INFORMATION SECURITY POLICY

Polaris Group, LLC

Neucleos-1 Platform Services

Document Version: 1.0

Effective Date: December 12, 2023

Classification: CONFIDENTIAL

Document Control

Version	Date	Author	Description
1.1	Dec 12, 2024	Jason Bowman (Founder)	Initial release

1. Purpose and Scope

1.1 Purpose

This Information Security Policy establishes the framework for protecting the confidentiality, integrity, and availability of information assets managed by Polaris Group, LLC in connection with the Neucleos-1 Platform Services. This policy defines the security requirements, responsibilities, and operational controls necessary to identify, mitigate, and monitor information security risks.

1.2 Scope

This policy applies to:

- All information systems, applications, and infrastructure supporting the Neucleos-1 Platform
- All employees, contractors, and third-party service providers with access to company systems
- All data processed, stored, or transmitted through Neucleos-1 Platform Services
- Physical and logical security controls protecting organizational assets
- Third-party integrations and API connections (including financial services integrations)

1.3 Platform Overview

The Neucleos-1 Platform is an enterprise AI application platform featuring real-time collaboration, company analytics and workforce intelligence, AI agent orchestration with persistent memory, and multi-platform deployment capabilities. The platform utilizes a hybrid

data architecture with Convex as the real-time reactive backend and PostgreSQL for long-term data storage.

2. Information Security Governance

2.1 Governance Structure

Polaris Group, LLC maintains a governance structure with clearly defined roles and responsibilities for information security:

- **Strategic Director:** Overall accountability for information security strategy and policy approval
- **Security Operations:** Day-to-day implementation and monitoring of security controls
- **Development Team:** Secure development practices and code security
- **All Personnel:** Compliance with security policies and reporting of security incidents

2.2 Policy Framework

This policy is supported by operational procedures and standards that provide detailed implementation guidance. The framework is reviewed annually and updated as needed to address emerging threats and regulatory requirements.

3. Risk Management

3.1 Risk Assessment Process

Polaris Group, LLC conducts ongoing risk assessments to identify, evaluate, and prioritize information security risks. The risk management process includes:

1. **Asset Identification:** Cataloging all information assets including data, systems, and infrastructure
2. **Threat Assessment:** Identifying potential threats to organizational assets
3. **Vulnerability Analysis:** Evaluating weaknesses that could be exploited
4. **Risk Evaluation:** Determining likelihood and impact of identified risks
5. **Control Selection:** Implementing appropriate controls to mitigate risks
6. **Continuous Monitoring:** Ongoing assessment of control effectiveness

3.2 Risk Treatment

Identified risks are addressed through risk treatment strategies including mitigation, transfer, acceptance, or avoidance. All risk treatment decisions are documented and approved by appropriate management.

4. Access Control

4.1 Access Control Policy

Access to information systems and data is controlled based on the principle of least privilege. Users are granted only the minimum access necessary to perform their job functions.

4.2 Authentication Requirements

The Neucleos-1 Platform implements robust authentication controls:

- Multi-factor authentication (MFA) required for all administrative access
- Integration with Clerk for secure identity management and multi-tenant authentication

- Auth tokens validated server-side on every request
- Session management with appropriate timeout controls
- Password complexity requirements enforced

4.3 Authorization Controls

Authorization is enforced through:

- Role-based access control (RBAC) with organization-scoped permissions
- Convex functions running in sandboxed V8 environment with auth validation
- API key management with appropriate scoping and rotation
- Regular access reviews and recertification

5. Data Classification and Protection

5.1 Data Classification

Data is classified according to sensitivity and regulatory requirements:

Classification	Description	Handling Requirements
Confidential	Sensitive business data, PII, financial data	Encryption required, access logging, restricted sharing
Internal	Internal business operations data	Access controls, standard handling
Public	Publicly available information	No special handling required

5.2 Data Protection Controls

The following controls protect data throughout its lifecycle:

- **Encryption at Rest:** All sensitive data encrypted using industry-standard encryption (AES-256)
- **Encryption in Transit:** TLS 1.2+ for all data transmission
- **Key Management:** API keys and secrets managed server-side only, never exposed to clients
- **Data Backup:** Regular automated backups with tested restoration procedures
- **Data Retention:** Defined retention periods with secure disposal procedures

6. Physical Security

6.1 Infrastructure Security

The Neucleos-1 Platform is deployed on enterprise cloud infrastructure with comprehensive physical security controls:

- **Cloud Infrastructure:** Hosted on SOC 2 Type II compliant cloud providers (Vercel, Railway, Convex)
- **Data Center Security:** Provider facilities include 24/7 security, biometric access, CCTV monitoring
- **Environmental Controls:** Fire suppression, climate control, redundant power systems
- **Geographic Redundancy:** Multi-region deployment for disaster recovery

6.2 Endpoint Security

All devices accessing organizational systems must comply with:

- Full disk encryption enabled

- Up-to-date operating systems and security patches
- Anti-malware protection with current definitions
- Screen lock after inactivity timeout

7. Network Security

7.1 Network Architecture

The platform implements defense-in-depth network security:

- **Network Segmentation:** Logical separation of production, development, and management networks
- **Firewall Controls:** Restrictive firewall rules with default-deny posture
- **DDoS Protection:** CDN-based protection against distributed denial of service attacks
- **API Gateway:** Centralized API management via Hono framework with rate limiting

7.2 Monitoring and Logging

Comprehensive logging and monitoring is implemented:

- Security event logging for all authentication and authorization events
- Application and infrastructure logs retained for security analysis
- Real-time alerting for security anomalies
- Log integrity controls to prevent tampering

8. Incident Response

8.1 Incident Response Plan

Polaris Group, LLC maintains an incident response capability to detect, respond to, and recover from security incidents. The incident response process includes:

1. **Detection and Analysis:** Identifying and validating potential security incidents
2. **Containment:** Limiting the scope and impact of confirmed incidents
3. **Eradication:** Removing the root cause of the incident
4. **Recovery:** Restoring systems to normal operation
5. **Post-Incident Review:** Documenting lessons learned and improving controls

8.2 Incident Reporting

All personnel are required to report suspected security incidents immediately. Incident notifications to affected parties and regulators will be provided as required by applicable laws and contractual obligations.

9. Business Continuity

9.1 Business Continuity Planning

Polaris Group, LLC maintains business continuity capabilities to ensure critical operations can continue during disruptions:

- **Recovery Objectives:** Defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
- **Backup Strategy:** Regular automated backups with multi-region replication
- **Disaster Recovery:** Documented procedures for service recovery
- **Testing:** Periodic testing of recovery procedures

10. Third-Party Security

10.1 Vendor Management

Third-party service providers are assessed for security risks before engagement and monitored throughout the relationship:

- **Due Diligence:** Security assessment before onboarding vendors with data access
- **Contractual Requirements:** Security obligations defined in vendor agreements
- **Ongoing Monitoring:** Regular review of vendor security posture

10.2 Key Service Providers

The Neucleos-1 Platform relies on the following key infrastructure providers, all of which maintain appropriate security certifications:

- **Convex:** Real-time database and serverless functions (SOC 2 compliant)
- **Railway:** API gateway and PostgreSQL hosting (SOC 2 compliant)
- **Vercel:** Web application hosting (SOC 2 Type II compliant)
- **Clerk:** Identity and authentication services (SOC 2 compliant)

11. Secure Development

11.1 Secure Development Lifecycle

Security is integrated throughout the software development lifecycle:

- **Secure Coding:** Developers follow secure coding guidelines and best practices
- **Code Review:** Security-focused code review before deployment
- **Dependency Management:** Regular updates and vulnerability scanning of dependencies
- **Environment Separation:** Isolated development, staging, and production environments
- **Secrets Management:** API keys and credentials managed securely, never committed to code repositories

12. Compliance and Monitoring

12.1 Regulatory Compliance

Polaris Group, LLC maintains compliance with applicable laws, regulations, and industry standards. The organization monitors regulatory developments and updates controls as needed.

12.2 Security Monitoring

The effectiveness of security controls is continuously monitored through:

- Regular security assessments and vulnerability scanning
- Security metrics and key performance indicators
- Automated security monitoring and alerting
- Periodic internal audits of security controls

13. Training and Awareness

All personnel receive security awareness training appropriate to their role. Training covers:

- Information security policies and procedures

- Recognition and reporting of security threats
- Safe handling of sensitive data
- Social engineering and phishing awareness

14. Policy Review and Updates

This policy is reviewed at least annually or upon significant changes to the business, technology, or threat landscape. Updates are approved by management and communicated to all relevant personnel.

15. Policy Approval

This Information Security Policy has been reviewed and approved by:

_____

Jason

Strategic Director

Polaris Group, LLC

Date: December 2, 2024

Appendix A: Definitions

- **Confidentiality:** Ensuring information is accessible only to authorized individuals
- **Integrity:** Maintaining accuracy and completeness of information
- **Availability:** Ensuring authorized users have access when needed
- **PII:** Personally Identifiable Information
- **MFA:** Multi-Factor Authentication
- **RBAC:** Role-Based Access Control
- **RTO:** Recovery Time Objective
- **RPO:** Recovery Point Objective