# **🏃 Sprint Plan for ClockKo Wellness App Involving the Backend, Cloud, and CyberSecurity Team**

This plan breaks down the project into feature-focused sprints, clarifying where the Backend, Cloud Engineering, and Cybersecurity teams come in for each sprint.

## **🏁 Sprint 0: Project Setup & Core Infrastructure**

* Backend: Set up base API and database structure; prepare API docs; provide dev endpoints.
* Cloud Engineering: Provision dev/test environments, set up CI/CD pipelines, basic monitoring/logging.
* Cybersecurity: Document **security requirements** based on app features, Classify data by **sensitivity levels** (High/Medium/Low).

## **🔐 Sprint 1: Authentication**

* Backend: Implement auth endpoints (JWT), user database, session management.
* Cloud Engineering: Integrate auth with environment, set up secret storage for keys.
* Cybersecurity: Define authentication policy (password rules, MFA, account lockouts) advise on enforcing secure password storage (bcrypt/Argon2 with salts). Implement Multi-Factor Authentication (MFA) for admin or sensitive accounts.

## **⏱️ Sprint 2: Time Tracking**

* Backend: Time-tracking APIs, data models for work sessions, handle time events.
* Cloud Engineering: Ensure APIs are deployed and monitored, prepare logging for time tracking events.
* Cybersecurity: **Secure the time‑tracking API endpoints** with proper authentication (JWT, OAuth). Enforce **role‑based access control (RBAC)** so users can only view or edit their own records.

## **📋 Sprint 3: Task Management**

* Backend: CRUD endpoints for tasks, reminders, task timers.
* Cloud Engineering: Manage deployment of new features, monitor for performance spikes.
* Cybersecurity: Secure **task API endpoints** with authentication (JWT, OAuth) and **role‑based access control** so only authorized users can manage tasks. Ensure **encryption at rest and in transit** for all task data. Suggest monitoring strategies for **suspicious behavior,** such as mass task deletions or modifications.

## **🧘‍♂️ Sprint 4: Guided Shutdowns**

* Backend: End-of-day reflection endpoints, store user reflections.
* Cloud Engineering: Update monitoring for new backend flows.
* Cybersecurity: Securely store document reflections with encryption at rest (AES-256) and in transit (TLS 1.3). Advise on access controls to ensure only the reflection owner (and authorized services) can access it. Ensure compliance with **NDPR** and other privacy regulations — including defining **data retention** and deletion timelines for reflections.

## **👩‍💻 Sprint 5: Virtual Co-working**

* Backend: Real-time presence APIs, room management, WebSocket setup if needed.
* Cloud Engineering: Support for real-time backend infra (WebSockets/services), scaling testing.
* Cybersecurity: Pen-test real-time comms, review input validation, protect against abuse (e.g., spam).

## **📊 Sprint 6: Wellness Reports**

* Backend: Analytics endpoints, reporting logic, data aggregation jobs.
* Cloud Engineering: Schedule/report background jobs, monitor resource use.
* Cybersecurity: Anonymization of sensitive data, access control for reports.

## **🎯 Sprint 7: Community Challenges**

* Backend: Endpoints for challenges, leaderboard, progress tracking.
* Cloud Engineering: Deploy and monitor challenge features, handle scaling.
* Cybersecurity: Ensure fair play, protect leaderboard endpoints from tampering.

## **🎁 Sprint 8: Reward System**

* Backend: Endpoints for points, badge assignment, redeemables.
* Cloud Engineering: Support transactional consistency, monitor for abuse.
* Cybersecurity: Review reward logic for fraud, secure redemption process.

## **🧑 Sprint 9: Profile & Settings**

* Backend: User profile endpoints, settings persistence.
* Cloud Engineering: Roll out profile features, backup user data.
* Cybersecurity: Secure user data updates, privacy controls, access reviews.

## **🧩 Sprint 10: Shared UI, Polish & Accessibility**

* Backend: Support any additional API needs discovered during polish.
* Cloud Engineering: Optimize deployments for performance, review infra cost.
* Cybersecurity: Final accessibility & a11y security review, audit for vulnerabilities.

## **🧪 Sprint 11: Testing & Documentation**

* Backend: API documentation, assist with integration/end-to-end testing.
* Cloud Engineering: Test deployment pipelines, review rollback procedures.
* Cybersecurity: Conduct full app pen-test, review audit logs, compliance check.

## **🚀 Sprint 12: MVP Review, Bug Fixes, & Deployment**

* Backend: Final bug fixes, performance tuning, production support.
* Cloud Engineering: Finalize production rollout, monitoring/alerting, disaster recovery.
* Cybersecurity: Final security review, incident response plan, sign-off for go-live.

# **📌 Notes**

* Backend team should begin API design ahead of each frontend sprint; sync regularly with frontend for contract alignment.
* Cloud Engineering is involved at each stage for CI/CD, infra, and deployment support.
* Cybersecurity reviews and tests should be done early (shift-left) and at each sprint’s completion.
* Each sprint should include code review, documentation, and a demo, with all teams participating as relevant.