INFO SHEET

Planview Clarizen: A Secure Projects & Work Solution

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

How does Planview Clarizen support your needs? Just ask.

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

Planview Clarizen has an established information security management system (ISMS), which was awarded ISO 27001 certification by Intertek,an independent auditor. Additionally, Planview Clarizen 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.

2. 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 Clarizen production environmentis protected by a robust network infrastructure that provides a secure environment for all customer data. The Clarizen 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.

3. How would I be informed were there an incident or breach that could potentially expose confidential 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.

4. What processes are in place to make Planview Clarizen less vulnerableto known web-application attacks?

The Planview Clarizen 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

"The security of your data is our priority. Planview Clarizen is ISO27001 certified with role-basedaccess controls and encryption of customer data both in transit and at rest."

– ***Chief Information Security Officer - Planview, Inc.***

development team leverages industry guidelines, such as the Open Web Application Security Project (OWASP), Secure Coding Guide.

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

Planview Clarizen customer instances reside on a shared and secure multi-tenant environment segregated by multiple firewalls. Customer databases are multi-tenant, and each customer is given their own logical database that contains only their data. Though network and server infrastructure are shared across the user base, Clarizen's robust architecture logically separates customer data to prevent unauthorized access. There is no network visibility between any customer instance.

6. How is sensitive data stored and transmitted by the Planview Clarizen service protected? Which encryption methods are used?

Customer data in transit is encrypted with the TLS v1.2 protocol and is sent only through encrypted channels. All data is stored within an Oracle RAC database.The Oracle database is constantly monitored for anykind of data corruption or anomaly. Integrity checks are performed at every point within the storage architecture including the primary, standby, and disaster recovery database components.

In addition to the internal Oracle integrity checks, upon customer request, Planview Clarizen enforces data encryption at rest using the industry-standard AES-256 algorithm. Data encryption at rest is enhanced by implementing encryption keys that enable strong logical and physical controls to prevent unauthorized access.

7. 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.

8. Which of my data stored in the Planview Clarizen solution can be viewed by Planview Clarizen staff?

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

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

Data centers are located in different areas depending on customer location. For US customers, the data center is located in Sunnyvale, CA. For European customers, we have data centers located in the Netherlands – Amsterdam .

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.

10. What data-backup and data-retention policies apply to the information stored on Planview Clarizen production servers?

Planview Clarizen is configured to perform differential backups everyday and. The full back up is retained at the DR colocation facility for 7 days before it is sent to the cloud backup location and retained for 365 days.

Internally, customer data is never backed up to removable media.

11. What is the backup schedule for Planview Clarizen servers? How much data could my organizationpotentially lose?

For the Planview Clarizen service, daily full backups occur on a nightly basis. The maximum amount of data loss that would occur is 24 hours. All efforts are made to minimize this recovery time.

12. What are the RTO and RPO of the disaster recovery solution for the Planview Clarizen service?

For the Planview Clarizen service RPO (Recovery Point Objective) is 24 hours, and the RTO (Recovery Time Objective) is 12 hours.

In the event of a major disruption or disaster at one or both production sites, an emergency response team consisting of selected Planview staff, is summoned to activate the disaster recovery plan.

13. How long are backups and operating data retained?

Upon customer exit, data persists in the backup system for 365 days after the contract termination date.

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

Customer data is deleted by an automated process 90 days after the end of the customer's term. All customer production, sandbox and test instances are deleted.

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

All Planview Clarizen users are required to authenticate with a unique username /password combination. These credentials are always encrypted when transmitted over the Internet. A standard combination of password length and complexity is required of all users, but your organization can customize controls to enforce your own securityrequirements.

16. Does Planview Clarizen supportSingle Sign On ("SSO") for the login procedure?

Yes, Planview Clarizen supports Single Sign On ("SSO"), using the Security Assertion Markup Language ("SAML") and Active Directory Federation service for enterprise clients. This allows network users to access the Planview Clarizen 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.

17. Can we mitigate our security risk by limiting access to the Planview Clarizen solution through filteringIP addresses?

IP address ranges can be configured to allow customers to specify the IP addresses that can access their Planview Clarizen instance to provide an extra layer of control and security.

18. Is Planview Clarizen a PCI DSS-certified merchant/service provider?

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

19. Is Planview Clarizen HIPAA compliant?

Because Planview Clarizen does not store or process any medical related data, the service does notfall under the requirements for HIPAA compliancy.

20. Does Planview Clarizen supporttwo-step verification (aka two factor authentication)

Yes, With SSO enabled, Planview Clarizen supports two factor authentication.

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

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