cmi The business IT experts

Your Data Backup and Disaster Recovery Policy

Every day, your business creates vast swathes of data; data which travels further, manages more processes and is shared across a wider range of technologies than ever before. That's why a Data Backup and Disaster Recovery Policy is crucial

Before the COVID outbreak over 50% of businesses worldwide didn't hold a documented Disaster Recovery Plan

On average, 33% of all sensitive folders on any business server are not protected from unauthorised access

Almost half of all UK businesses (46%) and a quarter of charities (26%) suffered a cyber security breach in 2020

The average time to contain the impact of a breach is 280 days – or 315 days from a malicious attack

Compromised credentials and misconfigured folders were the main cause for almost 20% of malicious data breaches

Understanding RTOs and RPOs

Two crucial elements of your Disaster Recovery Policy are your Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)

Recovery Time Objective (RTO)

The RTO covers the amount of time your business can reasonably operate during a data disaster, before it starts suffering from serious setbacks.

Recovery Point Objective (RPO)

The RPO asks how many hours you can afford to lose in a breach; typically, an acceptable time frame between a data breach and the most recent data backup.

Understanding RTOs and RPOs isn't only about creating manageable timeframes, but also identifying the nature and volume of data that needs protecting, and the proportionate solutions.

6 Steps to a Diligent Disaster Recovery Plan

Before setting out your Disaster Recovery policy, you need to develop a tried and tested recovery plan. Here's everything that's crucial to yours.

Know Your Infrastructure

First, conduct a full inventory of your hardware and software. Identify your crucial solutions and what the impact of any compromises might be. Consider systems that are crucial to business applications, and those which will need resolving most rapidly.

Conduct a Business Impact Analysis

With the assistance of department and technical admins, identify the impact that different impact scenarios could have on their technologies. Determine your RTOs and RPOs, and crucial technologies that could severely impact the business if compromised.

Establish Roles and Responsibilities

Everybody has their role in a disaster event – from preventing to recovering. Nonetheless, your plan should designate emergency roles and points of contact in the event of an emergency. Points of communication with vendors, partners and third-parties should also be clarified.

Identify and Prioritise Data

Your business has a responsibility to numerous data compliance legislations, so it's important to identify your most sensitive data, where it resides and how it is protected. Your next priority is crucial operations data – anything that gets your systems back up and running as quickly as possible.

Deploy Recovery and Backup Solutions

Once you've identified all that needs protecting, you then need to deploy the right technical response; typically, this will be a Cloud solution or on-prem hardware. Ensure that data backups are regular and conducted well within RPO goals, and that your backup sites are designated specific data and recovery roles.

Test Regularly

With everything in place, it's essential to test your Data Backup and Disaster Recovery Policy regularly and in a controlled environment. A Managed Service Provider could regularly manage and monitor your backups and will test your setup regularly at the point of installation.

Enshrine Your Policy

Cement everything you've tested and implemented into your Data Backup and Disaster Recovery Policy.

Your Policy Document

Your policy document provides legal and technical definitions that ensure everything is adhered to, outlining:

- The purpose of the document
- The scope of your Data Backup and Disaster Recovery Plan
- Your internal and external resources
- Your designated hardware and backup utilities
- Methods for acceptable regular backups
- Acceptable backup reporting metrics
- Management and migration of media
- Retention periods
- Company policies
- Compliance responsibilities

Implementing a Data Backup and Disaster Recovery Policy can be difficult – and that's before you deploy the necessary hardware and software. With our Data Backup and Disaster Recovery Policy template, you've everything you need to set your company safety in stone.

DOWNLOAD

cmi The business IT experts

References (L-R)
1: https://www.mercer.com/content/dam/mercer/attachments/global/gl-2020-mercer-covid-19-global-survey-coronavirus-impact-to-global-market.pdf
2: https://info.varonis.com/hubfs/docs/research_reports/2021-Financial-Data-Risk-Report.pdf
3: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020
4 and 5: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf

0800 023 2696
hellocmi@newcmi.com