Sprint 4 Planning Document

Project: Community Service App for the Government of Ontario
Team: PRJ666 – Team ReportEase
Sprint Duration: Weeks 11–13 (3 Weeks)

Sprint Goal

Sprint 4 focuses on securing the application, implementing advanced administrative features, ensuring compliance with privacy regulations, and setting up production-level backups. The primary objectives are to finalize role-based access control, enforce data protection standards, introduce system analytics, and complete system configuration tools before deployment.

Sprint Team Members & Assigned Tasks

Name	Assigned Tasks
Vrundaben Vijaykumar Patel	CS-023: Register Admin and Clerk Users, CS-027: Admin Config Panel
Sanskar Parakhlal Pardesi	CS-024: Role-Based Access Control Enforcement, CS-026: UI Customization
Nadi Aung Lin	CS-029: Data Encryption & Privacy Compliance
Abhi Mansukhbhai Chakrani	CS-025: Admin Analytics Dashboard
Yash Patel	CS-028: Secure MongoDB Integration, CS-030: Backup & Recovery

---

Sprint Scope

This sprint delivers security, privacy compliance, admin tools, and analytics features:

- Implement role-based user promotion and management.
- Enforce backend access control using middleware.
- Develop analytics dashboard for admins.
- Provide customizable admin control panels.
- Harden MongoDB security with encryption and access control.
- Align with Ontario privacy laws with encryption and data consent.
- Set up automated backup and recovery mechanisms.

Sprint Backlog Items

ID	Title	Description	Assignee	Effort (SP)
CS-023	Register Admin and Clerk Users	Promote users to clerk/admin with audit logs	Vrundaben Patel	4
CS-024	Access Control Enforcement (RBAC)	Enforce role-based access on routes and APIs	Sanskar Pardesi	5
CS-025	View System Analytics (Admin)	Provide system-level analytics dashboard	Abhi Chakrani	4
CS-026	UI Customization Based on Role	Dynamic UI components based on user role	Sanskar Pardesi	4
CS-027	Admin Controls for System Config	Manage system settings and user roles	Vrundaben Patel	5
CS-028	Secure MongoDB Integration	Harden DB with encryption and role control	Yash Patel	5
CS-029	Data Encryption and Privacy Compliance	Ensure data protection and FIPPA compliance	Nadi Lin	6
CS-030	Backup and Recovery Setup	Daily backups and admin restore options	Yash Patel	4

Sprint Task Breakdown

- **CS-023:** Implement user promotion flow, integrate with admin dashboard, and validate role updates with audit logs.
- **CS-024:** Apply middleware for route protection, log unauthorized access attempts, and test enforcement.
- **CS-025:** Build analytics dashboard with charts for issue trends, feedback ratings, and resolution times.
- **CS-026:** Customize sidebars, dashboard views, and available options based on logged-in roles.
- **CS-027:** Develop configuration panel for admins to manage departments, roles, and preferences.

- **CS-028:** Secure MongoDB with .env configs, validate access permissions, and enable data encryption.
- **CS-029:** Encrypt sensitive user data, ensure consent forms in registration, and implement privacy policy page.
- **CS-030:** Set up automated backups, build restore functionality, and display backup logs to admins.

Sprint Acceptance Criteria

- Role management and promotions functional with audit tracking.
- Unauthorized access prevented with middleware enforcement.
- Analytics dashboard displays system insights with filter options.
- UI adapts dynamically based on user role with no exposure of restricted features.
- Admin control panel operational for system settings.
- MongoDB secured with encryption, validated .env usage, and access control.
- All sensitive data encrypted and privacy policies enforced.
- Backup system operational with verified recovery tests and logs visible.

Sprint Deliverables

1. Fully integrated role-based access management.
2. Admin dashboard with system analytics and filters.
3. Configurable system settings panel for administrators.
4. Secured MongoDB integration with tested access control.
5. Encryption of sensitive user data and implemented privacy policy.
6. Automated daily backup setup with admin recovery access.
7. Updated Vercel deployment with final security and admin modules.
8. Comprehensive documentation of configurations and security settings.

Definition of Done (DoD)

- All features developed, tested, and merged into main/dev branches.
- MongoDB secured and validated with encryption and RBAC.

- UI tested for role-specific visibility and permissions.
- Admin tools validated for role management and analytics.
- Privacy policies integrated and reviewed against FIPPA.
- Backup and recovery tested in staging environment.
- Deployment updated with new features and access logs reviewed.

Sprint Risks & Mitigation

Risk	Mitigation Strategy
Role misassignment or bypass	Implement thorough role-based tests and audits
Encryption causes data access issues	Validate with test data before production rollout
Backup failures or restore errors	Perform scheduled restore tests and log validations
Privacy compliance gaps	Conduct checklist review against FIPPA with advisor
Analytics data inconsistency	Validate data sources and test filters thoroughly

---

Sprint Timeline

Week	Key Activities
11	Begin CS-023, CS-024, CS-026, initial MongoDB security setup (CS-028)
12	Develop analytics (CS-025), admin config (CS-027), data encryption (CS-029)
13	Finalize backup & recovery (CS-030), integrate all features, staging deployment, full testing

---

Sprint Review & Demo Goals

- Show role promotion and enforcement in the admin dashboard.
- Demonstrate real-time analytics dashboard with filters.
- Walk through admin configuration settings and role control.
- Verify secured MongoDB setup with encryption and access control.
- Show privacy policy integration and data encryption flow.
- Trigger and recover from a backup in the demo environment.

- Validate GitHub commits, updated CI/CD pipelines, and production deployment readiness.