**CB Training Services Limited**

**Cyber Security Policy**

**Policy Objective**

The purpose and objective of this Information Security Policy is to protect CB Training Services Limited information assets (including data printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or video, spoken in conversation), from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage and maximise return on investment and business opportunities.

**The Policy**

Information will be protected from a loss of: confidentiality (ensuring that information is accessible only to authorised individuals); integrity (safeguarding the accuracy and completeness of information and processing methods) and; availability (ensuring that authorised users have access to relevant information when required).

Regulatory and legislative requirements will be met (this includes the requirements of legislation such as the Companies Act, the General Data Protection Regulations, the Computer Misuse Act and the Copyright, Design and Patents Act).

CB Training Services Limited continuity plans will be produced, maintained and tested (this will ensure that information and vital services are available to users whenever they need them).

Information security training will be made available to all staff where applicable.

All breaches of information security, actual or suspected, will be reported to, and investigated by, the Information Security Manager.

Guidance and procedures will be produced to support this policy. These may/will include incident handling, information backup, system access, virus controls, passwords and encryption.

The role and responsibility of the designated Information Security Manager is to manage information security and to provide advice and guidance on implementation of the Information Security Policy.

The designated owner of the Information Security Policy, Chris Bateman, has direct responsibility for maintaining and reviewing the Information Security Policy.

All managers are directly responsible for implementing the Information Security Policy within their business areas.

It is the responsibility of each employee to adhere to the Information Security Policy.

The Policy will be reviewed by the designated owner of the Information Security Policy – typically not more than 1 year from the date approved.