Prompt Meta-Guidelines – Workplace-AI-Prompts

This document defines the meta-guidelines for designing and using prompts in Version‑2 of the Workplace-AI-Prompts project. It ensures clarity, consistency, compliance, and robustness across all workflows and templates. These guidelines are refined from industry practices, LLM safety literature (e.g., OWASP), and real-world adoption feedback.

# 1. Core Prompt Structure

[CONTEXT BLOCK]  
Role: <e.g. Incident Manager, Vendor Lead, Receptionist>  
Scenario: <Brief description of the situation>  
System / Tools involved: <optional>  
Constraints & Policies: <e.g. safety rules, data privacy, tone>  
Output Format: <specify structure: JSON, bullets, table, email>  
Required Fields: <placeholders for data to be filled>  
  
[PROMPT BODY]  
You are [Role]. Based on [Scenario + Required Fields + Constraints], generate …

This structure enforces context, constraints, and clarity before execution, making prompts auditable and reusable.

# 2. Pre-Flight Checklist

* 1. All required fields (role, context, date, etc.) are filled.
* 2. Output format is specified (table, JSON, email, etc.).
* 3. Constraints & policies are defined (tone, data rules, limits).
* 4. Scope is limited to one task at a time.
* 5. Max length or sections are set to control verbosity.
* 6. Edge/error cases are specified (fallback instructions).
* 7. Human review required is flagged before final use.

# 3. Guardrails & Validations

• Sensitive Data Filter: If inputs contain IDs, financials, or PII, request redacted version.

• Step-Limit Rule: No more than 5 sub-steps per prompt; further steps should be iterative.

• Explain-Before-Action: Ask AI to summarize reasoning before giving outputs.

• Fallback Template: If missing data, AI should respond with a safe template asking for more info.

• Version Tagging: Include version tag (e.g., v2.0-2025) for traceability.

# 4. Why This is Stronger than Existing Kits

Most public prompt libraries provide unstructured requests without context blocks or validations. By embedding context, constraints, guardrails, and review steps, these meta-guidelines reduce hallucinations, increase repeatability, and align with AI safety recommendations (e.g., OWASP LLM risks). They transform prompts from one-off commands into structured, industry-acceptable playbooks.