ISMS BACKUP POLICY

Introduction

In order to ensure business continuity in the event of information on the Organisation's systems being destroyed or corrupted, it is vital that our data is backed up regularly and reliably. In addition, it may be advisable to make and keep hard copies of certain information for future reference or confirmation.

Responsibilities

The Internal IT Manager is responsible for arranging daily backups and event log monitoring.

Application Software

1. The Organisation uses proprietary software that is covered by application and user licenses.

2. The Internal IT Manager ensures that any purchased software is recoverable in the event of loss of the equipment on which it is installed.

Specific SAAS backups regimes include:

- Autotask Workplace is backed up automatically with snapshots available at file and folder level each time a file is deleted.
- Other cloud services such as Continuum, Autotask PSA, Office 365 etc. are all provided by vendors who have achieved ISO certifications so our data is secure within their cloud.
- Files held in office 365 applications including outlook are stored in a recycle bin for 30 days before being deleted.

Cloud Storage Backup

The Organisation ensures that its cloud storage is backed up at agreed intervals by the cloud services provider and that this is verified at suitable intervals by documentary evidence.

Policy Sign-off

Date of Issue:	27/10/2020
Date of Next Review:	15/10/2021
Name:	Tim Barber
Signed:	

Amendment History

Version	Modified On	Modified By	Comments
1.0	15/09/2020	Jo Holloway	
2.0	27/10/2020	Jo Holloway	Update of responsibilites
3.0	27/10/2020	Jo Holloway	Date change