IT & DATA SERVICES

Offsite Data Storage

Keeping all of your data in one place — on-site, on a single platform, or under a single point of failure — is one of the most common and most consequential risks an organisation can carry. Our offsite data storage service provides secure, documented, and independently held copies of your critical data and physical records, giving you the resilience, compliance evidence, and recovery capability your business depends on when it matters most.

WHY OFFSITE STORAGE MATTERS

Ransomware, fire, flood, theft, hardware failure, and accidental deletion are all capable of destroying on-site data without warning. Organisations that store their only backup in the same environment as their primary data are, in practice, operating without a meaningful recovery capability. Offsite storage ensures a clean, uncompromised copy exists regardless of what happens to your primary environment — a fundamental requirement of any credible business continuity or disaster recovery plan, and a regulatory expectation under UK GDPR.

STORAGE OPTIONS

Cloud & Managed Backup

Encrypted, automated backup to secure, geographically separated cloud infrastructure. We assess your backup posture, identify coverage gaps, and implement solutions meeting your RTO and RPO requirements.

- RTO & RPO assessment
- Encrypted, automated backup
- Regular restore testing

Tape & Media Vaulting

Secure collection, transportation, and offsite vaulting of backup tapes and removable media — with full chain-of-custody documentation and scheduled rotation for an air-gapped backup copy.

- Secure collection & transport
- Environmentally controlled vault
- Scheduled rotation & retrieval

Physical Records Storage

Paper-based records subject to regulatory retention stored securely offsite in indexed, catalogued storage. We manage collection, barcoding, inventory, and on-demand retrieval.

- Indexed & barcoded storage
- On-demand retrieval
- Retention schedule management

Document Scanning & Archiving

Physical records digitised and stored as encrypted, searchable digital archives — reducing physical storage requirements while maintaining accessibility and compliance.

- High-volume scanning
- OCR & searchable PDF output
- Encrypted archive storage

Immutable & Air-Gapped Backup

Ransomware targets backup infrastructure first. Immutable, write-once storage ensures a protected, unalterable copy exists beyond the reach of any attack — with recovery validation and testing.

- WORM storage architecture
- Ransomware-resilient design
- Recovery validation & testing

Backup Audit & DR Review

Many organisations assume their backups work — until they need them. We independently audit your backup and recovery capability, testing restores and validating whether your arrangements would support real recovery.

- Backup coverage review
- Restore testing & validation
- RTO/RPO gap analysis

DID YOU KNOW?

- An estimated 93% of ransomware attacks specifically attempt to destroy or encrypt backup data before deploying the main payload.
- The 3-2-1 rule — three copies of data, on two different media types, with one offsite — is the minimum baseline recommended by the NCSC.
- Many organisations discover during an incident that their backups have been silently failing for weeks or months — untested backups offer no more protection than no backup at all.
- Storing backup media in the same building — even in a fireproof safe — does not constitute offsite storage and will not satisfy most business continuity frameworks or insurers.
- Cloud backup alone is not always sufficient — without immutability controls, a compromised admin account can delete cloud backups just as easily as on-premises ones.

Whether you need a backup audit, a managed offsite arrangement, or help designing a resilient recovery architecture, we can help.

services@apexpointdata.com