



Data Retention Policy

A Simple Guide to Developing Effective Policies

Data Backup: Developing an Effective Data Retention Policy

By Global Data Vault

Archiving one's data is a challenge for every business, whether the business is a billion dollar enterprise or a SOHO. Data loss can be devastating to the profitability of any enterprise, and data recovery can be a nightmare if not planned for correctly. Developing and committing to an effective data retention policy is something that each business owner wrestles with, and correct implementation can mean life or death of a company in a disaster situation. Understanding how your data is retained is the foundation of any effective data retention policy.



Data retention is no new concept, but the method has certainly evolved. The early days of data retention policies were historically done in a classic “son – father – grandfather” routine where “son” is most current data backup, “father” is a previous older version of the data backup, “grandfather” is oldest version of the data backup in the rotation. In the old days, you might have had 5 daily backup tapes, each of which were considered the “sons.” Then you would save all your data every Friday for 4 to 5 weeks and those were the “father.” On the 5th Friday, you took the oldest Friday out of the rotation and saved that into the “grandfather” batch. And viola, that was the extent of your data retention policy. It was a gigantic storage capacity hog, and it was time intensive.

Sometimes the time required for each data backup was so many hours that starting a backup at the close of business did not always guarantee that it would be done by the start of the next day. This period is called the Backup Window. In order to try to shorten the Backup Window, a technique called Incremental Backup was introduced. An Incremental Backup only includes files that were changed since the last Full Backup. Incremental Backup adds a layer of complexity and attendant risk into the data backup process.

If you experienced a data loss or corrupt files, not only did going back to a father or grandfather tape require a more complete backup, you had to cross your fingers that the previous generation was pretty darn complete, not to mention the restore time was significant. For example, if you had to go back to a particular week or a month – it would require going back to several tapes and piecing it together by putting the incremental backup of Monday's tape with Tuesday's tape, Tuesday's tape with Wednesday's tape, Wednesday's tape with Thursday's tape, and so on until you got the entire data set restored. The likelihood of tape failure during that process was high and that ensured some level of data loss.

Today's data retention policies have come of age with new technology. Gone are the days of incremental backup tape, its required massive storage capacity, and risky reinstalls. Disc environments have become commonplace and because the modern method is to only save the data that has changed, your storage

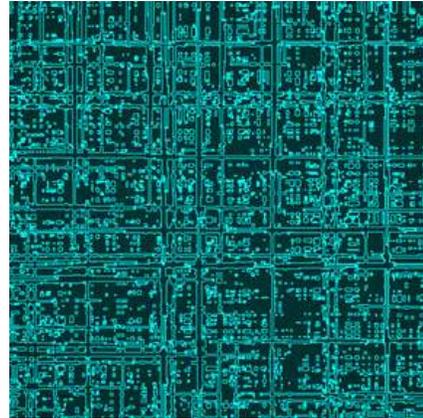
Please visit www.globaldatavault.com for complete details.



requirements are much less, the restore process quicker and the risk of failure significantly less. And the fact that only changed data is moved, no longer adds complexity and risk – because all of the data required for a recovery is assembled in one place at the time the backup is made.

...

Having covered the history of and comparison of tape backup environments to disc backup environments, we'll move on to understanding how your data is retained which is the first and critical step to designing a data retention policy, but the next steps are a bit more murky and complex.



Depending on the industry in which you do business, your data retention policy may be dictated by legal or business retention requirements. For example, legal retention requirements would include:

- Each state has unique legal requirements on how long medical records must be maintained
- Every business' tax records are to be kept for at least 3 years – but there many exceptions to this rule:
 - You must keep all employment tax records for at least 4 years after the date that the tax becomes due or is paid, whichever is later.
 - In Texas, Sales and Use Tax records must be retained for four years.
- Businesses subject to OSHA regulations have specific requirements on how long their data must be retained
- Food manufacturers are required to track all the ingredients and their location of origin in the unfortunate event of poisoning
- Machine shops are required to maintain records on where the material origin in the event of product failure

The Massachusetts Society of Certified Public Accountants has published a great resource on this subject here.

Aside from what you are legally required to do, there are compelling business arguments for retaining your data for considerable time. Ask yourself how long you need to maintain customer or accounting records. Go through the many scenarios that could impact your business, for example, do you offer any type of warranty or credits? Is there any opportunity for a recall of your manufactured items? What is the general practice within your industry for maintaining business records? What if you were to sell the business, how long of a history would a potential acquirer want?

Start your data retention policy by inviting key employees to a brainstorming session and ask, what if we need to go back in time to retrieve for data for:

- A tax records audit
- A labor law compliance audit
- A product liability lawsuit
- An employment practices claim

Please visit www.globaldatavault.com for complete details.



- An employee tort such as a sexual harassment claim

and start to build your policy around these scenarios. Double check it against both the legal data retention requirements and your own business retention needs.

...

That's took a look at the challenges that different industries face when considering what data to maintain and for how long. And even though each company has different requirements, the common thread to every data retention policy is that your data is everywhere. Encompassing all of it may be nearly impossible and while this checklist is not exhaustive, it's a great foundation to any data retention policy. Paired with an advanced data backup system, you'll rest easy knowing your critical information is safe and easily recoverable.



Finally, we provide a data checklist and questions to ask when setting your policy.

To get started, assess what you have. Your business has many types of data that you will want to consider within your data retention policy:

- Financial data
- Databases
- Email
- Documents
- Pictures / videos
- Production data
- System state information

Furthermore, the location of the data must be considered. You may actually create a different DRP for each one, depending on what you keep where.

- Servers – what is stored on your server?
- Databases – what is stored there and how do the legal and business requirements dictate what you need to maintain and for how long?
- Desktops – do you need to backup files that are saved on desktops? And if so, how long do you need them? Typically desktop files are not retained as long as server data.
- Email – The content of the data must be evaluated
- What is in your emails? Many companies may feel that email is unimportant to core business, but others may use email as an integral part of their order processing or customer service functions. Take the case of a freight forwarder for example, where almost every email has a document attached with key business information. That freight forwarder's exchange server is, therefore, huge and critically important to back up. In this case, the freight forwarder may have customers that contact them years later looking for items that were to be forwarded to a particular

Please visit www.globaldatavault.com for complete details.



location. For them, email is imperative to backup. Your business may have a similar communications issue.

- Recovery – how will your business recover its data from a potential problem or data loss? How long can you survive without your data before your business practice will be impacted? Take a reality check of your data retention policy and ask:
 - Would it provide the necessary recovery?
 - Would it restore in the time frame and as you needed? Test it!

Frequency – Is there a danger of data loss, do you need to backup your data more frequently than once per day, and how long do you keep your data?

- An example of the frequency of a retention policy would be:

- Retain every daily backup for 10 days
- Retain every weekly backup for 6 weeks
- Retain every monthly backup for 14 months
- Retain every year-end backup for 7 years

Evaluating the soundness of your data retention policy begins with asking your executive staff, is this right, is it sufficient, and is it cost effective? There is a balance you'll need to achieve between cost to maintain data and the legal requirements that your company is subject to. Furthermore, brainstorm the "what-if's" scenarios and determine what data would be needed to recover properly:

- What if we had a partial data loss of data such as a server failure
- What if we had a complete data loss such as a premises disaster
- What if we had widespread corruption of data from a virus
- What if we suffered a data loss from deliberate sabotage
- What if we accidentally destroyed important data
- What if we need to go back in time for data for:
 - A tax audit
 - A labor law compliance audit
 - A product liability lawsuit
 - An employment practices claim
 - An employee tort such as a sexual harassment claim

Finally, on your checklist, make sure there are no "islands of data" outside the policy –

- Laptops
- Desktops
- Remote offices

There is no one size fits all for a data retention policy. Each company has its unique needs, cost parameters and legal requirements that will dictate what is essential and mandatory to maintain the business in the event of a disaster or data loss. Start with the checklist above and add to it to fit your individual business and legal requirements.

Request Information

Global Data Vault (GDV) was founded in 2002 to provide superior technology for backup and disaster recovery services. With a worldwide customer base, GDV's fast growth is a function of high quality solutions and an exceptional value proposition. To learn more about Global Data Vault, visit us at [Global Data Vault](http://GlobalDataVault.com).

Department	Email	Phone
Sales	sales@globaldatavault.com	214-363-1900 x 1
Support	support@globaldatavault.com	214-363-1900 x 2
Customer Service	billing@globaldatavault.com	214-363-1900 x 3

Please visit www.globaldatavault.com for complete details.

