

Project Overview

The Rochester Genesee Regional Transportation Authority seeks to procure a secure, user-friendly board management software platform that enhances governance, streamlines board operations, and supports engagement across all stakeholders. The selected solution must align with organizational values of transparency and operational efficiency.

1. Functional Requirements

A. Document Management

1. Secure upload, storage, and sharing of board materials (e.g., agendas, minutes, policies)
2. Version control and audit trails
3. Role-based access permissions

B. Meeting Management

1. Agenda creation and distribution
2. Internal resolution creation, editing, and approval
3. Distribution of Resolutions to Board members
4. Minute-taking tools with action item tracking
5. Calendar integration (e.g., Outlook, Google Calendar)
6. RSVP and attendance tracking

2. Security & Compliance

- A. Vendor shall be compliant the National Institute of Standards and Technology (NIST) control framework standards.
- B. All systems that handle controlled unclassified information (CUI), personal identifiable information (PII), or information that is considered confidential must be encrypted at rest and in transit using encryption/cryptographic algorithms (e.g. AES-256), key lengths, and protocols consistent with current NIST guidelines.
- C. Audit Logs must be implemented for all systems that handle CUI, PII, or information that is considered confidential.
- D. HTTP and protocols utilizing SSL/TLS shall use TLS 1.2 or later with 256-bit or larger key size for all data in transmission.
- E. Data stored outside of application system(s) or their respective databases must be protected by encryption in line with NIST recommendations.
- F. All data pertaining to RGRTA or its Covered Persons shall be stored within the United States.
- G. A SOC 2 or similar report, to demonstrate the appropriate safeguards are in place for the protection of confidential data shall be provided to RGRTA upon request.
- H. Encryption keys shall be chosen randomly from the entire key space and all private keys shall be kept confidential. Key Lifecycle Management shall be consistent with NIST guidelines.
- I. Encryption keys shall allow for data retrieval, recovery for forensic or administrative use.
- J. Multi-Factor Authentication (MFA) shall be employed for all users to gain access to view, modify, add, execute, or delete information.
- K. Annual security assessments of systems shall be conducted through an independent third party including but not limited to Penetration Testing, Web Application Testing, and Vulnerability Assessment.
- L. RGRTA shall be notified of any planned or unplanned outages that would cause an interruption in service. Except for emergency security maintenance, systems are expected to be available and functional 24/7/365.

- M. Cybersecurity Incidents, Data Breaches, or those of similar nature shall be tracked, documented, and reported. Potential incidents or breaches shall be reported to RGRTA in writing within twenty-four (24) hours of suspicion/discovery to the Director of Technology Innovation, or his designee.

3. Accessibility & Usability

- A. Mobile app availability (iOS and Android)
- B. Offline access to board materials
- C. Intuitive user interface for non-technical users
- D. ADA/WCAG accessibility compliance

4. Collaboration & Engagement

- A. Discussion threads or commenting on documents
- B. Notifications and reminders
- C. Task assignment and tracking
- D. Ideally, integration with Microsoft Teams and Zoom, but at a minimum Zoom.

5. Administrative & Reporting Features

- A. Dashboard for board activity and engagement metrics
- B. Exportable reports (PDF, Excel)
- C. Customizable templates for agendas and minutes
- D. Resolution tracking and archival
- E. User management and onboarding tools

6. Implementation & Support

- A. Vendor shall adhere to timeline for deployment and onboarding provided in technical proposal
- B. Training resources shall be provided to include (live, recorded, or documentation)
- C. Dedicated customer support (email, chat, phone)
- D. SLA and uptime guarantees