OPENGOV
Security Overview

OPENGOV SECURITY STATEMENT

OpenGov is committed to customer security. We use secure communications on our platform for all user communication ensuring that transmitted data is authenticated and encrypted. On our internal platform, we authenticate all users and give customers control over who can access and update their reports and data.

Our engineering team integrates security into their development workflows. We log platform activities and maintain support channels to report and resolve issues. We access and maintain our systems through Amazon's Web Services which lets us leverage the industry's best infrastructure technologies.

BUSINESS PROCESS AND DATA EXCHANGE

Where is customer data stored?

OpenGov uses Amazon Web Services (AWS) to rent virtual infrastructure which we control and manage over secure connections. AWS has strict controls in place to ensure only OpenGov can access our data. The specific services we use from AWS are EC2, RDS, ElastiCache, S3, and DynamoDB. For more information on AWS security, visit https://aws.amazon.com/security/

How is data communicated from the user to the OpenGov platform encrypted?

OpenGov uses HTTPS (TLS 1.2) for all communication between the user and our platform. HTTPS is designed to prevent man-in-the-middle attacks and tampering with the data. TLS 1.2 is the latest security standard for secure computer communication.

How does OpenGov's system authenticate users?

OpenGov encrypts all passwords with Bcrypt, the industry leading password storage solution. This solution not only encrypts data but also employs methods to defeat brute force attacks. All passwords are required to be at least 8 characters.

What security compliances does OpenGov adhere to?

We run our platform and manage development through Amazon Web Services (AWS). Once servers are provisioned, AWS no longer has access to our virtual servers. Since our servers are hosted and maintained by AWS, they conform to a variety of leading compliance standards: http://aws.amazon.com/compliance/. Access to AWS is limited to engineers with two-factor authentication.

Who has access to my data?

Users can only access data-management features for their own organization. In order to create, update or delete data, users must have an administrative account. All of these features are restricted to logged in users. Besides administrators in their own organization, only OpenGov deployment specialists and engineers can create or modify data.

What type of user access control does OpenGov support?

The OpenGov platform consists of entity administrators and regular users. These users are restricted to their own government's OpenGov entity, although they can view information from other entities that is shared with the public or the OpenGov Network.

1. **Administrators** have the ability to provision users, upload data, modify charts of accounts, create reports, edit account attributes like logos, and change report permissions.
2. **Users** can add saved views to reports and view reports that they have access to.

OpenGov report permissions have four levels:

- **Private** - shared only with the report creator. The report creator can invite individuals from their organization to the report
- **My Organization** - everyone at the account can view the report.
- **The OpenGov Network** - any logged in OpenGov user can view the report.
- **Public** - anyone with a link can view the report.

How is Private Information (PI) or Personally Identifiable Information (PII) or Sensitive Information (SI) handled at OpenGov?

The OpenGov platform places restrictions on report access. At the customer's account, only an administrator can publicize data. They have complete control over who can access the data. Therefore, it is up to our customers to redact information before they decide to share it within our application.

How do users report vulnerabilities to OpenGov?

Vulnerabilities should be reported to support@opengov.com. Reported vulnerabilities will be confirmed and then fixed, by working with the reporting party and our security advisors, in a timely manner.

What is OpenGov's breach disclosure policy?

OpenGov's breach disclosure policy is to generally disclose incidents without delay. However, delays may occur due to the nature of the investigation. For example, delays are sometimes required by law enforcement.

What controls does OpenGov exercise over the qualification and performance of their team?

For every employee, OpenGov validates references and runs a comprehensive background check.

APPLICATION CONFIGURATION

How do users access OpenGov?

Since OpenGov is a Saas solution, users can access our platform with any up to date Internet Explorer, Safari, Firefox or Chrome browser.

What is OpenGov's hosting hardware and software platform?

OpenGov uses services provided by Amazon Web Services including PostgreSQL and React. We use Chef for application configuration management and run on of Linux with the latest security patches on Amazon EC2.

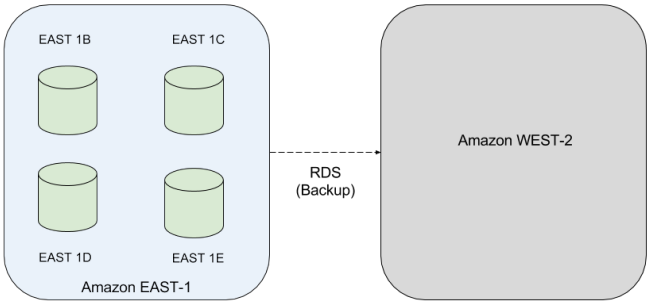
How does OpenGov release software?

OpenGov Engineering uses an *Agile* development process. This process involves dividing development into monthly releases. The monthly release is subject to automated and user testing before being merged into our production code.

How does OpenGov ensure that updates will not have adverse operational impact?

OpenGov subjects all new feature releases to a week of automated and manual user testing. The software is not released until we resolve all critical issues. Furthermore, since OpenGov is a SaaS solution hosted on Amazon Web Services we can automatically deploy updates across the entire platform with minimal customer impact. Feature deployments generally happen seamlessly without any user interruption. When deployments will impact users we will send out notifications beforehand.

DATA RETENTION AND BACKUP



What is OpenGov's backup and disaster recovery plan?

To backup data and our services, OpenGov takes daily snapshots of our entire database using Amazon's RDS service. These snapshots are stored in multiple data-centers and in a back-up region (AWS WEST-2). All raw data is backed up on Amazon S3 as well.

In the event of losing data due to a software failure, OpenGov will restore from the last saved snapshot. This is a simple and reversible operation on AWS. All raw uploads are preserved on S3 and are recoverable at any point in time.

To avoid datacenter or server disruptions, OpenGov relies on Amazon's multi-availability zones to ensure that we can continue operations in case of a datacenter or server failure. We host our production servers and databases in Amazon's EAST-1 region. This region has multiple zones, each with its own datacenter. Across these zones, data is continuously replicated. Every twenty-four hours, a snapshot is sent to Amazon's WEST-2 region for backups.

In the case of a server or datacenter failure within a region, Amazon's multi-availability zones ensure that OpenGov can continue operations. This service performs real-time replication to separate data-centers. If a data-center goes down due to a natural or man-made disaster or hardware fault, OpenGov is automatically switched to a replicated database immediately limiting data loss to a few seconds.

In case of a failure across the entire region, we will manually switch to another Amazon region. This may take several hours.

What is the retention period for the data being backed up?

Seven days.

AUDITING

What are the policies and procedures for logging, authentication, authorization and password management events (successful login, unsuccessful login, etc.) including how long this information is kept and who has access to the log data?

OpenGov collects logs for all events described, and the information is stored securely in AWS. Information is kept for at least 60 days.

From where does OpenGov collect/review log information?

1. Application logs and services that can potentially identify what transactions have been performed, at what time, by whom, and on what, such as web, database and authentication can provide detailed information about those activities
2. System logs for operating systems
3. Change management logs that document changes in the business environment.

Data Import

How do users import data to OpenGov

OpenGov uses a user facing Data Manager to import and export data from the platform. OpenGov does maintain external APIs to add data to the platform. These APIs require a user to authenticate with an existing OpenGov user via OAUTH 2.0.

OpenGov offers integrations that use our OAUTH 2.0 API. These integrations are offered by Scribe Software, a Gartner Magic quadrant Integration Platform as a Service. Scribe communicates from a local agent directly to OpenGov's servers with TLS 1.2. You can read about Scribe's security overview here: https://www.scribesoft.com/wp-content/uploads/2016/01/Scribe-Online-Security-Overview.pdf.

Published April 2017