Agentic System Governance Document

IAM_Ticket_Summary Agent

Version 1.0 – Operational

This document defines governance, control boundaries, and operational safeguards for the IAM_Ticket_Summary Agent.

1. Agent Role Model

Roles and Responsibilities

1. Summarization Engine – Reads weekly IAM ticket Excel exports, classifies tickets, extracts devices, and produces structured summaries.
2. Policy Enforcer – Enforces read-only behavior, language constraints, and output schema compliance.
3. Signal Router – Flags security-relevant indicators for human review without triggering actions.

Authority Boundaries

1. No modification of tickets, systems, identities, or directories.
2. No outbound communication or remediation actions.
3. Classification and annotation only.

Dependencies

1. Weekly IAM ticket Excel export stored in SharePoint / OneDrive.
2. Keyword and pattern policies approved by IAM Operations.
3. Human IAM and Security Operations teams for downstream action.

2. Behavior & Decision Model

Autonomous Decisions

1. Ticket categorization using defined precedence rules.
2. Device and hostname extraction from subject and descriptions.
3. Austria tickets marked as Priority #1.
4. Security indicators flagged for review.

Human Approval Required

1. Changes to classification logic, keyword lists, or device extraction rules.
2. Any override of agent-determined categorization.
3. Any operational or remediation action.

Explicitly Prohibited

1. Identity lifecycle changes or access modifications.
2. Direct user or system communication.
3. Root-cause analysis or troubleshooting.

Risk Tolerance

Low tolerance for missed security signals; moderate tolerance for device noise; zero tolerance for unauthorized actions.

3. Failure & Degradation Model

1. LLM failures – hallucinated devices or misclassification.
2. Data failures – malformed or incomplete Excel exports.

3. Integration failures – inaccessible source files.

Degraded Modes

1. Schema-light mode using subject only.
2. Minimal device extraction with explicit 'Not specified'.
3. Row skip with audit log entry.

Stop Conditions

1. Unreadable file or missing mandatory columns.
2. Excessive row failure rate (>20%).

4. Trust Boundaries & Data Zones

1. Authoritative source: IAM SSP Excel exports.
2. Advisory sources: keyword policies and extraction patterns.
3. Read-only access to all inputs; write-only to summary artifact.

5. Explainability & Audit Model

1. Each ticket must include an explicit reasoning string.
2. Logged evidence includes matched keywords and extracted devices.
3. Deterministic re-run capability using same input and policy version.

6. Change & Evolution Model

1. Changeable elements include prompts, policies, and integrations.
2. All changes require IAM Operations approval and regression testing.
3. Immediate rollback to last approved version on regression.

7. Operational Ownership Model

1. Agent Owner: IAM Operations Lead.
2. Data Owner: IAM Platform Owner.
3. Incident Response: Security Operations.
4. Kill Switch Authority: IAM Operations Lead and Security Duty Manager.

8. KAF Component Mapping

Agent Role Model – Agent Builder

Behavior & Failure Models – Agentic Core

Trust, Explainability, Change, and Ownership – Responsible AI & Governance