

DATA PROTECTION GUIDELINES:

When it comes to data loss protection, there simply are no guarantees – however, you can significantly minimize your risk by following some or all of the suggestions listed below.

MAINTENANCE AND ENVIRONMENT:

There are many ways to minimize data loss, ranging from the manner in which you maintain your computer equipment to where you actually store your backup media.

Suggestions included in this checklist will increase the service life of your equipment and reduce the chance or frequency of general hardware/software failures:

- **DO NOT MOVE ANY EQUIPMENT WHILE IT IS POWERED ON!**
- Avoid exposing your equipment or media to static electricity or magnetic items in any form.
- Run scandisk, error-checking and defrag utilities regularly.
- Keep all virus and malware/spyware software up-to-date and scan frequently.
- Frequently scan flash drives, CDs, DVDs, external hard drives and other external storage media for viruses and malware.
- Never perform significant hardware or software upgrades without having a complete backup of all your data.
- Create backup CDs of all critical installation CDs and write installation codes on the label side of each CD.
- CDs do not last forever! Cheap CDs may last from 5-10 years if handled and stored correctly – more expensive CDs with 50-100 year life spans are available, but can just as easily be damaged. For these reasons, you should reburn your CDs and dispose of old CDs every 3-5 years and/or make sure the same data is stored on your hard drives. No media is 100% reliable.
- Print all user passwords, encryption codes, etc and store in a safe place or in a fire safe with restricted access.
- Store all of your installation CDs in a CD case and in one location. Store all of your backup CDs in a CD case and in an offsite location.
- Invest in backup power supplies for any equipment you want to protect from violent power spikes or surges – make sure they have ports for network and phone connections.
- Provide adequate space around your equipment for proper air flow and circulation.
- Extreme fluctuations in temperatures: When introducing cold electronic devices to warmer temperatures, give the device enough time to acclimate to the warmer temperature before connecting or powering up that device.
- Heat: Operation of electronic components in temperatures of more than 70 degrees will shorten the service life of those components. Keep your equipment away from sunlight or heat exposure of any kind.
- Moisture: Keep your equipment away from moisture or condensation of any kind.
- Vibration: Keep your equipment away from other equipment that moves or vibrates in any way. Do not move your equipment (especially hard drives) while they are powered on.
- Elements: Keep your equipment away from windows, drafts, heaters, smoke, steam and other elements that can cause or contribute to eventual or progressive failure.
- **IF YOU HEAR UNUSUAL NOISES OR DETECT UNUSUAL ODORS, TURN OFF ALL EQUIPMENT IMMEDIATELY, AND CALL US AT 970.209.3967.**

REASONABLE PROTECTION:

Suggestions included in this checklist will provide you with a reasonable level of protection from data loss:

- Develop, implement and test a “Data Loss Contingency Plan”.
- Implement the use of security passwords and data encryption utilities whenever possible.
- Establish mid-day, daily, weekly, and monthly backup routines that include 1) multiple mirrored, cloned or raid internal hard drives, 2) alternating off-site external backup drives, 3) DVD/CD copies and/or, 4) tape drives and/or, 5) online remote data backups.
- Verify and test your backups regularly – in other words, simulate a full restoration of the data from one or all of your backup routines and verify that the restored data is current and accessible.
- Run “data integrity” tests of your proprietary databases – vendors of most proprietary applications will provide a utility to check the integrity of your data. Try to run those at least once a month – weekly, if possible.
- Install internal thermostats in your most critical workstations and servers and configure them to send automated alerts when the operating temperature exceeds 70 degrees Fahrenheit. If safe operating temperatures cannot be easily maintained, install more cooling devices or move the equipment to a cooler part of your building.
- Laptops should always have CMOS passwords, user passwords and the most sensitive data should be encrypted. Data should be backed up to 1) an external hard drive, 2) CD/DVD copies, 3) usb flash drives and/or 4) a remote server – daily!
REMEMBER – DATA ON A LAPTOP IS FAR MORE LIKELY TO BE LOST, CORRUPTED OR STOLEN THAN ON A DESKTOP PC!
- Give serious thought to the consequences of leaving your alternating backups in the hands of employees. Those backups usually include “sensitive” information and nobody cares as much about company data as the owners do.

SUPPLEMENTAL PROTECTION:

Suggestions included in this supplemental checklist will further reduce your risk during the most extreme data loss situations:

- Perform daily restore tests of all backup routines.
- ALWAYS scan flash drives, CDs, DVDs, external hard drives and other external storage media for viruses and malware.
- Encrypt all working and backup data with a variety of encryption keys – restrict access to all encryption keys.
- Install an auxiliary server and/or workstation ready and waiting at all times in the event your primary systems fail.
- Bolt or tether your most critical workstations and/or servers to the ground or a wall to reduce chances of theft.
- Setup the most critical workstations and/or servers in a climate controlled room with restricted access.
- Install and regularly test the operation of a gas-powered generator that will provide 7 to 30 days of auxiliary power in the event of a disaster.
- Conduct frequent or annual disaster preparedness simulations to identify any weaknesses in your data loss contingency plan.
- Print everything and store hard copies in fire/water proof facilities with restricted access.

BACKUP DEVICE ADVANTAGES:

Internal hard drives – lowest cost per MB; fast; most reliable;

External hard drives – lowest cost per MB; fast; reliable;

Internal tape drives – very portable; good alternative or “Plan B”

External tape drives – very portable; good alternative or “Plan B”

Internal DAT or disk cartridge drives – very portable; good supplement or “Plan B”

External DAT or disk cartridge drives – very portable; good supplement or “Plan B”

USB Thumb/Flash/Zip drives – very portable; fast;

Online remote server storage – offsite; good supplement;

BACKUP DEVICE DISADVANTAGES:

Internal hard drives – none worth noting;

External hard drives – fairly easy to damage in transit;

Internal tape drives – slow; easily damaged or corrupted in transit; tapes stretch; extremely sensitive to heat and static; extremely slow recovery; tedious sorting process; can get very expensive;

External tape drives – slow; easily damaged or corrupted in transit; tapes stretch; extremely sensitive to heat and static; extremely slow recovery; tedious sorting process; can get very expensive;

Internal DAT or disk cartridge drives – slow, easily damaged or corrupted in transit;

External DAT or disk cartridge drives – slower, easily damaged or corrupted in transit;

USB Thumb/Flash/Zip drives – very limited capacity; highest cost per MB; easily overwritten or corrupted;

Online remote server storage – very slow and can be expensive over time; potential for corruption during transfer in either direction;

INDUSTRY STATISTICS:

- Despite spending millions for enhanced security, redundant backups, highly skilled technicians and climate controlled facilities – British Governmental Agencies still managed to lose tens of thousands of private records when a “flash drive” mysteriously vanished from the premises.
- The average service life of a computer hard drive is 4 years. External hard drives and laptop hard drives have a much shorter service life than desktop pc hard drives.
- Microsoft claims that 5% of Windows computers experience some type of crash an average of twice per day. Most go undetected and behind the scenes until the culmination of these crashes overwhelms the operating system causing application and/or data corruption.
- Approximately 30% of all PC users have lost most or all of their critical data at one point in their life time.
- Approximately 93% of the companies that were without their most critical data for ten days or more during a disaster filed for bankruptcy within that same year. Approximately 50% of those same companies had filed for bankruptcy immediately after the disaster.
- Elevations of 10,000 feet or more increase the risk of hard drive failure and data loss.
- Approximately 5% of all desktop pcs purchased during the last 3 years will crash within the first year and 12% within four years. Approximately 15% of all laptops will crash within the first year and 22% within four years.

Ask us how we can help make sure that your office is HIPAA compliant?

Questions? Please call Marcum at 970.209.3967 or email info@970data.com or visit www.970data.com

MDPRSrev120908