LLM Email Drafting Agent – Engineering Requirements (v1.0)

Generated: 2025-08-13T21:30:35.123794Z

# 1. Introduction

The LLM Email Drafting Agent (the “Drafting Agent”) generates supplier-facing negotiation emails from structured templates, enforces guardrails, supports buyer edits with re-validation, and sends via configured mail providers. It is triggered by the Opportunity Agent and Negotiation Agent with template suggestions and pre-filled values and must produce natural, human-like subjects and contact identity while maintaining full, invisible traceability through headers and reply-alias routing.

# 2. Scope

In scope: Template selection, JSON-only LLM compose, validation & regen loop, HTML rendering, subject/preheader generation, signature, invisible traceability (headers/reply alias), buyer edits & re-validation, sending (SMTP/SendGrid), export (.docx/.eml), audit events.

Out of scope: Market/benchmark claims, supplier portal UI, pricing analytics (handled by Opportunity/Policy engines).

# 3. Functional Requirements

FR-1.0 Template Selection — Load by template\_id; error on unknown. Supports base templates and 8 outreach templates.

FR-1.1 Placeholders — Replace {{VAR\_NAME}}; unknown vars remain visibly unchanged.

FR-1.2 Sections — intro, instructions, what\_good\_looks\_like, how\_to\_respond, deadline, signature.

FR-1.3 Tables — Render [TABLE:id] and [OPTIONAL:TABLE:id]; supplier-editable columns (id, header, type, precision, required).

FR-1.4 Guardrails — Supplier-safe language; no benchmark/market/peer claims; invite strongest pricing/options.

FR-2.0 JSON-only Compose — LLM returns valid JSON (sections, tables, email\_html, compliance).

FR-2.1 Min-Words — Enforce per-section thresholds (intro, instructions, WGLL, HTR).

FR-2.2 Banned Phrases — Reject/sanitize banned phrases/regex.

FR-2.3 Required Tables — Ensure all tables\_required are present.

FR-3.0 Natural Subject — 48–72 chars soft; no codes/brackets/ALL-CAPS/“!!!”; pattern bank per template.

FR-3.1 Preheader — 60–90 chars; concise ask; no IDs/codes.

FR-3.2 Friendly From — From: "{{Your\_Name}} ({{Company\_Name}})" <negotiations@yourdomain.com>.

FR-3.3 Reply-Alias Traceability — Unique Reply-To per thread: negotiations+{{opaque}}@yourdomain.com.

FR-3.4 Header IDs — Message-ID, In-Reply-To, References, X-Opportunity-ID, X-Negotiation-ID, X-Draft-ID.

FR-3.5 Link Hygiene — Clean/first-party short URLs; tracking optional per tenant.

FR-4.0 Regen Loop — Self-heal → validate → targeted LLM fix (max 3 attempts).

FR-4.1 Naturalness Lints — Fail on leftover placeholders in subject/preheader/signature; all-caps; excessive punctuation; double spaces; intro readability check.

FR-5.0 Rendering — Convert template markdown to HTML; append signature block.

FR-5.1 Exports — Provide .docx and .eml exports.

FR-6.0 Buyer Edits — Allow edits to unlocked sections/subject; re-validate on each edit.

FR-6.1 Diff & Audit — Store generated vs edited; expose diff; persist edit audit.

FR-7.0 Sending — /send supports SMTP/SendGrid; headers whitelist (X-\*, threading); returns provider status.

FR-7.1 Dry-Run — Simulate send without provider call.

FR-8.0 Opportunity Coverage — Must draft for ALL opportunities base data exposes via (a) direct template from Opportunity Agent, (b) mapped templates, (c) safe fallback (value-gap or BACO), (d) admin can add templates without redeploy.

FR-8.1 Coverage Matrix — Maintain intent→[template\_ids] mapping and coverage metrics; log gaps.

FR-8.2 Unknown Types — Select closest template by required inputs; include reason in audit.

FR-9.0 Events — Emit draft.created, draft.validated, draft.failed, draft.sent with correlation IDs.

FR-10.0 RBAC — Agents may draft/validate; only Buyers/Admins may send.

FR-11.0 Config — Tenant toggles: subject rules, banned phrases, min-words, attempts, provider, link tracking, reply alias.

FR-12.0 Idempotency — Same inputs → same JSON/HTML (except generated IDs/timestamps).

# 4. Data Model

stylebook — version, templates[], tables[], global.detail\_controls.

template — id, subject\_template, body\_template\_markdown[], sections\_required[], variables[].

table\_def — id, columns[{id,header,type,precision,required}], editable\_by\_supplier.

draft — draft\_id, template\_id, values{}, sections{}, tables[], email\_html, subject, preheader, headers{}.

guardrails — ban\_phrases[], ban\_phrases\_regex[], min\_words{}.

trace\_binding — draft\_id, message\_id, reply\_alias\_token, x\_headers{}.

events — type, payload, opportunity\_id, negotiation\_id, draft\_id, ts.

# 5. Processing Flow

1) Handoff from Opportunity/Negotiation (template\_suggestions, prefill\_values, guardrails).

2) Select template (coverage matrix; fallback if needed).

3) Compose (LLM) → JSON-only.

4) Self-heal (pad, add tables, sanitize).

5) Validate (naturalness → structural → guardrails).

6) Targeted regen (fix only failing items).

7) Buyer edit (optional) → re-validate.

8) Render HTML + subject + preheader + signature.

9) Send (SMTP/SendGrid) with headers + reply alias.

10) Emit events & persist audit/trace binding.

# 6. Output Schema (Draft Payload)

subject — Natural, human-style subject (no codes).

preheader — Hidden preview text.

sections — intro, instructions, what\_good\_looks\_like, how\_to\_respond, deadline, signature.

tables — List of table IDs included.

email\_html — Rendered HTML body.

headers — X-Opportunity-ID, X-Negotiation-ID, X-Draft-ID; provider threading headers.

compliance — word\_counts{}, banned\_phrases\_found[], naturalness{subject\_ok, preheader\_ok, readability\_score}.

audit — template\_id, selected\_via (direct/fallback), coverage\_reason, opportunity\_intent.

# 7. Opportunity Coverage (Must-Have)

Complete coverage: draft for any opportunity the base data exposes via direct mapping or safe fallback; still invite strongest pricing and capture required commercial tables.

Extensible: admins can add templates and update mapping without redeploy.

Evidence: metrics for direct match vs fallback; send/read/reply rates by template.

# 8. Non-Functional Requirements

Performance — Compose+validate+render ≤ 2.0s p95 (LLM latency excluded if external).

Determinism — Same inputs → same JSON/HTML (excluding IDs/timestamps).

Reliability — 99.9% monthly availability for /draft, /validate, /render, /send.

Security/Privacy — PII masking; redacted secrets; TLS; encryption at rest.

RBAC & Audit — Role checks on /send; retain edit/send audit ≥ 24 months.

Compliance — No IDs in visible subject/body/signature; no hidden HTML comments carrying codes.

Regional Controls — Data residency flags (EU/UK).

# 9. Acceptance Criteria

1) Happy path: direct template suggestion → passes validation → send OK with headers + reply alias.

2) Coverage fallback: unknown intent → fallback template selected → passes guardrails with best\_offer\_table.

3) Naturalness checks: leftover {{…}} or ALL-CAPS subject fails → regen fixes within 2 attempts.

4) Guardrails: phrase “benchmark indicates” sanitized to neutral invite for strongest pricing.

5) Buyer edit: edit triggers re-validation; must pass before send.

6) Determinism: identical inputs produce identical JSON/HTML (excluding IDs/timestamps).

7) Threading: reply uses In-Reply-To/References; inbound routes via reply alias token.

8) Exports: .docx and .eml open correctly.

9) Metrics: coverage metrics show at least one fallback and one direct-match case.

# 10. Implementation Notes (Informative)

Validation order: naturalness → structural → guardrails; regen narrows to failing elements first (subject/preheader/intro).

Subject pattern bank per template (6–10 variants) to avoid repetition.

Headers whitelist to prevent injection; provider adapters set threading/trace headers, never the visible body.

Coverage mapping lives in config; unknown intents choose nearest template by required sections/tables.