No Problem IT
Safe. Secure. Sorted.

BACKUP, DISASTER RECOVERY & BUSINESS CONTINUITY

Disaster Recovery and Data Backup.

How important is data to your business? The answer is that it is probably essential as we all rely on data to run our systems every day - it is something we may even take for granted.

But what would happen if you were to suffer some form of catastrophic data loss?

Data loss is when data has either been deleted or corrupted and can no longer be accessed. There are several ways in which this can occur, such as hardware failure, problems with software, or human error.

Having a solid backup and disaster recovery strategy is essential for minimising the impact of unplanned downtime on your business. Backing up can take some effort, but thanks to new software, hardware, and services, it's easier than ever.

Backup and Disaster Recovery Defined.

Backup is the process of copying data, so it is available in case of loss or damage. Your backed up data is protected and can be restored if needed.

Disaster recovery involves the plans and processes for re-establishing access to data and IT resources after an outage – with minimal disruption to business operations.

Understanding the backup terms RTO and RPO

RTO – Recovery Time Objective

How long your business can go without accessing critical data? That is how long before the consequences of the failure become damaging to business?

The RTO defines how much downtime a business can cope with, i.e., the amount of time between the unexpected failure and when access to critical data must be restored.

RPO – Recovery Point Objective

How much data are you willing to lose in the event of a disaster?

The RPO defines how much time can pass during a disaster, before the amount of data lost exceeds the company's allowable threshold or tolerance. E.g., if the last good copy of data is 12 hours ago and your RPO is 20 hours than it is still within the parameter.

Business Continuity

Business Continuity is about having a plan to deal with critical data loss, so your organisation can continue to function with as little disruption as possible.

321 – The industry standard for backup

Having just one copy of data is not always enough.

For example, if your business has data backed up to an external drive which is kept in a different location, you have a backup copy.

However, if the other location incurs a natural disaster (a fire for example), it would not be possible to access your original data or data copy from either location.

For this reason, it is recommended to follow the 321-backup rule. This includes also having a server with a local image, stored in off-site location.

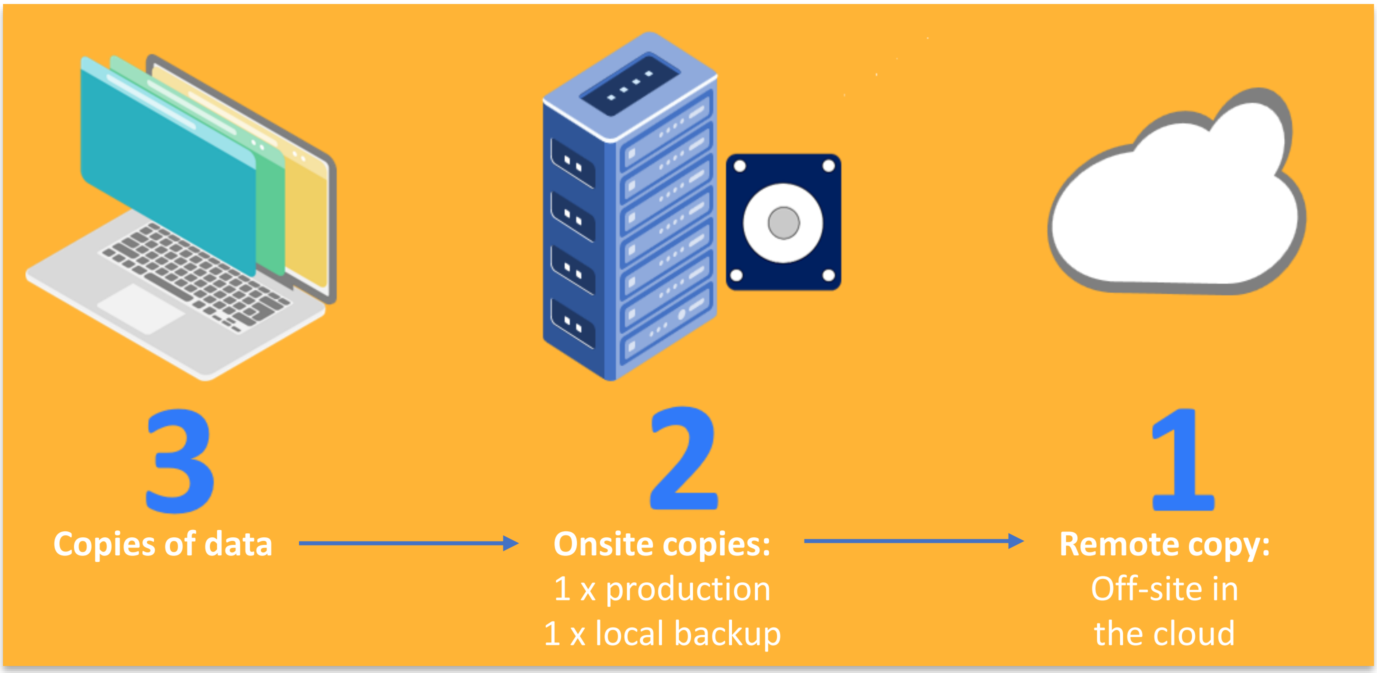
So, businesses have:

The original data | Copied data on an external hard drive | One copy stored off-site in the cloud.

Did you know?

40% of small businesses do not backup their data.

60% of small businesses do not recover from critical data loss.



3 **Copies of data** → **2** **Onsite copies:** 1 x production 1 x local backup → **1** **Remote copy:** Off-site in the cloud

The 321 backup rule results in the quick recovery of data - as you always have something ready to go.

In the event of a local failure and disaster, you can connect somewhere and access critical data.

Microsoft 365 is a good use of Business Continuity, especially as if one of their datacentres go down for any reason, you can always access your data from another one.

Backup Solutions available through No Problem IT

Traditional Backup:
Local and Cloud Based

Image-Based Backup:
VEEAM and Storagecraft

Cloud:
Acronis and Microsoft 365

Traditional: Local and Cloud Backup

This method of data backup and recovery backs up files and folders to hard disk storage, either locally or in the cloud. This is a good solution if you are concerned purely about data. As an example, a traditional nightly backup of data to a local disk would have an RPO of up to 24 hours. The RTO can be anywhere from a couple of hours, up to a week depending on volume of data: 10MG could take 25 mins to download whereas 7GB would take closer to 7 days.

Disk backups are still widely used and provide a reliable form of file and folder backup. Depending on speed of connection and volume of data, they can produce several RPO's of several backups in a day.

Remote Working: with this method, a backup agent is installed on each machine that needs to be backed up. In the case of agentless VM backup, sometimes no agents are required with a local server.

Image-Based Backup using VEEAM and Storagecraft

Servers can be either individual piece of hardware, or more commonly these days virtual machines on a single hypervisor (a virtual machine monitor, that is computer software, firmware or hardware that creates and runs virtual machines).

In both cases, the process would be to create a backup image of the entire server on a regular basis to be able to restore files, folders or even the entire server in the event of a failure. The options for backing up in either scenario is different. StorageCraft is used to back up the single hardware server and Veeam to back up the virtual server.

On Premise Solution: Uses external storage on a NAS or similar to hold the server images locally.

Cloud solution: In addition to, or as a replacement to local storage,
the images are pushed to the cloud.

veeam

StorageCraft

VEEAM is a single platform solution for businesses with multiple servers, be it cloud, virtual and / or physical servers.

VM Backup provides a simple, reliable, and flexible solution for all organizations, from SMB to Enterprise

Storagecraft is a single cross-platform solution that protects a mixed, hybrid environment.

Its backup and disaster recovery software works alongside VEEAM to ensure business systems and data (both on-premises and Remote Office) are fully protected and always available.

Cloud: Microsoft 365 and Acronis Data Security

Cloud-based backup and recovery provide organisations with access to systems and data in a secure, virtual environment. Microsoft 365 has a wide range of powerful services, and many features and benefits such as reduced downtime, flexibility, and lower upfront costs.

The difference between availability and backup

Despite its many benefits, there are some valid concerns regarding data loss and protection for any business using Microsoft 365. The primary aim of 365 is to provide their customers with an 'always on' service. Although they do have backups and retention policies, they refer more to availability and not recovery. Microsoft's backup policies help determine who is responsible for the data loss:

Microsoft's responsibilities:

- Hardware failure
- Software failure (on the server's side)
- Natural disaster
- Power outage (in a datacentre)

Customers' responsibilities:

- Human error
- Software errors (on the customer's side)
- Malware attacks
- Hacker attacks
- Malicious insiders

Microsoft's Recovery options:

Sharepoint: items deleted are stored in a secondary recycle bin for 93 days, after which they are deleted permanently. As a result, that data becomes irretrievable.

Exchange Online: deleted emails are sent to a folder where they are stored for 30 days. Items deleted from there are sent to a secondary 'Recoverable Items' folder, with a 14-day default retention period.

One Drive: like Exchange Online, this has a 30-day retention period for items belonging to deleted accounts to be recovered. However, once the 30 days have elapsed, deleted data cannot be retrieved.

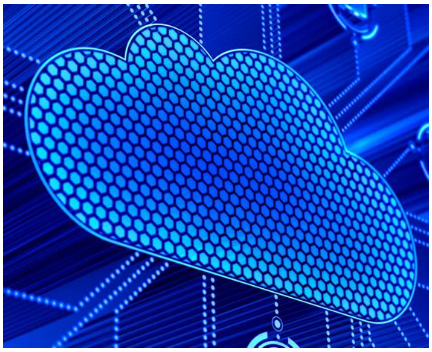
How to keep data protected with Microsoft 365

While Microsoft 365 offers excellent security, privacy and compliance policies, the bottom line is that their service-level agreement addresses availability, not recovery.

Ultimately, the responsibility of data backup and protection of highly sensitive company data or mission critical data lies on the customer.

So, data loss and protection are still a concern when using Microsoft 365, but this worry can be avoided when we combine it with a complete backup and recovery solution like Acronis.

Although Microsoft 365 has ways of restoring data, the process can be time-consuming and complicated. This is why it's worth using an expert 3rd party solution to take responsibility for data.

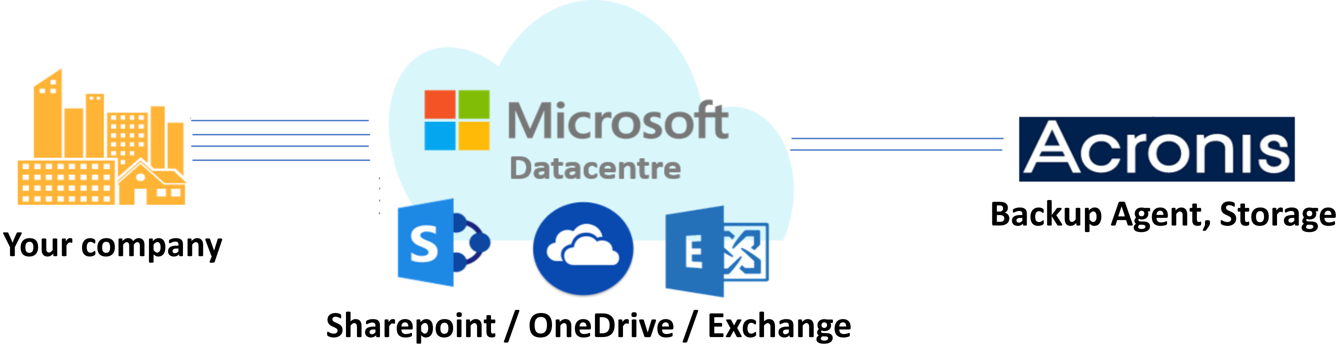


Acronis Backup for Home and Business

NPIT partner with Acronis, the global leader in backup technology, to provide **'No Problem 365 Backup as a Service'**. All Exchange and SharePoint 365 data is backed up *directly* to the Acronis Tier 4 datacentres in London. This is done via a cloud-to-cloud link that does not require local computer agents to be installed.

Recovery of data is simple – just call and within minutes we can find the email, file or folder that has been deleted / corrupted.

With this solution you can be confident in the knowledge that your Microsoft 365 Email and Data is compliant for all the recovery, retention, and data security regulatory requirements of your business.



Your company

Microsoft
Datacentre

Sharepoint / OneDrive / Exchange

Acronis
Backup Agent, Storage

No Problem IT's Complete Protection Solution

No Problem IT are here to help with all your data protection and ongoing security needs.
We provide hands-free IT support that will help ensure all your data is kept as safe as possible.

Services include:

- **Critical Data Security Consultation:** define your business' RTO and RPO and structure the data backup and retention policies accordingly.
- **Set up industry-standard backup routine of your data:** including all business-critical data and server images as required for your business.
- **Full data migration:** to Cloud and Microsoft 365
- **Patching and Updating Systems:** carrying out regular, security updates and ensuring that systems are operating to the highest standard. This is to overcome problems regarding critical stability and other major risks.
- **Carrying Out Upgrades:** ensure software and hardware on your network is up-to-date and business compliant.

Protect Your Business from Data Loss
To find out more about the services that we offer, get in touch today.

No Problem IT
enquiries@npit.co.uk **020 3358 8000** npit.co.uk