

AI - Glossary of Terms

Agent: An AI system that uses a LLM to perceive goals and context, then autonomously selects and executes actions such as calling tools, responding to workflows without human involvement to achieve specific outcomes beyond simple responses.

Artificial Intelligence (AI): Computer systems designed to perform tasks that typically require human intelligence, such as learning from data, recognizing patterns, understanding language, making predictions, and generating content.

Chatbot: A software interface powered by Generative AI that simulates human conversation by interpreting the user inputs and prompts by generating text or voice responses. This interface is regularly improved upon with updated LLM models.

Generative AI: AI systems trained on large language models that can generate new content, including text summaries, images, audio, video, executable code and suggestions.

Hallucination: When an AI system generates plausible-sounding yet false, inaccurate or fabricated output.

Human Review: The requirement that a qualified person evaluates AI-generated content of recommendations for accuracy, bias, appropriateness and alignment with SelfDesign's mission, values, and legislative obligations to PIPA before it is used, shared, or acted upon. Human review means a person reads, understands and takes responsibility for the final decision or output.

Intellectual Property: We mean the following when we say intellectual property:

- all trademarks (including logos), trade dress, corporate names, business names, trade names and domain names, whether or not they have been registered, or are registrable or are the subject of applications for registration;
- all work protectable by copyright, including any literary, artistic, dramatic or musical work, whether or not it has been registered or is the subject of application for registration;
- all confidential information, trade secrets, and know-how;
- all discoveries, inventions, innovations, designs, works of authorship, algorithms, drawings, compilations of information and analyses, methods, processes, techniques, specifications, source code, improvements and ideas; and
- all other intellectual and industrial property, whether or not it has been registered, or registrable, or is the subject of any applications for registration.

Large Language Model (LLM): A large-scale dataset trained on text data to learn patterns in language, enabling word prediction, interpreting prompts, and performing text-based question answering and summarization.

Local Processing: The use of AI models or tools that run on devices or infrastructure controlled either by the organization or the individual user, where data is processed and does not leave the device or environment to a third-party AI service.

Model Context Protocol (MCP): An MCP server is a program that exposes tools, data, or capabilities to an AI model through the Model Context Protocol — a standard developed by Anthropic for connecting LLMs to external systems. Think of it as a translator and gateway: the server speaks MCP on one side (so any MCP-compatible AI client can talk to it the same way) and whatever the underlying system speaks on the other side (a database, an API, a file system, a SaaS app like Gmail or Asana, etc.). The AI doesn't need custom integration code for each service — it just needs to know how to speak MCP.

A server typically offers some combination of:

- **Tools** — actions the model can invoke (send an email, query a database, create a ticket)
- **Resources** — data the model can read (files, records, documents)
- **Prompts** — reusable templates the user or model can call up

Personally Identifiable Information (PII): Any information that can be used to identify a specific individual, either on its own or when combined with other information. This includes, but is not limited to, names, email addresses, phone numbers, physical addresses, dates of birth, identification numbers or any combination of information that makes an individual identifiable.

Sensitive Data: Information that requires heightened protection because its unauthorized disclosure, misuse, or loss could cause significant harm to individuals, the organization, or its stakeholders. This includes, but is not limited to, identity, health, or financial records, contractual agreements, legal matters, unpublished or in-draft strategic plans, security detail, or other intellectual property.

Third Party AI Service: Any AI Tool, platform, or API operated by an external vendor where prompts, data, or content are transmitted outside of organizationally managed infrastructure or an individual user's device for processing.