

Enterprise-class security and precise access controls keep your data safe

U.S. government agencies and Fortune 100 corporations depend on Agiloft to keep their data safe. That's why we work tirelessly to ensure that every part of the Agiloft application, infrastructure, and organization implement the best practices necessary to provide military-grade security to our customers. And we engage third party security specialists to actively test compliance.

We employ a multi-layered security policy, which is summarized below.

Development Process

The code is developed in accordance with the CERT Secure Coding Standard for Java, and the OWASP Enterprise Security API (ESAPI) is used within the application to implement security best practices.

Third Party Validation

Agiloft was tested by a security team from the U.S. Air Force and approved for deployment on the Secure Network at the U.S. Department of Defense. We then asked the team for their recommendation for further security testing. The U.S. Air Force security team recommended [Knowledge Consulting Group](#) (KCG, now part of [ManTech International Corporation](#)).

Agiloft engages KCG/ManTech to perform in-depth penetration assessments of the Agiloft application and our hosting infrastructure after all major upgrades. This assessment uses both manual and automated techniques to search for technical vulnerabilities. In addition, we engage KCG to test the organization for resilience against social engineering attacks, a critical area of security which is too often overlooked. A copy of the most recent security audit can be provided upon receipt of a signed NDA.

Agiloft was also reviewed and approved for deployment by a security team from the National Aeronautics and Space Administration (NASA).

The product was audited by Skyhigh Networks and received the highest possible rating of Enterprise-Ready. The Skyhigh CloudTrust™ Program provides an objective and comprehensive evaluation of a service's security controls and enterprise readiness based on a detailed set of criteria developed in conjunction with the Cloud Security Alliance (CSA).

We welcome additional security audits that current or potential customers may wish to perform, and we will provide any assistance required to conduct a rigorous evaluation.



Agiloft was tested by a security team from the U.S. Air Force and approved for deployment on the Secure Network at the U.S. Department of Defense

Hosting Infrastructure

With our Hosted Service, you have the choice between two different options — a hybrid vXchnge/AWS hosting solution or an AWS-only hosting solution. Both [vXchnge](#) and [AWS](#) offer full regulatory compliance with key standards such as SSAE 18, SOC 2 Type II, and HIPAA. For more complete security and compliance details, refer to the information listed on each provider's website. For further information about Agiloft's Hosted Service, see our [Agiloft Hosted Service](#) datasheet.

Build/QA Process

The build process includes scanning for malware using both Symantec Endpoint Protection and NOD32. In addition, the build process includes virus scanning by Clam. QA uses Burp Suite Pro to test security against exploits by malicious external users or internal power users.

Application Security

The Agiloft application provides precise access control at the record and field level, all managed by extensible group permissions. Agiloft implements

security best practices such as encrypting passwords using the SHA-2 one-way hash function and protecting all communications with SSL/TLS encryption. Login sessions are automatically expired and terminated after a period of inactivity.

The net result of the above permission controls and support for data encryption is secure, precise access and full compliance with privacy standards such as HIPAA.

Audit trails are provided at the record and field level for changes to both the data and metadata. Integrity is maintained at both a physical level through a transactional database with foreign key integrity constraints and at the business/logical level through an active integrity manager. To ensure transparency, we offer a security information packet containing our CAIQ, ITDR, and other related information, available upon request.

Privacy

We offer hosting on servers located in Ireland or Australia for full compliance with EU and Asian data privacy laws, including GDPR. We are also a member of the U.S.-EU Privacy Shield network.

Agiloft welcomes additional testing. If you would like to conduct a security audit, we will do everything possible to assist your choice of security firm.

For More Information

Contact a Product Specialist today at 1-888-727-2209 Ext. 1 to learn more about Agiloft security and request our security information packet, or visit <https://www.agiloft.com/software-security.htm>.

About Agiloft

Over 3 million users at organizations ranging from small enterprises to U.S government agencies and Fortune 100 companies depend on Agiloft's top rated product suites for [Contract Management](#), [Service Desk](#), [Custom Workflow](#), and more. Agiloft specializes in automating processes that are too complex for competing vendors. Our best practice templates and adaptable technology ensure rapid deployment and a fully extensible system. For more information, visit <https://www.agiloft.com>.