



This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.

<https://e-janco.com>

Backup and Backup Retention Policy



2025



Table of Contents

Table of Contents.....3

Backup and Backup Retention Policy.....4

 Policy.....4

 Applicability4

 Backup Versus Archive.....4

 Archiving Implications Sarbanes-Oxley5

 SOX – Section 8025

 Record Retention Requirements.....5

 Artificial Intelligence Impact on Backup and Recovery.....5

 Types of Backups7

 Storage Management8

 Minimal Backup Policy8

 System Specific Backup Policy13

 Backup Retention.....15

 Documentation and Backup Media Labeling.....15

 Issues to Manage with SLAs for Backup.....17

 Proposed Service Level Agreement Metrics18

Appendix.....19

 EU Safe Harbor Act Compliance and Data Backup Conflicts.....20

 Backup - Best Practices21

 Cloud Backup – Best Practices24

 Mobile Device and Work From Home Users Backup - Best Practices.....25

 Electronic Forms26

 • Outsourcing Security Compliance Agreement

 • Telecommuting Work Agreement

 • Remote Location Contact form

 • Vendor Contact Information form

 • Work From Home Contact Information form

 Job Descriptions.....27

 • Manager Artificial Intelligence

 • Manager Compliance

 • Manager Disaster Recovery and Business Continuity

 • Manager Security and Workstations

 • Manager WFH Support Manager WFH Support

What’s New28



Backup and Backup Retention Policy

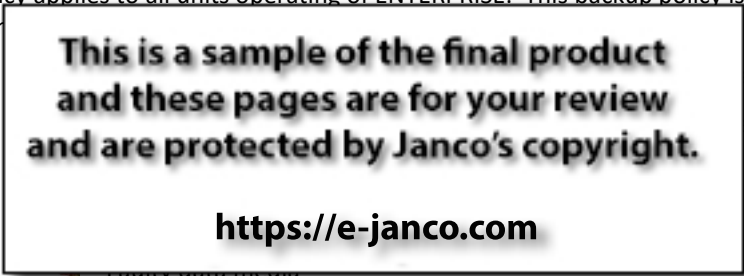
Policy





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 comprehensive System Specific Data Backup Policy. System-specific backup policies must at least fulfill the requirements of the Minimal Data Backup Policy.

Applicability

This policy applies to all units operating of ENTERPRISE. This backup policy is defined to protect the following situation



-  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.



Types of Backups

Backups are created to avoid situations of losing precious data. Backups can be created daily, weekly, or monthly basis. Backups prove useful at the time of data loss, data inaccessibility, software malfunctions, drive corruption, etc. Before a backup strategy is developed, the types of backups that be performed need to be understood. Defined below are five (5) types.

Type of Backups	Description	Appropriate Use
Full Backup	<p>A full backup creates a copy of every file on a storage device. It is also the most costly in terms of effort, time, and dollar output.</p> <p>The media for this can be static (tape, an optical disk), dynamic (disk to disk), or cloud</p> <p>These backups are often used as mandated archive copies.</p>	<p>Annual (verified) Backup Monthly Backup Weekly Backup Daily Backup</p>
Incremental Backup	<p>An incremental backup creates copies of only those files or records on a storage device that have changed since the last backup. It is also more complex to restore when a complete file needs to be restored but it takes less effort to create.</p>	<p>Weekly Backup Daily Backup</p>
Data Replication	<p>tolerance, or accessibility. The same data is stored on multiple storage devices – either in the same physical location or in a remote location via network connectivity</p>	<p>Real-Time</p>
Data Deduplication	<p>Data deduplication (often called "intelligent compression" or "single-instance storage") is a method of reducing storage needs by eliminating redundant data. Only one unique instance of the data is retained on storage media, such as a cloud, disk, or tape. Redundant data is replaced with a pointer to the unique data copy.</p> <p>This is often used for emails where the same email can be stored in several user accounts or for attachments that are duplicated.</p>	<p>Annual (verified) Backup Monthly Backup Weekly Backup Daily Backup</p>
Transaction Log Backup	<p>A transaction log backup creates copies of only those records (in some cases before and after images of records) on a storage device that have changed since the last backup. It requires a version of the application program to run all of the transactions since the last full backup</p>	<p>Daily Backup</p>

This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.

<https://e-janco.com>



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 Data	Latest Version plus	Annual (verified) Backup Monthly Generations Weekly Generations
Application Data	Daily with real-time transaction files	Annual (verified) Backup Monthly Generations Weekly Generations Daily Generations
Software licenses, encryption keys, & Protocol Data	Weekly	Annual (verified) Backup Monthly Generations Weekly Generations
Mobile Device Data (WFH)	On connect or at least weekly	Monthly Generations Weekly Generations

This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.

<https://e-janco.com>

© 2025 Copyright Janco Associates, Inc. - <https://e-janco.com>



System Specific Backup Policy

Type of Data	System Specific Backup Policy	Backup Retention Policy ²
System software ³	Latest Version plus patches At Least Weekly	Annual (verified) Backup Monthly Generations Weekly Generations
Application support software ⁴	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
Application Data	Daily with real-time transaction files	Annual (verified) Backup Monthly Generations Weekly Generations Daily Generations
Software keys & Protocol Data	Weekly	Annual (verified) Backup Monthly Generations Weekly Generations
Mobile Device Data (WFH)	On connect Exception Report for failure to back up at least weekly	Annual (verified) Backup Monthly Generations Weekly Generations

This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.

<https://e-janco.com>

² In the mainframe world versions are called “generation” we have opted to use the term generations. Annual backups rarely are used in the recovery process rather they are used as archival copies to meet mandated and audit requirements.

³ System software includes both Operating Systems (OS) and application support systems such as SQL and SAP.

⁴ This is vendor or third party supported software that is necessary to operate



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

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>



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



**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>








What's New





2025

-  Updated forms
-  Updated job description





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