Technical Security Addendum: NICO Secure AI-Accelerated Workflow

1. Secret Management

- All secrets (keys, certificates, credentials) are stored exclusively in Azure Key Vault.
- Developers never input secrets into chat-based AI interfaces.
- Pipelines reference Key Vault via secure variable groups.
- Azure DevOps Workload Identity Federation (OIDC) eliminates static service principals.

2. Identity & Access Controls

- Entra ID (Azure AD) provides single sign-on across Cursor, GitHub, and Azure DevOps.
- Conditional Access and MFA enforced for all administrative roles.
- SCIM provisioning ensures least-privilege role assignment.
- GitHub Codespaces tokens are short-lived and scoped per session.

3. GitHub Codespaces Security

- Codespaces run in isolated containers with ephemeral VMs.
- Organization-level policies restrict machine types, port forwarding, and extensions.
- Devcontainer images are hardened, prebuilt with Az CLI, Bicep, Terraform, and PowerShell.
- Logs and telemetry feed into enterprise audit systems.

4. Cursor IDE Security

- Cursor Enterprise enforces zero data retention.
- Privacy Mode ensures code is not retained for training.
- SOC 2 Type II compliance, TLS 1.2+, and AES-256 at rest.
- Administrators can disable indexing or limit AI scope to approved repos.

5. Azure DevOps Pipelines

- Service connections authenticate via federated identity (OIDC).
- Key Vault integration masks secrets from logs.
- Pipeline YAML templates enforce governance (linting, security checks).
- Logs stored securely with immutability for audit purposes.

6. Secure Data Flow (Textual Diagram)

Developer (Codespace) → Secure Login (OIDC) → Azure
Developer (Codespace) → Key Vault (RBAC scoped) → Secrets retrieved on demand
Cursor IDE → AI assistance (no secrets in context)
Pipeline → OIDC → Key Vault → Deploy IaC (Bicep, CLI, PowerShell)

Audit → Logs in Azure Monitor + GitHub/Azure DevOps audit streams

7. Conclusion

This technical model ensures secrets are never exposed, identities are federated, and development environments remain isolated and auditable. It meets enterprise security benchmarks while enabling significant productivity improvements.