System Overview - Persona App with VPN Automation

Core System Components

Persona Management Engine

- **Multi-persona orchestration**: Concurrent identity management across platforms
- **Profile consistency validation**: Demographic, behavioral, and content alignment
- **Session isolation**: Separate browser contexts per persona
- **State synchronization**: Real-time persona status across all active sessions

VPN Automation Layer

- **Required Providers**: NordVPN, ExpressVPN, or Surfshark (API-enabled)
- **Geographic Requirements**:
  - **Cebu City Node**: Primary Philippines presence
  - **Manila Node**: Secondary Philippines location
  - **Additional APAC**: Singapore, Tokyo, Sydney for regional authenticity
- **Connection Management**: Automated switching, health monitoring, failover protocols
- **IP Validation**: Real-time geolocation verification against expected persona location

Platform Integration Hub

- **Social Media APIs**: Twitter/X, Instagram, TikTok, LinkedIn, Facebook
- **Content Scheduling**: Platform-specific optimal timing algorithms
- **Rate Limiting**: Respect platform API limits and avoid detection
- **Cross-platform Analytics**: Engagement tracking and behavioral consistency

Guardrails & Compliance Engine

- **Content Safety**: Automated screening for policy violations
- **Behavioral Analysis**: Natural posting patterns, engagement simulation
- **Risk Assessment**: Real-time scoring based on activity patterns
- **Audit Trail**: Complete forensic logging for compliance and debugging

Technology Stack

Backend Architecture

- **Framework**: Node.js/Express with TypeScript
- **Database**: PostgreSQL with encrypted storage (AES-256)
- **Session Management**: Redis for high-performance multi-persona state
- **Message Queue**: Bull/BullMQ for asynchronous task processing
- **API Gateway**: Rate limiting, authentication, request routing

Frontend Application

- **Framework**: React 18 with TypeScript/Vite
- **State Management**: Zustand for persona state, TanStack Query for server state
- **UI Components**: shadcn/ui with Tailwind CSS
- **Real-time Updates**: WebSocket connections for VPN status and platform activity

Security Infrastructure

- **Encryption**: AES-256-GCM for data at rest, TLS 1.3 for data in transit
- **Authentication**: JWT with refresh tokens, MFA support
- **Key Management**: HashiCorp Vault or AWS KMS integration
- **Network Security**: Zero-trust architecture with VPN-aware routing

Data Flow Architecture

Persona Activation Workflow

1. **Persona Selection**: User selects target persona and platforms
2. **VPN Connection**: Automated connection to persona's geographic location
3. **Browser Context**: Isolated session creation with persona-specific fingerprinting
4. **Platform Authentication**: Secure credential management and login automation
5. **Content Pipeline**: Scheduled posting with guardrail validation
6. **Monitoring**: Real-time tracking of all persona activities

VPN Integration Points

- **Connection Verification**: Continuous IP/location validation
- **Automatic Failover**: Switch to backup nodes on connection failure
- **Geographic Compliance**: Ensure persona location matches VPN endpoint
- **Performance Monitoring**: Latency and bandwidth optimization

Scalability & Performance

Horizontal Scaling

- **Microservices**: Persona engine, VPN manager, platform integrations as separate services
- **Load Balancing**: Distribute persona sessions across multiple instances
- **Database Sharding**: Partition persona data by geographic region
- **Caching Layer**: Redis for frequent lookups, CDN for static assets

Performance Targets

- **Persona Switch Time**: <30 seconds including VPN connection
- **Platform Response**: <2 seconds for content posting
- **Concurrent Personas**: Support 50+ active personas per instance
- **Uptime**: 99.9% availability with automated failover

Monitoring & Observability

Application Metrics

- **Persona Activity**: Active sessions, posting frequency, engagement rates
- **VPN Performance**: Connection success rate, latency, geographic accuracy
- **Platform Health**: API response times, rate limit usage, error rates
- **Security Events**: Failed authentications, suspicious activity, policy violations

Alerting Framework

- **Critical**: Proxy disconnections, platform API failures, security breaches
- **Warning**: High error rates, approaching rate limits, unusual behavior patterns
- **Info**: Successful persona switches, scheduled content delivery, proxy health status

Compliance & Legal Framework

Data Protection

- **GDPR Compliance**: Data minimization, right to deletion, consent management
- **Regional Requirements**: Philippines Data Privacy Act compliance
- **Platform Terms**: Adherence to each social media platform's terms of service
- **Audit Requirements**: Complete activity logging for regulatory review

Risk Management

- **Detection Avoidance**: Behavioral analysis to prevent platform detection
- **Content Moderation**: Automated screening before posting
- **Geographic Restrictions**: Respect platform availability by region
- **Rate Limiting**: Platform-specific posting frequency controls