Cassadaga Valley Central School Information Technology Disaster Recovery Plan 2015

Risk Assessment

Level	Descriptor	Example detail description
1	Rare	May occur only in exceptional circumstances
2	Unlikely	Could occur at some time
3	Possible	Might occur at some time
4	Likely	Will probably occur in most circumstances
5	Almost certain	Is expected to occur in most circumstances

Qualitative measures of consequence/ impact*

Level	Descriptor	Example detail description
1	Insignificant	No loss of data, systems running normal
2	Minor	Some applications need to be reinstalled, data is intact.
3	Moderate	Some data corruption or data loss
4	Major	Extensive corruption or compromise of security
5	Catastrophic	Total loss of data and hardware, compromise of security

Qualitative risk analysis matrix – level of risk*

Likelihood	***Consequences***				
	1 Insignificant	**2 Minor**	**3 Moderate**	**4 Major**	**5 Catastrophic**
1 (Rare)	Low	Low	Medium	High	High
2 (Unlikely)	Low	Low	Medium	High	Extreme
3 (Moderate)	Low	Medium	High	Extreme	Extreme
4 (Likely)	Medium	High	High	Extreme	Extreme
5 (Almost certain)	High	High	Extreme	Extreme	Extreme

Risk Identification

1. Some of the data is corrupted
2. Some data is lost and some is corrupted
3. Data is lost and hardware is damaged
4. Security is compromised
5. Data is lost and security is compromised

Risk Quantification (1= low, 5= extreme)

Risk type	Likelihood	Consequences	Overall rating
Data Corruption	(1) Systems have been stable historically	(1) initial financial outlay minimal	Low
Data Loss	(2) Major system changes occur	(3) requires data retrieval from backups	Medium
Data Loss – Hardware Loss	(1) Servers are protected and hardware has an average life of 6 years. Backups are run daily.	(4) interruption of system processes and the necessity of replacement hardware	High
Security Compromised	(1) Servers run antivirus and are patched with latest windows updates	(5) costly in terms of public confidence and possible confidential data misused	Extreme
Data Loss – Security Compromised	(1) Servers are protected and hardware has an average life of 6 years. Backups are run daily.	(5) costly in terms of public confidence and possible confidential data misused	Extreme
Network Offline	(1) Servers are connected to a WAN with fibre provided by Time Warner	(3) may require some data retrieval	Medium

Risk Treatment

The district takes many approaches to reduce the likelihood of data loss or the breach of security.

The district uses router and firewall services supplied by the WNYRIC to prevent probing on various ports. The firewall is currently housed inside the district and is on a UPS system. The firewall ports are managed by the WAN support from the WNYRIC with input and review by the Technology Coordinator.

The use of a World-Wide-Web content filter is used to prevent malware and spyware from entering from harmful sites. The district uses 8e6 technologies to filter all district computers that are connected to the Internet.

Client machines are loaded with anti-spyware software.

Servers have antivirus to detect malware and viruses. Servers have Clamwin AV on them and receive automatic updates. The spamfilter/gateway has AVG AV on it to prevent viruses from infecting the email gateway.

A Windows update server has been built to allow for reporting of Microsoft Windows Patches and Service Packs on all Windows XP client machines.

Uninterrupted power supplies are on the servers to give 30-45 minutes of battery backup.

The district uses a combination email gateway/spam filter to reduce spam, malware, and viruses from entering the wide area network. LogSat Software is the spam filtering software that the district uses. The district does not allow email from countries outside of the United States. The filtering software permits white lists and black lists to be created.

Offsite backups are performed nightly to disk. Business application server, Library, and Special Education server is backed up to the WNYRIC every evening. Student Management data is backed up from the server room in the HS to the Cassadaga Elementary Building nightly.

Recovery

Data Corruption/Loss	-	use Volume Shadow Copies for quick retrieval Retrieve file from backup server Reload application if necessary
Security Breached	-	Contact WNYRIC and ask them to check activity logs Determine the files and ports responsible Take server offline and run Antivirus/anti malware tools Contact WNYRIC and ask them to check activity logs Notify the District Superintendent of the violation
Hardware Failure	-	Troubleshoot and determine the point of failure Replace the hardware that has failed If a hard disk has failed run recovery tools
Network Failure	-	Contact WNYRIC if the problem appears to be Internet Contact Time Warner if the HS is online but Elementary schools are offline. Be prepared to retrieve data from backups

Revised 4/3/2009