



Platform security and development standards

An overview of security and development standards related to SQLdep cloud platform



Secure and reliable platform is our top priority

SQLdep cloud platform deploys industry-standard security practices to establish data secure environment. Multiple layers of operational and organizational security are applied alongside with change management processes to ensure compliance with the strict industry regulations.

What's SQLdep

SQLdep is a cloud service (SaaS) for automated analysis of SQL queries. Aim of the service is to provide information about data-lineage and impact analysis to accelerate data-warehouse development cycles.

Industry standards

ISO 27001 - General principles of design, implementation, maintenance and improvement of data security were implemented through the guidelines of international standard ISO/IEC 27002 -- Information Security Policies -- Access Control -- Physical and Environmental Security and other norms related to ISO 27002.

ITIL - Best practises from ITIL (Information Technology Infrastructure Library) were used to establish processes related to platform support and maintenance.

OWASP - Web application security is maintained through methodologies as covered in OWASP Developer Guide or OWASP Secure Coding Practises.

Application Security

Account & data management

Account registration is required to obtain access to Dashboard and REST API.

Through the Dashboard customer can manage the account, set-up level of data visibility and has the option to remove the data entirely from the server.

Data transport

Any communication is done strictly via secured connection over HTTPS (SSL). Secure protocol versions are used: SSH 3.0 / TLS 1.0 or higher. Domain SQLdep.com uses a signed certificate from globally trusted certification authorities like GeoTrust, Inc.

Operational security

Change management process

Any change in the software is carefully analyzed by engineering team and fully tested on the stage environment before deployment. Source code is subject to version control and is maintained in central GIT repository. Production and stage is completely separated.

Backups

To ensure data protection the backup strategy is in place. Backups are stored on physically separate location. Data transfer is done through a secure connection and the data itself are always encrypted.

Servers and Physical security

Managing technical vulnerabilities

Dedicated personnel is responsible for monitoring and patching all the servers. Relevant security patches are immediately applied. At least once a year a full scale audit is scheduled while utilizing tools such as Nessus, Nmap, Burp, etc.

Dedicated servers

Service is available on dedicated servers while hosted in certified data centers. All data belonging to Customer are automatically encrypted at rest. Two step verification is required for any authorized personnel to access the servers while principle of least privilege is strictly applied.



twitter.com/sqldep

fb.com/sqldep

join@sqldep.com

www.sqldep.com