# Backup Protection Against Ransomware

## A Practical Checklist for IT Managers

*For IT managers in UK businesses, schools, colleges, and multi-academy trusts*

| # | CONTROL | IN PLACE | PARTIAL | GAP | OWNER / NOTES |
|---|---|---|---|---|---|
| 1 | **Backup repositories audited for network exposure**<br>*Are any backup targets directly accessible from your production network using standard credentials? Attackers reach what they can reach.* | ☐ | ☐ | ☐ | |
| 2 | **At least one offline or air-gapped backup copy maintained**<br>*The 3-2-1-1-0 standard requires one copy that cannot be reached, modified, or deleted from within your primary network — even by an authenticated admin account.* | ☐ | ☐ | ☐ | |
| 3 | **Immutability enforced at the storage level**<br>*Software-level immutability can be disabled by a compromised admin account. Hardware-enforced immutability cannot. Confirm which your environment has. (Only available via Object First)* | ☐ | ☐ | ☐ | |
| 4 | **Backup administrator credentials protected under privileged access management**<br>*Ransomware groups harvest credentials specifically to authenticate against backup consoles and delete recovery points before triggering the visible attack.* | ☐ | ☐ | ☐ | |
| 5 | **Retention window reviewed against current threat timelines**<br>*Modern ransomware operators typically move within four to six days. A retention window of at least 14 to 30 days with active monitoring coverage reduces the risk of having no clean restore point.* | ☐ | ☐ | ☐ | |
| 6 | **Full restore test completed within the last 90 days**<br>*A backup that has never been restored is not a backup. It is an assumption. Document the test, the result, and the time taken.* | ☐ | ☐ | ☐ | |
| 7 | **Cyber insurance policy reviewed for backup-related requirements**<br>*A growing number of insurers expect immutable backup or air-gapped copies as standard controls. Confirm your policy requirements and ensure you can evidence them.* | ☐ | ☐ | ☐ | |

☐ In place — operates as documented ☐ Partial — exists but not fully operational ☐ Gap — absent or unverified

### WHERE MOST ORGANISATIONS NEED TO START

The most common gap we find is not the absence of a backup solution — it is a backup strategy that was designed for a simpler threat environment and has not been reviewed since. If you are uncertain whether your current posture would survive a ransomware attack, the practical starting point is two questions: is immutability enforced at the storage level, and when did you last test end-to-end recovery under realistic conditions?

**Design and Management Systems Limited**
2A–4 Avery Hill Road, New Eltham, London, SE9 2BD
Company Registered in England No 054112088 · VAT No: 863 6963 77

Tel: 01322 420140
dmsystem.co.uk · enquiries@dmsystem.co.uk