SOUTH EAST iT
YOUR TECHNOLOGY PARTNER

7-Step Business Continuity Checklist

How to Keep Your Business Running During an IT Disruption

http://southeastit.com.au

Downtime Is No Longer a Rare Event

Cyberattacks, system failures, and human error can disrupt business operations at any time. For small and mid-sized businesses, even a short outage can lead to lost revenue, reduced productivity, and damage to customer trust.

The good news is that most disruptions can be planned for. This checklist will help you understand your risks and take practical steps to keep your business running.

Step 1

Understand What Downtime Would Cost Your Business

Not all systems are equal. Some are critical to daily operations, while others can wait.

Start by identifying your most important systems and how long your business could operate without them. This helps you focus recovery efforts where they matter most.

Why this matters

Without clear priorities, recovery efforts can be slow and misaligned with business needs.

Ask Yourself

	YES	NO
Do you know which systems must be mended first?	☐	☐
Do you have a defined target for how quickly your business needs to be back up and running?	☐	☐
Do you understand what downtime would cost our business per hour per day?	☐	☐

An IT provider can help you define recovery priorities and timelines.

Step 2

Know Where Your Data Lives

Your business data may be spread across servers, cloud platforms, employee devices, and third-party applications.

Create a simple inventory of:

- **Critical files and databases**
- **Cloud applications (Microsoft 365, Google Workspace, etc.)**
- **Local systems and devices**

Why this matters

You cannot protect or recover what you do not fully understand.

Ask Yourself

	YES	NO
Do you know where all critical data is stored?	☐	☐
Are all the systems we rely on being actively managed?	☐	☐

An IT provider can help map your environment and identify gaps.

Step 3

Make Sure Your Data Is Properly Backed Up

Backups are your safety net, but not all backups are created equal.

Effective backups should be:

- **Automatic and frequent**
- **Stored securely and separately from your main systems**
- **Protected from being altered or deleted**

Why this matters

Many modern attacks target backups first. If backups fail, recovery becomes significantly harder.

Ask Yourself

	YES	NO
Are backups happening consistently?	☐	☐
Are backups stored in a secure, separate location?	☐	☐
Can backups be accessed quickly in an emergency?	☐	☐

An IT provider can design a backup plan tailored to your business and test it regularly to avoid surprises.

Step 4

Confirm You Can Actually Recover Your Data

Having backups is only part of the solution. You need to know they work.

Regularly test:

- **How quickly data can be restored**
- **Whether systems come back online as expected**
- **Whether key applications function after recovery**

Why this matters

Unverified backups often fail when they are needed most.

Ask Yourself

	YES	NO
Has your company tested a full recovery in the last 12 months?	☐	☐
Did your last recovery meet your target restoration time?	☐	☐

An IT provider can run recovery tests and validate your readiness.

Step 5

Secure Access to Your Systems

Many cyberattacks start with compromised login credentials. This risk grows as employees access systems across hybrid and remote work environments.

Reduce risk by:

- **Using multi-factor authentication (MFA)**
- **Limiting administrative access**
- **Monitoring login activity across devices and locations**

Why this matters

If attackers gain access through a single compromised account, they can often move laterally across systems undetected.

Ask Yourself

	YES	NO
Are all critical systems protected with MFA?	☐	☐
Do employees have only the access they need?	☐	☐

An IT provider can implement and manage secure access policies that protect your systems without slowing down your team.

Step 6

Ensure Your Team Can Operate During a Disruption

Disruptions don't always happen at convenient times. Whether it's a cyber incident, system outage, or office disruption, your team needs to be able to continue working.

Ensure you have:

- **Secure access to systems from multiple locations**
- **Clear communication channels during an incident**
- **Defined processes for continuing critical work**

Why this matters

Business continuity depends on your team's ability to keep operations moving, even when normal conditions are disrupted.

Ask Yourself

	YES	NO
Could our team continue working if key systems or locations were unavailable?	☐	☐
Do we have a clear way to communicate during an incident?	☐	☐

An IT provider can help ensure your team can stay productive during disruptions.

Step 7

Have a Clear Response Plan

When something goes wrong, speed matters. A clear plan helps reduce confusion and downtime.

Your plan should define:

- **Who is responsible for what**
- **How incidents are reported and escalated**
- **Steps to contain and recover from disruptions**

Why this matters

Without a plan, response times increase and impact worsens.

Ask Yourself

	YES	NO
Do we have a documented response plan?	☐	☐
Does everyone know their role in an incident?	☐	☐

An IT provider can help you define recovery priorities and timelines.

You Don’t Have to Do This Alone

Managing business continuity and cybersecurity can be complex, especially as threats continue to evolve.

An experienced IT provider can help you:

- **Identify risks and vulnerabilities**
- **Implement secure backup and recovery solutions**
- **Monitor systems and respond to threats**
- **Build a long-term continuity strategy**

Take the First Step Towards Resilience

If you answered “no” to any of these questions or weren’t sure how to answer, a quick assessment with a trusted IT provider can show you exactly where you stand and help you build a stronger, more resilient business.

SOUTH EAST iT
YOUR TECHNOLOGY PARTNER

Contact Us Today

03 9111 1740

http://southeastit.com.au