Non-Functional Requirements & Disaster Recovery

for **Contact Center & Campaign Promotion System**

By **Incloud Solutions Pvt Ltd**

Availability & Resilience

- Overall SLA:
  The CRM system (Contact Center + Campaign Promotion) will maintain 99.9% uptime for production. This is critical because downtime directly affects both customer service responsiveness and ongoing campaigns.

- Contact Center:
  - RTO: ≤ 2 hours — customer tickets and inquiries must be accessible quickly, since service delays directly affect SLAs with end customers.
  - RPO: ≤ 15 minutes — loss of more than a few tickets is unacceptable, hence frequent incremental backups.
  - Failover: The contact center is deployed across multi-AZ in AWS, with automatic failover for the database and application tier. Auto-scaling policies ensure agent workloads are not interrupted during traffic spikes (e.g., seasonal product launches or service outages).

- Campaign Management:

  - RTO: ≤ 4 hours — campaign execution can tolerate slightly longer downtime than support tickets but must be restored quickly to avoid missed events or promotions.
  - RPO: ≤ 2 hours — marketing data and event registrations can be re-processed if minimal loss occurs.
  - Failover: Recovery requires manual restart following a runbook, ensuring that scheduled campaigns resume with accurate tracking (avoiding duplicate sends).

- Messaging Channels (Email, WhatsApp):
  - RTO: ≤ 1 hour — outbound notifications (campaigns, confirmations) must recover fast since they are time-sensitive.
  - RPO: ≤ 30 minutes — message queues ensure retries, but some in-flight data may be lost beyond this window.
  - Mechanism: Message brokers with retries, DLQs, and idempotent sends prevent duplication or permanent loss.

Environment & Data Management

- Environment Separation:
  - Production: Live system serving customers and campaigns.
  - Staging: Mirrors production with anonymized data for integration testing.
  - Development: Sandbox for feature development and unit testing. This prevents accidental leakage of customer data and ensures stable releases.

- Data Masking:
  - Customer names, phone numbers, and email addresses are anonymized in staging/dev. Example: “John Smith” → “User123,” phone/email replaced with dummy values. This ensures GDPR alignment and prevents misuse of real personal data in lower environments.

- Configuration Management:

    - Campaign templates (email/WhatsApp), routing rules, and contact flows are stored in Git repositories.
    - Secrets (SMTP credentials, API keys for WhatsApp, etc.) managed in AWS Secrets Manager with automatic 90-day rotation.

Error Handling & Reliability

- Retries & Backoff:
    - Failed email/WhatsApp sends automatically retried with exponential backoff (e.g., 1 min, 2 min, 4 min).
    - Avoids overwhelming external messaging providers during temporary outages.

- Idempotency:
    - Ticket creation is idempotent → prevents duplicate tickets if retries occur.
    - Campaign sends carry unique IDs, so a prospect never receives duplicate messages even after a system retry.

- Dead Letter Queues (DLQs):
    - Outbound failures (email bounces, WhatsApp delivery failures) go to DLQ.
    - The Ops team reviews DLQ daily and take corrective action (e.g., update invalid email addresses).

Security & Compliance

- IAM & Access Control:
    - Agents → can only view/handle assigned tickets.
    - Supervisors → can reassign and review division-level tickets.
    - Campaign Managers → limited to managing campaigns/events.
    - Enforced via role-based IAM + application RBAC.

- Encryption:
    - In transit: All customer interactions (inquiries, campaign confirmations) secured with TLS 1.2+.
    - At rest: AES-256 applied to databases (tickets, campaigns), S3 objects (attachments, campaign media), and call recordings.

- Compliance:
    - CIS AWS Baseline applied to infrastructure.
    - GDPR alignment for data collection, customer consent, and opt-out from campaigns.
    - Audit trails required for all marketing activities and support ticket updates.

- Audit Logging:
    - Ticket updates include who, when, what action.
    - The campaign sends logged with template, recipient, timestamp.
    - Ensures traceability for compliance audits.

Integration Requirements

- CRM/Contact Center Integration:

- REST APIs with OAuth2 authentication.
- Ensures tickets and campaigns are updated securely from external tools (e.g., ERP, mobile apps).

- 3rd-Party Messaging (Email/WhatsApp):
  - Circuit breakers prevent cascading failures if the provider is down.
  - Timeouts (30s default) ensure the system doesn't hang on slow external responses.

- Ticketing & Feedback:
  - Feedback forms (post-event, campaign response) automatically log back into the CRM.
  - Integrated with a survey system to generate insights.

Operations & Monitoring

- SLO/SLA Metrics:
  - Tickets are not updated within 48h → Escalation.
  - Email bounce rate > 5% → Alert.
  - Campaign send error > 1% for 5 min → Alert.
  - Queue backlog > 2 min avg age → Alert.
  - RDS CPU > 80% for 15 min → Alert.

- Monitoring:
  - CloudWatch dashboards for ticket processing, campaign delivery rate, database health, and queue backlogs.
  - Logs stored in S3 with Athena queries for trend analysis.

- Escalation Path:
  - Tier 1 On-call Agent → Supervisor → IT Team → Management (all within 1h escalation window).

- Ops Cadence:
  - Weekly SLA/SLO review with ops team.
  - Monthly reporting to management with recommendations for improvement.

Disaster Recovery (DR)

- Backups:
  - Daily RDS snapshots for ticket/campaign databases (with PITR enabled).
  - S3 buckets (attachments, campaign media) with versioning + cross-region replication.

- Runbooks:
  - Documented procedures for resuming campaigns without duplicate sends.
  - Ticket continuity ensured by re-processing messages from DLQ.

- DR Drills:
  - Conducted at least annually and after major releases.
  - Simulate failure of one AZ and validate that campaigns, contact flows, and messaging channels resume within defined RTO/RPO.