Executive Summary: NICO Secure AI-Accelerated Workflow

Prepared for: National Indemnity Company (NICO)
Prepared by: Tata Consultancy Services (TCS)
Author: Derek Brent Moore, Security Architect

This initiative introduces a secure, AI-accelerated engineering workflow leveraging Cursor IDE, OpenAI's Codex-style models, GitHub Codespaces, and Azure DevOps Pipelines. The solution is designed to improve productivity by an order of magnitude while maintaining rigorous security and compliance standards.

Business Value

Productivity at Scale: AI-assisted development and containerized cloud environments accelerate delivery timelines.**Security by Design:** All secrets remain in Azure Key Vault; no credentials are entered into chat or stored in code.**Governance & Oversight:** Clear accountability across onsite/offshore roles ensures quality and compliance.**Enterprise Readiness:** Aligns with NICO's security posture and enables TCS to deliver cutting-edge solutions securely.

Key Security Principles

No secrets in AI chat interactions.Secrets stored only in Azure Key Vault, accessed via secure variables and parameters.Azure DevOps Pipelines use federated identity (OIDC) for authentication — eliminating long-lived credentials.All development occurs in isolated, auditable GitHub Codespaces environments.

Oversight & Team Structure

Onsite: Security Architect (author), Application SME, Senior Project Director.**Offshore:** Security Engineer, Automation Engineer, Database Expert.**Guidance:** Onshore Principal Security Architect (governance and oversight).

Decision Request

We request approval to standardize on this secure AI-accelerated workflow. By adopting this approach, NICO will gain measurable productivity improvements, reduced security risk, and a repeatable governance model that can scale across future initiatives.