EXIGENT

Disaster Recovery Checklist

Stay one step ahead of potential disaster with a reliable data backup and recovery plan

When it comes to data backup and recovery, being prepared for potential disasters - both manmade and natural - is a critical element of business continuity and success. That's why it's crucial to have a disaster recovery solution you trust.

Before disaster hits, ask yourself:

- Do we have a disaster recovery strategy in place? If yes, is it trustworthy?
- When was the last time we tested our backup and disaster recovery solution?
- How long does it take to fully recover from a disaster with our current solution?
- How long can our organization realistically be down? 1 hour? 1 day?
- What is the financial impact of downtime for our business?
- When a physical disaster strikes, is there an offsite copy of our data available?

As you create a disaster recovery plan, consider these steps:

Identify types of disasters that could impact your business and outline how to determine what is happening. Consider:

- Natural disasters in your geography
- Hardware or software malfunction
- Cyber attack
- Internal sabotage
- Long-term power or internet outage

Understand how each type of disaster would effect your business. Evaluate the potential impact on data, employees, access control, customer service, production, supply chain, communications and more.

Consider what technology you will use in your process to operational recovery:

- File restore
- Local virtualization
- Off-site virtualization

Establish recovery priorities and goals. Assess the types of data and systems your organization has, create a way to categorize each type, and determine the priority for restoring data and systems according to type.

If the original systems within your organization need to be restored, determine your process: bare metal restore or virtual machine restore.

How will you confirm and test recovery? Consider network testing, equipment recovery, file and data restoration and how to then confirm user access to all resources and data.

Don't forget to include contact information for key personnel who will guide the disaster recovery response as well as external vendors that may need to be involved.