Workbooks

Information Security Policy

Workbooks' objective is to preserve the confidentiality, integrity and availability of information that it either owns or is entrusted with.

To achieve these objectives, the company has implemented an Information Security Management System (ISMS) in accordance with the international standard ISO/IEC 27001. Within the Workbooks ISMS are a number of topic specific policies and control documents, which are available to all Workbooks employees

The purpose of this policy is to protect Workbooks' assets from all relevant threats, whether internal or external, deliberate or accidental.

It is the policy of Workbooks that:

- Information is made available with minimal disruption to staff and customers as required by the business process;
- The integrity of this information is maintained;
- Confidentiality of information is preserved;
- Regulatory, legislative and other applicable requirements related to information security are met;
- Appropriate information security objectives are defined and, where practicable, measured;
- Appropriate Business Continuity arrangements are in place to counteract interruptions to business activities and these take account of information security;
- Appropriate Information security education, awareness and training is available to staff and relevant others working on behalf of the company;
- Breaches of information security, actual or suspected, are reported and investigated through appropriate processes;
- Appropriate access control is maintained and information is protected against unauthorized access; and
- Continual improvement of the information security management system is made as and when appropriate.

This policy is approved by senior management and is reviewed at regular intervals or upon significant change.

Workbooks is ISO 27001:2013 certified. A copy of the certificate can be found here.

Physical security of our servers is achieved through their being located in CCTV-monitored Tier-1 data centres in the UK with biometric systems, certified entry procedures and 24x7 manned security.

Availability is achieved through using buildings with redundant power and air-conditioning systems and through the use of two physically-separate locations with a high-speed network connecting them. Our policy is to implement systems with no single points of failure. All hardware has remote-management capability.

Network security is achieved through the application of multiple layers of protection, including packet filters/ ACLs, firewalls, and other techniques which are confidential. External specialist organisations are used to perform vulnerability scans at the network level and to do more involved penetration testing. All data transfer happens under strong encryption; all access to the Workbooks secure website uses 256-bit SSL. Careful design. All systems are built on the principle of 'least privilege' such that processes run with the minimum set of capabilities and software is not present on the operational systems unless it is specifically required. The operating system is under tight

version control and we closely monitor for reports of security vulnerabilities in the OS and its components.

Our Development and QA processes are geared towards a controlled release cycle with a focus on avoiding security vulnerabilities and data corruption. The processes are extensive and include both automated and manual testing at many levels: unit, integration, system and functional. System changes are only permitted under a full Change Control process with signoff by senior Workbooks management.

Data is accessed and copied only over strongly-encrypted connections. We implement separate databases for each customer to add an additional layer of security above an extensive Permissions/Capabilities model which allows functions to be limited to specific roles or groups of users. Underpinning all data storage is a row-level security model which allows users to hold private data securely and permits control over whether users can read, modify, change access or change ownership on a record-by-records basis.

Staff Education and Training is a cornerstone of our information security policy. All staff are trained when they join Workbooks and receive regular training through-out their employment with Workbooks. We also vet all new joiners using a third-party organisation. Supplier Assessment is also a key part of our security process. All new suppliers who have access to Workbooks data are evaluated against our security standards. Sub-processors and sub-contractors are covered by a specific policy, which can be found here.