INFO SHEET

Planview Spigit: A Secure Project Collaboration Solution

The security of your information is as critical as your business is dynamic. That's why we built Planview Spigit™ on a foundation of the industry's most stringent data security standards.

How does Planview Spigit support your needs? Just ask.

1. What third-party audits are performed in the Spigit environment?

Spigit is independently audited against a rigid set of SOC 2 controls annually.

A copy of this documentation can be requested by customers or prospects with an NDA in place.

In addition to using third-party evaluations of our information security practices and general IT controls, we subject our infrastructure and application to regular vulnerability scans. Finally, annual penetration tests are carried out by independent third parties. We also have these tests repeated whenever we make significant changes to the Spigit environment.

2. How do I request to have a penetration test of Spigit conducted?

We have an open policy that allows our clients to perform penetration tests of our service. The penetration test may be performed either by you or a third party whom you appoint, provided that relevant non-disclosure agreements have been completed and testing pre-conditions including such items as dedicated time frames and defined test types, have been met.

3. What steps do you take to protect my information from unauthorized network access, such as malicious internal users, external hackers, viruses, and other types of malware?

The Planview Spigit production environment is protected by a robust network infrastructure that provides a secure environment for all customer data. The Spigit service is on a physically segregated network that requires VPN access and two factor authentication for administrative access.

Planview® also monitors and analyzes system logs to identify unusual traffic patterns, potential intrusion attempts and other security threats. Planview also uses other 3rd party tools and services to provide end-to-end network visibility and protection.

4. How would I be informed were there an incident or breach that could potentially expose sensitive user information?

Planview has developed security incident responses and escalation procedures to ensure timely and effective handling of all situations. If there were ever a security incident that could cause a major service disruption or lead to the exposing of client data, you would be informed promptly.

"The security of your data is our priority. Spigit is ISO27001 certified with role-based access controls, 99.8% uptime, and encryption of customer data both in transit and at rest."

– Lance Wright, Director of Information Security - Planview, Inc.

5. What processes are in place to make Spigit less vulnerable to known web-application attacks?

   The Spigit solution is constructed on a multi- tier architecture, consisting of web servers, application servers, and database data storage.

   Planview uses best practice coding standards and an established software development life cycle that incorporates security from the very start; our development team leverages industry guidelines, such as the Open Web Application Security Project (OWASP), Secure Coding Guide, SANS CWE Top 25, and CERT Secure Coding.

6. How is my organization's data segregated from that of other clients?

   The hosting environment is a single tenant database and application components that assure segregation, privacy and security isolation within a multi-tenant physical hosting model.

   We do not store user data on backup media; instead, we rely on full backups that are shipped to a physically different co-location site.

7. How is confidential data stored and transmitted by the Spigit service protected? Which encryption methods are used?

   Data in transit is over HTTPS only and is encrypted with the TLS v1.2 protocol. User data, including login information, is always sent through encrypted channels.

   All data stored in the Spigit solution is automatically encrypted with a unique key, using the AES-256 encryption algorithm. Encryption keys are stored separately, with precautions taken to prevent unauthorized access both to encrypted data and their corresponding encryption keys.

8. What staff has access to the production databases?

   Only a very limited number of system operation team members have access to the production databases, and access is granted on a least- privilege, need-to know basis. Access is reviewed semi-annually, and requires VPN connection with multi-factor authentication.

9. Which of my data stored in the Spigit solution can be viewed by Spigit staff?

   Customer data can only be viewed by Customer Care and Customer Success Managers. Access to customer data is only allowed for support purposes.

10. Where are Spigit production servers located, and how is access to my assets and/or information controlled, physically secured, and restricted solely to authorized staff?

Customer instances, including data, are hosted in geographically disparate data centers. Customers may choose the location to host their data in based on corporate location or user base location in an effort to minimize latency.

The hosting provider is an ISO 27001-certified service organization that provides 24-hour physical security.

Security measures include comprehensive identification, access control and monitoring systems, automatic fire protection, redundant climate control, and fail-over power supply.

11. What data-backup and data-retention policies apply to the information stored on Spigit production servers?

Spigit backup processes include a nightly full backup that is encrypted and housed in facilities in the same geographical region as the primary storage. Data backups are retained for 30 days.

Internally, customer data is never backed up to removable media. All data will be returned to the client in an encrypted flat file at the end of term.

12. What is the backup schedule for Spigit servers? How much data could my organization potentially lose?

A full backup of the Spigit is performed on a nightly basis and is securely stored at an offsite facility.

13. What are the RTO and RPO of the disaster recovery solution for the Spigit service?

For the Spigit service, there are 3 categories of disaster type. The RPO for all categories is 24 hours.

Category 1 – 4 hour RTO
This would be characterized by single or multiple hardware failures within the primary data center, or the intentional destruction of data within the data center. This would include disk, server, network firewall, or other equipment failure(s), or human induced non-physical destruction of data or environment. This damage would require the repair of the affected components, and the recovery of data.

Category 2 – 2 day RTO
This would be characterized by single or multiple hardware destruction within the primary data center. This describes serious and non-repairable damage to the hardware or rack infrastructure. This damage would likely require relocation within the data center facility, extensive equipment and software replacement, followed by data recovery.

Category 3 – 7 day RTO
Primary data center is destroyed or seriously compromised. Recovery requires replacing destroyed SaaS infrastructure in alternate data center, and recovery of data.

14. How long are backups and operating data retained?

Data backups are retained for 30 days.

15. How is my organization's data disposed of at the time of contract termination?

Customer data is deleted by an automated process 30 days after the end of the customer's term. Data can also be terminated immediately depending on the contract terms of agreement.

16. What controls are implemented and enforced that protect user credentials and ensure a secure login procedure?

Spigit recommends customers manage user access and authorization through integrated SSO. Spigit supports SAML 2.0 for SSO. In circumstances where SSO is not possible, Spigit does support local usernames / passwords for user access. For those user accounts users are required to authenticate with a unique username / password combination. These credentials are encrypted when transmitted over the Internet (HTTPS) and when at rest in the Spigit database. A standard combination of password length and complexity is required of all users, but your organization can customize this to enforce your own security requirements.

17. Does Spigit support Single Sign On ("SSO") for the login procedure?

Yes, Spigit supports Single Sign On ("SSO"), using the Security Assertion Markup Language ("SAML 2.0"). This allows network users to access the Spigit solution without having to log in separately, with authentication federated from Active Directory. This reflects the industry's standard procedure for SSO that is widely in use. Multi-factor authentication can be integrated with SSO if desired.

18. Can we mitigate our security risk by limiting access to the Spigit solution through filtering IP addresses?

Spigit does have the ability to support IP whitelisting if so desired by a customer.

19. Is Spigit a PCI DSS-certified merchant/ service provider?

Spigit does not process credit card information, and thus does not require PCI (Payment Card Industry) certification.

20. Is Spigit HIPAA compliant?

Because Spigit does not store or process any medical related data, the service does not fall under the requirements for HIPAA compliancy.

21. Does Spigit support two-step verification (aka two factor authentication)?

Spigit supports SAML 2.0 SSO integration. Please consult with your SSO provider if multi-factor authentication is supported.

Have a question you didn't see answered here? Let us know at **security@planview.com**

For more information about Planview Spigit security, visit **Planview.com/Trust**