Governance & SOP Playbook: NICO Secure AI-Accelerated Workflow

1. Standard Operating Procedures (SOPs)

- No Secrets in Chat: Developers must never paste secrets into Cursor or any AI chat interface.
- Secure Terminal Entry: Secrets must be entered only via secure terminal commands into Azure Key Vault.
- Codespaces Usage: All development must occur inside GitHub Codespaces with approved devcontainer images.
- AI Guidelines: Cursor Enterprise Privacy Mode must always be enabled; indexing must be limited to approved repos.

2. Approval Gates

- Pull Request Templates: Every PR must include a security checklist.
- Mandatory Code Review: At least one security reviewer must approve all PRs.
- Secret Scanning: GitHub Advanced Security scanning must be enabled and enforced.
- Branch Protection: Critical branches (main, release) require signed commits and review.

3. Audit & Compliance Procedures

- Audit Logging: Enable audit streams in GitHub, Azure DevOps, and Cursor Enterprise.
- Access Reviews: Conduct quarterly reviews of all SSO and SCIM-provisioned accounts.
- Incident Response: Any suspected secret exposure triggers immediate Key Vault rotation.
- Compliance Mapping: Ensure practices align with CIS, CSA, and NIST standards.

4. Roles & Responsibilities

- Security Architect (Onsite): Accountable for governance enforcement.
- Principal Security Architect (Onshore): Provides oversight and approvals.
- Offshore Security Engineer: Implements SOPs in pipelines and environments.
- Application SME & Automation Engineer: Ensure development conforms to security guardrails.
- Senior Project Director: Manages reporting and escalations.

5. Conclusion

The SOPs, approval gates, and audit procedures defined in this playbook ensure that NICO’s adoption of AI-accelerated workflows is both secure and compliant. They provide a repeatable framework for future enterprise-scale projects.