IT POLICY

SECURE DATA BACKUP & RECOVERY

Secure Data Backup & Recovery

Backup data and archive data must be stored off-site at a professional data storage facility or a geographically distant second Operating Company managed site, in a secured, environmentally controlled room. Backup media must be encrypted and transported in a secure fashion.

Backups

The configuration of the backup process (i.e. the lists of systems and data) must be documented and must be configured to comply with OCU Data Handling and Retention Policy.

Failed backup jobs must be tracked, and the cause and remediation documented.

Back up jobs must be configured so that current-month financial data can be restored within 1 business day (assuming that the IT infrastructure is fully operational).

Restore Testing

Regular backup and data restoration tests must be performed for all servers storing financial, HR, payroll, data from clients where the contract requires it, and other business-critical data.

Test results should be documented as well as all corrective action taken for any failures.

Backup Monitoring

Test results of the restore of whole applications and their data sets must be documented and reviewed for improvement to restoration procedures.

Signed.....Date: 15/01/21
Brian Lynch – Head of IT

Signed.....Date: 15/01/21
Vince Bowler - Managing Director