

Tool design and MCP checklist

Tools a model can use correctly and safely.

Developer

TOOL DESIGN

- Few tools with distinct jobs
- Names that say what happens: `cancel_booking`
- Descriptions say when not to use it
- Strict schemas: enums, formats, required fields
- Concise structured results; helpful error messages
- Separate reads from writes
- Least privilege and per-user credentials
- Confirmation before consequential writes

LOOP ESSENTIALS

- Validate arguments
- Timeouts and capped iterations
- Idempotency keys on writes
- Log every call with arguments and results

MCP 2026-07-28 IN SHORT

- Stateless core: no initialize handshake or session ID
- Requests carry version and capabilities inline
- Routing headers; cacheable list results
- Server questions became multi-round-trip requests
- Extensions: Tasks, MCP Apps. Roots, Sampling, Logging and HTTP+SSE deprecated
- State = explicit handles the model passes between tools
- Pin SDK versions and read the migration notes

SECURITY

- Tool descriptions can be poisoned
- Vet third-party servers like code
- Human confirmation and audit logs
- Stateless is not secure

Conversational AI Design, a free course. Reviewed October 27, 2026. conversationalaidesign.com