CONTINUITY HUB · WILLIAM TYGART OPINION

If Revoking One AI Vendor Breaks Five Workflows, You Built an Extension Cord Instead of a Breaker Panel

By Will Tygart · Published November 27, 2026 · Two-Page Continuity Reference

Direct Answer: Direct API keys and Zapier-style webhooks turn third-party AI incidents into an all-or-nothing shutdown choice. Decoupling external AI inside a $7/month sacrificial Google Workspace blast-zone seat with an asynchronous Sheet or Drive queue lets continuity teams sever a compromised AI vendor in under 60 seconds without taking internal operations dark.

1. The Continuity Trap: Self-Inflicted Blackout on Revocation

In our continuity playbook on compromised AI keys, we documented the worst choice an incident commander can face: leave a leaked secret live and fund an intrusion, or revoke the key and take internal intake, triage, and dispatch queues dark. That trap exists because teams wire external AI directly to production using long-lived bearer keys and synchronous webhooks. In 1886, William Stanley did not run `3,000V` transmission power straight to desk switches—he put step-down converters in the basement to isolate building circuits. A `$7/month` sacrificial Google Workspace seat (`airlock@company.com`) performs that exact step-down isolation for AI continuity.

Grid / Continuity Principle	1886 Step-Down Architecture	Direct AI Extension-Cord Failure	Sacrificial OAuth Blast-Zone Control
Voltage / Trust Isolation	William Stanley stepped 500V–3,000V down to 100V in basement converters	External AI agents write straight into ERP, Slack, or ticketing APIs	External AI writes only to a $7/mo airlock seat (30 GB shell, 0 legacy files)
Sacrificial Break Point	Edison US227226 enclosed lead wire melts inside protective tube	Revoking a leaked shared API key halts five internal production queues	Block one OAuth Client ID in Admin Console; internal scripts stay online
Asynchronous Buffer (RPO)	Substation isolation prevents feeder faults from blacking out the block	Synchronous webhooks drop requests mid-flight during vendor outages	Append-only Google Sheet / Drive intake folder buffers state safely
Failover & Recovery (RTO)	Modular branch circuits restore safely section by section	Emergency key rotation breaks hardcoded connectors across 12 SaaS apps	100,000/day Apps Script pulls validated payloads into internal queues

2. Why Asynchronous Workspace Buffers Protect RTO and RPO

- **Zone Isolation (NIST SP 800-207):** External AI vendors receive OAuth tokens scoped strictly to `drive.file` or a staging Sheet on the `$7/mo` airlock seat—never primary production secrets.
- **Sub-Minute Kill Switch:** Blocking the vendor's Client ID in Workspace Admin API Controls severs external access immediately while internal credentials stay untouched.
- **Human-Inspectable Recovery Queue:** When a vendor goes down or misbehaves, operations teams can still inspect pending rows in Sheets or `!Review-Draft` queues and route them manually or via a backup model.

3. The 60-Second Sacrificial Cutover Runbook

Aligning with NIST SP 800-34 Rev. 1 contingency planning and NIST SP 800-161 supply-chain containment, separating Zone A (untrusted AI intake) from Zone B (internal Apps Script relays) turns chaotic key-hunt emergencies into a four-step drill.

Continuity Tabletop Stage	Direct-Key Architecture (High RTO)	Sacrificial OAuth Blast Zone (< 60s Cutover)	NIST Continuity Anchor
T+00:00 · Vendor Breach Alert	Incident commander debates revenue halt vs. leaving key live	Admin opens Security > API Controls > Manage Third-Party App Access	NIST SP 800-34 Contingency Detection
T+00:45 · Emergency Severance	Must find every script/Zapier task holding the leaked bearer key	Toggle vendor Client ID to Blocked; active OAuth tokens revoke globally	NIST SP 800-207 Zero Trust Enforcement
T+05:00 · Queue Continuity	Downstream CRM, dispatch, and billing workflows stall simultaneously	Internal Apps Script drains validated rows already in Sheet/Drive buffer	NIST SP 800-161 Supply Chain Resilience
T+30:00 · Controlled Restoration	Manual credential re-keying and untested webhook replay across apps	Switch intake seat to backup AI provider; replay quarantined files cleanly	100,000/day Apps Script Queue Replay

4. Quarterly Key-Kill Tabletop Verification

- **Test single-click vendor block:** Practice blocking a non-critical OAuth Client ID in Admin Console and time how long token revocation takes.
- **Verify zero secret co-mingling:** Confirm production CRM, ERP, and Slack webhooks live solely in internal Apps Script `ScriptProperties`, invisible to Zone A.
- **Pre-stage fallback intake:** Keep a local CSV/manual intake export of the buffer Sheet so staff stay operational even if the entire SaaS layer degrades.
- **Rehearse secondary model swap:** Verify Zone B relays can pull from an alternate intake folder fed by a secondary AI provider within your RTO window.

5. Primary Continuity & Technical Sources

- Edison Tech Center — William Stanley's 1886 Step-Down Transformer
- U.S. Patent 227,226 — Edison Safety-Conductor Enclosed Fuse (1880)
- NIST SP 800-34 Rev. 1 — Contingency Planning Guide for Federal Information Systems
- NIST SP 800-207 — Zero Trust Architecture
- NIST SP 800-161 Rev. 1 — Cybersecurity Supply Chain Risk Management
- Google Workspace Admin Help — Block or Restrict Third-Party App Access

Operational resilience guidance for business continuity practitioners; adapt cutover runbooks to your regulatory framework and offline backup posture.