Cloud Hosting Services FAQ

General Questions

Do I have to request a code update?

- All hosted clients are scheduled for regular code updates and all mandatory code updates are taken care of after hours. If for any reason a client wants an unscheduled code update, we can perform during normal business hours (8:30-4:30) through a ticket request.

Do I need to request an upgrade?

- Hosted clients are typically upgraded within 6-8 weeks after the version release. If for any reason you would like to be upgraded earlier, please make a request to support.

Who monitors the hosted environment?

- We have a dedicated DevOps team that monitors the hosted environment and proactively addresses issues that may occur.

When is maintenance performed?

- Maintenance is performed monthly and after hours as to not interfere with client's workdays.

Security Questions

Do you offer multi-factor authentication (MFA)?

- Currently it is not offered but we are planning on adding said functionality in the future with a target date of 2023.

Is the data encrypted between host and client?

- Yes, data is encrypted through RMI and over SSL transport layer.

Is data at rest encrypted?

- Important personally identifiable information (PII) is encrypted at rest and the keys to this encryption are client specific.

What are the backup procedures for the hosted environment?

- Snapshots are taken of the underlying instances (and all associated data) with the following retention settings:
    - Weekday snapshots retained for a month
    - Monthly snapshots retained for a year
    - End of year snapshots retained indefinitely
- Additionally, EGT DataVault also persists all client data to S3 as an alternate backup avenue.

Is the service being monitored?

- Yes, we use a combination of built-in AWS monitoring tools as well as our own remote monitoring and management (RMM) platform to proactively assess our environment.

Who has access to the hosted environment?

- We restrict access to our host servers to a limited number of internal personnel with various levels of permissions depending on their role.

What are the password requirements?

- Minimum of 8 characters.
- Password is case sensitive.

Can anyone else access my MCSJ database?

- No, aside from EGT personal granted access in order to perform their job functions.
- Access to your specific installation must be configured on each client with specific parameters along with the username and password authentication required to access the application.

Who manages active users?

- We require a designated party from your municipality to manage active users and security levels.