



**Animal Intelligence Software, Inc.**  
3505 NW Anderson Hill Road, suite 204  
Silverdale, Washington 98383  
(360) 692-7736 FAX (360) 692-2629

## ***Creating a backup strategy for your network***

October 4, 1999

### **Introduction**

Backup is an essential part of protecting your computer network and its data. Since data backup goes well beyond merely copying your **AI** or VSS data files, *Animal Intelligence Software, Inc.* considers backup a *system* process rather than an *application* process. This means that neither **AI** nor VSS contain any facilities for data backup; rather, you are expected to backup their data as part of a larger strategy to backup all of the data on your network.

This whitepaper describes one way of creating a reliable, verifiable backup system. There are many strategies and their ease of use and cost can vary greatly. Discuss this and other strategies with your network vendor to arrive with a strategy that will work for you and your business. By *work* we mean a system that is affordable to you, and that you will rigorously maintain. We must stress at the outset that the responsibility of creating and maintaining backups falls to you and your network vendor.

### **Why backup?**

Computers, like all mechanical devices, will eventually fail. A hard disk in a computer spins at between 3,600 and 7,200 revolutions per minute, and its read/write heads “fly” at less than four thousands of an inch above its surface. Over time, the mechanism of the drive will become worn and the drive will fail. When this happens, your data is gone. Professional data-recovery companies typically charge \$150 or more just to estimate the cost of recovering data from a failed drive, and the actual recovery costs often exceed \$1,000 – if the data can be recovered at all. If not, you are faced with starting over from scratch – a daunting, even more expensive task when you factor in the cost of data-entry by your staff or a paid data-entry service.

When compared with these numbers and the prospect of your computer system being “off-line” for days or even weeks, the relatively small cost of a tape backup system and the regimen required to maintain it seems to be a no-brainer. Yet we get calls too often from panicked clients who have come in to work Monday morning to a failed server, and they have nothing to fall back upon.

### **Tape, Zip, or what?**

To backup your network you need two things: a backup drive and backup media. Based on the size of your network, your comfort with exposure and your willingness to re-install all applications vs. have everything re-installed as part of a full restore, the system that you actually employ can vary.

We *always* recommend a tape drive system over all other methods. Tape drives are relatively inexpensive, the tapes are orders of magnitude less expensive per megabyte of storage than any other medium, and they are convenient. Another reason to use tape over any other medium is that tape is the only method that can currently back up an entire hard disk without using multiple pieces of media.

We recommend a tape backup drive with sufficient capacity to back up your entire server hard disk with a single tape. Most backup strategies involve unattended operation while your business is closed. It is very inconvenient to have to get up at 2am and drive down to the office to put in a new tape, and in the morning after the office opens it's too late to continue your backup.

The specific technology you choose is entirely up to you and your pocketbook. Our experience has shown that with proper care, most specifically regular cleaning, all tape drive technologies are extremely reliable.

## Recommended Strategy

At AIS we use a 10-tape backup strategy, also called the Father-Son strategy. With this method, four tapes are used during the week and the rest are used each Friday. Here's a diagram:

The strategy starts on a Friday with a full system backup. The following Monday, put in tape two and perform a *differential backup*. This means that only the data that has changed since Friday's backup is backed up again. On Tuesday, the third tape is used and again a differential backup is performed, backing up everything that has changed since Friday. Continue through the week. The week-day tapes are called daily backups. With this *differential strategy*, you only need the last full backup and the last daily backup tape to completely restore your system.

This strategy results in a six-week archive of your data. After the Friday where tape 10 is used you start over with tape 1.

At AIS, we've modified this strategy slightly. Since we do not have a huge amount of data, backing up our entire server – about 1.9 billion bytes right now – only takes our tape drive about 45 minutes. At 11pm, who cares? So instead of performing a differential backup on weeknights, we perform a full backup every night. We still maintain the same rotation so we end up with backup of data that is up to six weeks old, but restoring our system (yes, we've had to do it once) only takes the most recent tape since every tape is a full backup. We recommend this modification to our clients.

<b>Friday</b>	<b>Tape 1</b>	<b>Full backup</b>
Monday	Tape 2	Differential backup
Tuesday	Tape 3	Differential backup
Wednesday	Tape 4	Differential backup
Thursday	Tape 5	Differential backup
<b>Friday</b>	<b>Tape 6</b>	<b>Full backup</b>
Monday	Tape 2	Differential backup
Tuesday	Tape 3	Differential backup
Wednesday	Tape 4	Differential backup
Thursday	Tape 5	Differential backup
<b>Friday</b>	<b>Tape 7</b>	<b>Full backup</b>
Monday	Tape 2	Differential backup
Tuesday	Tape 3	Differential backup
Wednesday	Tape 4	Differential backup
Thursday	Tape 5	Differential backup
<b>Friday</b>	<b>Tape 8</b>	<b>Full backup</b>
Monday	Tape 2	Differential backup
Tuesday	Tape 3	Differential backup
Wednesday	Tape 4	Differential backup
Thursday	Tape 5	Differential backup
<b>Friday</b>	<b>Tape 9</b>	<b>Full backup</b>
Monday	Tape 2	Differential backup
Tuesday	Tape 3	Differential backup
Wednesday	Tape 4	Differential backup
Thursday	Tape 5	Differential backup
<b>Friday</b>	<b>Tape 10</b>	<b>Full backup</b>
Monday	Tape 2	Differential backup
Tuesday	Tape 3	Differential backup
Wednesday	Tape 4	Differential backup
Thursday	Tape 5	Differential backup
<b>Friday</b>	<b>Tape 1</b>	<b>Full backup</b>

If your clinic is open more than five days per week you will need more tapes for the daily backups. If you are open overnight instead of during the day, you will set up your system to backup in the middle of the day instead of at night. Work with your network vendor to design a strategy that will work best for you.

## Take your data offsite

A backup tape sitting beside the server it backed up helps if your hard disk crashes, but isn't any good at all if it's just another melted pile of goo next to the melted pile of goo that used to be your server that just burned up with your office. Your backup strategy needs to take into account not just a server crash, but

also fire, theft, and damage by other means. Make it a habit to throw last night's tape in your briefcase every day, and to save your weekly backup tapes **offsite** so you'll be protected in case of the ultimate tragedy.

## Verification

Backup only works for you if you can restore your data after a crash. We have had more than one instance where our client rigorously adhered to a backup strategy but didn't realize their tape was not reliable, or that their network consultant had forgotten to turn off the "append" feature of their backup software. As a result, when their hard disk crashed they discovered none of their tapes worked.

Moral: don't assume that just because your tape software *says* it backed things up ok, it actually did. Have your network vendor teach you how to restore data, and periodically restore a few files. This gives you the assurance that your system is working and that you know how to restore your data in the event of a crash. Make sure you are taught how to restore to a different folder than where the data was originally stored, so you avoid restoring an old version of a file. You don't have to fully restore your system during these tests – just a few files at random to ensure that the tape is readable.

Do this every few weeks, and you won't have to worry about whether or not your tapes are good – you'll know they are because you tested them yourself.

## Clean your drive

The most common cause of failed backups is a dirty tape drive. Drive cleaning cassettes are inexpensive and work well. Using one every two weeks takes just a minute while changing tapes. If during your verification process you discover your tape has not backed up correctly, or you see a message in the morning telling you the process aborted, the most likely cause is a dirty drive. Your network vendor can help you choose a cleaning strategy.

## Conclusion

Your business data is an extremely valuable asset, and you need to protect it. Backup strategies are simple to implement, relatively convenient, and essential to your business peace of mind. Because they are machines with moving parts that eventually wear out, every computer hard disk *will fail* eventually; you don't want to be caught unprepared when – not *if* – it happens. In the meantime, you don't want to take the chance that your server won't be stolen or destroyed, so it pays to be prepared.

It is your responsibility to back up not only your **AI** or VSS data, but the other data you use on a daily basis as well. Your network vendor will assist you in creating a strategy that will work for you.