



AI/ML Base Model



Model Inputs



Model Outputs



Data Security

What goes here?

Fill this in with a sentence on the problem being solved and list the goals used to guide the model.

Why important?

Model goals affect the way in which the model behaves and the outcomes it provides.

What goes here?

- Model Type -- AI/NLP, AI/ML, GenAI (language), GenAl (vision), etc.
- Name of any base model, version, vendor & limitations
- Training data sources, time period, languages, etc.

Why important?

Knowing if a company trained its own model or use a pre-trained base model helps you know what to ask about data usage & security. Details on the training data help you determine potential biases & ask how they were mitigated.

Why important?

To know how data from your project or other additional data contributes to the outputs.



Model Scope & Limits

What goes here?

Information about where the model can be applied versus what is out of scope, information on any known limitations or research biases.

Why important?

To avoid biased, inaccurate or unreliable results from using the model where it does not apply. To know about limitations that vary by usage occasion.

What goes here?

Intermediate & final outputs

Why important?

Intermediate outputs affect a model's "decision" or final outputs

Why important?

To ensure users know confidential information is secure.



Model Performance / Validation

What goes here?

- Describe testing & evaluation including model performance & human involvement (if any)
- List guardrails that prevent model outcomes with negative effects
- Evidence that model "decisions" are applied relatively evenly to individuals (socially unbiased)

Why important?

Information provided here will demonstrate the degree to which the model-building company has thoughtfully evaluated the AI model & outputs from computational and human impact angles.