



Solutions For Accounting

**Solutions Hosting:
Frequently Asked
Questions**

QUESTIONS

➤ **Where is data physically located?**

Microsoft Azure – typically UK South (unless an alternative is requested by the customer).

➤ **In which data centre tier does a particular data set reside?**

Microsoft, do not publish information on TIA tiering. Details of their certification and compliance can be found [here](#).

➤ **What processes are in place in case of outage or downtime events?**

Customer data is backed up daily with the following retention policy:

- Daily backups held for 1 week
- Weekly backups held for 4 weeks
- Monthly backups held for 12 months

(Backups are of the server(s) in their entirety, customers will remain responsible for application data backups (e.g. Sage 50 backups taken within the program).

Additionally, data centre equipment failures and protection from environmental risks are covered by the IT controls of the hosting provider, Microsoft. This is an extract from their published documentation:

- The data centres have dedicated 24x7 uninterruptible power supply (UPS) and emergency power support, which may include generators. Regular maintenance and testing is conducted for both the UPS and generators. Data centres have made arrangements for emergency fuel delivery. The data centre has a dedicated Facility Operations Centre to monitor the following:
- Power systems, including all critical electrical components – generators, transfer switch, main switchgear, power management module and uninterruptible power supply equipment.
- The Heating, Ventilation and Air Conditioning (HVAC) system, which controls and monitors space temperature and humidity within the data centres, space pressurization and outside air intake. Fire Detection and Suppression systems exist at all data centres. Additionally, portable fire extinguishers are available at various locations in the data centre. Routine maintenance is performed on facility and environmental protection equipment.

“Protecting against external and environmental threats and supporting utilities” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 9.1.4 and 9.2.2. For more information review of the publicly available ISO standards we are certified against is suggested.

- Environmental controls have been implemented to protect the data centre including:
- Temperature control
- Heating, Ventilation and Air Conditioning (HVAC)
- Fire detection and suppression systems
- Power Management systems

“Protecting against external and environmental threats” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 9.1.4. For more information, a review of the publicly available ISO standards we are certified against is suggested.

We review these processes regularly.

➤ **Can we obtain a copy of your incident management process?**

We do not provide copies of our internal processes, we regularly review them. Please also refer to question 10.

➤ **Are you accredited? If so, which industry standard(s)?**

Solutions for Accounting are Cyber Essentials Plus accredited. In connection with Azure, Microsoft, has ISO27001/27002/270018 certification. For details, please see [here](#).

➤ **Can you provide regular SAS 70 type II reports or SSAE16 Type II reports?**

Our hosting provider, Microsoft, provides SOC 1 Type 2 and SOC 2 Type 2 reports on request for customers.

➤ **Is traffic to and from the cloud service encrypted? If so, at what level?**

Traffic to and from the cloud services is encrypted at the transport level (HTTPS).

➤ **If data resides on local hardware, is it encrypted at rest?**

Classified data residing on local hardware is encrypted at rest.

➤ **What types of Intrusion Detection Systems are being used, if any?**

Network isolation and firewall policies are in place. Network traffic inside the datacentre is monitored by our hosting provider, Microsoft.

➤ **Have there been any attacks in the past? If so, how were the attacks managed and was the data compromised?**

Solutions for Accounting operates a documented incident management procedure to handle a multitude of incident types, this includes security related incidents such as a breach scenario. We do not routinely publish information on attacks; however, our policy is to comply with our statutory obligation and to follow the guidance from the UK Information Commissioners Office on breach reporting.

➤ **How will I be alerted to potential intrusion events and other security threats?**

Solutions for Accounting's policy is to comply with our statutory obligation and to follow the guidance from the UK Information Commissioners Office on breach reporting.

➤ **Do you conduct independent penetration testing?**

Yes, Solutions and Accounting regularly conduct penetration testing via third parties.

We do not share penetration testing results.

➤ **For initial login – do you support whitelisted IP's, MFAs etc?**

Login is via Azure Active Directory (EntraID). Solutions for Accounting do not handle login processes as this is delegated to Microsoft. Please refer to their documentation for more information. Multi Factor Authentication is enforced as standard as part of this approach.

➤ **Do you utilise containers or VM's? What hardening mechanisms they use to protect the OS layer?**

Virtual Machine for this deployment, these services are further hardened to remove insecure cyphers from the system. By default, end users of the deployment are not granted administration privileges.

➤ **Do you follow Microsoft best practices?**

Yes, we have regular contact with Microsoft personnel including Microsoft architects.

➤ **How do they vet employees who will have physical access to the network and compute infrastructure that hosts your application?**

No Solutions for Accounting employees have physical access to the network and compute infrastructure that hosts our applications. Our hosting provider, Microsoft, publishes the following on their vetting process:

"All Microsoft US-based full-time employees (FTE) are required to successfully complete a standard background check as part of the hiring process. Background checks may include but are not limited to review of information relating to a candidate's education, employment, and criminal history."

They do not publish information for non-US based employees.

➤ **How do they securely delete or destroy my data when requested?**

An agreed period of retention at the termination of your agreement, after which all data will be deleted.

The actual destruction of data is covered by the IT controls of the hosting provider, Microsoft.

➤ **What browsers are supported?**

This deployment works via Azure Virtual Desktop.

➤ **What compatibility do you have with Microsoft Office Suite applications?**

The Microsoft Office suite of applications can be used in Solutions for Accounting's hosted environment provided the license supports 'shared computer activation'.

➤ **Is there access on mobile devices?**

Your solution in its entirety is accessible via Azure Virtual Desktop, which includes iOS and Android apps.

➤ **Is information stored on mobile devices, if so, is it encrypted in transit and at rest?**

No data is stored on a mobile device when using the Azure Virtual Desktop apps.

➤ **Will you complete an individual security questionnaire for my business/institution?**

Unfortunately, it's not possible to provide individual responses. This document is designed to cover all common questions. Should you have a specific question that this document has not addressed, please let us know.

➤ **Who is responsible for operating system upgrades?**

Operating system upgrades are carried out by Solutions for Accounting.

➤ **How does user management & assignment work, what level of traceability is available?**

User accounts for the hosting solution will be created and maintained by Solutions for Accounting.

Login to your product is via Microsoft Entra (formerly Azure Active Directory Domain Services).

Customers should ensure that user access is regularly reviewed in line with their business processes.

➤ **How do you inform customers of maintenance windows and/or service disruption?**

Maintenance windows are set for every Friday evening, we do not utilise all of these periods.

Where appropriate and possible, Solutions for Accounting will also make every effort to inform customers of any disruption that may affect their service.

➤ **Do you support Active Directory?**

Solutions for Accounting supports Microsoft Entra (formerly Azure Active Directory Domain Services) in this instance, customers Active Directories cannot be used for authenticating into this environment.

➤ **How does Sage 50 authenticate?**

Sage 50 uses independent usernames and passwords for authentication.

➤ **Is Antivirus protection installed?**

Endpoint managed antivirus protection is used in all Solutions for Accounting hosted environments.

➤ **What 3rd party applications can I install?**

If you have any requirements for other software or integrations with Sage 50 to be installed these will be reviewed on an individual basis.