ALOE

Privacy and Security Datasheet

- Security Controls
- Security Practices
- Privacy & GDPR
- Security Customizations

1 (480) 686-7762
info@BigforkTech.com

bigforktech.com

ALOE

Security Controls

Server and Data Isolation

All of your data and the ALOE application live and run on a single cloud server instance dedicated to you and not shared with any other customers or 3rd parties. This is the major security measure of the ALOE system which ensures that you always remain in control over your own data.

HTTPS

All web traffic between users and ALOE is always over full-time HTTPS, secured by an SSL certificate from Let's Encrypt. This ensures that internet eavesdroppers can't see your data going over the wire.

Roles Based Access

ALOE comes preset with the following roles: Administrator, Power User, Normal User, Create Only, Read Only, and Assignee Only. This enables the right people to have the right access.

Secure Passwords

Passwords are stored in a one way salted PKCS5S2 hash which prevents the passwords from being reverse engineered.

bigforktech.com
(480) 686-7762
info@BigforkTech.com

ALOE

Security Controls (continued)

Web Application Firewall

All web traffic is protected by a web application firewall that will reject bad traffic and common web site attacks.

Network Firewall at AWS

Your server sits behind a protective firewall at Amazon Web Services (AWS) that blocks all traffic that is not related to your ALOE application.

Encrypted Volume at AWS

All of your attachments and database data is stored on an encrypted volume. This ensures that even if someone were to gain physical access to the hard drives, you and your data still remain protected.

bigforktech.com
(480) 686-7762
info@BigforkTech.com

ALOE

Security Practices

Enterprise Password Policies

ALOE supports a variety of password polices such as complexity and strength requirements, age expiration, user lock-outs, and reuse elimination.

Login Audit Logs

ALOE maintains an audit log of who and when users log in.

Server Management via SSH Keys

All administrative logins use SSH keys. There are no root passwords accepted. This ensures that administrator account access can't be brute-forced or guessed.

Strict Port Access

Access to the server is only allowed from ports 80 and 443 via the internet. Additionally, port 22 is also allowed but only from a small specific range of management IP addresses.

bigforktech.com
(480) 686-7762
info@BigforkTech.com

ALOE

Privacy and GDPR

Ability to Delete Individual Rows

Your Power Users will have access to remove any individual data whose retention policy dictates it be removed.

Expiring Backups Per Data Retention Policy

Backups automatically expire and get deleted after a 64 day retention period. This is optional.

Encrypted Backups Stored on S3

Backups are encrypted before leaving the server, this ensures your data never lives anywhere outside of your server.

You Always Own the Data

You can delete or export all of your data at any time. There are a variety of export formats such that you will be able to transfer your data for maximum portability.

No 3rd Parties Have Access

Unless you specifically enable it through integration features like with Docusign, Salesforce, Email, or Firebase, no 3rd party will have access to your data or system.

bigforktech.com
(480) 686-7762
info@BigforkTech.com

ALOE

Security Customization

Run Your Own Agents

Because this your server, dedicated to you, we will install and run any of your own monitoring agents or enterprise security software.

Access to Logs

We can ship audit logs out to a location that you can monitor and access in the case when you need to centrally aggregate your system logs for monitoring and review.

bigforktech.com
(480) 686-7762
info@BigforkTech.com