Data Management Solutions
Validate ▪ Create ▪ Convert

Security Statement

Policy Statement

This policy sets forth information security standards for the protection of client information through the Data Management Solutions- Data Validation Platform software.

Maintaining the confidentially and integrity of client information stored, processed, or transmitted is a requirement of all personnel. This policy applies to information in any format including electronic and hard copy.

The security policy ensures that:

- Information will be protected against unauthorized access.
- Confidentiality of information will be assured.
- The integrity of information will be maintained.
- Availability of Information for business processes will be maintained.
- All actual or suspected information security breaches will be reported and thoroughly investigated.
- Information security training is available for all employees.
- Procedures exist to support the policy, including virus control measures, passwords, and continuity plans.

The security of our client's data is of utmost importance as we have and will continue to explore measures to ensure the safety of our client's data. Our secure Data Management Solution: Data Validation Platform web application has been thoroughly tested through Veracode's cyber-security experts. This robust penetration and application security testing allowed Data Management Solutions- Data Validation Platform to put parameters in place to mitigate risk and provide a sound portal for your data auditing and reconciliation needs.

Data Storage

All data is housed in an encrypted **DigitalOcean** managed database. Data is encrypted in transit with SSL (secure sockets layer) and at rest with LUKS (Linux Unified Key Setup) with automatic updates with security patches.

Electronic Authorization & Application Hosting

Access to Data Management Solutions (DMS) is handled through Amazon Web Service (AWS) Cognito for user authentication and control access authorization. Additionally, custom authorization code within the application for each API route exists so users can only access data from the organization and company they belong to.

Application hosting is within Vercel who is SOC2 Type 2 compliant. The data housed within the application is encrypted at rest (AES-256) and in transit (HTTPS / TLS), including sensitive information like access tokens and secrets.

Ongoing Security:

Annual application security auditing and penetration testing is performed through Veracode to identify vulnerabilities and loopholes to prevent cyber-attacks such as SQL Injection and Cross-site scripting.