Back-up and recovery policy

Template

Content

[Authority and review 3](#_Toc160453441)

[Document control and review 3](#_Toc160453442)

[Version management 3](#_Toc160453443)

[Intro 4](#_Toc160453444)

[Responsibilities 4](#_Toc160453445)

[Backup and recovery procedure 4](#_Toc160453446)

[RPO and RTO 5](#_Toc160453447)

[Access to backup and encryption 5](#_Toc160453448)

[Offsite backup 5](#_Toc160453449)

[Back-up monitoring 5](#_Toc160453450)

[Recovery test 5](#_Toc160453451)

[ANNEXES 6](#_Toc160453452)

[Intro 6](#_Toc160453453)

[ANNEX 1: GFS Backup Schedule 7](#_Toc160453454)

[What is Grandfather-Father-Son backup? 7](#_Toc160453455)

[The principle of GFS backup rotation 7](#_Toc160453456)

[Example of a G-F-S scheme 7](#_Toc160453457)

[Schematic representation G-F-S 7](#_Toc160453458)

[Types of data backup techniques 8](#_Toc160453459)

[Full data backup 8](#_Toc160453460)

[Incremental data backup 8](#_Toc160453461)

[Differential data backup 8](#_Toc160453462)

[Mixed data backup 8](#_Toc160453463)

[ANNEX 2: 3-2-1 backup strategy 9](#_Toc160453464)

[3-2-1 backup rule 9](#_Toc160453465)

[The importance of the 3-2-1 rule 9](#_Toc160453466)

[3-2-1 backup management 10](#_Toc160453467)

[3-2-1 SUMMARY 10](#_Toc160453468)

# Authority and review

## Document control and review

|  |  |
| --- | --- |
| **Document check** |  |
| Author |  |
| Owner |  |
| Date created |  |
| Last revised by |  |
| Last revision date |  |

.

## Version management

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date of approval** | **Approved by** | **Description of change** |
| 1.0 |  |  |  |

# Intro

Critical information and information systems must be protected against data loss and data damage. Backup and recovery procedures enable us to restore information in case of disaster scenarios such as system failure, fire, accidental deletion or malware outbreak.

Backup is not necessary when data loss is acceptable or when other control measures are used to overcome disaster situations. A common example is a PLC system that contains a static configuration that can be easily redeployed or replaced in case of a disaster.

This policy document is part of a set of policy documents that **support [Organisation]** in establishing a sound cybersecurity strategy.

# Responsibilities

The owner is responsible for an efficient backup and recovery process that meets business needs. Operational tasks can be delegated to system administrators or vendors.

# Backup and recovery procedure

A backup and recovery procedure must be in place for all critical systems. The backup procedure should define the following topics:

-What information are you backing up (systems AND data)?

-Make a backup

-Backup monitoring

-When and how often to backup?

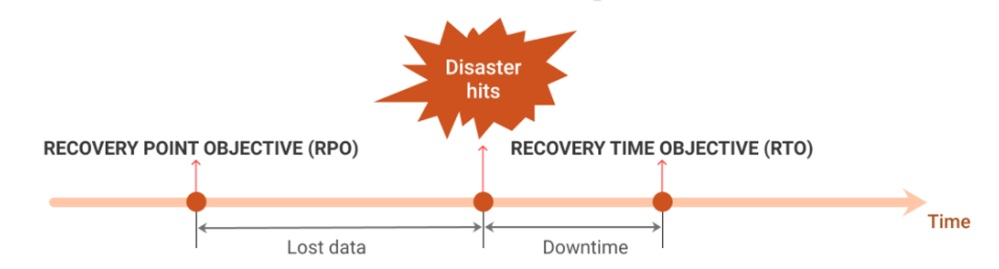
-How long to keep the backup?

-How and where to store the backup?

-How backup data is transferred?

## RPO and RTO

The backup procedure should meet business needs for RPO (recovery point objective) and RTO (recovery time objective), e.g. based on risk assessment and information classification.



The RPO defines the maximum period during which data can be lost due to a major incident. For example, if a static copy is made every night at 2 a.m., the maximum data loss is 24 hours.

RTO (recovery time objective) is the length of time required to recover data.

For this, use the GFS scheme, for example. (**See ANNEX 1: GFS Backup Schedule.)**

## Access to backup and encryption

Access to backups should have at least the same level of protection as the original data. When confidential backup data is physically or logically stored or transported in a way that the data could be available to unauthorised persons, the data should be encrypted.

Examples include:

* Network traffic for backup.
* Backup media stored or transferred by persons who should not have access to the original data.
* Backup files on media stored in a location that may be accessible to persons who should not have access to the original data.
* The backup encryption key needed to decrypt the off-site media should not only be stored on-site.

## Offsite backup

To avoid loss of both the information and the backup, backup data should be stored in a different physical location from the data itself whenever possible. An overview of off-site media should be available. For this, use the 3-2-1 backup strategy, for example. (**See ANNEX 2: 3-2-1 backup strategy**)

## Back-up monitoring

The backup process should be monitored to ensure proper operation and to address errors. Proper operation should be able to be demonstrated by logs, reports or an automated system.

## Recovery test

For all backup methods used for critical systems, recovery tests should be performed at least once a year. An operational restore (unplanned) outside a scheduled periodic test restore can be counted as a recovery test.

# ANNEXES

## Intro

Both diagrams in subsequent annexes can be deployed separately.

The **Grandfather-Father-Son** (GFS) backup schedule is used in environments with relatively large amounts of data or systems, when one does not have enough time to perform backups between a certain time and/or when it is important to be able to go back in time far and in detail. this schedule does not take into account the backup media or location of the backups.

The **3-2-1** scheme is often taken as a basis. This means you have at least three full copies on two different media. Important here is that one of the different media is in a different location. However, the 3-2-1 rule does not talk about the RPO-RPO of the backup.

As explained earlier, both schemes can be used separately. However, there is added value in combining both with each other. The GFS scheme focuses on the RPO-RTO of the data, whereas the 3-2-1 strategy focuses on storing the backups made.

The following example clarifies the use of both principles:

All data are on a NAS (Network Attached Storage) with the disks in RAID 10\*. Via a backup server, this NAS is backed up every night on a separate NAS. This NAS is linked to the backup server via a separate network. A full backup of the data currently takes more than 12 hours. To still back up the changing data, the GFS schedule is chosen. The weekly and monthly backups are additionally copied through to a secure cloud environment. In this way, we have combined the 3-2-1 strategy with the GFS backup schedule. [\*https://en.wikipedia.org/wiki/Nested\_RAID\_levels](*https:/en.wikipedia.org/wiki/Nested_RAID_levels)

The following figure provides a schematic representation of the above



## ANNEX 1: GFS Backup Schedule

### What is Grandfather-Father-Son backup?

The GFS backup rotation technique is a popular **data backup** method that allows full and partial copies to be combined to different media to both reduce backup time and improve storage security. Many articles can be found on what the grandfather-father-son backup strategy entails.

### The principle of GFS backup rotation

In the grandfather-father-son backup technique, the three planned steps create backups:

* The **"grandfather (G)"** - full backup to a particular site, one off site or multiple sites ;
* The **"father (F)"** - another full backup, more regularly, to faster storage;
* The **"son (S)"** - incremental backup (or differential backup) to the same storage as "father"

### Example of a G-F-S scheme

The GFS schedule starts with the **daily backups**. Usually, there are four backup media labelled for the day of the week they are backing up, for example, Monday to Thursday. Each tape is called for use on the labelled day. If only a one-week version history of files is maintained, then each tape is overwritten every week. To keep a 3-week version history of files (recommended), more tapes are needed. For example, this week's Monday tape will not be overwritten for another 3 weeks.

**Weekly backups** follow a similar scenario. A set of up to five weekly backup media is labelled "Week1", "Week 2", and so on. Full backups are recorded weekly on the day a "Son" media is not used. According to the above example, these would be "Friday" tapes. This "Father" medium is reused monthly. Five weekly tapes are needed to keep a file history of one month, as some months have 5 weeks

The last set of three media will be labelled "**Month1**", "Month2" and so on, depending on which month of the quarter they will be used. This "Grandfather" media records full backups on the last business day of each month. If your backup plan follows a fiscal business calendar, your monthly tape will take the place of the Week 4 or Week 5 weekly/Father tape, depending on the month. If your backup schedule follows calendar months, then your monthly backup will vary throughout the year, replacing a daily or weekly tape. Usually, monthly tapes are overwritten quarterly or annually (recommended), depending on version history requirements.

### Schematic representation G-F-S

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Monday** | **Tuesday** | **Wednesday** | **Thursday** | **Week 1** |
| **Monday** | **Tuesday** | **Wednesday** | **Thursday** | **Week 2** |
| **Monday** | **Tuesday** | **Wednesday** | **Thursday** | **Week 3** |
| **Monday** | **Tuesday** | **Wednesday** | **Thursday** | **Month1** |

### Types of data backup techniques

Every file backup software offers at least one data backup method, the full backup, for copying an entire data set to a final bit. However, other data backup types exist, often to save time and space for regular backups. These backup types are:

* **Full backup** - complete copying of data as described earlier;
* **Partial backup** - only copy data changed after the last backup:
  + **Incremental backup** - only copy data changed after the last incremental backup
  + **Differential backup** - only copy data changed after the last full backup
* **Mixed backup** - a sequence of full backups and some partial backups, repeatedly rotated:
  + Mixed incremental backup - a chain of full and single incremental backups;
  + Mixed differential backup - a set of full and single differential backups.

Full backup is a basis for any differential backup or incremental backup, as well as mixed backups.

### Full data backup

A full backup assumes that every time you run the task, the entire data set is copied to the chosen location. A full backup takes up a lot of space, time and PC resources and often makes many unnecessary data copies, because most of the data in the dataset does not undergo any changes between backups.

### Incremental data backup

Incremental backup processes only files that have appeared or changed since the previous incremental backup. After an initial full backup, each subsequent backup will be incremental, storing only a difference between the current dataset and a previous incremental copy.

### Differential data backup

Differential backup is very similar to incremental backup, but uses different types of data backup strategies. After an initial full backup, each subsequent backup will be incremental, storing only a difference between the current dataset and a previous incremental copy.

### Mixed data backup

This approach is a combination of the two different types of backups: full and partial backups (incremental or differential). It is also similar to a versioned backup technique. In this method, a full backup takes place followed by a fixed amount of partial backups.

## ANNEX 2: 3-2-1 backup strategy

The **3-2-1 backup** is a proven data protection and recovery method to ensure that data is adequately protected and that up-to-date backup copies of the data are available when needed. The basic concept of the 3-2-1 backup strategy is to make three backups of the data to be protected, store the backups on two different types of storage media and send one backup of the data to another location.

In the classic 3-2-1 backup scenario, backup software is used to back up mission-critical data, with the backup of the data stored on another on-premises data storage device. During that process, or immediately afterwards, two more backups of the data are stored on two other devices; traditionally, at least one of those devices was a tape library. Tape was a standard part of the process because it was easy to create a portable backup of the data in the form of a tape cartridge that could be easily shipped off site. In many environments, however, tape has been replaced by a hard disk storage system.

Although the 3-2-1 backup approach has been a cornerstone of data protection in large and small data centres for decades, it is a concept still embraced by most backup software and hardware vendors as "best practice" for the effective use of their products. Vendors acknowledge that the general concept is still valid regardless of how or where a company stores its data -- even as new requirements and big data have made the 3-2-1 equation slightly more complicated.

### 3-2-1 backup rule

The 3-2-1 backup strategy consists of three rules:

* **Three data copies**. Three copies of backups of all critical data should be made regularly -- daily or more often -- including the original data and at least two backups.
* **Two types of storage.** Two different storage types should be used to store the data. Both copies of the backup data should be stored on two different storage types to minimise the risk of failure. Types of storage devices may include an internal hard drive, external hard drive, removable storage drive, tape library, secondary storage array or cloud backup environment.
* **One off-site location**. One copy of the backup data should be sent to an off-site storage facility. At least one data copy should be stored at an off-site location to ensure that natural or geographical disasters cannot affect all data copies. This copy may be physically delivered to the off-site location, as with tape-based backups, or may be replicated to the secondary location via telecommunication facilities.

### The importance of the 3-2-1 rule

The 3-2-1 backup strategy is recognised as a "best practice" for information security and data protection professionals. While the process does not guarantee that all data will never be compromised in any way, the strategy eliminates some of the risks associated with backup procedures. The 3-2-1 methodology is important to ensure that there is no single point of failure for data. An organisation is covered not only if a copy becomes corrupted or if a technology fails, but also if there is a natural disaster or theft that destroys the physical storage types.

The data recovery process using the 3-2-1 method would look as follows:

* Original (active) data has been corrupted, damaged or lost. If the production copy of data is not available, the first alternative is to restore the required data from the backup copy stored internally on another media or secondary storage system.
* Second data copy is unavailable or unusable. If the system - tape or disk - used to store the second data copy is not available or if the data copy is damaged, outdated or otherwise unusable, the off-site copy must be retrieved to the internal servers.
* Restart the 3-2-1 process as soon as possible. Once a suitable data copy has been attached and operation restored, the backup process should restart as soon as possible to ensure that the data remains adequately protected.

These days, backups are not just insurance policies that are tucked away until something goes wrong. Companies get more value out of their backup datastores by using that data for things like developing and testing new applications. Contemporary approaches to programming, such as DevOps, require easy access to data as close as possible to live application data to ensure that applications are developed properly in a real-world environment. Backup data fulfils this perfectly well, as it is likely to be freshly generated regularly and frequently.

Analytical applications may also need access to large amounts of current data. By using fresh backup data, the results of the analytical process are likely to be more reliable and accurate. Stricter controls and management of data companies are needed to ensure that these applications get the best possible data, while maintaining the primary concepts of 3-2-1 backup. Note that if one of the backup copies is used for application development or analytics, it may be modified or unavailable, rendering one of the required three copies unusable if recovery is required.

Data integrity has always been a key concern in data protection activities. It is not enough to just back up data and lock away the copies; it is necessary to ensure that backups are complete, undamaged and recoverable. Recovery testing helps with this, as does using some of the more advanced features that backup apps offer to detect ransomware and other threats. Again, these concerns do not necessarily get in the way of a 3-2-1 backup approach, but they can add some steps to the process, such as regularly scheduled recovery tests.

### 3-2-1 backup management

There are some basic principles for a successful 3-2-1 backup implementation:

* All data copies are identical and up-to-date.
* The media on which the copies are stored are readable media.
* All specimens and equipment are tested and confirmed to be working.
* Remote copies are stored securely.
* Recovery of single/multiple files or a full backup is regularly tested.
* Internal data copies are on different storage systems and networks and cannot be accessed from outside the company.

The backup software used in the 3-2-1 process can be very useful because it can automatically control the disposition of backups while cataloguing all backup activity. Most backup apps have also added features to check for threats such as malware, ransomware and viruses in backup copies.

### 3-2-1 SUMMARY

**Store 1 of these offsite (**secure storage, cloud,...)

2 different media

Keep data on at least **2 types of storage**.  
 (Local disk, NAS, Tape,...)

Make **3 copies** of backup data.   
 (1 primary and 2 backups

1 copy off-site

3 copies of data