



WHAT IS **ENCAMP**?

Encamp is a SaaS platform built on AWS to automate environmental reporting to **all 50 states** in the U.S.



Easily import reporting data into Encamp (**Excel templates** let you do it in bulk).

Encamp **integrates with all state portals** to simplify reporting and read the data from previous years' reports.

With one click, Encamp **submits your reports** and pays all required fees (again on your behalf)



Frequently Asked Questions



Does Encamp have access to our data?

We can only access your facilities info for support purposes, and change data only if you request it.

Will Encamp ever share the data you have access to?

Nope. Your data leaves our platform only when we submit compliance reports on your behalf.

Other questions we answer frequently

We're always happy to answer questions, but these are the ones that get asked most often.

If you have other ones, send them to us at [Contact Encamp](#).

What data is stored in Encamp?

Encamp stores data only to build environmental requirements profiles and compile compliance reports. We don't store any data considered confidential.

What tech stack is Encamp using?

Our platform runs on a serverless stack within AWS: AppSync (hosted GraphQL api), AWS Lambda functions, AWS DynamoDB (database), and Amazon S3 (file storage).

Is Encamp SOC 2 or ISO27001 certified?

Encamp's policies are written under the guidance of SOC 2. We're currently working to implement our SOC 2 ready certification; an SOC 2 audit is scheduled in 2021.

Are third party audit reports available?

Audit reports will be implemented in 2021. Until then, our third-party vulnerability scans and assessments are available.

Does Encamp have a business continuity and disaster recovery plan?

Our business continuity and DR plan was implemented when we started in 2017. We review it on a regular basis and adjust it accordingly when conditions change.

Is SSO available for our company?

We're on track for Single Sign-on in 2021.

Other questions we answer frequently (continued)

Have you had a breach of personal/health/payment data in the last 10 years?

Fortunately, no. But if we ever do, our response plan includes determining how a breach occurred, fixing the problem, and issuing a full report to each Encamp customer that's been impacted.

Does your company have a formal background check policy?

All Encamp employees must agree to a background check after accepting a job offer and before their first day of work. We also conduct reference checks from previous employers.

Does Encamp use anti-malware on all systems including servers and workstations?

Our operations team manages all systems remotely using a software distribution agent.

How soon are accounts disabled upon a user's termination or changes to job role?

For a user's termination, access is disabled immediately. For job role changes, access is modified within one full business day.

How does Encamp handle physical security?

Encamp is a fully remote workforce, so we don't host physical servers. Our operations team monitors all devices used by employees; devices are locked using a strong password and two-step authentication when not in use. Passwords are updated on a regularly scheduled basis.