

FINANCIAL REPORTING AND ACCOUNTING STANDARDS POLICY

Effective Date: January 15, 2024

WHEREAS, Nexus Industrial Intelligence, Inc., a Delaware corporation (the "Company"), develops and deploys artificial intelligence and machine learning solutions for industrial applications; and

WHEREAS, the Company seeks to establish comprehensive standards for financial reporting, internal controls, performance metrics, and risk management appropriate for its artificial intelligence software business; and

WHEREAS, the Board of Directors has determined it to be in the best interests of the Company to adopt this Financial Reporting and Accounting Standards Policy (this "Policy").

NOW, THEREFORE, the Company hereby adopts the following Policy:

1.0 FINANCIAL REPORTING AND ACCOUNTING STANDARDS

1.1 Generally Accepted Accounting Principles

The Company shall prepare all financial statements and reports in accordance with United States Generally Accepted Accounting Principles ("GAAP") as established by the Financial Accounting Standards Board ("FASB"). Compliance shall extend to:

(a) **Quarterly Financial Statements.** Unaudited financial statements prepared within 45 days of quarter-end, including: (i) Balance sheet; (ii) Income statement; (iii) Statement of cash flows; and (iv) Statement of shareholders' equity.

(b) **Annual Financial Statements.** Audited financial statements prepared within 90 days of fiscal year-end, with full disclosures as required by GAAP.

1.2 Revenue Recognition Standards

(a) **SaaS Subscription Revenue.** The Company shall recognize revenue from its NexusCore™ Industrial AI Platform subscriptions in accordance with ASC 606, with the following specifications:

(i) Performance obligations shall be identified separately for software access, implementation services, and ongoing support;

(ii) Transaction price shall be allocated based on standalone selling price; and

(iii) Revenue shall be recognized ratably over the subscription term for software access, and as services are performed for implementation.

(b) **Multi-Element Arrangements.** For contracts containing multiple performance obligations:

(i) The Company shall evaluate whether promised goods or services are distinct;

(ii) Allocation of transaction price shall utilize observable standalone prices when available;

(iii) Revenue recognition timing shall be determined separately for each distinct performance obligation; and

(iv) Contract modifications shall be evaluated to determine whether they constitute separate contracts or modifications to existing arrangements.

(c) **Professional Services Revenue.** Recognition of implementation, consulting, and training services shall adhere to:

(i) Time-and-materials billing shall be recognized as services are performed;

(ii) Fixed-price arrangements shall utilize percentage-of-completion methodology; and

(iii) Milestone-based contracts shall recognize revenue upon achievement of specified deliverables.

1.3 Software Development Costs

(a) **Capitalization Criteria.** The Company shall capitalize software development costs in accordance with ASC 350-40 when:

(i) Technological feasibility has been established;

(ii) All planning, designing, and testing activities have been completed;

(iii) Management has authorized and committed to funding the project; and

(iv) Future economic benefits are probable and can be reasonably estimated.

(b) **Amortization.** Capitalized costs shall be amortized over the estimated useful life of the software, not to exceed 3 years.

1.4 Artificial Intelligence Development Costs

(a) **Research Phase Expenses.** Costs incurred during the research phase of AI development shall be expensed as incurred, including:

(i) Conceptual formulation of alternatives; (ii) Search for applications of new AI technologies; and (iii) Initial prototyping and testing of AI models.

(b) **Development Phase Capitalization.** Costs eligible for capitalization during AI development include:

(i) Design of chosen AI architecture; (ii) Training data preparation and model training; (iii) Testing and validation of AI models; and (iv) Integration with existing software platforms.

1.5 Financial Controls and Procedures

(a) **Internal Control Framework.** The Company shall maintain internal controls in accordance with COSO framework, including:

(i) Control environment assessment; (ii) Risk identification and evaluation; (iii) Control activities implementation; and (iv) Monitoring procedures.

(b) **Documentation Requirements.** The Company shall maintain detailed documentation for:

(i) Revenue recognition decisions and methodologies; (ii) Capitalization analyses and calculations; (iii) Useful life determinations; and (iv) Periodic review procedures.

1.6 Disclosure Requirements

(a) **Financial Statement Notes.** The Company shall provide comprehensive disclosures regarding:

(i) Revenue recognition policies; (ii) Significant judgments and estimates; (iii) Capitalization criteria and amortization methods; and (iv) Contract assets and liabilities.

(b) **Segment Reporting.** The Company shall disclose segment information in accordance with ASC 280, including:

(i) Operating segments identification; (ii) Aggregation criteria application; and (iii) Required quantitative and qualitative disclosures.

2.0 INTERNAL CONTROLS AND COMPLIANCE FRAMEWORK

2.1 Sarbanes-Oxley Compliance

(a) The Company shall maintain internal controls in accordance with SOX Section 404, including:

(i) Documentation of all significant processes, workflows, and decision matrices;

(ii) Risk assessment procedures with quarterly reviews and updates;

(iii) Testing and monitoring protocols with defined success criteria;

(iv) Regular evaluation of control effectiveness and remediation procedures;

(v) Documentation of all material changes to internal control systems; and

(vi) Annual certification of internal controls by executive management.

(b) Control Documentation Requirements:

- (i) Detailed process narratives and flowcharts;
- (ii) Control objective statements and risk matrices;
- (iii) Testing schedules and methodologies; and
- (iv) Evidence retention protocols and archival procedures.

2.2 AI Development Controls

(a) Model Validation Procedures

- (i) All AI models shall undergo documented validation before deployment, including: - Performance testing against established benchmarks - Bias assessment and mitigation procedures - Security vulnerability scanning - Resource utilization analysis
- (ii) Changes to production models shall require: - Written approval from the Chief AI Officer - Documentation of modification rationale - Impact assessment on existing systems - Rollback procedures and contingency plans
- (iii) Version control requirements: - Unique identifiers for all model versions - Comprehensive change logs - Archive of previous versions - Documentation of deployment history

(b) Development Environment Controls

- (i) Segregation of development, testing, and production environments;
- (ii) Access controls based on role and responsibility;
- (iii) Code review and approval workflows; and
- (iv) Automated testing and validation protocols.

2.3 Data Security Controls

(a) The Company shall implement controls to ensure:

- (i) Segregation of customer data through: - Logical separation of databases - Customer-specific encryption keys - Access control matrices - Data classification protocols
- (ii) Encryption requirements: - AES-256 encryption for data at rest - TLS 1.3 for data in transit - Key management procedures - Regular encryption audit protocols
- (iii) Access controls including: - Multi-factor authentication - Role-based access control (RBAC) - Regular access reviews - Privileged account monitoring
- (iv) Security testing requirements: - Quarterly penetration testing - Monthly vulnerability assessments - Continuous security monitoring - Incident response procedures

2.4 Compliance Monitoring and Reporting

(a) Regular Compliance Assessment:

- (i) Monthly control effectiveness reviews;
- (ii) Quarterly compliance reports to executive management;
- (iii) Annual independent audit of control framework; and
- (iv) Documentation of all compliance exceptions and remediation efforts.
- (b) Reporting Requirements:
 - (i) Immediate notification of control failures to management;
 - (ii) Monthly compliance metrics dashboard;
 - (iii) Quarterly trend analysis and risk assessment; and
 - (iv) Annual compliance certification and attestation.

2.5 Training and Awareness

- (a) Required Training Programs:
 - (i) Annual compliance training for all employees;
 - (ii) Role-specific control training for technical staff;
 - (iii) Quarterly security awareness updates; and
 - (iv) Documentation of training completion and comprehension testing.

3.0 FINANCIAL PERFORMANCE METRICS AND KPIS

3.1 Revenue Metrics

(a) Annual Recurring Revenue (ARR)

- (i) Calculated as: $\text{Monthly Recurring Revenue} \times 12$
- (ii) Excludes one-time implementation fees and professional services
- (iii) Must be reported quarterly with year-over-year comparative analysis
- (iv) Includes all subscription-based revenue streams, properly adjusted for multi-year contracts

(b) Net Revenue Retention Rate

- (i) Calculated as: $(\text{Current Period ARR from Existing Customers}) \div (\text{Prior Period ARR from Same Customers}) \times 100$
- (ii) Must be tracked separately for each customer segment and product tier
- (iii) Expansion revenue shall be documented with specific attribution to upsells, cross-sells, or usage increases

3.2 Customer Metrics

(a) Customer Acquisition Cost (CAC)

- (i) Calculated as: $(\text{Sales \& Marketing Expenses}) \div (\text{Number of New Customers})$
- (ii) Must include all direct and allocated costs, including: - Sales personnel compensation and benefits - Marketing campaign expenses - Sales enablement tools and technologies - Customer acquisition-related travel expenses - Proportional overhead costs
- (iii) Shall be calculated and reported monthly, with trailing twelve-month averages

(b) Churn Rate

- (i) Logo Churn: $(\text{Customers Lost}) \div (\text{Total Customers at Start of Period})$
- (ii) Revenue Churn: $(\text{Lost ARR}) \div (\text{Total ARR at Start of Period})$
- (iii) Must be analyzed by customer segment, contract value, and tenure

3.3 Profitability Metrics

(a) Gross Margin

- (i) Calculated as: $(\text{Revenue} - \text{Cost of Goods Sold}) \div \text{Revenue} \times 100$
- (ii) COGS shall include: - Cloud infrastructure costs - Customer support personnel - Technical operations staff - Third-party software licenses - Data processing fees

(b) Customer Lifetime Value (CLV)

- (i) Calculated as: $(\text{Average Revenue per Account} \times \text{Gross Margin \%}) \div \text{Churn Rate}$
- (ii) Must be evaluated against CAC for ROI analysis

3.4 AI Performance Metrics

(a) Implementation Success Rate

- (i) Percentage of successful AI model deployments within specified timeframes
- (ii) Must track: - Model accuracy rates - Processing time improvements - Error reduction percentages - Customer satisfaction scores

(b) Technical Performance

- (i) System uptime and availability metrics
- (ii) Response time and latency measurements
- (iii) Model retraining frequency and effectiveness

3.5 Reporting Requirements

- (a) All metrics must be reported monthly to executive management

(b) Quarterly board presentations shall include: - Variance analysis against targets - Industry benchmark comparisons - Trend analysis and forecasting - Risk assessments and mitigation strategies

(c) Annual audit requirements: - Independent verification of calculation methodologies - Data integrity validation - Compliance with accounting standards - Documentation of any methodology changes

4.0 RISK MANAGEMENT AND DISCLOSURE REQUIREMENTS

4.1 AI Technology Risk Disclosures

(a) The Company shall disclose material risks related to:

(i) AI model accuracy and reliability, including: - Performance degradation metrics - Model drift assessment protocols - Validation failure scenarios - System reliability benchmarks - Error rate tolerances

(ii) Algorithm bias and fairness, encompassing: - Demographic impact assessments - Training data bias evaluations - Fairness testing methodologies - Bias mitigation procedures - Regular equity audits

(iii) Technical obsolescence, addressing: - Technology lifecycle projections - Upgrade requirements - Legacy system dependencies - Migration pathways - Compatibility assessments

(iv) Competitive technological developments, including: - Market position analysis - Innovation gap assessments - Patent landscape monitoring - Emerging technology impacts - Strategic obsolescence risks

(b) Risk disclosure documentation shall:

(i) Be updated quarterly or upon material changes (ii) Include quantitative risk metrics where applicable (iii) Maintain audit trails of risk assessments (iv) Document mitigation strategies (v) Detail contingency plans

4.2 Data Privacy Compliance

(a) The Company shall maintain compliance with:

(i) GDPR requirements for EU customer data, including: - Data minimization protocols - Consent management systems - Cross-border transfer mechanisms - Data subject rights procedures - Breach notification processes

(ii) CCPA requirements for California residents, addressing: - Opt-out mechanisms - Data inventory maintenance - Consumer request handling - Service provider obligations - Annual compliance reviews

(iii) Industry-specific data protection regulations, encompassing: - Sector-specific requirements - Regional compliance obligations - International data standards - Industry best practices - Regulatory updates

(b) Privacy compliance measures shall include:

(i) Regular privacy impact assessments (ii) Data protection officer appointment (iii) Employee training programs (iv) Vendor compliance verification (v) Documentation maintenance

4.3 Intellectual Property Protection

(a) The Company shall implement procedures to:

(i) Document and protect proprietary AI algorithms through: - Source code documentation - Development process records - Access control protocols - Confidentiality agreements - Innovation tracking systems

(ii) Maintain trade secret protection via: - Information classification protocols - Security measure implementation - Employee confidentiality provisions - Third-party restrictions - Monitoring procedures

(iii) Register copyrights for software code where appropriate, including: - Registration timing protocols - Deposit requirements - Update procedures - Derivative work protection - International filing strategies

(b) Intellectual property management shall include:

(i) Regular IP portfolio reviews (ii) Competitive analysis updates (iii) License agreement monitoring (iv) Infringement detection systems (v) Enforcement protocols

4.4 Implementation and Monitoring

(a) The Company shall establish:

(i) Risk management committee oversight (ii) Quarterly compliance reviews (iii) Annual risk assessment updates (iv) Regular stakeholder reporting (v) Independent audit procedures

(b) Documentation requirements shall include:

(i) Risk register maintenance (ii) Compliance tracking systems (iii) Incident response records (iv) Mitigation measure effectiveness (v) Performance metric tracking

EXHIBITS

Exhibit A: Revenue Recognition Decision Tree **Exhibit B:** Control Testing Procedures
Exhibit C: KPI Calculation Methodologies

SIGNATURE PAGE

IN WITNESS WHEREOF, the undersigned has executed this Policy as of the date first written above.

NEXUS INDUSTRIAL INTELLIGENCE, INC.

By: _____ Name: Dr. Sarah Chen Title: Chief Executive Officer

By: _____ Name: David Kumar Title: Chief Financial Officer

ATTEST:

Corporate Secretary