



A Computer and Data Safety Plan for Municipal Offices in Vermont

[09-13-02 UPDATE]

Available online at
<http://crs.uvm.edu/municipal/erm/cdsp.htm>

A Computer and Data Safety Plan for Municipal Offices in Vermont

[09-13-02 UPDATE]

A working document first conceived by the
Vermont Electronic Records Management Working Group
in the summer of 2002.

Currently maintained and updated by the UVM Center for Rural Studies,
under the guidance of the Working Group.

Please check <http://crs.uvm.edu/municipal/erm> for more information and
future updates.

Available online at
<http://crs.uvm.edu/municipal/erm/cdsp.htm>



HOW TO USE THIS DOCUMENT

This Computer and Data Safety Plan for Vermont Municipalities was first conceived by the Vermont Electronic Records Management Working Group¹ in the summer of 2002 and is currently maintained and updated by the Center for Rural Studies², under the guidance of the Working Group. This is meant to be a dynamic working document that can keep up with changes in technology and its use in Vermont's many municipal governments. Please check <http://crs.uvm.edu/municipal/erm> to stay apprised of updates to this plan, as well as the continuing dialogue on electronic records management in Vermont. In addition, please feel free to share your comments with the Center for Rural Studies and the Working Group.

This document is not meant to act as your municipality's computer and data safety policy. Rather this is meant to be a plan to follow when drafting your town's policy. Every town in Vermont is unique, with different resources and needs. Additionally, Vermont's towns create and use electronic records to varying different degrees. Therefore the Electronic Records Management Working Group has outlined the basic considerations that we believe towns should account for when drafting their disaster management protocols, including:

DESIGNATION OF A COMPUTER AND DATA SAFETY COORDINATOR

An important first step. The entire municipal office will benefit from the designation of one person with the job of ensuring proper computer and data safety. This coordinating position could be responsible for writing and updating the town's disaster management protocols, overseeing preventative measures, coordinating the recovery options, and – most importantly – maintaining staff awareness and training. This plan doesn't necessarily advocate the designation of a whole new staff position, just some new duties for an existing staff-member.

IMPLEMENTATION OF PREVENTATIVE MEASURES

Essentially, there are two components to effective computer and data safety in the municipal office. The first piece is prevention. In order prevent lost, stolen, or damaged data, town officers should be aware of the *digital media* that their electronic records and information are kept on, be aware of the *physical space* where their I.T. hardware is located, implement proper *power source* management, and put effective *data migration* and *security* strategies into play.

DISASTER RECOVERY MEASURES

Prevention is important, but it is only half the battle. The other half is essentially focused upon two little words hyphenated together: *back-ups*. Municipal officers may find that performing back-ups, storing back-ups, and just determining what should be backed up in the first place, can be a little more complicated – and important – than one would think.

OTHER SECTIONS in this plan include a collection of additional tips and a glossary of some of the more obscure information technology terms presented in the document. Terms followed with a "9" are included in the glossary.

¹ Please see Appendix C for more information on the membership and activities of the Electronic Records Management Working Group

² A nonprofit service department of the University of Vermont. Contact: crs@uvm.edu, (802) 656-3021



SECTION 1.

DESIGNATION OF A COMPUTER AND DATA SAFETY COORDINATOR

The municipal office should designate one staff member as the person responsible for disaster recovery and for the implementation of preventative measures. The Coordinator's duties should include:

WRITE, UPDATE, AND FOLLOW THE TOWN'S COMPUTER AND DATA SAFETY POLICY. All municipal office protocols and procedures concerning computer and data safety should be documented and updated immediately whenever changes are mandated. The reason for this documentation is twofold: (1) to eliminate any ambiguity or confusion concerning the procedures for disaster management in the town office and (2) to provide guidance and institutional memory to other office staff in the event that the Coordinator is unable to perform his/her duties.

In addition, official copies of the municipality's Computer and data safety policy should be made. It is suggested that one copy is kept in the town vault and another kept somewhere off-site so that the loss of one copy will not leave the municipal office without written instructions for maintaining disaster management procedures. New copies should be made every time the municipality's disaster management policy is updated.

OVERSEE PREVENTATIVE MEASURES. Precautions for the prevention of I.T. disaster and damage are listed in the next section. It is the duty of the Coordinator to verify that the necessary steps have been taken to ensure that municipal information is not lost, corrupted⁹, or stolen due to power surges, water damage, physical deterioration of storage media⁹, unauthorized operator intrusion, and so forth.

COORDINATE BACK-UPS AND COPIES. If the corruption or loss of municipal information does occur, properly followed back-up procedures will ensure that the situation can be remedied. It is the duty of the Coordinator to coordinate back-up⁹ procedures in the municipal office and the storage of copies offsite.

MAINTAIN STAFF AWARENESS AND TRAINING. It does a municipal office no good to have only one person who is aware of the necessary disaster management procedures. The Coordinator should make sure that the entire office staff and new staff are aware of the existence of the municipality's disaster management policy. Some office staff should be trained in the necessary procedures so that there is redundancy in case the Coordinator can't fulfill his/her duties.



SECTION 2. IMPLEMENTATION OF PREVENTATIVE MEASURES

Your municipal office's computer and data safety policy should address the advantages and disadvantages of the media being used to store the electronic records, the space where the media are kept, precautions to prevent damage from power surges and water, and the security of the information being stored.

DIGITAL MEDIA are the defining feature that sets electronic records apart from other forms of municipal information. Special computer hardware⁹ and software⁹ is required in order to read electronic records. Included in the hardware category are various types of digital media, each with their own inherent advantages and disadvantages. Consider the following explanation provided by the Minnesota State Archives Department:

Your electronic records are digital data that are stored on digital media. Digital data exists, at its most basic level, as just 0 and 1, or on and off. For example, black and white photographs in the newspaper are printed as a series of either black or white dots (0 or 1, on or off). The complex organization of a large number of dots allows the human eye to complete the image. The digital data in an electronic record uses the same principle to organize digital data into the record to make the record readable. A bit (short for binary digit) is the smallest unit of data in a computer. A bit has a single binary value, either 0 or 1. Digital data is stored on digital media. Digital media are divided into two types:

Magnetic. On magnetic media, the digital data is encoded as microscopic magnetized needles on the surface of the medium (e.g., disk or tape).

Optical. On optical media, the digital data is encoded by creating microscopic holes in the surface of the medium (e.g., compact disc).³

From a disaster prevention standpoint, some would say that optical media (e.g. compact discs) are safer places to put municipal information because the information stored there cannot be erased by an opposing magnetic field⁹ or the electro-magnetic pulse⁹ produced by a power surge. However magnetic media (e.g. floppy disks and hard drives) are more versatile and can be reused – i.e. new information can be added on or written over⁹ old data. Most CD's can only be written to once or twice and are very appropriate for copies of data that can't be overwritten are desired. This is a decision that your municipality must make when considering how much information needs to be stored, and how important it is.

THE PHYSICAL SPACE where electronic records are stored and accessed must also be designed and organized in certain ways in order to maximize safety from physical threats. Computers, servers⁹, and back-up storage media should be kept in dry, well-

³ Minnesota State Archives Department, Minnesota Historical Society. March 2002. *Electronic Records Management Guidelines: "Digital Media."* <http://www.mnhs.org/preserve/records/electronicrecords/erdigital.pdf>



ventilated areas. All equipment should be kept away from windows and walls containing water pipes in order to minimizing damage from leaks. Efforts should be made not to keep equipment under areas of the ceiling containing pipes as well. A burst pipe during a cold Vermont winter could do a lot of hardware damage.

Ample space should be provided around important I.T. equipment. Cramped quarters result in bumped and toppled computers and servers, seriously harming the components within. Along these lines, such equipment should also be placed securely on even, sturdy surfaces. Loose wires can be snagged and should be neatly organized and tucked out of the way.

POWER SOURCES and all other connections to computers and servers should be managed to minimize potential damage. Power surges can damage the information on computers and servers by overwhelming their power management devices and causing damaging shorts and electro-magnetic fields that wipe out data. Power outages and brownouts⁹ can also cause damage by disrupting routine maintenance activities that ensure the integrity of stored data. Computers, servers, and other electrical equipment that process your municipality's electronic records should be isolated from potential power fluctuations. Surge protectors⁹ are very common and somewhat effective against power surges, but uninterruptible power sources⁹ (UPS) provide better overall protection. A UPS stores electricity for use during a power outage and will also divert power surges in an effort to maintain a consistent feed of electricity to your equipment.

In fact, any and all physical inputs and outputs to your equipment can be potential vehicles for power surges. For instance, excess electricity can run into your computer through the phone or network jack if lightning strikes the outside lines. This can cause damage even when the computer is turned off and the power supply is hooked up to a surge protector. There are surge protectors that can be applied to phone and network⁹ lines, and it is suggested that your municipal office explores these options.

| |
|--|
| <p>Note: in the event of an electrical surge, all surge protectors should be checked and replaced if necessary.</p> |
|--|

DATA MIGRATION is another consideration for your municipal computer and data safety policy. Eventually the equipment you use for processing, accessing, and storing electronic records will break down, resulting in information damage. Hard drives⁹ in computers and servers will eventually suffer mechanical failure, resulting in total loss of data. Floppy disks can become moldy in time. CD's are known to warp. Many of these problems can be delayed if media are properly stored and taken care of, but the effects of time are inevitable. Media can also become obsolete, a problem which will become most apparent if one needs to access data from a source that computers are no longer designed to access. Steps must be taken to make sure that your municipality's electronic records can be moved to new media before problems or obsolescence occur and retention schedules are violated.



Plans should be made to address data migration every 2-4 years (e.g. the purchase of a new computer or server or the transfer of data to a new type of storage medium, if available). It is necessary to ensure that the various hardware and software you use to store and access your data will be compatible with future versions, in order to make migration possible. One suggestion is to stay away from excessively proprietary⁹ hardware and software. More “open” hardware and software will have a higher probability of compatibility with advances from other companies, if such a change becomes necessary. Consult your hardware or software vendor on what their products can offer you for compatibility down the line. Getting a “second opinion” from another source familiar with the hardware or software in question is also a wise idea.

DATA SECURITY is a consideration with a focus on a more intentional and insidious form of I.T. disaster: information vandalism and theft. Your municipality should address steps to curtail unauthorized attempts to access electronic records. These attempts can come in many different forms from many different avenues. The sensitivity of the information and the manner(s) in which it is stored and accessed will affect the extensiveness of the security precautions needed. Here are a few common tips.

Control and limit access to all equipment and storage media. There will probably be some information and processes that only authorized municipal officials should be privy to. Assess the situation and take the necessary precautions. Passwords are one common way to ensure proper access to town information. Access to email, computer and server administration, the municipal website, and any particular directories containing sensitive information (e.g. the grand list) should be governed by passwords. Here are some general rules for passwords:

1. Do not choose an obvious password—for instance your first or last name or the name of anyone close to you and birthdays or other significant dates.
2. Do not use the same letter more than once in any password. That would make it easier to crack.
3. Utilize your full alphanumeric options—use letters and numbers AND symbols like “&” if possible.
4. Use long passwords—at least 8 characters long. This makes them harder to crack.
5. Do not write your password down. It could get misplaced and/or stolen. It may be appropriate to write down hints to help you remember, but these should not be left on your desk or anywhere else in your office.
6. Change all office passwords regularly (monthly or quarterly, depending on the sensitivity of the information they are guarding).



Nevertheless, passwords can sometimes be subverted, and threats are not always standing there in the municipal office with you. Computers and servers can also be accessed remotely through network lines, either by hackers or by viruses. If your computer were on a network, it would be a good idea to turn all file sharing off if those services are not used regularly. If your municipal server contains any sensitive information, you should invest in a firewall⁹ program that adds another “layer” between your network line and the outside world.

[A firewall] is a form of Internet security that stands between a private network and the Internet. It is like a wall in that it can prevent unwanted traffic from passing either way⁴.

Be sure to seek advice when choosing and setting up a firewall program. And be ready for an increase in blocked attempts to get into your server. A new firewall may attract more hackers seeking a challenge.

Computer viruses⁹ are also a common way in which information is corrupted or lost, often by using the computer against itself. Most viruses simply try to overload your server with simple requests (such as sending an email to everyone in your address directory), while some more insidious specimens operate with the objective to delete or corrupt important files and drivers on your system, rendering it useless. Variations on the theme include “back doors⁹” and “Trojan horses⁹” that attempt to achieve unwanted access and use of your computer or server. Either way, viruses are an unwelcome intrusion with malicious intent. Anti-virus programs act as the primary line of defense by scanning your computer and monitoring emails and downloads for viruses trying to get in. McAfee and Symantec are two companies that make anti-virus programs commonly used in computers today. Once your office has purchased and installed an anti-virus program, there are a few steps that should be followed:

1. Most anti-virus programs offer online downloads of new virus files that keep it up to date. Make sure to perform these “live updates” regularly, either manually or by performing a scheduling function.
2. When you receive unsolicited virus warnings over email, always check the website of your anti-virus company first. They keep track of new viruses, and they also have information on common virus hoaxes. Most virus warnings are really hoaxes trying to trick you into deleting important files yourself.
3. Even with the anti-virus program installed, your best defense is shrewd email and download management. Most email programs are set up to preview emails as soon as you click on them with the mouse. This action can trigger a virus that hasn’t been caught yet. Never open unsolicited or suspicious email. If you receive an email that you know to be a virus, shut down your email program and scan your computer with the anti-virus program.

⁴ Geek.com. 2002. *Technical Glossary*. <http://www.geek.com/glossary>



CHAPTER 3. DISASTER RECOVERY MEASURES

The implementation of preventative measures will significantly decrease your town office's chances for an incident of information loss or corruption; however your municipal computer and data safety policy must also provide contingencies just in case an accident or attack does occur. Your office should have protocols in place that allow for recovery from disaster, primarily through the replacement of lost, stolen or corrupted files with copies of the files that were backed up beforehand. No matter how much information your town has in electronic format, how sensitive it is, or how it is made available to the public, your municipal office needs a plan in place to routinely back-up the data and keep the copies in a safe place.

WHAT TO BACK UP. The first requirement for backing up your town's electronic records and information is to document what they are and where they exist on the computer or server. The office's Computer and Data Safety Coordinator or another appointed person should keep track of the nature and location of files that need to be backed up, and this information should also be noted in the town's computer and data safety policy. The highest priority data to be backed up would be the pieces of information that also qualify as public records and fall under retention schedules. An electronic public record can be anything from an email message to a digitized land record. It is suggested that files that need to be backed up are kept in the same general folder or directory on the particular computer or server.

Note: backed up data is not a substitute for archived data. A back-up is meant to be stored and used for recovery and recovery only. It cannot replicate the accessibility that is required for archives, nor fulfill the legal obligations. In fact, your electronic archives are precisely what you should be backing up.

HOW TO PERFORM THE BACK-UP. Basically there are two ways to back up data, and the decision to use either method normally depends on the number, size, and diversity of the files in question. A few files located in the same computer directly could easily be backed up manually, while an entire server full of files is best handled by a program written specifically for creating back-ups. The end results can be very different. Manual back-ups can take time, but if a file is lost, the copy can easily be transferred from its storage space back into the original location. Back up programs, on the other hand, copy everything quickly and automatically, but they normally compress all of the copies so that they take up as little storage space as possible. Those files need to be decompressed by the program to be put back into use, which lengthens the recovery process. When deciding whether to create back-ups manually or with special software your town should also take into account the fact that Vermont towns are collecting more and more electronic records every year, and the use of automatic back-up programs could be an inevitability.



See Appendix B. for instructions on how to set up an easy, rudimentary back-up program by writing a simple batch file.

Your town will also need to consider what type of media to store the backed up data on. Recordable CD's are an option for smaller back-ups, while magnetic tapes that hold many gigabytes of data are a necessity for larger jobs. Different back-up software packages use different types of media too. The inherent advantages and disadvantages of different digital media types should also be a consideration.

HOW OFTEN FILES SHOULD BE BACKED UP. Municipal data should be backed up weekly, but your town could decide on schedules with more or less frequency for different types of data depending on the importance of the information, how often it is used, how often it is updated, and whether or not the originals exist on paper in the vault or another location. Some back-up programs will allow you to create full back-ups as well as incremental back-ups that take less time to perform. With that feature, it would be possible to create a weekly full back-up complemented by daily incremental back-ups.

HOW MANY COPIES SHOULD BE MADE. The number of copies that are made during the back-up procedure is a decision that your town should make depending on the importance of the data, and the quality of the storage medium. Paper copies are also a possibility; especially while laws still exist that maintain paper as the default for public records in municipal government. For instance, paper copies could be made of all emails that qualify for public record and could be kept in the town vault. The more ways in which municipal information is copied and stored, the more options your office will have for recovery in the event of a disaster.

STORING THE BACK-UPS. The necessity for off-site storage of backed up data cannot be emphasized enough in this document. The foolhardiness of keeping back-up media on top of the computer or server that contains the original data is obvious: one fire or water leak could wipe out both the originals and the copies. The ideal situation would be to keep back-ups in a safe place in a separate building, preferably under the care of town employees. The town vault is another possibility, but temperatures reached within a vault during a fire could possibly damage many types of storage media. It also goes without saying that your town should avoid storing back-ups on a floodplain.

In addition, some back-ups should be stored indefinitely, ideally a monthly or yearly copy. Older back-ups have the advantage of not being subject to file corruption that can occur over time. If a town office reuses all back-up media again and again, then an undetected file corruption would be allowed to proliferate throughout all of the existing copies. This could put your office in quite a bind if it needs to replace a file that only exists in a corrupt form on all of the back-ups. An untouched back-up from a previous



year would come in very handy in that situation. It is especially imperative that these permanent monthly or yearly back-ups are kept off-site.

Note: one way to ensure that your server vendor is keeping back-ups offsite is to require them to send you back-up tapes or discs periodically. However, you will need to be able to provide proper storage. You will also need to consider the risks involved with sending potentially sensitive information through the mail or by courier.

An effective way to make sure that your files and back-up media aren't corrupt is to randomly test them. Schedule a weekly exercise in which you use the back-up media to recover one or two files chosen at random. If the operation goes smoothly, you can be relatively sure that your back-up is in good shape. However, it is recommended that you perform these random recoveries in a test directory, rather than overwriting the files on your computer or server. If corruption is found, you will need to determine whether it exists in the original files or just on the back-ups. Hopefully it will simply be a matter of discarding a corrupt back-up medium.

THE IDEAL BACK-UP SITUATION. There are many limiting factors to how sophisticated a municipal government's back-up policy can be, the two largest factors being time and money. Nevertheless electronic records are becoming more prevalent in Vermont's town government, and an impending priority shift could free up more resources for proper and effective disaster management measures. An example of an ideal back-up plan for a town server would be:

1. The purchase of back-up and recovery software that puts copies of files onto digital tape cartridges or other appropriate media and can be scheduled to run specified back-up procedures on specified files at specified times.
2. *Daily*: incremental⁹ back-ups are performed. These tapes are stored in the server room to allow for quick file recovery when needed. These tapes are reused weekly on their assigned day.
3. *Weekly*: full back-ups are performed and stored in the town vault. These tapes can be reused weekly, except for those from the first week of each month, which are kept for one year and then reused. Once a week, a random recovery should be performed on one or two files, to be sure that the back-up media and files are not corrupt.
4. *Monthly*: full back-ups are performed. Two copies are made. One set of copies is kept in the town vault. These tapes are reused each year. The other set is kept offsite in a town facility and is only brought back to be reused after two years.
5. *Yearly*: full back-ups are performed. Two copies are made. One set of copies is kept in the town vault. These tapes are reused every two years. The other set is kept offsite in a town facility and is *never* reused.



IN THE EVENT OF A DISASTER... There is little that this plan can do to guide you through the exact recovery steps needed after data is lost or corrupted. Every town will have its own unique situation, equipment, facilities, programs, etc. First of all, whatever your situation may be, it is necessary that all recovery procedures be documented in detail in your town's computer and data safety protocols so that they may be followed correctly, whether or not the Computer and Data Safety Coordinator is present.

In general, recovery of a file may be as simple as replacing it with the most recent copy from back-up. In the case of more sophisticated back-up programs, the software may ask you to insert the most recent full back-up, choose the file or directory that needs to be recovered, and begin the process. Often any incremental back-ups that have been performed after the full back-up will need to be inserted in order to account for any changes to the file over time.



SECTION 4. ONE MORE THING...

It can safely be said that the biggest obstacle standing between Vermont's municipalities and the successful implementation of all of the suggestions in this plan is a current lack of resources, primarily money and staff. Unfortunately a shift in municipal resource priorities will probably be along time coming. In the meantime, there are a few things that you can do to make computer and data safety in your municipality a little easier:

DEALING WITH VENDORS

Many towns contract with vendors for various municipal I.T. activities. One common example is the use of a vendor's server to store municipal information and make it available to the public via an official town website. Typically in this case, the vendor takes on many of the disaster management responsibilities. Nevertheless it is suggested that towns make no assumptions and take nothing for granted in vendor negotiations. The disaster management considerations in this document should be applied to a vendor contract just as they would be applied to a municipal disaster management policy. It is in the town's interest to make sure that the vendor is taking the precautions worthy of the importance of the municipal information that they are taking into their care.

COORDINATION ACROSS TOWN DEPARTMENTS

Your Computer and data safety policy will be most effective if all of the departments and officers in your town share the resources, responsibilities, costs, and duties necessary for ensuring the safety of everyone's electronic information. There is no reason why your town's listers, clerk's office, planning office, public works department, police department, and fire department should each have their own disaster management policies and Computer and data safety Coordinators when it is possible to integrate data resources and responsibilities with today's information technology. You may want to use the formation of your policy as an excuse to bring everyone to the table to discuss I.T. use in your municipality. As the various officers and departments in your town begin to share databases, information, and the duties to keep them safe, you may find your use of time becoming much more efficient.

CONTINUING THE DIALOGUE

Logically, successfully implementing computer and data safety strategies is much more effective than talking about them. But the discussion must continue. It is especially important for towns to share their experiences – positive or negative – so that we all may profit together in the end. No one knows how to help a municipal officer better than another municipal officer. Trainings and workshops are a great place to share experiences. Those that have yet to subscribe to the MUNINET municipal official email listserv should check out <http://list.uvm.edu/archives/muninet.html> and give it a shot. The Electronic Records Management Working Group site at <http://crs.uvm.edu/municipal/erm> and the Vermont State Archives site at <http://vermont-archives.org/records/managing.html> are also good places to go for information.



SECTION 5. GLOSSARY OF I.T. TERMS

Back Door (virus) – actually a back door isn't a virus in of itself. Rather, it's a case of viruses trying to take advantage of back doors. A back door is a hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

Back-up – a copy of data that is made, which can then be recovered if the original data is lost, stolen, or damaged. In this document, back-up refers to both the backed up information as well as the media that the data is stored on.

Brownout – a reduction or cutback in electric power, especially as a result of a shortage, a mechanical failure, or overuse by consumers.

Compact Disc (CD) – a small optical disk on which data such as music, text, or graphic images are digitally encoded through a laser etching. In turn, CD's are also read by lasers.

Computer Virus – a program that makes unbidden copies of itself. Sometimes these copies are added on to executable files, and other times they are part of Word or Excel documents, called Macro Viruses. The virus will usually have some eventual effect on systems that are infected. Often, the intent of a virus is malicious. Sometimes the intent is not malicious, but due to the spreading of the virus, it becomes a malicious act. In this document, the word virus is used to represent the entire spectrum of automatic or directed intrusions into computer software, including worms, Trojan horses, crackers, etc.

Corrupt (files) – when a file that cannot be read by computer software because portions of the file's actual data code (1's and 0's) have been changed or removed in some way.

Electro-Magnetic Pulse – the pulse of intense electromagnetic radiation generated by certain physical events, e.g. the explosion of a power line transformer. This pulse can damage computer files by changing the data being kept on the magnetic disks inside.

Firewall – a form of internet security that stands between a private network and the Internet. It is like a wall in that it can prevent unwanted traffic from passing either way. Another good way to keep out computer viruses and the like.

Floppy Disk – this is any type of disk media which is not rigid. Often, it's contained in hard cases, which can lead to confusion in identification. Commonly, the term is used to describe 1.44MB 3.5 inch diskettes, but it applies to any media such as Zip disks, which are floppy in nature if removed from their casing.

Hard Drive – a device that physically stores data in your computer. Much like a floppy disk, but the system is closed and the disks are hard (usually metal, although some glass versions have been developed). The closed system gives the possibility of more



precision, so the drive is much faster and can hold much more data. Also called a hard disk drive.

Hardware – this refers to any physical pieces of a computer. For example, the computer itself, a monitor, a printer, memory, and a video card are all hardware. See also software.

Incremental Back-up – a type of back-up that saves time by only copying files that have been changed or added since the last full back-up was performed. Thus incremental back-ups still require the performance of periodic full back-ups.

Information Technology (I.T.) – applied computer systems, both hardware and software, and often including networking and telecommunications. This document uses information technology to include computer data and information as well.

Magnetic Field – a condition found in the region around a magnet or an electric current, characterized by the existence of a detectable magnetic force at every point in the region and by the existence of magnetic poles. A computer hard drive uses a magnetic field to keep all of the microscopic pins properly aligned, producing the 1's and 0's of digital code. However, an opposing magnetic field, can disrupt the pins' alignments.

Media (digital, storage, back-up, etc.) – the plural form of medium. In this document, medium would refer to any item that can physically carry computer code (i.e. data and information), magnetically, optically, or otherwise.

Network – this refers to a group of interconnected computers. The computers must be capable of transferring data to form a true network. This normally necessitates the connection of computers and servers with network lines, wires that are physically akin to phone lines.

Proprietary (computer software and formats) – designed and supported by a private individual or corporation under a trademark or patent. Proprietary qualities may raise the chance that software is not compatible for other systems or codes. In the language of computer hackers and users, proprietary implies a product not conforming to open-systems standards, and thus one that puts the customer at the mercy of a vendor who can inflate service and upgrade charges after the initial sale has locked the customer in.

Server – this refers to a machine whose sole purpose is to supply data, so that other machines can use it. This also describes any software process that runs on a server machine, and responds to client processes or programs locally, or across a network.

Software – the programs that run on computer hardware. This can include operating systems, office suites, games, and Web browsers. Software runs on hardware.

Surge Protector – A specialized electrical outlet that uses capacitors to keep spikes in the power supply from damaging electronic devices.

Trojan Horse (virus) – this describes a computer program that appears to be something useful, but then does something malicious to your computer. This could range from destroying data to laying dormant and someday hijacking your computer to be used as part of a denial of service attack. Anti-virus programs will protect you from known Trojan horses, but strictly speaking, Trojan horses are unlike viruses, as they do not replicate. However, combination virus / Trojan horses can replicate.



Uninterruptible Power Source (UPS) – this is a device that contains a battery and some circuitry to supply your computer with power for a limited time (depending on the battery) if there is any sort of interruption in the outlet power. Most also have features that allow them to absorb power surges as well.

Written Over (data) – data code that has been recoded into new data on its medium. Thus the old data is lost forever. (Unless there's a back-up, of course!)

GLOSSARY SOURCES:

Dictionary.com. 2002. <http://www.dictionary.com>

Geek.com. 2002. *Technical Glossary*. <http://www.geek.com/glossary>



APPENDIX A. COMPUTER AND DATA SAFETY CHECKLIST

The writers of this disaster management plan operate under no illusions that Vermont's municipalities have unlimited resources for the implementation of new information technology policies. It may help some towns to begin incorporating pieces of the plan until a full computer and data safety policy can be implemented over time. What follows is a checklist of various computer and data safety practices for towns that prefer the step-by-step approach.

- ✓ Integration between town officers and departments in order to share the resources and responsibilities required for adequate computer and data safety.
- ✓ Designation of the Computer and Data Safety Coordinator.
- ✓ Documentation and revision of computer and data safety protocols.
- ✓ Computer and data safety training for new staff.
- ✓ Regular computer and data safety training for all staff.
- ✓ Storage of computers and servers in safe areas, on sturdy surfaces, away from possible leaks.
- ✓ A data migration plan addressing compatibility of current programs and hardware with future advances.
- ✓ Protocols for creation of effective passwords and periodic changing of old passwords.
- ✓ Purchase and implementation of a firewall (if online).
- ✓ Purchase and implementation of anti-virus software for computers and servers.
- ✓ Regular performance of back-ups.
- ✓ Storage of (some) back-ups off-site.
- ✓ Designation of (some) back-up media to not be reused.
- ✓ Weekly performance of random back-up recovery tests.



APPENDIX B.

SETTING UP A BATCH FILE TO PERFORM A BACK-UP OPERATION

Courtesy of David Deutl, Information Systems Specialist at the University of Vermont

Note: while the following is a quick and easy way to systematically copy desired files to a different location, the user will still have to ensure that back-up media are stored properly and that monthly and yearly back-up data is not overwritten.

The rule of thumb protocol is to store all of your files in one primary directory, and organized within sub-directories. When this protocol is followed, you will only have to copy one directory and all of your data and documents will be carried along. I have used the analogy of having a packed suit case with everything you will need when you and your wife head out the door to have a baby. You do not want to go searching around for items in a panic, and you don't want or need the couch and kitchen sink. There are some files that can not be directed to be located in MY DOCUMENTS, but you will be able to identify these as exceptions, such as:

- Bookmarks/Favorites
- Address Book
- E-Mail

Once you have identified all of the files and directories that you want to back up, and where you want to copy them to, a simple batch file can automate the process.

The following batch file was created with NOTEPAD and 'saved as' backup.bat in the root directory (C:\backup.bat). It was made a shortcut on the Desktop by dragging it from WINDOWS EXPLORER using the right mouse button and 'create shortcut' when the mouse button was released.

Example:

```
xcopy C:\mydocu~1\*. * /s/d Z:\mybackup  
  
xcopy C:\progra~1\Netsca~1\user\bookmarks.htm /d Z:\mybackup\mail  
  
xcopy C:\progra~1\Qualcom\Eudora\*.toc /d Z:\mybackup\mail  
  
xcopy C:\progra~1\Qualcom\Eudora\*.mbx /d Z:\mybackup\mail  
  
xcopy C:\progra~1\Qualcom\Eudora\*.* /d Z:\mybackup\mail
```

What this batch file does: any time the desktop shortcut is double clicked, each line of the file is executed. XCOPY is an old DOS command that copies files and directories from one disk or storage media to another.



The first part of the command is the location of the files that you want to copy. DOS only recognizes 8.3 naming protocols and does not recognize long file names or spaces. 8.3 means 8 characters followed by a 3 digit extension assigned by the application that it was created in. **DO NOT USE THE LAST THREE CHARACTERS FOR YOUR OWN NAMING CONVENIENCE.** This is the primary cause for errors in opening files when emailed or transferred by floppy disks.

If the directory is more than eight characters (including spaces), use only the first six characters followed by a tilde (~) and the numeral one (1).

File names can be named individually (bookmarks.htm) or using wildcard characters (* = all characters, and ? = single character; *.* will copy all files in a directory, *.toc will copy all files with .toc as the extension)

The next part of the command has the switches that can control the operation. The first switch (/s) lets all of the subdirectories be copied along with all of the files in MY DOCUMENTS. This is one of the reasons that it is important to organize your files within sub-directories within MY DOCUMENTS. The second switch (/d) checks the date of the file and only copies new files or files that have been changed since the last time the batch file was run. Needless to say, the first time this batch file is run, it may take a relatively long time to copy all of the files, but each subsequent time it is run, it will finish the operation quickly.

The final portion of the command identifies the location that the files will be copied to - Z:

This batch file can be modified to copy files to a ZIP drive, network file server, or any writeable media that is recognized with a drive letter in WINDOWS EXPLORER or MY COMPUTER.



APPENDIX C.

THE VERMONT ELECTRONIC RECORDS MANAGEMENT WORKING GROUP

The Electronic Records Management Working Group was formed by the Center for Rural Studies in the summer of 2002 as part of a grant from the Vermont Historical Records Advisory Board. The goals of the grant are to provide education and training for those Vermont municipal officials and employees who are responsible for maintaining and preserving records in electronic format and to identify and create resources pertaining to electronic records management. The working group is made up of representatives from various Vermont municipalities as well as the Center for Rural Studies, the Vermont Municipal Clerks' and Treasurers' Association, the Vermont League of Cities and Towns, Vermont Public Records, and the Vermont Secretary of State's Office.

For more information on the working group and electronic records management in Vermont, contact Will Sawyer, Center for Rural Studies, at william.sawyer@uvm.edu or Gregory Sanford, State Archivist, at gstanford@sec.state.vt.us.

Visit <http://crs.uvm.edu/municipal/erm> and <http://vermont-archives.org/records/managing.html> for more information on municipal computer and data safety and electronic records management in Vermont and around the nation.