Endpoint Security & Asset Management

Addendum to Information Security Policy

Polaris Group, LLC | Neucleos-1 Platform Services

Effective Date: December 2, 2024 | Version 1.0

1. Operational Context

Polaris Group, LLC operates as a solo-founder technology company with a cloud-native architecture. This operational model has specific security implications:

- **Single Operator:** One authorized user (founder/Strategic Director) with full administrative access
- **No Corporate Network:** All infrastructure is cloud-hosted; no on-premises servers or corporate LAN
- **Cloud-Native Production:** Production systems managed entirely by SOC 2 compliant cloud providers
- **Simplified Attack Surface:** Minimal endpoints reduce complexity and exposure compared to traditional enterprises

2. Asset Inventory

2.1 Physical Endpoints

Asset	Type	Security Controls
Apple Mac Studio	Development Workstation	M4 Ultra, macOS, FileVault, Gatekeeper

2.2 Cloud Infrastructure Assets

Provider	Service	Compliance	MFA Enabled
Convex	Real-time DB, Functions	SOC 2	Yes
Railway	API Gateway, PostgreSQL	SOC 2	Yes
Vercel	Web App Hosting	SOC 2 Type II	Yes
Clerk	Identity & Auth	SOC 2	Yes
GitHub	Source Control	SOC 2 Type II	Yes
OpenAI	AI Services	SOC 2 Type II	Yes

Asset Discovery: Cloud infrastructure visibility is maintained through provider dashboards. The single physical endpoint is directly managed by the operator. Quarterly reviews confirm asset inventory accuracy.

3. Endpoint Security Controls

3.1 macOS Security Features (Development Workstation)

The development workstation utilizes Apple's integrated security framework:

Control	Description & Status
FileVault	Full disk encryption using XTS-AES-128 with 256-bit key. **ENABLED**
Gatekeeper	Prevents execution of unsigned/unnotarized software. **ENABLED**
XProtect	Built-in malware detection with automatic signature updates. **ENABLED**
MRT	Malware Removal Tool - automatic malware remediation. **ENABLED**

Control	Description & Status
System Integrity Protection	Protects system files and processes. **ENABLED**
Firewall	Application-level firewall blocking unauthorized incoming connections. **ENABLED**
Automatic Updates	macOS and security updates applied automatically. **ENABLED**
Screen Lock	Auto-lock after 5 minutes of inactivity; password required on wake. **ENABLED**

3.2 Production Infrastructure Security

Production assets (server instances, databases, functions) are fully managed by cloud providers. Polaris Group does not manage underlying server infrastructure. Security responsibilities follow the shared responsibility model:

- **Provider Responsibility:** Physical security, hypervisor security, network infrastructure, OS patching on managed services
- **Polaris Group Responsibility:** Application code security, access control configuration, API key management, data classification

4. Vulnerability Management

4.1 Patching Strategy

Asset Type	Patching Approach
Development Workstation	macOS automatic updates enabled; critical patches applied within 48 hours of release
Cloud Infrastructure	Managed by providers (Convex, Railway, Vercel) - automatic patching
Application Dependencies	npm/pnpm audit run weekly; Dependabot alerts monitored on GitHub

4.2 Vulnerability Scanning

Given the cloud-native architecture with a single managed endpoint:

- **Endpoint:** Apple Silicon Macs receive security updates through Apple's automatic update system. macOS includes continuous runtime protections (XProtect, MRT) that scan for known malware signatures.
- **Dependencies:** GitHub Dependabot provides automated vulnerability scanning of npm packages with alerts and automated PRs for fixes.
- **Production:** Cloud providers perform infrastructure vulnerability scanning as part of their SOC 2 compliance programs.

5. Device Policy

As a solo-founder organization, all devices used for business purposes are company-owned and directly managed. There are no employees or contractors using personal devices (BYOD) for business operations. Should the organization expand, a formal BYOD policy will be established before any personal devices are permitted for business use.

6. Access Control Summary

All production assets and critical systems are protected with multi-factor authentication:

- Cloud provider consoles (Convex, Railway, Vercel, Clerk): MFA enabled
- Source control (GitHub): MFA enabled with hardware key support
- AI services (OpenAI, Anthropic): MFA enabled
- Financial integrations (Plaid): MFA enabled

- Development workstation: Biometric authentication (Touch ID) + password

Access reviews are performed quarterly to verify that API keys, tokens, and service accounts remain necessary and properly scoped.

7. Review and Maintenance

This addendum is reviewed and updated:

- Quarterly: Asset inventory verification
- Annually: Full policy review aligned with main Information Security Policy
- As needed: Upon significant infrastructure changes or new asset types

_____

Jason

Strategic Director, Polaris Group, LLC

Date: December 2, 2024