Scope of Work:
Cloud-Based Policy Management System

1. Introduction

The City of Atlanta is the capital of Georgia with a population of approximately 480,000. The Atlanta metropolitan area is home to more than 6 million people and is the ninth-largest metropolis in the United States. Atlanta is the seat of Fulton County, and a small portion of the city extends eastward into Dekalb County. The City of Atlanta is also a major transportation hub containing the busiest airport in the world, Hartsfield-Jackson Atlanta International Airport.

The Atlanta Police Department serves a jurisdiction of 514,439 with a daily service population of approximately one million and in 2020 processed 95,805 incident reports per year including 21,600 Part One crime reports and 56,733 Part Two crime reports. APD is accredited through Commission on Accreditation for Law Enforcement Agencies, CALEA. As a full-service police agency, the Department has adopted a community-oriented philosophy and relies heavily upon community input and collaborative problem-solving strategies. It is through heightened community involvement in public safety matters that the Atlanta Police Department will most effectively address its many priorities, including, but not limited to youth-related crime, domestic violence, and the perception of crime in Atlanta. With an authorized strength of more than 2,000 sworn officers and over 500 civilian personnel, APD is the largest law enforcement agency in the State of Georgia, and a dedicated, high-profile force for positive change in our communities. The mission of APD is to create a safer Atlanta by reducing crime, ensuring the safety of our citizens, and building trust in partnership with our community.

The Planning, Research, & Accreditation (PRAU) Unit of the Atlanta Police Department (APD) is responsible for developing and maintaining the departmental policies, command memorandums and forms that govern all operations of APD, while leading and coordinating the Department's attainment and maintenance of state and national accreditation.

To achieve the above tasks, the APD requires a document management platform that guides our vital documents to include policies, forms, and subpoenas from the upload and approval process with the command staff to dissemination to personnel throughout the Department. Along with policy and document management functions, the platform must provide capabilities for training scheduling, course creation, survey creation, document archiving and accreditation.

2. Objectives

The cloud-based Policy Management System will:

- Provide secure, centralized access to all agency policies, SOPs, and operational guidelines.
- Automate policy lifecycle management: creation, review, approval, distribution, acknowledgment, and archival.
- Enable remote and multi-location access for authorized personnel while maintaining CALEA and CJIS compliance.
- Deliver real-time reporting, dashboards, and audit capabilities for compliance monitoring.
- Enhance accountability and awareness across all agency personnel.
- Ensure agency compliance with CALEA standards, CJIS regulations, and other applicable legal mandates.
- Facilitate accountability and awareness among agency personnel through tracking and certification workflows.

3. Scope of Services

The vendor shall provide the following services:

3.1 Cloud System Design and Configuration

- Configure the system for cloud deployment with secure multi-tenant or dedicated cloud architecture.
- Mobile applications for accessibility wherever there is internet access.
- Enterprise licensing for at least 3000 accounts.
- Unlimited or high-capacity storage.
- Implement CALEA-compliant user roles, permissions, and workflow approvals.
- Enable indexing, and classification aligned with law enforcement operations and regulatory standards.
- Integrate with cloud-accessible internal systems (e.g.,
-
- CJIS-compliant repositories, intranet portals).

3.2 Policy Lifecycle Management

- Enable drafting, editing, version control, and archival of policies and SOPs.
- Implement automated review schedules, notifications, and approval workflows consistent with CALEA standards.
- Track acknowledgments by personnel to ensure agency-wide compliance, allowing for up to 24 reviewers/approvers.
- Provide audit trails for legal, compliance, and internal review purposes.
- Ability to track signatures and generate reports for individual users and the documents they have signed off on.
- Ability to send inbox alert notifications and messages.

3.3 Compliance, Reporting, and Audit

- Generate audit-ready reports on policy status, review cycles, employee acknowledgment, and CALEA/CJIS compliance.

- Maintain tamper-proof audit logs accessible for remote review.
- Provide dashboards for agency leadership to monitor compliance and policy effectiveness.
- Ability to generate and disseminate surveys.
- Ability to disseminate subpoenas.

3.4 Security and Access Control

- Role-based access control (RBAC) with CALEA-defined roles (analyst, supervisor, administrator).
- CJIS-compliant encryption for data in transit and at rest.
- Multi-factor authentication, secure SSO, and IP restrictions for cloud access.
- Continuous monitoring and logging of user activity for security audits.
- Maintain secure audit logs for all user activity.

3.5 Training and Documentation

- Provide cloud-specific training for administrators, policy owners, and agency personnel.
- Deliver detailed cloud system user manuals, workflow guides, and policy SOP documentation.
- Conduct workshops on CALEA-compliant cloud policy management best practices.

3.6 Support and Maintenance

- Provide 24/7 cloud system support, updates, and troubleshooting.
- Ensure system uptime per Service Level Agreement (SLA), including disaster recovery and business continuity plans.
- Implement automatic software updates and security patches without downtime.

4. Technical Requirements

Requirement Category	Requirement Description	CALEA/CJIS Compliance Notes	Priority / Status
System Architecture	Cloud-hosted multi-tenant or dedicated environment	Must meet CALEA cloud standards; supports multi-location access	Mandatory
	Scalable infrastructure to handle all agency personnel	Supports vertical and horizontal scaling	Mandatory
	Geographic redundancy for disaster recovery	Ensures continuity of operations	Mandatory
	SaaS web-based interface	Accessible via modern browsers	Mandatory
Security & Access Control	FIPS 140-2 encryption at rest; TLS 1.2+ in transit	CJIS-compliant encryption required	Mandatory
	Role-Based Access Control (RBAC) aligned with agency roles	CALEA-defined roles: Analyst, Supervisor, Administrator	Mandatory
	Multi-Factor Authentication (MFA) and Single Sign-On (SSO)	SAML 2.0 / OAuth 2.0 for identity management	Mandatory

	Tamper-proof audit logs of all user activity	Required for CALEA audit readiness	Mandatory
	Continuous monitoring & vulnerability management	Penetration testing, patch management	Mandatory
Policy Lifecycle Management	Drafting, editing, version control	All policies and SOPs tracked digitally	Mandatory
	Automated review schedules and approval workflows	Ensures CALEA/SOP compliance	Mandatory
	Policy categorization, tagging, indexing	Supports rapid retrieval and reporting	Mandatory
	Acknowledgment tracking for all personnel	Audit-ready compliance tracking	Mandatory
	Policy archival and retention management	Legal & CALEA retention requirements	Mandatory
Data Migration & Historical Records	Data Migration & Historical Records	Data Migration & Historical Records	Mandatory
	Migration of historical audit trails (edits, approvals, access logs)	Must retain full auditability for CLEA and legal review	Mandatory
	Migration of version history for all policies and documents	All prior versions must remain accessible and traceable	Mandatory
	Migration of employee acknowledgment records	Must maintain proof of acknowledgment for compliance audits	Mandatory
	Data validation and reconciliation post-migration	completeness and accuracy of migrated data	Mandatory
	Chain-of-custody documentation for migrated records	Required for evidentiary and legal integrity	Mandatory
Integration Capabilities	Integration with CJIS-compliant databases	Secure APIs required	Mandatory
	RESTful or SOAP API support	Supports external system communication	Mandatory
	LDAP/Active Directory integration	Centralized user management	Mandatory
	Single Sign-On support	SAML 2.0 / OAuth 2.0	Mandatory
Performance & Availability	99.9% system uptime SLA	High availability for operational continuity	Mandatory
	Average page load ≤ 2 seconds; workflow ≤ 3 seconds	Ensures operational efficiency	Mandatory
	Supports concurrent users' agency-wide	Automatic scaling as needed	Mandatory
Reporting & Analytics	Customizable dashboards for policy status & compliance	CALEA and CJIS audit-ready	Mandatory
	Exportable reports (PDF, CSV, Excel)	Required for leadership & legal review	Mandatory
	Audit trail and reporting for policy changes	Supports CALEA compliance reporting	Mandatory
User Interface & Accessibility	Web-based, mobile-responsive interface	ADA / Section 508 compliant	Mandatory
	Compatible with Chrome, Edge, Firefox, Safari	Ensures accessibility for all personnel	Mandatory

Maintenance & Support	24/7 technical support with SLA	Defined response/resolution times	Mandatory
	Automatic software updates and patches	Zero-downtime updates preferred	Mandatory
	Cloud monitoring & alerting for performance/security	Continuous operational oversight	Mandatory
Disaster Recovery & Backup	Daily automated backups	Geographically redundant storage	Mandatory
	Recovery Time Objective (RTO) ≤ 4 hours	CALEA operational continuity requirement	Mandatory
	Recovery Point Objective (RPO) ≤ 15 minutes	Data integrity & continuity	Mandatory
	Periodic disaster recovery testing	Supports CALEA audit and certification	Mandatory

5. Deliverables

- Fully configured cloud-based PMS with CALEA compliance.
- User and administrator manuals and workflow documentation.
- Training completion documentation for all personnel.
- Compliance and audit-ready reports and dashboards.
- Final acceptance report with agency sign-off.
- Final acceptance report signed by agency leadership.

6. Assumptions

- Agency will provide existing policy documents, SOPs, and CALEA compliance requirements.
- Stakeholders will participate in requirements review, testing, and approvals.
- Necessary integration access to internal systems will be provided:
    - Commission on Accreditation for Law Enforcement Agencies (CALEA) web based digital accreditation process – Current partner PowerDMS
    - Georgia Police Accreditation Coalition (GPAC)
    - Atlanta Citizen Review Board
    - Several Internal Systems