Tool Name

Tool:

Owner:

System touched:

Data touched:

Tool Class

-] Read-only.
-] Approval-gated write.
-] Paid action.
-] Destructive action.
-] Regulated action.
-] Public/customer-visible action.
-] Internal-only action.

Required Controls

-] Input schema.
-] Output schema.
-] Least-privilege scope.
-] Tenant isolation.
-] Rate limit.
-] Prompt-injection test.
-] Audit event.
-] Approval gate.
-] Rollback path.

Approval Questions

1. What could go wrong if this tool is called by the wrong agent?
2. What could go wrong if the input is malicious?
3. What could go wrong if the output is wrong?
4. Who can approve this action?
5. How is the decision logged?
6. How can the tool be disabled?

Decision

-] Approved as read-only.
-] Approved with human gate.
-] Internal pilot only.
-] Blocked pending redesign.