SECURITY INFORMATION

Sage People

Data security overview

We know the value of your HR and People data, and the importance of keeping it secure. We constantly review and update our services in the light of evolving best practice

Introduction

Organizations today are facing increasing pressure to secure and protect employee data to ever higher standards. Regulations such as the GDPR are requiring organizations to ensure they are taking data security seriously.

When it comes to the privacy and security of customer data, there is nothing more important to us at Sage, and we have invested heavily in our own security and carefully evaluated the security of our partners.

Sage adopts a defence-in-depth approach to security and has put in place a framework of protective measures, based on recognised industry best practices, designed to protect the confidentiality, availibility, and integrity of our customers' data.

This overview outlines the key ways in which we do this and some of the steps that our customers can take themselves to protect their data.

Built on Salesforce

The Sage People application is developed and hosted on the Salesforce platform, the world's leading enterprise cloud services provider, and one of the most secure and trusted.

Salesforce policies, procedures, and technologies have been validated by many of the world's most security conscious organizations and the platform is certified as compliant with some of the most rigorous, industry-accepted security, privacy, and reliability standards:

- ISO 27001, 27017 and 27018
- SOC-1 Type II (SSAE 16/ISAE 3402)
- SOC 2 Type II (AT-101 Trust Principles Report)
- SOC 3 (SysTrust)
- Truste Privacy Seal
- PCI-DSS
- TUV Certificate

ISO 27001	ISO 27017	ISO 27018
SOC 1	SOC 2	SOC 3
PCI DSS	TRUSTe International Privacy Verified Powered by TrustArc	Salesforce BCRs

A full list of ceritifcations and more detail is available at Salesforce Trust.

Shared security responsibility model

Sage People control and manage the secure development of our software, including all updates and patches, change management and incident management directly related to our software.

Salesforce are responsible for for managing the platform the Sage People software is hosted on, including all operating systems, databases, network infrastructure, security monitoring and physical security of the data centers.

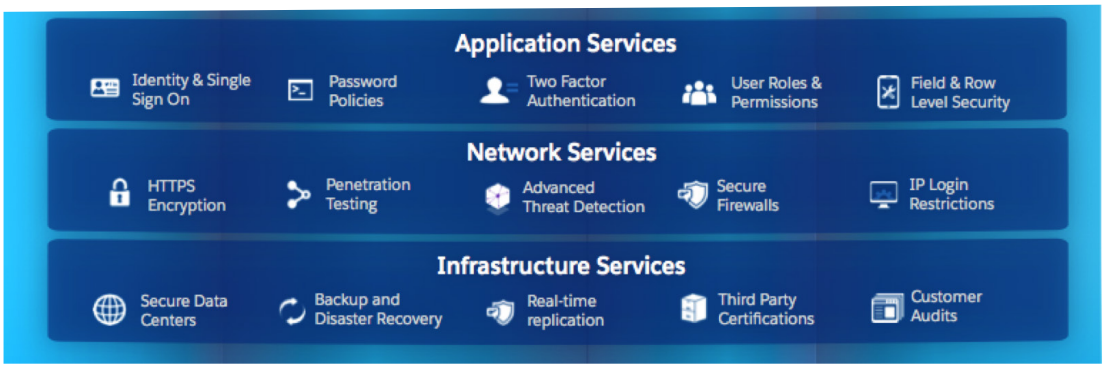
Sage People customers must ensure that they configure and monitor their authorization, identity management, access controls and privelages, using the functionalityprovided by the platform and our application, to meet their own security requirements.

Salesforce Platform as a Service (Paas)

The Salesforce platform is a fully managed, cloud based service, meaning that the set-up, maintenance, upgrades, patching and monitoring of the servers, networks, and associated infrastructure is all provided by Salesforce. In addition, we can take full advantage of the multiple layers of security controls and functionality provided by the platform, allowing our customers to benefit from features such as identity management, authentication, access control and single sign-on.

Other critical services, such as securing access to the data centres where your data is stored and processed, protecting your data from unauthorised access and providing resilience to ensure high availability, is included in the Platform as a Service (PaaS) upon which the Sage People application is built.

A diagram summarising the services that Salesforce manage on behalf of our customers is provided below:



Physical security: fortifying the data centres

Access to Salesforce facilities is strictly controlled, with multiple levels of defence including bullet resistant perimeter walls, vehicle barriers, CCTV, alarms, guard stations, biometric scans, security doors and cages.

Access is protected by an electronic control system, with an array of access-controlled doors, which are monitored 24/7 by an on-site Security Team. Visitors must be pre-registered and approved, are required to sign in at reception and must be escorted at all times whilst on the premises. Access to server rooms is restricted to authorised personnel via swipe card and server cabinets are locked with access to keys also restricted.

Technical and network security

To prevent data being intercepted whilst using Sage People, all connections are protected with Transport Layer Security (TLS) encryption (version 1.2 or higher). Perimeter firewalls and edge routers are used to block unwanted transmission protocols and servers are protected by intrusion detection systems.

Defence in depth is provided by internal firewalls that segregate the application and database tiers. The application and database servers themselves are hardened to industry and vendor best-practice guidelines and continuously monitored to detect any changes.

Customers also have the option to encrypt some custom fields before they are saved in the database, and mask their contents based on the access permissions assigned. This is a complex area and one that Sage People recommend further discussion around, as encryption as a technology imposes certain limitations and impacts some application functionality.

Threat monitoring

Sophisticated security tools are used to monitor system activity in real-time to capture and detect and prevent malicious events, threats and intrusion attempts.

State-of-the-art intrusion detection systems are used to detect common types of attacks, which means that every network in the production environment is monitored continually for potentially malicious network traffic. Application and database activity are monitored with security event management tools to proactively alert operators to potential internal and external threats.

Authentication and identification

Standard login to Sage People is via a unique username and password, and numerous options are available to ensure that passwords are secure and routinely changed. We also support single sign-on (SSO) from a variety of identity providers and customers can choose to use their own identity provider by utilizing the various options available, including Security Assertion Markup Language (SAML).

Customers can restrict when and from where their users can access Sage People. Multi-factor authentication (MFA) is available for identity verification to add another layer of protection and we support common mobile MFA methods such as Salesforce and Google Authenticator, email and Short Message Service (SMS) options.

Backup and disaster recovery

Data is replicated in real-time to a 100% full-scale replica disaster recovery data centre, and then backed up to primary and secondary disaster recovery data centres. The data is encrypted in transit and whilst stored, and never leaves the secure data centres. All activity is securely logged, and evidence of destruction is recorded when data reaches the end of its lifecycle.

To ensure these backup processes are working properly, Salesforce schedules Disaster Recovery exercises which are conducted several times per year.

Organizational security: how we operate internally

At Sage People, our commitment to security, privacy, reliability, and trust is adopted by the entire company. There is an over-arching Information Security Policy supported by processes and procedures which form the ISO 27001:2013 certified Information Security Management System (ISMS). We have a Customer Protective Zone, with specific measures in place to govern how we handle customer data.

All of our employees receive information security and privacy training as defined by our Information Security Policy. Employees that handle customer data receive additional training specific to their roles before access is given. Access is strictly limited to only those who require it, and this is reviewed on a regular basis.

Software security

Sage People have a clearly defined secure software development lifecycle (SSDLC) to ensure all changes and releases to our software are carried out in a secure, controlled manner. The SSDLC includes design, development, testing and release phases with security considered at all stages. Changes to the application are strictly controlled and versioned in our source code control system. Releases are announced in advance and scheduled to provide the least impact.

All members of the Product Engineering team routinely receive security training and we have a Salesforce Security Champions programme to further promote security best practice.

Useful links

Sage's approach to information security and a copy of our information security policy is available at Sage Security Governance.

Additional information about Salesforce's security and privacy programs is available at Salesforce Trust.