

SUPPLEMENTAL PROJECT · PROOF OF CONCEPT · ONE-PAGE SUMMARY

Brampton HR AI Mentor: Government RAG with Guardrails

A government-flavored proof that an AI assistant can be trusted to stay inside approved sources, cite them, and say “I don’t know” when the source does not support an answer. A retrieval-augmented HR policy assistant that answers employee questions from official policy documents only. Personal proof of concept inspired by the City of Brampton’s HR modernization goals; not an official City of Brampton product.

Role: Solo Engineer **Stack:** Python · LangChain · FAISS · Google Gemini API · Streamlit

Corpus: Official Brampton HR policies incl. HRM-150, HRM-160, HRM-210

Status: Working PoC · qualitative success criteria

WHAT IT IS

An end-to-end RAG prototype that ingests curated HR policy PDFs, indexes them in a persisted FAISS vector store with policy ID, section heading, and page number as metadata, and exposes a Streamlit chat interface where every answer is grounded in policy text and accompanied by citations.

PROTECTION-BY-DESIGN GUARDRAILS

- **Scope enforcement:** if no retrieved chunk meets the similarity threshold, the assistant answers “I don’t know” and suggests contacting HR instead of guessing.
- **Policy-only answers:** the system prompt explicitly forbids inventing rules or referencing unapproved sources; answers are built only from retrieved chunks, with no open-internet retrieval.
- **Citations required:** the model must quote or cite the underlying policy text on every answer.
- **HR-aware chunking:** documents are split with section headings and policy numbers preserved as metadata for traceability.
- **Auditable by leadership:** inline citations let HR review, verify, and refine responses.
- **Simple by intent:** a small, opinionated build that shows how to start safely with generative AI in a regulated domain.

PROTOTYPE OUTCOMES

Cited

Every answer grounded in policy text

Refuses

Declines out-of-scope questions rather than hallucinate

Traceable

Policy ID, section, and page on record

BUSINESS IMPACT

Overloaded HR inboxes and repetitive policy questions are a universal public-sector problem, but so is the risk of an AI inventing policy. This PoC demonstrates the safety-and-compliance pattern a government deployment demands and provides a template any municipal or enterprise HR team can expand toward self-service.