



Sage SalesLogix Cloud | Data Protection Policy

Introduction

Sage understands that its customers' data is important and takes multiple measures to ensure it is protected. The following policy outlines the procedures and structures in place to protect customer data.

Single Tenant Customer Systems

The Sage SalesLogix Cloud CRM solution stores customer data on virtual instances that are specific to individual customer accounts. This means that data and databases are not shared between customers and are completely separated from other systems. This provides the customer with an important advantage over multi-tenant systems that store data on shared database platforms. In multi-tenant systems, a security weakness in one part of the system may allow access to other data once the system is breached.

With Sage SalesLogix Cloud, all customer systems and customer data are isolated and specific to one customer account. In addition to the advantages of individual database storage, single tenant systems such as Sage SalesLogix Cloud provide another important advantage—crash isolation. While system outages are rare, it is possible for either multi-tenant or single-tenant systems to fail. However, if a multi-tenant system fails, *all* of the tenants are at risk. For customers using Sage SalesLogix Cloud, an extra layer of isolation exists. All individual customer instances are separated from each other and a failure in one instance does not affect any other instance.¹

Backup / Restore

The Sage SalesLogix Cloud system stores customer data on virtual instances that are specific to individual customer accounts. Each system performs a full daily backup during an overnight maintenance window. Full backups are performed on a seven (7) day rotation schedule. Consequently, the farthest back a customer may restore data is seven (7) days in the past.

Of course, customers may elect to perform any additional backups they wish. Customer backups are performed at their option, or by utilizing the services of their business partner. Backup files may be stored on the customer's allotted storage volume, or may be backed up to an on premise location.

The restore process is simple. Contact Sage Customer Support or your business partner. A request will be made to restore your data from the most recent backup. When that is completed, Sage will notify you that your restore has been completed successfully. Database restore requests will be processed in accordance with the Service Level Agreement (SLA). A notification email will be sent to the customer and / or partner contact indicating that the request has been received, when the restore will take place, and a confirmation email is sent again when the process is complete.

Sage SalesLogix Cloud customers are provided one restore per quarter at no charge. Additional restore requests will be processed for a fee.

¹It should be noted that Sage has partnered with Amazon to utilize their EC2™ infrastructure. While customer systems are isolated from one another, they do share the overall Amazon EC2™ infrastructure. Amazon has massive redundancy across thousands of servers and storage, but a widespread outage across all of their data centers might impact Sage customers.



Disaster Recovery

Although a full system outage is very unlikely, Sage has developed and tested a Disaster Recovery process. One important advantage of the Sage SalesLogix Cloud service is that customer systems can be created from scratch in a matter of minutes. As noted above, all customer data is backed up on a nightly basis. Once a new system is available, all that remains is to restore the most recent data backup and customer systems would be back online. This capability is built into automated Sage tools that can perform this task efficiently.

Another important advantage of the Sage SalesLogix Cloud service is that by leveraging the Amazon EC2™ infrastructure, we have the ability to build new customer systems in separate “availability zones,” which are regions of the Amazon infrastructure and represent geographically separated data centers. So for example, if a widespread outage occurred on the west coast of the U.S., all customer systems can be restored on the east coast, where hopefully the cause of the problem (such as an earthquake) did not have a similar impact.

In addition to everything Sage has planned for incident response, the entire Amazon EC2™ infrastructure has multiple layers of fault tolerance, duplicate backup strategies, and disaster recovery capabilities.²

Sage’s own set of tools and customer tracking information is secured in the same way as customer systems. Through backups and recovery procedures we ensure customer account information can be recreated and back online should a widespread outage occur. In addition, our own systems and tools are replicated on physical servers in our offices.

Authorized Access

Certain actions taken on customer instances require authorized Sage employees to access customer data. Backup and restore procedures, for example, require validation and access privileges in order to complete these tasks. In isolated cases it may also be necessary for Sage Customer Support to access customer data in order to troubleshoot reported issues specific to a customer’s application. In such cases, Sage will specifically request customer permission to investigate issues in the database.

All Sage employees are subject to internal data protection policies and confidentiality obligations that work to protect customer data.

Online Security

Sage takes the security of customer data seriously. The Sage SalesLogix Cloud application has been fully reviewed and audited for online security. Using top-tier, third-party vendors, Sage SalesLogix Cloud has been audited for a wide variety of security threats, including:

- Unauthorized access to sensitive information
- Unauthorized modifications or deletion of information
- Performance of unauthorized operations or transactions
- Illegal impersonation to a different user or entity
- Performance of unauthorized operation that will affect the system's SLA
- Performance of unauthorized operation that will cause complete Denial of Service (DoS)

² Sage will make all commercially reasonable efforts to recover from a disaster. However, no guarantee is made that customer systems or data can or will be restored.

- Exploitation of existing security control to perform fraudulent activity

Areas of the SalesLogix Cloud service that were audited include:

- User separation: The ability of one user of the system to access, modify, or manipulate the mailing list of another user. This will be tied in with the examination of the user management mechanisms relating to login processes and authentication.
- Source code review: The level of coding employed on the source code of the plug-in, as it is being deployed as part of the Sage SalesLogix Online Application.
- Web Services:
 - Connectivity between the browser and the Web Services interface
 - How Web Services cope with malicious code
 - Attempts to damage the availability of Web Services
- Authentication mechanisms with regards to a user of the Sage SalesLogix online application being able to access information regarding another user and/or bypass the process by which a user is granted the ability to trigger the transmission of emails.
- Authorization mechanisms with regards to a user once they have been granted access to the application to be able to manipulate information regarding another user and/or a component of the system that they do not have access to.
- Auditing mechanism (e.g. log quality, log protection, sensitive information handling, alert mechanisms)
- Password management mechanisms (policy, minimum requirements)
- Cryptography usage (e.g. standards, algorithm usage, key management, digital signature usage, secure hashing)
- Secure transport mechanisms (mainly confidentiality and integrity protection mechanisms implementation related to each transport)

In addition to the efforts Sage performs to ensure online security, customers should also know that the Amazon EC2™ infrastructure itself has world-class intrusion control capabilities. Customer systems are protected by multiple layers of secure firewalls, network security protocols, and system isolation that provide significant protection against online threats.

Summary

Sage is committed to ensuring customer data is protected. The capabilities and procedures listed above demonstrate our resolve to ensure our customers operate in a secure and reliable environment, and can continue to enjoy the benefits of choosing Sage SalesLogix Cloud.



About Sage SalesLogix

Sage SalesLogix provides a complete view of customer interactions across departments—providing information and insights for better planning, managing, and forecasting. Your teams will have the tools to increase sales, reach more profitable customers, enhance the customer experience, and anticipate customer needs. Sage SalesLogix offers flexible access, deployment, and payment options to address business requirements.

About Sage Group, plc

Sage is a leading supplier of business management software and services to 5.8 million customers worldwide. From small start-ups to larger organizations, we make it easier for companies to manage their business processes.

©2010 Sage Software, Inc. All rights reserved. Sage, the Sage logos, and the Sage product and service names mentioned herein are the registered trademarks or trademarks of Sage Software, Inc. or its affiliated entities. Amazon Web Services, the “Powered by Amazon Web Services” logo, Amazon EC2, and EC2 are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries. All other trademarks are the property of their respective owners.

Sage

8800 N. Gainey Center Dr., Suite 200
Scottsdale, AZ 85258
www.sagecrmsolutions.com | 800-854-3415
www.sagesaleslogix.com