

Guide to Data Protection Best Practices

A TANDBERG DATA WHITE PAPER ON BACKUP AND ARCHIVAL STORAGE BEST PRACTICES

Faced with meeting their own needs for supporting data growth, security, environmental, economic needs, and regulatory compliance, businesses today must address the dual challenges of safely storing and protecting their corporate data—at a time when the quantity of the information they generate and consume daily has grown exponentially and IT budgets are under even greater scrutiny for cost savings and efficiencies. However, data protection is a business imperative now more so than ever before; the failure to properly manage and safeguard corporate data can result in business disruption, devastating losses or the potential failure of the business itself.

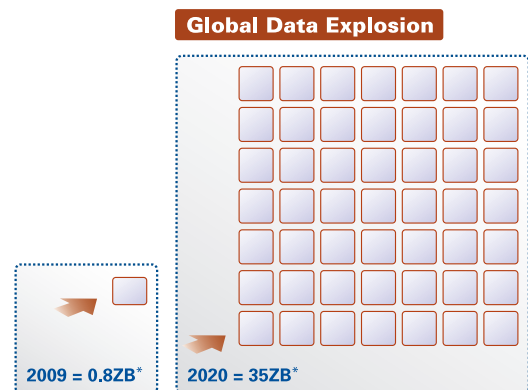
This white paper discusses how businesses must first develop an appropriate strategy and then make the right technology choice from multiple storage options in order to establish best practices for data protection.

Data, Data Everywhere

In 2009, amid the ‘Great Recession,’ the amount of digital information grew 62% over 2008 to 800 billion gigabytes (0.8 Zettabytes). Digital information created between 2009 and 2020 is forecasted to grow by a factor of 44x. It’s also expected that by 2020, the percent of digital information requiring additional security will grow from 30% to 50%.

In 2010 35% of digital information created is discarded because we don’t have available capacity. This number is expected to grow to 60% over the next several years.

The number of files, images, records and other digital information containers will grow by a factor of 67, each needing to be managed, secured and protected. Despite



*ZB = Zettabyte (1 trillion gigabytes)
 Source: IDC
 RDX with AccuGuard

Guide to Data Protection Best Practices

this growth, the number of IT professionals globally will grow only by a factor of 1.4. The cumulative effect is driving CIOs to seek out new levels of agility, efficiency and control by moving quickly toward private cloud computing environments. Digital information created in 2010 = 1.2 Zettabytes is equivalent to:

- The digital information created by every man, woman and child on Earth 'Tweeting' continuously for 100 years
- 75 billion fully-loaded 16 GB Apple iPads, which would fill the entire area of Wembley Stadium to the brim 41 times.
- A full-length episode of FOX TV's hit series '24' running continuously for 125 million years.
- 707 trillion copies of the more than 2,000-page U.S. Patient Protection and Affordable Care Act signed into Law in March 2010. Stacked end to end, the documents would stretch from Earth to Pluto and back 16 times or cover every inch of the United States in paper 3 feet deep.

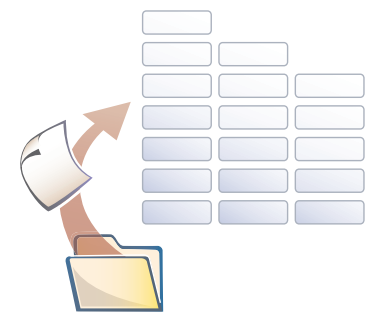
All of this may not come as a surprise to the executives running businesses of all sizes across the globe. They face a daily deluge of data from every department—administrative, financial, legal and operational. And this data comes in a multitude of forms, such as emails, text files, presentations, voice mails, faxes, invoices, employee records, Website content, photographs and even physical samples, such as product samples or historical printed documents.

A Convergence of Factors

At the same time, these businesses must comply with recordkeeping requirements defined by state and federal regulators, their industry and legal precedence. Certain industries have regulations mandating how information must be used, stored and retained before being destroyed, and these retention requirements vary significantly from one type of data to another, according to the Association for Information and Image Management (AIIM).

Amid this era of increasing compliance, IT budgets are now even leaner and meaner. Gartner had originally expected IT budgets to grow 3.3% in 2009, but it has revised that figure downward to between 0% and 2.3%, with a worst case scenario of -2.5%. Faced with those numbers, total cost of ownership (TCO) and return on investment (ROI) will continue to drive IT budget planning and spending. However, businesses now see that it is essential not just to look at the price of IT hardware, but at the whole product lifecycle.

With that in mind, the cost of running and maintaining equipment—particularly the energy consumed by each piece of equipment—has come under increased scrutiny. According to an IDC report on Worldwide Server Power and Cooling Expense 2006-2010, "for every dollar spent on computer hardware, another 50 cents is spent on energy. Within the next four years, that number will rise by 54%." Further, Gartner predicts that this trend will get even worse, with energy costs consuming up to one-third of IT budgets within the next several years. (Source: SearchStorage.com, SNW: "Users Thrash Out Green Storage") For companies "going green," this is as much about maximizing cost savings as it is about saving the planet.



Despite this convergence of negative factors, businesses today require 24x7 access to data. Instant access to data is now taken for granted, whether in the office, on the road or working remotely. At the same time, this has become a business imperative because unmanaged or poorly managed data can

Guide to Data Protection Best Practices

“bury decisions under even higher piles of conflicting data.” (Source: Relevance by David Appgar) This lost or hard-to-find information can reduce overall productivity and lead to missed opportunities to grow the business—from losing reputation to losing individual sales to losing customers.

Data: The Lifeblood of Any Company

Corporate data is a strategic asset. Improperly managed, it can become a significant liability. In the case of a litigation request, for example, companies are responsible for producing the required information needed for their defense—and this now includes email correspondence.

As a result of these developments, businesses and corporate executives have gained a vivid awareness of the need to back up their data as part of their overall business continuity and disaster recovery plan. This includes the regular backup and archiving of data so that in the event of a natural disaster, such as a fire, water damage, etc., they can quickly access another copy of their corporate data and be back in business again as quickly as possible.

With the cost of IT system downtime so expensive—between \$84,000 and \$108,000 for every hour—the cost of even one day of lost business can be devastating, particularly in today’s economy. (Source: Gartner, IDC, Forrester, Yankee Group) In fact, it is reported that 90% of businesses that lose all of their data go out of business within the following 12 months.

Remarkably, however, 40% of all small- and medium-sized businesses (SMBs) don’t back up their data at all, and 60% of all data is stored on PC desktops and laptops. (Source: Small Business Computing). Looking at small office/home office (SOHO) users, only 73% who have a personal backup device use it to back up at least monthly, and only 40% back up daily. (Source: IDC Worldwide Personal Storage 2007–2011 Forecast and Analysis)

Truth or Consequences

To protect themselves adequately, businesses must improve how they manage and protect their business records. As new regulatory rules are created and the number of disaster recovery scenarios increase, Information Lifecycle Management (ILM) now plays a pivotal role in helping companies adhere to new standards while incurring minimum management headaches. ILM is not a specific technology. Instead, it is a combination of processes and technologies that determines how data flows through an environment. By doing so, it helps companies manage their data from the moment it is created to the time it is no longer needed.

As part of ILM, records management is the practice of identifying, classifying, archiving, preserving and destroying records. An on-going process, records management requirements must be designed and integrated into both business processes and the technical infrastructure. These requirements state that records must be:

- Retained on the basis of their value to the organization, rather than their physical or logical characteristics
- Created and maintained for many reasons, including to preserve rights, fulfill compliance obligations, document business processes, provide customer service and mitigate risk
- Managed on a media-neutral basis and retained in accordance with approved policies, procedures and schedules
- Retained for the same time period, regardless of the media on which specific records are stored

Guide to Data Protection Best Practices

Backup vs. Archiving

Good records management includes both backup and archiving. However, while these terms are often used interchangeably, it is important to distinguish between them when considering a records management process. Backup is used for data recovery, while archiving is used for preserving and retrieving data in the event of a disaster, inquiry or litigation. In simple terms, think of backup as short-term and archival as long-term.

Specifically, **backup** is a snapshot or picture of the state of the data before it disappeared or was destroyed, with the data periodically overwritten as it changes. In the backup process, a copy of data at a specific point in time is created in case something should happen to the original. Therefore, in the case of a failure, the data can be reconstructed from that time. This concept is very similar to backing up a Word document either automatically or with the “Save” button on a computer, except that the backed up data is stored on a remote device. Fixed disk storage devices are typically used for backup because of their speed and ability to provide instant access to the data on the disk.

On the other hand, *archiving* is long-term and unalterable. Used for compliance or disaster recovery, redundancy and physical separation are crucial to effective archiving. Archived files can be kept for decades, usually at an offsite location, and two or more remote copies are better than one to properly safeguard this data. Tape is typically used for archiving because of its affordability, reliability and portability. Additionally archiving unused data to tape minimizes the costs of keeping the unused data live on disk.

Retention schedules are the foundation of a successful records management process. These schedules take into account an organization’s legal, regulatory and operational requirements while providing guidance on how long records need to be kept and what to do with them when they are no longer needed. It is important to develop a schedule for backing up and archiving all computer records and for keeping current copies of all paper and computer files off-site and accessible. (Source: Small Business Administration)

To do so, it is vital to determine what data needs to be backed up and what data needs to be archived. This can be done with your legal department or advisor along with the business users of the data. At the same time, the archival retention periods for the various types of data need to be determined. It is also vital to remember that not all data has the same requirements, while some data may have overlapping requirements.



FILE TYPE	INCREMENTAL BACKUP (Daily)	FULL BACKUP (Weekly)	OTHER BACKUP (Monthly/Archive)
Data files	100GB	500GB	500GB
Critical files (may be backed up several times a day)	Yes		
System files (typically backed up once a month)			Yes

Guide to Data Protection Best Practices

Right-sizing Equipment

But having the right policy in place also means having the “right size” equipment in place. Due to the wide variety of data storage products and formats available today, businesses face a challenging purchasing decision. It is important to remember that the amount of data needed to be stored varies significantly based on the industry and the regulations required in that industry. However, this is a much more useful metric in defining the size of a business with regard to data storage requirements than the number of employees or sales revenue.

Because capacity demand increases are similar across businesses in the same industry regardless of size, it is equally important to determine how businesses administer their data storage. However, what is different is the means of dealing with meeting these capacity demands. Fortune 500 companies behave differently than SMBs; they have different priorities and different needs.

How Often Is Often Enough?

With data files changing every time someone enters new information, many companies back up the data files every day (or only those files that have changed) and then perform a complete backup of the entire system on a weekly, biweekly or monthly basis. For your company, you can determine the necessary frequency of backups by asking yourself how often the data changes and how critical are the different types of data files. In other words, how much data can you afford to lose without causing your business undue hardship?

The best strategy is to devise a schedule that works for the majority of your data files. You can schedule a daily backup of new and modified data files, for example, and then a weekly backup of all files. If you have critical files that must be backed up more often, you can back up these files throughout the day.

Once properly defined, these specific business characteristics will help turn the available data storage options into a solution that will best meet your individual business needs.

Types of Backup

Software applications include options for copying the full set of system files, for copying a partial set of new or modified files, and for copying selected, individual files. Most companies use a combination of full and partial backups by performing nightly backups on files that have changed throughout the day, then full backup of all files on a weekend day.

PARTIAL BACKUPS

A partial backup copies all files that have been added or changed since the last backup job. There are two main types of partial backups: incremental and differential.

Incremental Backups

- If you need to save time and cost during regular backup jobs, choose a plan that includes full and incremental backups. In this strategy, you perform a regular backup of all files (weekly, biweekly, etc.), then a more frequent backup (daily) of only the files that have changed since the last backup session. This full/incremental backup method means that fewer files need to be copied and less time is required for the backup procedure. However, this method can also make a complete system restore slower if you have created many different incremental backup tapes (one for each day of the week, for example), or if you need to restore only a particular file and must hunt through several different incremental backup tapes.

Guide to Data Protection Best Practices

Differential Backups

- If you need to save on restore time and hassle in the event of a disaster, choose a plan that includes full and differential backups. In this strategy, you perform a regular backup of all files (weekly, bi-weekly, etc.), then a more frequent backup (daily) of all files that have changed since the last full backup session. This full/differential backup method helps the restore process run more efficiently, because only one full backup tape and one differential backup tape are required for a complete restore of the system. However, this method is slower on the backup process because more files are copied daily.

FULL BACKUPS

A full backup copies all the files on the system—the system files, the software files, and the data files. You should perform a full backup on a weekly, bi-weekly, or monthly basis. With a full backup of your data set on tape, you can restore your entire system if a disaster destroys the original files.

BACKUP TYPE	ADVANTAGES	DISADVANTAGES
INCREMENTAL All new or modified files since last full or partial backup	Faster backup time due to fewer files. Reduced wear on backup device and tape. Fewer tapes may be required.	Slower restore times as more than two tapes may be required (the full backup tape and each incremental backup tape). Higher cost of downtime.
DIFFERENTIAL All new or modified files since last full backup	Faster restore times due to only 2 required tape sets (the full and differential backup tapes). Lower cost of downtime in a system disaster.	Slower backup process because more files are copied. Increased wear on backup device and tape. More tapes may be required.
FULL All data is backed up	Less complexity, simplifies restore operations. Faster restore times. Reduces the risk of data loss.	Longer backup window required because all files are copied. Increased wear on backup device and tape. More tapes are required.

Guide to Data Protection Best Practices

User Scenarios

As a leading global supplier of data protection technologies, Tandberg Data offers a complete range of tape libraries, tape autoloaders and tape drives, storage software, media and disk-based storage solutions. All of these are designed to meet the growing storage requirements of businesses by offering scalability, reliability and the backward compatibility features that ensure both cost-effective operation and long-term investment protection.

Let's take a look at some representative businesses scenarios and see how Tandberg Data's products offer the perfect solution.

SCENARIO 1: SMALL OFFICE AND INDIVIDUAL SOLUTIONS

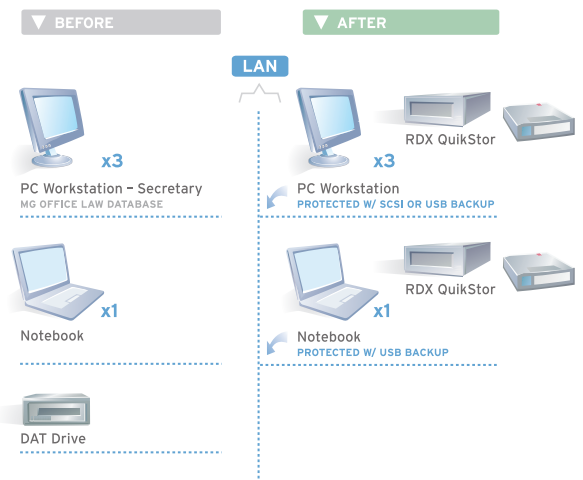
The first scenario (for small businesses) is a law office that includes the attorney, a secretary and a part-time assistants. The secretary uses a standard desktop PC with Office and mail applications installed as well as a specialized database application software for law practice. The attorney's desktop PC is in the same networking workgroup and can access the database application on the secretary's PC. The attorney also uses a laptop, synchronizing local data from the office PC, enabling the ability to also work from home. The part-time assistant uses another desktop PC only for customer correspondence via letters or email. No one in the office is an IT specialist; the only backup done is when the secretary copies data from the secretary's PC onto an old digital audio tape (DAT) drive every Friday.

To summarize, there is a staff of three without an administrator. The company has three desktop PCs and one notebook. There is neither an application nor a backup server. Overall, the company has 120GB of data. Approximately, 0.4% is changed or created each day (0.6GB), resulting in an additional 10GB of data monthly, or 120GB annually. Most of their business is not time-critical. If the database application is not accessible for a day, it is problematic, but not a catastrophe. Downtime allowed equals one to two days.

The ease of use of Tandberg Data RDX® QuikStor™ is the perfect match for this environment. Because of the absence of an application or backup server and because the network environment and IT skills of the employees are limited, individual solutions for each PC and laptop are recommended—three Tandberg Data RDX QuikStor 160GB drives with external USB plus one or two extra 160GB cartridges per unit. RDX QuikStor is easy to install and easy to use, customers can go from out of box to backup in less than one minute.

The Tandberg Data RDX QuikStor is supplied with Tandberg Data AccuGuard™ backup and recovery software. AccuGuard is an easy-to-deploy solution that protects physical and virtual Windows servers or workstations. Tandberg Data AccuGuard™ data protection software delivers reliable, automated backup and recovery utilizing a powerful data deduplication engine designed to increase your effective storage capacity by up to 20 times.

It is recommended that one cartridge be used for daily backups of each computer, one for weekly backups and one for monthly backups. The weekly and month backup cartridges should be stored offsite for disaster recovery. As the business grows, the staff can simply upgrade to the next RDX cartridge capacity. Tandberg Data RDX cartridges range in size from 160GB to 1TB.



Guide to Data Protection Best Practices

SCENARIO 2: SMALL BUSINESS WITH LARGE DATA VOLUMES IN A MAC ENVIRONMENT

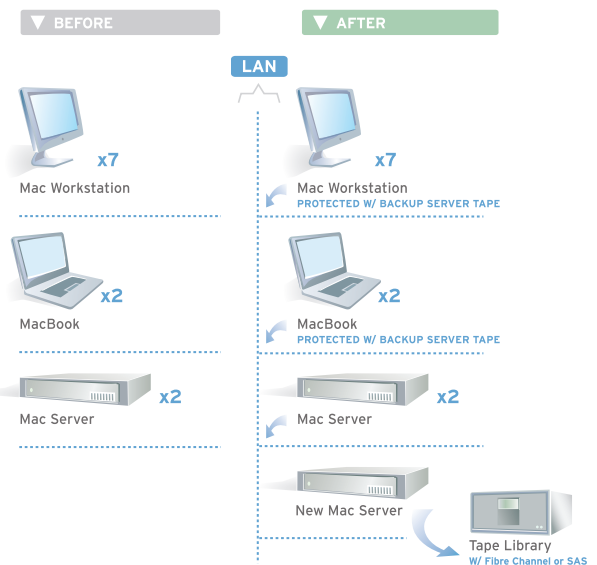
In this midsize business, a creative agency has a staff of four that produces huge amounts of desktop publishing (DTP) data with QuarkXpress, Photoshop, InDesign and other software on their Mac workstations. Additionally, they communicate via email and use various Office applications, Internet browsers, etc. The managing director and the secretary use standard Mac workstations and Office applications plus mail. Another Mac workstation and two MacBooks are used for customer presentations or for when the general manager wants to work from home. One server is used as a file server, the other as a multi-purpose application server for printing, Internet access, database and mail applications. No backup device is attached; only a simple disk-based storage is used. Backup and archiving policies do not exist, and any IT functions are handled part-time by one of the staff.

To summarize, the company has a staff of six and a part-time administrator. It has seven workstations and two notebooks, with two application servers. The company does not have a backup server. Overall, it has a total of 5TB of data. Approximately, 20% is changed or created each day (1TB), resulting in an additional 30TB of data monthly and 365TB annually.

With customers waiting and a huge amount of DTP data that has to be recovered in a disaster recovery scenario, downtime is limited to maximum of one day.

One of the existing servers would need to be turned into a backup server, and it is strongly recommended that another pure backup server be added to the networking environment. With the right clients installed, this would then be able to back up the file server as well as the application server and, if needed, some of the clients themselves. By using the right kind of backup and archiving software, this device will allow for a full initial backup as well as the archiving of any existing data and customer projects.

Nevertheless, for performance and security reasons, we would also recommend another dedicated backup server. Tandberg Data's StorageLibrary T40+ is the inexpensive, automated and easy-to-use solution for differential or incremental backup jobs, plus archiving when required. Tapes and affordable magazines allow efficient off-site storage and excellent TCO. The StorageLibrary T40+ Series is scalable to 453TB (compressed data), allowing businesses to grow their data protection solution as their data grows. In addition, Tandberg Data offers a complete range of backup and archiving solutions for Mac environments, and the company's automation products are certified with all major Mac backup software applications.

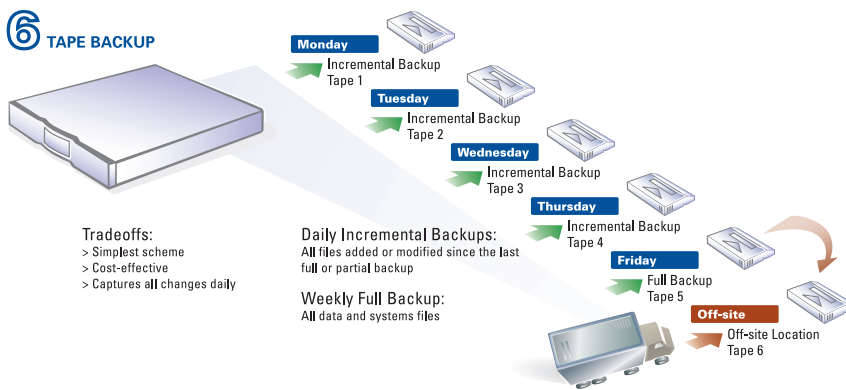


Guide to Data Protection Best Practices

Two Common Tape Rotations

While each individual business will have its own unique set up backup requirements, there are two common tape rotations that balance performance, cost and safety. The most simple and least expensive solution is the six-tape (or tape set) rotation. This consists of two alternating full backup tapes and one partial backup tape per day (based on a five-day work week). Expanding this to seven tapes gives you a separate full backup for off-site storage and keeps you from overwriting your only full backup copy. The chart below shows how you might create a six-tape schedule in a month:

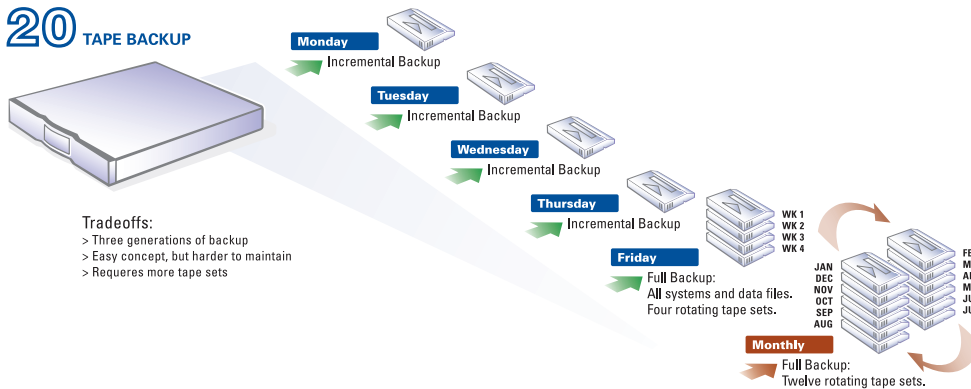
MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
				Friday 1
Monday	Tuesday	Tuesday	Thursday	Friday 2
Monday	Tuesday	Tuesday	Thursday	Friday 3
Monday	Tuesday	Tuesday	Thursday	Friday 4
Monday	Tuesday	Tuesday	Thursday	Friday 5
Incremental, Differential, or Full				Full



Guide to Data Protection Best Practices

The other common scenario—and the one most commonly used—is the Grandparent/Parent/Child scheme. Requiring approximately 20 tapes (or tape sets for larger amounts of data), it calls for partial backups on a daily basis on the “child” tapes, full backup weekly on the “parent” tapes and full backup monthly on the “grandparent” tapes. This chart shows how you might create a rotation schedule:

MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
				Week 1
Monday	Tuesday	Tuesday	Thursday	Week 2
Monday	Tuesday	Tuesday	Thursday	Week 3
Monday	Tuesday	Tuesday	Thursday	Week 4
Monday	Tuesday	Tuesday	Thursday	Month 5
Incremental, Differential, or Full				Full



However, remember these are only two possible scenarios and your own business needs will determine the most appropriate scenario for your business.

ROTATION METHOD	ADVANTAGES	DISADVANTAGES
SIX-TAPE	Requires only a few tapes, which provides an easy and cheap rotation method. It's ideal for small data volumes (as much capacity as one tape can hold).	Keeps only a week's worth of data, unless you regularly archive the full-backup tapes.
GRANDPARENT-PARENT-CHILD (GPC)	Provides the most secure data protection and implements monthly archival of tapes. It's also a simple method, supported by most software.	Requires more tapes, which can become expensive.

Review, Test, Revisit

Implementing the program itself is only the beginning. After it is underway, businesses must review the program to make sure it meets current rules and regulations. Employees must be assigned responsibility and receive regular training and reminders so they understand their roles. Their compliance must also be regularly reviewed. All of this involves dedicating some budget for program maintenance, testing and enhancement. It is also a smart idea to regularly test both the backup and recovery functions of the system to make sure it works as planned. Various threats and scenarios that can affect the business can be simulated so that employees can experience the process firsthand, such as practicing the recovery of a file that is several weeks old. Also, it is important to be aware that the business' backup and archiving needs may change as the business grows and changes.

Guide to Data Protection Best Practices

Best Practices Checklist

This checklist is provided as a guide to help outline your company's backup and archiving plan to secure your data and minimize costs.

- Network data backup plan—types of data
 - > Data files
 - > Operating systems
 - > Databases
 - > Application programs
 - > Application settings
 - > Windows device drivers
 - > Network settings
- What data can be archived to tape to free up disk storage resources, and reduce running costs
- How long must data be archived?
- Quantity of data to be backed up
 - > How much data will typically be stored in a full backup?
 - > How often will a full backup be done?
 - > How much data will typically be stored in a partial backup?
 - > How often will a partial backup be done?
- End user desktop and notebook backup scheme
 - > Desktop, notebook environments
 - > Application programs
 - > Application settings
 - > Data files
 - > Address books
- End user data backup recommendations (copy to network first)
- End user data recovery checklist—what to do and what not to do when suspecting data loss
- Network administrator data recovery checklist
- Prioritization: Which data to back up first
- Data backup strategy (schedule of full and partial backups)
- Choice of backup hardware with an eye to automation
- Choice of backup software
- Archive strategy (on-site and off-site backup storage locations)
- Tape management (how many tape sets; rotation plan)
- Restore process actually tested prior to needing it
- Capital investment budget (hardware, software, implementation)
- Operating budget—recurring costs

Guide to Data Protection Best Practices

Conclusion

Corporate data protection is now a critical business imperative. Businesses today must institute backup and archiving storage best practices to mitigate business risks, guarantee compliance, reduce costs and help improve the overall success of the business. The failure to properly manage and safeguard vital corporate data can result in business disruption, losses or the potential failure of the business itself.

Businesses must first develop an appropriate strategy and then make the right technology choice from multiple storage options in order to establish backup and archival storage best practices. Regardless of size or industry, it is vital for any business to implement a records management and storage process so that:

- Storage becomes highly reliable and error-free
- Archived assets are easy to preserve, locate, reuse and resell
- Archival storage becomes the standard, rather than a luxury
- Disaster recovery best practices can be instituted

With a perspective gained from more than 30 years in the storage business, Tandberg Data or its resellers can help design the most appropriate infrastructure to meet the unique needs and characteristics of your individual business. Your data is too precious not to be protected by the best, most affordable and highly efficient data storage solution in the industry.



About Tandberg Data

Tandberg Data is a leading global supplier of data protection solutions for small and medium-sized businesses. The company's wide range of cost-effective storage products and services provides customers with best-in-class tape, disk, removable disk and software solutions for backup, archiving and disaster recovery. These solutions are marketed through a global channel of qualified resellers, distributors and major server OEMs. An extensive service and support network supports all Tandberg Data products worldwide.

WP-BestPractices_EN_2011A

Tandberg Data GmbH
Feldstrasse 81
44141 Dortmund
Germany
Tel: +49 (0) 231 5436 - 0
Fax: +49 (0) 231 5436 - 111
00 800 8263 2374 (00 800 TANDBERG)
salesemea@tandbergdata.com
www.tandbergdata.com/emea

Tandberg Data Corporation
10225 Westmoor Dr., Ste. 125
Westminster, CO 80021
USA
Tel: 303.442.4333
Fax: 303.417.7170
Toll Free: (800) 392-2983
sales@tandbergdata.com
www.tandbergdata.com/us

Tandberg Data (Japan) Inc.
Dai 6 Ito Building 5F,
4-4-7 Ebisu, Shibuya-ku,
Tokyo, 150-0013
Tel: +81 3 5475 2140
Fax: +81 3 5475 2144
TDJ_sales@tandbergdata.com
www.tandbergdata.com/jp

Tandberg Data (Asia) Pte. Ltd
7 Tai Seng Drive
#02-00
Singapore 535218
Tel: +65 6593 4700
Fax: +65 6281 7358
salesapac@tandbergdata.com
www.tandbergdata.com/apac