Introduction

We take the security of our customers' data very seriously. We know how important it is to keep this data safe so we have put in place a set of protective measures, based on recognised industry best practises. This document contains a description of these measures to give our customers confidence that they can trust us with their data.

Our approach to security is under continual review, so we may change any of the descriptions in this document at any time and without notice.

Our overall approach to information security

We have a set of internal documents that are used to inform our employees about our approach to information security. These documents are regularly reviewed to ensure they remain up to date. Our employees are required to use these documents to understand how our information security approach applies to their work.

Information security responsibilities

We have a dedicated team that is responsible for overall information security at Sage. The security specialists make sure their knowledge of security stays up to date by keeping in contact with groups of technical security experts outside Sage. We also keep in contact with authorities such as privacy regulators. Our senior executives regularly discuss information security and take accountability for security within Sage.

Sage employees

We ensure reference checks are carried out on new employees and for roles which are particularly sensitive we do credit and criminal records checks. Our employment contracts include terms relating to information security. We provide training on our information security approach to all our employees to make sure they understand the role they play. If an employee does not follow our information security approach we may take disciplinary action against them. We encourage all our employees to report any information security concerns that they have using a dedicated mailbox, set up for that purpose.

Understanding the data that we handle

We keep track of the different types of data that we handle so that we can ensure it is properly protected. We keep a record of the data and all the software applications, computers and IT systems that handle it. We ensure that the protections we use are proportionate to the sensitivity of the data – more sensitive data may need extra controls. We train our employees to make sure that they do not misuse our IT systems in ways that could reduce the security of the data they handle.

Access to our customers' data

We apply rules to control which Sage employees can access customers' data. We only allow our employees to access customers' data if it is needed for them to do their job, for example, to provide technical support. We track and log all employees that have access to customers' data.

Encryption of customer data

Encryption is a way of scrambling data to help keep it secure. We often use encryption to protect our customer' data, for example where is being sent over the internet. We issue clear guidelines written by our security specialists for how our employees should use encryption. We make sure that we properly protect passwords and the keys that can be used to read encrypted data.

Buildings security

We store and process our customers' data in secure "Data Centres". These Data Centres are secure and access is restricted to those with appropriate permission. They are also built to be able to withstand fire, flood, lightning strike, power failures or other similar events. However as an additional precaution, we often store customers' data in multiple data centres so that if one is out of action, our products will keep working. Where we store data in more than one Data Centre, we make sure that the security of each Data Centre is of the same high standard.

Backup copies of customer data

We regularly make backup copies of our customer data so that if the original data is lost or damaged, we can replace it using the copy. We store the copies securely, taking the same care over them as we do over the original data.

Monitoring

We keep records of how our products are being used and how they are performing. We continually monitor these records so that we get early warning of security problems or other problems so we can understand the issue and fix any problems that occur. All monitoring data is kept securely.

Finding and fixing security problems

We use tools to scan computer hardware and software on a regular basis to look for weaknesses that could potentially lead to security problems. If we find these weaknesses, we fix them, on a priority basis. We make sure we test the fixes so that they don't cause new problems.

Despite adopting industry best practises, security problems can still happen. When they do, we have clear internal processes to ensure problems are quickly reported and handled by the relevant people. After a problem is fixed we learn from what happened to try to stop it from happening again.

Protection from the internet and viruses

We use a variety of software and hardware tools to make sure that unauthorised people cannot access our customers data over the internet, or get any kind of access to our computers.

We keep our computer systems up-to-date and run anti-virus software on them to prevent them becoming infected by computer viruses or other harmful software.

Software development

We use a variety of techniques to help stop security problems being introduced into our software as it is being written, and to find and fix problems before we make our software available for customers to use. All Sage employees involved in writing Sage software are trained in these techniques.

We make sure our software is protected so that no-one can change it without permission and we do a wide variety of tests before we make any changes available to customers. We carefully plan changes to reduce the risk that a change will cause a problem or disruption to our customers.

Our suppliers and partners

We use third-party companies across our business. Some of these companies handle our customers' data on behalf of Sage. Before we send data to any third-party, we review their approach to information security to make sure that we only rely on companies with good security standards and ensure that we have relevant contractual documentation in place.