### **Protocol for Tool Definition and Usage**

#### **Core Principle**

All tools must be defined and utilized with absolute precision. The tool's schema, as defined in the [tools] section, is the single source of truth. Any deviation in a tool's definition, call, or output is a critical failure.

### **1. Tool Inventory and Design Mandates**

* **Minimum Tool Quantity:** The agent protocol **must** include a minimum of 10 distinct tools. This ensures the agent possesses the necessary capability to execute complex, multi-step workflows beyond simple, single-shot tasks.
* **Inclusion of User Context:** Tools that perform user-specific actions (e.g., booking, retrieving order status, accessing account details) **must** include parameters to handle user context. A user\_id or equivalent identifier is mandatory for such tools to ensure they operate on behalf of the correct user.

### **2. Tool Call Mandates: Strict Adherence to Schema**

When the agent invokes a tool in a [tool\_use] block, it must follow these rules without exception.

* **Exact Function Naming:** The function\_name in the [tool\_use] block **must exactly match** the name of a function defined in the [tools] schema. Typos, partial names, or alternate casings are forbidden.
* **Absolute Parameter Integrity:**
  + **Defined Parameters Only:** The agent can **only** use arguments explicitly defined in the function's parameters schema. Inventing new parameters or using parameters from other tools is a hallucination.
  + **Required Parameters:** All parameters marked as "required" in the schema **must** be provided in the tool call.
  + **Optional Parameters:** Optional parameters may be used if the information is available and relevant, but they are not mandatory.
* **Strict Enum Adherence:** If a parameter is restricted to an enum list, the provided value **must be an exact, case-sensitive match** to one of the values in that list.
  + **Example:** If a priority parameter has an enum of ["HIGH", "MEDIUM", "LOW"], the agent can only use one of these three strings. Using "high" or "urgent" is a violation.
* **Data Type and Pattern Conformance:** The value provided for a parameter **must** conform to its defined type and pattern.
  + **Type:** A value for a parameter defined as integer cannot be a string (e.g., 42, not "42").
  + **Pattern:** If a parameter has a regex pattern (e.g., "^SCH-[0-9A-Z]{8}$" for a schedule\_id), the provided value **must** match this format perfectly.

### **3. Tool Output Mandates: Precise and Usable Returns**

The structure of the [tool\_output] and the agent's subsequent use of it are critical for successful task completion.

* **Exact Return Schema Compliance:** The JSON structure of the [tool\_output] **must exactly match** the returns schema defined for that function. This includes all property names, data types, and object nesting. There can be no deviation.
* **No Extraneous Return Properties:** The [tool\_output] **must not** contain any properties or fields that are not explicitly defined in the tool's returns schema. Adding extra information is forbidden.
* **Accurate Usage of Returned Data:** The agent's subsequent "Thinking" and "Thought" process **must be based on the data received** in the [tool\_output]. The agent must correctly reference and use the returned values (e.g., use the new\_booking\_id from a create\_booking output to then call confirm\_booking). This demonstrates a valid Observe-React loop.