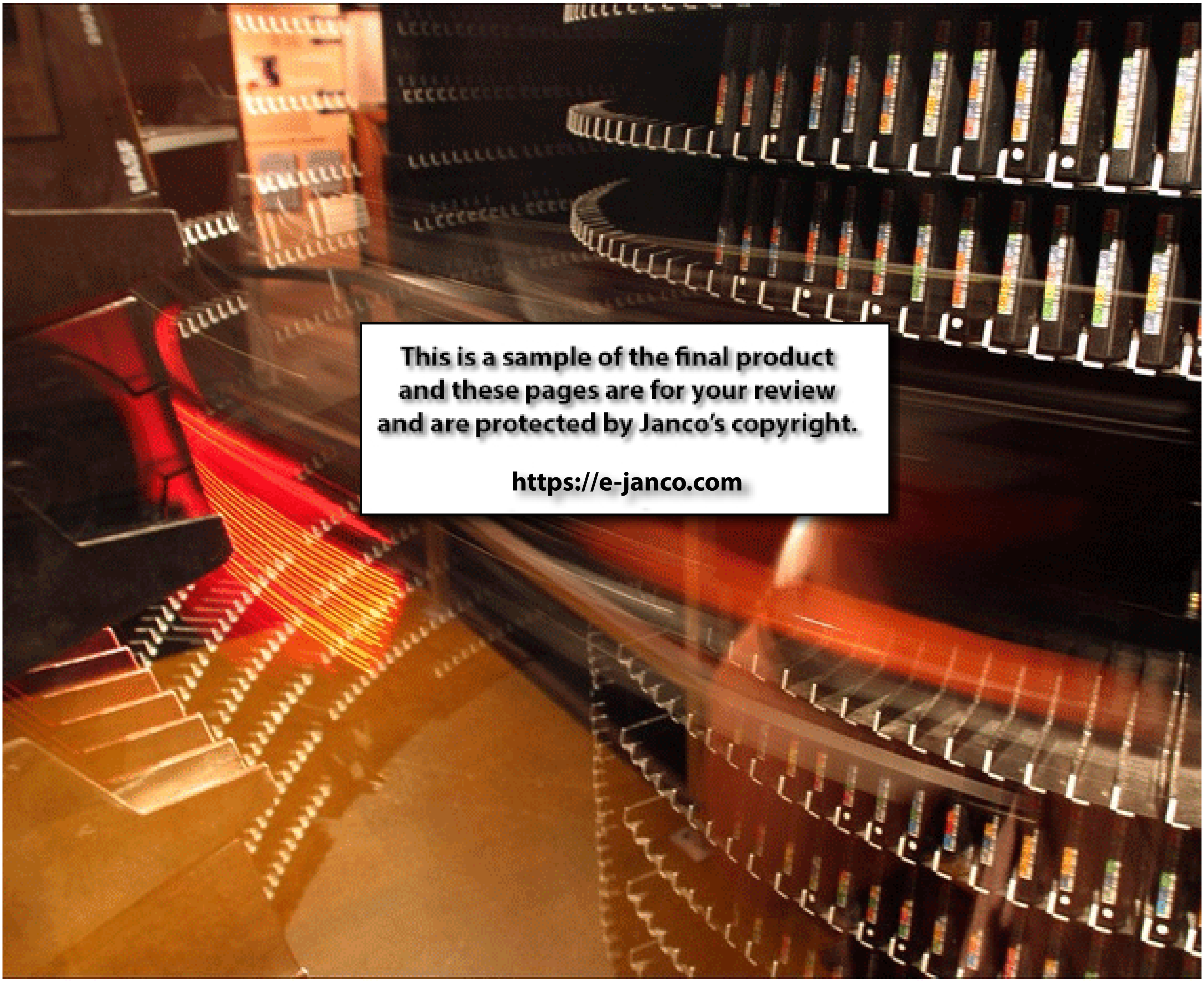

Backup and Backup Retention Policy

Janco Associates, Inc.

2024

Table of Contents

Backup and Backup Retention Policy

Policy

The purpose of this policy is to define the need for performing periodic computer system backups to ensure that mission-critical administrative applications, data and archives, and applications, users' data, and archives are adequately preserved and protected against data loss and destruction. Each ENTERPRISE unit responsible for providing and operating a mission-critical application must document and perform System Specific Data Backup or at least Minimal Data Backup periodically.

Computer systems that create or update mission-critical ENTERPRISE data daily need to be backed up to minimize the exposure to loss of mission-critical data. The unit responsible for providing and operating such systems must conduct a systematic and detailed investigation of all the influencing factors leading to the compilation of a comprehe policy must at least fulfill the requireme

Applicab

This policy to protect the following situations:

- Deliberate and/or accidental deletion of files with computer viruses etc
- Inadvertent deletion or overwriting of files
- Technical failure of storage device (head crash)
- Faulty data media
- Demagnetization of magnetic data media due to aging or unsuitable environmental conditions (temperature, air moisture)
- Interference of magnetic data media by extraneous magnetic fields
- Uncontrolled changes in stored data (loss of integrity)
- Enterprise assets that are processed and stored at remote locations including Work From Home

Backup Versus Archive

A backup process takes periodic or real-time images of active data to provide a method of recovering records that have been deleted or destroyed. Most backups are retained only for a few days or weeks as later backup images supersede previous versions.

A backup is designed as a short-term insurance policy to facilitate disaster recovery, while an archive is designed to provide ongoing access to decades of business information. Archived (historical) records are placed outside the traditional backup cycle for a long period, while backup operations protect active data that are changing frequently.

There are now over 10,000 regulations in place throughout the world that require records to be held for certain periods including Sarbanes Oxley (US); European Union Data Protection Act (EU) - GDPR; Electronic Ledger Storage Law (Japan); AIPA (Italy); and HIPPA (USA) to name but a few. Companies that do not comply face hefty financial penalties, bad PR, and even imprisonment for key board members.

Storage Management

Storage Management is a data storage process that moves data between high-cost and low-cost storage media. Storage Management is needed because high-speed storage devices, such as hard disk drive arrays, are more expensive (per byte stored) than slower devices, such as optical discs and magnetic tape drives. While it would be ideal to have all data available on high-speed devices all the time, this is prohibitively expensive. Instead, Storage Management policies are set so that the bulk of the backup data is on slower devices, and then backup data is transferred to faster disk drives when needed.

Minimal Backup Policy

Type of Data	Minimal Backup Policy	Backup Retention Policy
System software	Latest Version plus patches At Least Weekly	Annual (verified) Backup Monthly Generations Weekly Generations
Application software	Latest Version plus patches At Least Weekly	Annual (verified) Backup Monthly Generations Weekly Generations
System data	Daily	Annual (verified) Backup Monthly Generations Weekly Generations Daily Generations
Application Data	Daily with real-time transaction files	Annual (verified) Backup Monthly Generations Weekly Generations
Data (WFH)	weekly	Weekly Generations

Storage

Backup media, documentation on its use, and necessary hardware and software should be stored in a fireproof[1] and protected location. In the case of magnetic media, they should be in a case or vault that is shielded from electromagnetic radiation. For maximum safety, the archive media should be stored at a site that is removed from where the backup media is to be used if necessary.

Cloud Backup

Cloud backup, also known as online backup, is a strategy for backing up data that involves sending a copy of the data over a proprietary or public network to an off-site server. The server is usually hosted by a third-party service provider, who charges the backup customer a fee based on capacity, bandwidth, or the number of users. In the enterprise, the off-site server might be proprietary, but the chargeback method would be similar.

Online backup systems are typically built around a client software application that runs on a schedule determined by the level of service the customer has purchased. If the customer has contracted for daily backups, for instance, then the application collects, compresses, encrypts, and transfers data to the service provider's servers every 24 hours. To reduce the amount of bandwidth consumed and the time it takes to transfer files, the service provider might only provide incremental backups after the initial full backup.

Capital expenditures for additional hardware are not required and backups can be run dark, which means they can be run automatically without manual intervention.

In many enterprises, cloud backup services are primarily being used for archiving non-critical data only. Traditional backup is a better solution for critical data that requires a short recovery time objective (RTO) because there are physical limits to how much data can be moved in a given amount of time over a network. When a large amount of data needs to be recovered, it may need to be shipped on tape or some other portable storage media.

Cloud Storage versus Traditional Storage

Factor	Cloud Storage	Traditional Storage
Amount of Data	Best when the total amount to protect is less than 100 GB per 1 M e s c	For large amounts of data or environments with limited
Rate of Data Change	B le p	and tape, with tape transport off-site are more appropriate

[1] Fireproof typically means that if there is a non-catastrophic short duration fire the media will survive. It is best to have multiple copies in multiple distant locations.

Backup - Best Practices

There are best practices for backup and long-term data retention that are recommended by Janco Associates, Inc. They are:

Store data prudently and understand when to store and when to destroy

Consider the value of different types of data that must be stored, and how that value changes over time. While keeping all data close at hand on high-speed disks might seem ideal for access purposes, in reality, to do so could be prohibitively expensive in terms of both hardware purchases and the cost of power, cooling, and physical space, especially when compared with tape storage.

In a study, the University of California at Santa Cruz showed that 90% of data stored on NAS was never accessed again, and another 6.5% of the data was only accessed once more. It has been estimated that more than 95 percent of data stored is rarely accessed beyond 90 days after it wa

Separate

Sep a files on a
sep d it could be the
dif stem to a previous
sta

Manage your backup processes, procedures, equipment, software, and media

A best practice is to have a set of defined policies and procedures that manage and control it. The policies and procedures should include:

- Craft the processes and procedures you need to ensure backups are completed properly, including assigning responsibility for getting backups accomplished and monitoring the effort to spot problems, while also ensuring that those responsible are sufficiently trained.
- Ensure that backup copies are valid and can be successfully restored, which requires that you rank the importance of your data and establish ways that the most important data is backed up first and restored first. Be sure that you have adequate time to back up all the data that is important to your business, and be sure to understand the time required to restore that data in case of loss or corruption. This includes regularly checking and testing your equipment, media, and processes.
- Ensure that backup copies are safe. This means storing your backups in a logically and physically secured offsite location. It also means ensuring that you haven't backed up viruses and other malware, spam, and data that is not important or that is harmful to your business.
- Maintain backup logs so you — and your auditors — can track backup activities.
- Regularly revisit your backup/restore risks, procedures, and technologies to make sure they are adequate for business needs and conditions to evolve.
- Dispose of backup media carefully, making sure that they are physically destroyed so that their contents cannot be read by the unauthorized.

Cloud Backup – Best Practices

There are best practices for cloud backup and long-term data retention that are recommended by Janco Associates, Inc. They are:

- **Define specific business requirements for cloud data backup**. Don't forget to also address customer needs.
- **Conduct a Total Cost of Ownership (TCO) analysis**. Use a provider that can integrate archives, so you can move data sets from a backup plan to an archive plan and provide online search and retrieval functionality.
- **Encrypt the backup**. To ensure security, encrypt backup data. Store the encryption key in a place that is secure and will be available if you lose your facility.
- **Utilize Data De-Duplication**. Data de-duplication reduces overall storage and data transmission requirements. This, in turn, lowers storage and transmission costs.
- **Fol** ompliance related
  to involved, or
  co d insurance
  im
- **Tra** miliar with
  pr edia storage to
  you eded for large data
  re

- **Do not depend 100% on your cloud**. Back up locally and remotely — to both on-premise and cloud storage.
- **Have a local copy of all publicly accessible cloud data**. Back up the data locally before storing it in the cloud.
- **Have multiple cloud vendors**. Multiple vendors to mitigate risks and provide options when a recovery process is in place.
- **Test the entire process before you depend on it**. Validate that the backup and recovery process will work in your environment when there is a major outage. Ensure that backed-up data can be recovered on-premise or to another cloud vendor.
- **Include BYOD and WFH**. With the move towards BYOD devices and WFH the requirements and implications for backup need to be considered.

Mobile Device and Work From Home Users Backup - Best Practices

There are best practices for cloud backup and long-term data retention that are recommended by Janco Associates, Inc. They are:

- **Implement Work From Home Backup Processes** – Define procedures for WFH users
- to back up their devices. Include safeguards to be able to recover data that WFH users created or used.
- **Automatic Process to Purge WFH Data** - Have processes in place to purge data automatically when a WFH user is terminated or leaves the organization.
- **Backup Frequently** - Mobile Devices are just that so whenever you are at your base back up to your office or home computer. If you have access to the cloud, consider utilizing backup services that reside there.
- **Security Considerations** - Mobile data often is sensitive therefore only utilize solutions that are enc nts.
- **Re** d capacity. If you try ost. Sometimes a sim
- **Wr** rage devices sho ecovery operations. SD t them before attempting a recovery operation. Removable USB drives are more difficult since Windows does not have a way to manually mount their file systems as read-only.

  There is a Registry setting that works with Windows XP SP2 and higher; it forces all USB mass-storage devices into read-only mode. First, create a whole new key: ***HKLM\System\CurrentControlSet\Control\StorageDevicePolicies****.*

  Then create a REG_DWORD entry in it called ***WriteProtect.*** *Set it to 1 and you'll be able to read from USB drives but not write to them.*

- **Be patient** - If you're using a program that supports deep scanning at the cost of a slower recovery process, use it. The speed of this type of scan depends on your system's CPU rather than its I/O, as most of the work involves matching file signatures and checking for false positives.
- **Safely Unplug Mobile Devices** – USB devices, memory cards, and sticks generally tolerate immediate removal, but safely eject these devices before removing them. This reduces the possibility that data will be lost.

Electronic Forms

Three (3) Electronic forms are included with this policy template. They come separately in their directory.

Security

- Outsourcing Security Compliance Agreement
- Telecommuting Work Agreement

Disaster Recovery

- Remote Location Contact form
- Vendor Contact Information form
- Work From Home Contact Information form

Job Descriptions

One (1) job description is included with this policy template. It comes in its directory.

- Manager Artificial Intelligence
- Manager Compliance
- Manager Disaster Recovery and Business Continuity
- Manager Security and Workstations
- Manager WFH Support Manager WFH Support

What's New

2024

- Added section on AI use in backup and recovery strategy
- Added Job Descriptions
  - Manager Artificial Intelligence
  - Manager Compliance
  - Manager Disaster Recovery and Business Continuity
  - Manager Security and Workstations
- Updated forms
- Updated job description
- Updated graphic tables

2023

- Added materials to include Work From Home (WFH)
- Updated forms
- Updated job description
- Updated graphic tables

2022

- Added section on cloud backup "Best Practices"
- Updated forms to 2022 Edition
- Updated job description to 2022 Edition
- Updated graphic tables

2021

- Updated to include WFH
- Updated all included electronic forms
- Divided included forms into two categories – Disaster Recovery and Security
- Added forms
  - Work From Home Contact Information form
  - Telecommuting Work Agreement form
- Added a job description – Manager WFH Support