

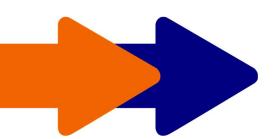
BUSINESS CONTINUITY AND SECURITY CHECKLIST

This checklist will help you understand what computer systems and processes need to be in place to ensure your business and network is secure, reliable, and recoverable.

This checklist is general in nature, and not everything will apply to all businesses.

If you have unticked boxes, speak to your IT support about what your needs are, or call us and we will work with you to put in place a cost effective solution.

DACKOI	
All files are backed up	
Any websites are backed up	
All emails are backed up, and deleted emails can be recovered	
Backups meet any legal data retention requirements	
A current copy of backups are always kept offsite	
Backups run automatically	
Backups, and the restore process have been tested	
DISASTER RECOVERY	
There is a documented disaster recovery plan	
The plan includes emergency replacement of computer equipment including	
laptops desktops, servers and network equipment	ш
There is a plan to recover all data	
All Line of Business software licenses/keys are saved and backed up	
I know how long I can afford to be off line and out of action	
There is a plan to handle inbound telephone calls	
EMAIL	
Effective SPAM filtering is in place	
Viruses are blocked before reaching my network	
Email systems are reliable	
Emails are signed using SPF, DKIM & DMARC	
I can synchronise my email contacts and calendars between all my devices	



RACKIID



NETWORK AND SECURITY

All computers have antivirus protection	
Antivirus software is monitored and kept up to date	
A firewall is in place and all open ports are documented	
Dangerous websites that can cause harm are blocked	
Staff understand Phishing and ransomware attacks	
Wi-fi is secure and has strong passwords	
Guest Wi-fi users can access the internet only and have no internal access	
Web content filtering is in place	
Laptop hard drives are encrypted	$_{-}\square$
Staff can only access information that is directly relevant to their job	
All staff have individual logins, no shared logins	$_{-}$
When a staff member leaves, all their access can be blocked	
Individual passwords are strong and not recorded anywhere	$_ \Box$
Two Factor Authentication is enabled	
RELIABILITY	
Computers are maintained, and software updated	
Internet connections are reliable and stable	
Automatic failover to a second internet connection is in place	
A UPS is installed on all essential equipment	
When services on servers stop, they are detected and automatically re-started	
Server hard disks can break without data loss or downtime	
Servers continue to operate/shutdown gracefully in a power outage	
Servers can be remotely started	
All computers send alerts of potential problems, before they arise	
All computers send alerts when components break	
SUPPORT	
Support staff are familiar with all systems	_ 🖳
Staff know who to contact for assistance	
Support staff are aware of my disaster recovery plan	_ ∐
Support staff are available and easily contactable	
A full record exists of all technical issues experienced	_ ∐
All system settings are documented	▮ٰ
Staff have access to technical "how to" help and documents	_ ∐
Support staff are able to remotely connect without assistance	
Remote support is fast and capable, Onsite support is rarely needed	Ш
MOBILITY SOLUTIONS	
Staff can securely work remotely	
Data and systems are remotely accessible	
Office phone system is remotely accessible	

