com
    301-272-2757
- Restoration of Applications and Data will be completed in the following order:
  - Restoration of OPALS
  - Restoration of Medianet
  - Restoration of user data (e.g. memos, letters)
  - Restoration of Mandarin
  - Restoration of Media Files (United Streaming, PowerMedia Plus etc)

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).

SchoolTool is the student information system used by the CTE centers. All student information is housed off-site at the NERIC in Albany. The contact information for SchoolTool:

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

Disaster Recovery Site

SLLBOCES is currently in the process of moving the DR site from the Washington Ed building (This building is to be sold) to the new DR site located at the Massena School Central Administration Building 84 Nightengale Ave Massena, NY 13662. This move will be completed by the end of 2014 – 2015 School year. This site is intended as a continuous, hot site for automated Failover and Recovery.

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, etc.

Responsibilities:

- Disaster Recovery Team –
- Craig Lalonde – Team Leader IT Supervisor
- Lori Remington - Network
- Brian Remington - Server
- Patti Morrow - Server
- Darin McHenry – LRC Support
- Coal Campbell – Help Desk
- Mike Allen – Remote location onsite Manager

Recovery Facilities:

- Fully Redundant Server Room
- Fully Redundant Servers and Data Storage
- Fully Redundant Network
- Voice and Internet connectivity
- Office Space

- 24 X 7 Access

Disaster Declaration:

- Identification
- Assessment
- Declaration
- Activation of DR Site
-

Restoration of Applications and Data will be completed in the following order:

  - Restoration of Financial system and Data
  - Restoration of Medical Plan system and Data
  - Restoration of Active Directory
  - Restoration of Application
  - Restoration of User Files
  - Restoration of Phone PRI(s) – Will take place at NWT.
  - DL - NERIC
  - VoIP - NWT
  - Access Control - NWT
  - Video - NWT

Communication:

- Employees
- Clients
- Vendors – Verizon/WLT/IBM/VMWare
- Authorities (If Needed)

Hardware and Software:

- IBM H22 Blade Center
- Zerto Replication Software
- VMWare

Maintenance and Support:

- IBM Monday – Friday 5 X 7

Phone 80-426-7378

- Zerto 24 X 7 Phone and E-Mail support, 1 response
  27-43 Wormwood Street
  Suite 530
  Boston, MA 02210
  www.zerto.com
  Phone 617-993-6331
  Fax: 617-209-4419
- VMWare Monday –Friday 5 X 7
  Phone 877-486-9273

Testing:

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

Contact:

- Appendix C

Appendix A - Network Diagrams

Network Diagrams are located on the following five pages.
(These are located in a separate PDF file)

Appendix B - Recovery Testing Record

Date	Location	Files Tested	Results	Signature

Appendix C - Emergency Contacts

Home and cell numbers listed below are ONLY to be used in the event of an emergency!

Appendix D - Policies

Policies:

- BOCES Personnel Use of Computerized Information Resources (5260) (Date: 2002)
- BOCES Student Use of Computerized Information Resources (6214) (Date: 2002)