

CapStorm for Government/Public Sector

Enabling Cross-Agency Insights and Compliance

Public sector organizations increasingly rely on Salesforce to manage citizen services, casework, and interdepartmental operations. But data in these environments must be protected, controlled, and compliant with state and federal mandates. CapStorm empowers government agencies to maintain full ownership of their Salesforce data—supporting secure backup, integration with approved platforms, and policy-driven retention without compromising constituent trust or regulatory compliance.

Industry Challenges

Government entities face unique data management pressures—balancing efficiency, transparency, and security across departments and jurisdictions.

- **Compliance with Regulations** – Data residency, retention, and access controls must align with legal and policy requirements
- **Cross-Agency Visibility** – Lack of centralized, real-time access limits collaboration and operational insight
- **Disaster Recovery Gaps** – Many agencies lack validated, auditable backup and recovery solutions
- **Sensitive Data Exposure** – Manual sandbox processes risk leaking PII or sensitive case information
- **Integration Barriers** – Getting data from Salesforce into platforms like Snowflake or Databricks remains a technical hurdle

Use Cases in Action

CapStorm helps government agencies ensure data continuity, support compliance, and strengthen internal operations.

- **Backup & Recovery for Data Governance** – Create validated backups of Salesforce data and metadata for legal inquiries, audits, or continuity planning
- **Cross-System Integration** – Replicate data in near real time to approved tools like Snowflake or Databricks for analysis and oversight
- **Secure Sandbox Seeding** – Populate development and training environments with sanitized, production-grade data to support agile project cycles
- **Field-Level Tracking & Retention Enforcement** – Maintain detailed history of data changes and automate enforcement of state or agency-specific retention policies
- **Data Residency & Control** – Keep sensitive citizen and agency data within government-managed environments, under your direct control

How We Solve Challenges

CapStorm enables secure data replication and governance workflows built to meet public sector standards.

- **CS:Enable** – Performs incremental Salesforce backups and secure replication into agency-approved systems
- **CS:Govern** – Automates retention policies, tracks field-level changes, and masks sensitive data for testing or development
- **Database Connectors** – Integrates Salesforce data into Snowflake, Databricks, SQL Server, or AWS for reporting, budgeting, and performance analysis

Who Benefits?

CapStorm supports cross-functional teams within government and public institutions:

- **Salesforce Admins** – Manage secure, policy-aligned backups and sandbox workflows
- **Data Integration Specialists** – Enable real-time data pipelines to approved analytics platforms
- **IT Security Leads** – Ensure data never leaves agency control, aligning with FedRAMP, CJIS, or internal protocols
- **Program Managers** – Gain better insight into operations and program performance
- **Compliance Officers** – Simplify audits and demonstrate continuous data oversight

Why CapStorm?

CapStorm delivers Salesforce data management purpose-built for public sector use. Our solutions provide near real-time replication, granular tracking, and complete control—without relying on vendor-hosted infrastructure or exposing sensitive data to external systems. Whether ensuring audit readiness, integrating platforms, or supporting digital government initiatives, CapStorm helps agencies stay secure, compliant, and in full control of their Salesforce data.

Keywords

Backup • Backup and recovery • Data backup • Data management • Data recovery • Data replication • Data restore • Disaster recovery • Incremental backup • Metadata backup • Restore metadata • Business continuity • Data archive • Data archiving • Data extraction • Data governance • Data integration • Data security • Metadata management • On premise software • On premise solution • Sandbox seeding • Data access • Data compliance • Data protection • Data reporting • Self-hosted software • Compliance • Data control • Recovery