
Before an

- ☐ Critical systems and data listed with owners
- ☐ Backups run automatically and at least one copy is off-site or offline
- ☐ A test restore has been completed in the last 6 months
- ☐ Admin passwords stored securely with an emergency access procedure
- ☐ Multi-factor authentication on email and finance systems
- ☐ Software licences and installers documented
- ☐ IT support contact and contract details recorded

During re

- ☐ Isolate affected devices if malware is suspected
- ☐ Confirm which backup point to restore from (RPO)
- ☐ Restore systems in priority order from the BIA
- ☐ Verify data integrity before resuming work
- ☐ Record every action in the incident log

Notes