# Security & Privacy Practices

Supplemental Addendum to Information Security Policy

Polaris Group, LLC | Neucleos-1 Platform Services

Effective Date: December 2, 2024 | Version 1.0

This document supplements the Polaris Group Information Security Policy with additional detail on incident management, network architecture, training, vendor management, independent testing, human resources, and consumer data privacy practices.

## 1. Incident Management

Polaris Group maintains a defined process for detecting, triaging, and resolving security-impacting incidents. This process is supported by automated alerting infrastructure and documented response procedures.

### 1.1 Detection

Security incidents are detected through multiple channels:

- **Automated Monitoring:** BetterUptime monitors service availability; alerts triggered on outage or degradation
- **Authentication Events:** Clerk webhooks report suspicious logins, failed authentication attempts, and user lifecycle events
- **Dependency Scanning:** Dependabot and npm audit identify known vulnerabilities in application dependencies
- **Application Logging:** Convex, Railway, and Vercel logs capture errors, anomalies, and operational events
- **Provider Notifications:** Security advisories from cloud providers (Convex, Railway, Vercel, Clerk)

### 1.2 Triage

Detected incidents are triaged by priority level:

| Priority | Classification | Examples | Response Target |
|---|---|---|---|
| **P1 Critical** | Active breach, data exposure, complete service outage | Unauthorized data access, credential compromise, production down | Immediate response |
| **P2 High** | Potential breach, critical vulnerability, partial outage | Suspicious activity patterns, high-severity CVE, degraded service | < 1 hour |
| **P3 Medium** | Security hygiene, moderate vulnerability, operational issue | Medium-severity CVE, configuration drift, failed jobs | < 24 hours |
| **P4 Low** | Informational, low-risk finding, routine maintenance | Low-severity CVE, service recovery notices, routine alerts | Review within 7 days |

### 1.3 Resolution Process

Security incidents follow a five-phase resolution process:

1. **Detection:** Incident identified via automated alerting or manual observation
2. **Containment:** Immediate actions to limit impact (revoke access, isolate systems, disable features)
3. **Eradication:** Remove root cause (patch vulnerability, rotate credentials, remediate configuration)
4. **Recovery:** Restore normal operations with verification of system integrity

5. **Post-Incident Review:** Document lessons learned, update procedures, implement preventive measures

### 1.4 Notification

In the event of a security incident affecting consumer data or Plaid integration, affected parties will be notified in accordance with applicable laws and contractual obligations. Plaid will be notified promptly of any incident that may affect data obtained through their API.

## 2. Network Architecture & Segmentation

Polaris Group operates a 100% cloud-native architecture with no on-premises infrastructure. Network segmentation is implemented at the cloud provider level.

### 2.1 Architecture Overview

| Layer | Provider | Network Controls |
|---|---|---|
| Web Application (Frontend) | Vercel Edge Network | CDN isolation, DDoS protection, WAF, HTTPS-only |
| Real-time Backend | Convex | Isolated function execution, no direct database access from internet |
| API Gateway | Railway | Private networking, service-to-service authentication |
| Database (Long-term Storage) | Railway PostgreSQL | No public endpoint; accessible only via application layer with SSL required |
| Database (Real-time) | Convex | Managed isolation; access only through Convex functions |
| Authentication | Clerk | Dedicated auth infrastructure, isolated from application data |

### 2.2 Environment Separation

Development and production environments are fully isolated:

- **Separate Instances:** Development and production use distinct Convex deployments, Railway services, and Vercel projects
- **Credential Isolation:** Each environment has unique API keys, database credentials, and secrets
- **No Cross-Access:** Development credentials cannot access production resources and vice versa
- **Data Isolation:** Production consumer data is never copied to development environments

### 2.3 Internet Exposure

Only necessary endpoints are exposed to the public internet:

- **Public:** Web application (static assets, client-side code)
- **Authenticated:** API endpoints (require valid session token via Clerk)
- **Internal Only:** Databases, backend functions, inter-service communication

## 3. Security Awareness & Training

### 3.1 Current State

Polaris Group is currently a solo-founder operation with no additional employees or contractors. The founder maintains security awareness through continuous professional development and direct operational responsibility for all security controls.

### 3.2 Founder Security Competencies

The founder maintains proficiency in:

- Secure software development practices (OWASP Top 10, secure coding standards)
- Cloud security architecture and configuration
- Authentication and authorization best practices
- Incident detection and response procedures
- Data privacy regulations and compliance requirements
- Phishing and social engineering recognition

### 3.3 Future Training Program

Upon team expansion, Polaris Group will implement a formal security awareness program including:

- Security awareness training during onboarding (within first week of employment)
- Annual security refresher training for all personnel
- Role-specific training for personnel with access to sensitive systems or data
- Phishing simulation exercises
- Documented acknowledgment of security policies

## 4. Vendor Management

### 4.1 Vendor Selection Criteria

Before onboarding any vendor that will process or store data, the following criteria are evaluated:

- **Security Certifications:** SOC 2 Type II certification required for vendors handling sensitive data
- **Encryption Standards:** TLS 1.2+ for data in transit, AES-256 for data at rest
- **Access Controls:** Support for MFA, role-based access, audit logging
- **Data Processing Terms:** Acceptable data processing agreement and privacy terms
- **Incident Response:** Defined breach notification procedures

### 4.2 Current Vendors

All production vendors have been vetted against the above criteria:

| Vendor | Purpose | Certification | MFA Enabled |
|---|---|---|---|
| Convex | Real-time database & backend | SOC 2 | Yes |
| Railway | API hosting & PostgreSQL | SOC 2 | Yes |
| Vercel | Web application hosting | SOC 2 Type II | Yes |
| Clerk | Authentication | SOC 2 | Yes |
| GitHub | Source control & CI/CD | SOC 2 Type II | Yes |
| Plaid | Financial data aggregation | SOC 2 Type II | Yes |
| OpenAI | AI services | SOC 2 Type II | Yes |

### 4.3 Ongoing Monitoring

Vendors are monitored on an ongoing basis:

- **Annual Review:** Security posture and certification status reviewed annually
- **Security Advisories:** Monitor vendor communications for security incidents or changes
- **Access Review:** Quarterly verification of access credentials and permissions

## 5. Independent Security Testing

### 5.1 Current State

As an early-stage startup, Polaris Group has not yet engaged independent auditors or penetration testers. Security assurance is currently provided through:

- **Automated Scanning:** Dependabot and npm audit for dependency vulnerabilities
- **Provider Certifications:** All infrastructure vendors maintain SOC 2 certification with regular third-party audits
- **Code Review:** All code changes reviewed against security checklist before deployment
- **Static Analysis:** TypeScript type checking and ESLint security rules

### 5.2 Planned Testing

Polaris Group commits to engaging independent security testing as the platform scales:

- **Penetration Testing:** Independent pen-test to be conducted prior to processing significant consumer data volume or upon achieving Series A funding
- **Security Audit:** Third-party security assessment to be conducted annually once team exceeds 5 personnel
- **SOC 2 Certification:** SOC 2 Type I audit to be pursued upon reaching product-market fit and scaling operations

## 6. Human Resources Security

### 6.1 Current State

Polaris Group is currently a solo-founder operation with no additional employees or contractors. The founder has sole access to all systems and maintains full accountability for all operations.

### 6.2 Background Check Policy

Upon hiring employees or engaging contractors, Polaris Group will implement the following background check requirements:

- **All Employees:** Criminal background check, employment verification, education verification
- **Contractors with System Access:** Criminal background check, reference verification
- **Roles with Financial Data Access:** Enhanced screening including credit check (where legally permitted)
- **Timing:** Background checks completed prior to granting system access

### 6.3 Access Provisioning

Upon hiring, system access will be granted based on:

- Principle of least privilege (minimum access required for role)
- Role-based access control aligned with job function
- Mandatory MFA enrollment before access granted
- Documented access approval by founder

### 6.4 Termination Procedures

Upon termination of any employee or contractor:

- All system access revoked within 24 hours (immediately for involuntary termination)
- API keys and credentials rotated
- Company equipment and data returned
- Exit interview including security acknowledgment

## 7. Consumer Consent

### 7.1 Consent Mechanisms

Polaris Group obtains explicit consent from consumers before collecting, processing, or storing their data:

**Financial Data (Plaid Integration):**

- Consumer initiates connection through Plaid Link interface
- Plaid displays data sharing disclosure and requests explicit consent
- Consumer authenticates with their financial institution
- Consent event recorded with timestamp and user identifier

**Account Creation:**

- Terms of Service and Privacy Policy presented before account creation
- User must affirmatively accept terms to proceed
- Acceptance recorded with timestamp

### 7.2 Consent Revocation

Consumers may revoke consent at any time:

- **Financial Data:** Disconnect financial account through application settings; access token invalidated, connection removed
- **Account Deletion:** Request account deletion; all associated data removed per data retention policy
- **Contact:** Users may contact support to request data deletion or consent revocation

### 7.3 Transparency

Consumers are informed about data practices through:

- **Privacy Policy:** Publicly accessible document describing data collection, use, and sharing practices
- **Terms of Service:** Clear description of service functionality and user responsibilities
- **In-App Disclosure:** Clear indication of what data is being accessed before connection

## 8. Data Minimization & Retention

Polaris Group is committed to collecting only data necessary for providing services, retaining data only as long as required, and securely deleting data when no longer needed.

### 8.1 Data Minimization Principles

- **Purpose Limitation:** Data collected only for specific, stated purposes communicated to the consumer
- **Collection Minimization:** Only data elements necessary for the stated purpose are collected
- **Access Minimization:** Data access restricted to systems and personnel that require it
- **No Data Sales:** Consumer data is never sold to third parties

### 8.2 Plaid Data Handling

Financial data obtained through the Plaid API is handled with particular care:

| Data Element | Handling | Storage |
|---|---|---|
| Access Tokens | Stored encrypted; used for API calls only | Encrypted database; never logged |
| Account Information | Used for account display; masked where appropriate | Encrypted database |
| Transaction Data | Used for service functionality | Encrypted database |

| Data Element | Handling | Storage |
|---|---|---|
| User Credentials | **Never collected or stored** | N/A - handled only by Plaid |

### 8.3 Data Retention Schedule

Data is retained according to the following schedule:

| Data Category | Retention Period | Deletion Trigger |
|---|---|---|
| Active User Account Data | Duration of account | Account deletion request |
| Financial Data (Plaid) | Duration of connection | Connection disconnected or account deleted |
| Plaid Access Tokens | Duration of connection | Connection disconnected; token invalidated |
| Deleted Account Data | 30 days post-deletion | Automatic purge after grace period |
| Audit Logs | 1 year minimum | Automatic purge after retention period |
| Security Alerts | Indefinite | Manual review and archival |

### 8.4 Data Deletion Procedures

When data reaches end of retention or deletion is requested:

6. **User Request:** User requests account deletion through application or support contact
7. **Verification:** Request authenticated and verified
8. **Token Invalidation:** Plaid access tokens invalidated immediately
9. **Data Removal:** User data marked for deletion; removed from active systems
10. **Grace Period:** 30-day grace period for accidental deletion recovery
11. **Permanent Deletion:** Data permanently purged from all systems after grace period
12. **Backup Propagation:** Deletion propagates through backup rotation cycle

### 8.5 Legal Compliance

Data retention and deletion practices comply with applicable regulations including:

- **CCPA:** California Consumer Privacy Act rights to deletion honored
- **GDPR:** Right to erasure supported for applicable users
- **Financial Regulations:** Retention periods aligned with applicable financial record-keeping requirements

## 9. Data Usage Policy

### 9.1 Prohibited Uses

Polaris Group explicitly prohibits the following uses of consumer data:

- **No Sale of Data:** Consumer data obtained through the Plaid API or any other source is never sold to third parties
- **No Unauthorized Sharing:** Consumer data is not shared with third parties except as required by law or with explicit user consent
- **No Secondary Marketing:** Financial data is not used for marketing unrelated products or services
- **No Data Aggregation for Sale:** Consumer data is not aggregated and sold as market research or analytics

### 9.2 Permitted Uses

Consumer data is used only for:

- Providing the services requested by the consumer
- Improving service quality and user experience

- Security monitoring and fraud prevention
- Compliance with legal obligations
- Communication with the user about their account or service

## 10. Two-Factor Authentication

### 10.1 Consumer-Facing Applications

Two-factor authentication (2FA) is enforced on all client-facing web applications through Clerk authentication infrastructure.

**Supported 2FA Methods:**

- **Authenticator Apps:** TOTP-based authentication (Google Authenticator, Authy, 1Password, etc.)
- **SMS Verification:** One-time codes sent via text message
- **Backup Codes:** Recovery codes provided during 2FA setup

### 10.2 Enforcement Policy

- **Required for Financial Data:** Users must enable 2FA before connecting financial accounts through Plaid
- **Session Security:** Sessions expire after period of inactivity; re-authentication required
- **Device Trust:** New device logins require 2FA verification

### 10.3 Administrative Access

In addition to consumer-facing 2FA, all administrative access to infrastructure requires MFA:

- Cloud provider dashboards (Convex, Railway, Vercel, Clerk)
- Source code repository (GitHub)
- Third-party service APIs (Plaid, OpenAI)
- Development workstation login

## 11. Document Review

This addendum is reviewed and updated:

- Annually, aligned with the main Information Security Policy review
- Upon significant changes to data handling practices
- Upon hiring first employees (HR section activation)
- Upon achieving security testing milestones

---

**Jason Bowman**

Founder, Polaris Group, LLC

Date: December 2, 2024