Network Backup Checklist

Whether this is the first time your organization has considered backing up data or you have a backup policy already in place; this handy checklist is a great way to prioritize and improve your organization's data security.

step 1 Does your organization currently have a policy for your data's safety and retention?

If you are unsure or the answer is no, this exercise is a great opportunity to clarify this with your administration[1]. By the end of this checklist, you will be well on your way to having a policy drafted or a current policy improved. If you have a current policy in place, this checklist will be a great way to check off items needed to follow your organization's protocol.

step 2 Identify your data.

Set up a matrix to identify all of the data in your organization and the amount of storage space that data requires. You will use this matrix to later classify and assign risk to your data. A simple spreadsheet can be very useful. Once your data is all logged into a spreadsheet, you can filter and sort by classification, risk and storage amount required to determine different scenarios of how to backup your data.

step 3 Classify your data.

Every organization classifies its data in different ways. If your organization's data were to disappear tomorrow, what critical elements would be necessary to maintain business "as close to usual" as possible? What would you need to keep the municipal offices open? If we all had unlimited resources, we could just say, "back it all up." But since that is not usually the case, let's begin this exercise by classifying your data into three categories.

How to Classify Your Data[2]

Restricted Data

Restricted data is considered to be highly sensitive business or personal information. Financial information for the organization, social security numbers of your students, patrons or employees and other critical business information would be considered restricted data.

Restricted data is intended for a very specific use and should not be disclosed except to those who have explicit authorization to review such data, even within a workgroup or department. Unauthorized disclosure of this information could have a serious adverse impact on the organization or individuals.

Sensitive Data

Sensitive data is data that has personally identifiable elements attached to it. For our members this could be students or patrons names, addresses or birthdates. Sensitive data is intended for use within the organization or within a specific department or group of individuals with a legitimate need-to-know. Unauthorized disclosure of this information could adversely impact the organization or individuals.

Public Data

Public data has been approved for distribution to the public by the data owner or through the organization's administration. Public data requires no authorization to view and may be considered informational in nature. While public data could be difficult to lose if a disaster occurred, day-to-day operations could continue and no harm would come to your organization legally if it were lost for a time period.

step 4 Assign risk within your data classifications – High, Medium and Low

Not all data is created equal. It is simple enough to classify your restricted data as critical to backup, but beyond that it might be difficult to distinguish what should be backed up and what can just be replicated or stored. For your sensitive data and public data, it is a good practice to take your information one step further and rate the risk of losing that information or that information becoming corrupt. To assign risk you will want to look at several factors. Is this data essential to continue business immediately? How many staff hours will it take to recreate this data? Decide what the risk of losing this data is for your organization's business continuity and "sub-categorize" the data risk as high, medium or low.

Assigning Risk

Below are some examples of how classifications and risk might look at an organization. Every organization is going to classifiy their data differently.

- Financial Systems - Restricted Data/Critical Risk
- Student Information Systems – Restricted Data/Critical Risk
- Teacher Home Directories – Sensitive Data/Average Risk
- Student Home Directories – Sensitive Data/Low Risk
- E-mails – Sensitive Data/Average Risk
- Learning Management Systems – Sensitive Data/ Average Risk
- Card Catalogues – Public Data/Average Risk

step 5 Choose a backup product.

When choosing a backup product, make certain you are comparing apples to apples. Does the product you are looking at offer encryption, support and compression/de-duplication? (De-duplication is the process of removing duplicate data from within a data set to decrease the overall stored size, which may help reduce your costs).

MOREnet's Network Backup service offers three types of data backup services and can backup as little as 2GB. Below are the three service offerings:

- Enterprise Backup - Windows, Mac and Unix Servers: including database, e-mail, sharepoint and other applications
- Files-only Backup - Desktop and Laptops only. Client Supports Windows Operating Systems
- Local-only Backup - Data can be backed up using the cloud backup software, but it will not be transferred to the vault and stored only locally

step 6 Determine the cost.

Now that you have several scenarios in place for your classified data and your data's risk, you will have an easier time of pricing the backup products you are investigating. Just remember step #5 and make certain you are paying for the same functionality when you are comparing products. What does your organization do with the files that are not being backed up?

[1] This checklist is a guideline to help your organization get started or improve the data security in case of a disaster or system failure. It does not replace legal advice.

[2]Classifications and definitions were in part created in reference to the University of Missouri System, Information Security - Data Classification. For more information visit: http://infosec.missouri.edu/classification/dc-sys-apps.html#dcl-defs.

step 7 What's does your organization do with the files that are not being backed up?

After you have determined what will be put in the Network Backup service, what should your organization do to maintain and secure the remaining data in your organization?

Network Storage: Making a copy of data and storing it with a remote storage service in a secure, off-site data facility. http://www.more.net/services/network-storage.

E-mail Archiving: Archiving e-mail accounts in a secure environment inexpensively. http://www.more.net/services/e-mail-archiving.

Data Replication: Replicating the data to another site or to a partnered organization.

step 8 Finish defining your data policy.

You have come this far, so why not determine what is left to define a data policy for your organization. Below are some other items to consider to get you started:

- Data retention policy – how long should your organization keep its information? Is there a law that determines this for your organization?
- Does your organization fall under any guidelines that would require special documentation, reporting or security?
- Does your organization have e-commerce?
- What is your e-mail retention policy?
- Does your organization have a formal procedure to put policies into place?

Need more assistance?

MOREnet is here to help. If you need assistance determining your backup needs or have questions regarding Network Backup, contact MOREnet Technical Support at help@more.net or by calling (800) 509-6673.

MOREnet
Be better connected.
221 North Stadium Blvd., Suite 201, Columbia, MO
(573) 884-7200 • info@more.net • www.more.net