

**Inside this issue:**

*Backing up data* 1-3

## Backing up data

*It's the 9<sup>th</sup> of the month, you arrive at the office to find:*

- *Your computer emits a strange noise, smell, or sudden flash, then simply quits.*
- *A brand-new skylight and a tree lying where your computer used to be.*
- *Your computer and USB drive has been stolen during the night.*
- *Your property now sports a brand new indoor swimming pool. (Hey, isn't that your monitor floating by?)*

### Now what?

Do these scenarios sound preposterous? Unfortunately, each one of these scenarios is all too real, especially to those customers that lived through them. Be they natural, man made, or simply due to parts wearing out, disasters happen and you can lose your data. This begs the question "What can I do about it?"

While the specific solution will vary, depending on your resources and the importance of your data, the short answer is to backup your data. Taking a regular backup of the important data on your system is the first line of defense when it comes to minimizing the impact of any sort of computing disaster. On the other hand, simply backing up and throwing the disk or USB drive in a drawer is not an adequate solution either (re: 3<sup>rd</sup> and 4<sup>th</sup> scenarios).

### I. What should I backup?

There are two common schools of thought on this issue: Mission-critical data only, and Everything. Each school has its own set of valid arguments, but which one you should choose depends on your specific circumstances.

Backing up only your critical data means that your backups complete faster, are much smaller, and as a result, are much more portable. However, if disaster strikes, you must also have the disks to reinstall your operating system and applications (in addition to your backup) in order to reinstall, but you will still lose any system customizations not included in the backup.



### **Coming in November:**

- From Client Care - Using the Log screen in the iMAX window
- Industry Insight - from "Guest"

### **Come meet us at the upcoming shows:**

SWAHMA on October 20th in San Antonio, TX  
PennDel AHMA October 28<sup>th</sup> in Dover, DE



### Continued data backup

A full system backup gets around the issue of peripheral data loss, but often only requires you to have the operating system and backup software install disks, in order to recover your system. The biggest downsides to a full system backup is that it takes significantly more storage capacity and that it takes significantly longer to complete.

#### **2. How often should I backup my data?**

Generally, you should not back up any more often than you can afford to lose your data. What this means to you is that if you can't afford to spend the time to recreate more than a day's worth of work at a time, you should backup daily. If you can afford to recreate an entire month's worth of work, backup monthly.

#### **3. Where should I store these backups?**

Backup media, ideally, should be stored in temperature and humidity-controlled environments, away from strong magnetic fields, and in a location that is physically separated from the original computer. A safe deposit box, a safe in the manager's (offsite) residence, or an online backup service are good examples of safe offsite storage options which you may choose to employ.

Please note: IPM-Software does not directly integrate with any online backup solutions at this time. Individual configuration is required, for further information; please consult the documentation provided by the service itself.

Again, there is no clear-cut answer for this question, primarily because it all depends on the type of data you are backing up. Conventional wisdom dictates that federal tax information should usually be retained for seven fiscal years. Per HUD, an individual resident's information should be retained for three years beyond the date of move out. What does this mean for your backup retention? IPM-Software generally recommends the following:

#### **4. How long do I keep the backup?**

Again, there is no clear-cut answer for this question, primarily because it all depends on the type of data you are backing up. Conventional wisdom dictates that federal tax information should usually be retained for seven fiscal years. Per HUD, an individual resident's information should be retained for three years beyond the date of move out. What does this mean for your backup retention?



### Continued data backup

IPM-Software generally recommends the following:

- Annual backups - at least 3 years (7 would be better),
- Monthly backups - at least 12 months,
- Weekly backups - at least a month,
- Daily backups - at least a week.

### **5. How do I know the backup is good?**

Backups should be tested on a regular basis to ensure they work and/or the media itself is still viable. An untested backup cannot be guaranteed as being “good.” With this in mind, set up a regular schedule where you test restoring a backup (preferably to an alternate location). Conducting this testing not only confirms the validity of your backups, but also that you will be able to restore your data if the worst should ever happen.

Please remember, the time to plan for disaster is now. If you wait till one strikes, your options shrink dramatically while the costs involved can rapidly skyrocket. The only way to make sure you are safe is to: 1) make a plan, 2) test it, and 3) most importantly, stick with it!

For more info on how to backup and restore your data, please refer to the following documents:

#### Cornerstone:

How to backup: [http://www.ipm-software.net/downloads/help\\_documents/CS%20Backup.doc](http://www.ipm-software.net/downloads/help_documents/CS%20Backup.doc)

How to restore: [http://www.ipm-software.net/downloads/help\\_documents/CS%20Restore.doc](http://www.ipm-software.net/downloads/help_documents/CS%20Restore.doc)

#### HUDControl:

How to backup: [http://www.ipm-software.net/downloads/help\\_documents/127%20-%20HUD%20-%20Backup%20instructions.doc](http://www.ipm-software.net/downloads/help_documents/127%20-%20HUD%20-%20Backup%20instructions.doc)

How to restore: [http://www.ipm-software.net/downloads/help\\_documents/012%20-%20HUD%20-%20how%20to%20restore%20data%20in%20HUDCONTROL%20%20and%20up.doc](http://www.ipm-software.net/downloads/help_documents/012%20-%20HUD%20-%20how%20to%20restore%20data%20in%20HUDCONTROL%20%20and%20up.doc)

#### IPMS:

How to backup: [http://www.ipm-software.net/downloads/help\\_documents/152%20-%20ipms%20-%20Backup%20instructions.doc](http://www.ipm-software.net/downloads/help_documents/152%20-%20ipms%20-%20Backup%20instructions.doc)

How to restore: [http://www.ipm-software.net/downloads/help\\_documents/160\\_IPMS\\_restore\\_data\\_into\\_ipms.doc](http://www.ipm-software.net/downloads/help_documents/160_IPMS_restore_data_into_ipms.doc)

#### RHS:

How to backup: [http://www.ipm-software.net/downloads/help\\_documents/161\\_rhs\\_Backup\\_instructions.doc](http://www.ipm-software.net/downloads/help_documents/161_rhs_Backup_instructions.doc)

How to restore: [http://www.ipm-software.net/downloads/help\\_documents/162\\_rhs\\_Restore\\_instructions.doc](http://www.ipm-software.net/downloads/help_documents/162_rhs_Restore_instructions.doc)