IT Infrastructure Redundancy and Resilience Document

Confidential Document

Prepared for: Potential Investors and Due Diligence Review

Company: Nexus Intelligent Systems, Inc.

Date of Preparation: January 22, 2024

1. INTRODUCTION AND PURPOSE

1 This IT Infrastructure Redundancy and Resilience Document ("Document") provides a comprehensive assessment of Nexus Intelligent Systems, Inc.'s ("Company") technological infrastructure resilience, disaster recovery capabilities, and system redundancy strategies.

2 The purpose of this document is to demonstrate the Company's technological robustness, risk mitigation protocols, and strategic approach to maintaining continuous operational integrity across critical technology platforms.

2. INFRASTRUCTURE OVERVIEW

1 Core Infrastructure Components

- Primary Data Center: AWS US-West-2 Region (Oregon)
- Secondary Disaster Recovery Site: Azure East US 2 Region (Virginia)
- Tertiary Backup Location: Google Cloud Platform US-Central1 (Iowa)

2 Infrastructure Specifications

- Total Compute Capacity: 672 vCPU cores
- Total Storage Capacity: 487 TB
- Network Bandwidth: 10 Gbps primary, 5 Gbps secondary connections
- Estimated Infrastructure Value: $2.4M USD

3. REDUNDANCY ARCHITECTURE

1 High Availability Design

The Company maintains a multi-region, multi-cloud redundancy architecture designed to ensure:

a) Immediate failover capabilities

b) Zero data loss potential

c) Continuous service availability

d) Geographically distributed risk mitigation

2 Redundancy Levels

- Application Layer: 99.99% uptime guarantee
- Database Layer: Synchronous multi-region replication
- Network Layer: Dual-path connectivity with automatic routing
- Storage Layer: Distributed RAID-10 configuration with instant snapshot capabilities

4. DISASTER RECOVERY PROTOCOLS

1 Recovery Time Objectives (RTO)

- Critical Systems: < 15 minutes
- Non-Critical Systems: < 2 hours
- Complete System Restoration: < 4 hours

2 Recovery Point Objectives (RPO)

- Transactional Systems: < 5 minutes data loss potential
- Analytical Systems: < 30 minutes data loss potential

5. SECURITY AND COMPLIANCE CONSIDERATIONS

1 Compliance Frameworks

- SOC 2 Type II Certified
- ISO 27001:2013 Compliant
- GDPR Data Protection Standards
- CCPA Privacy Regulations

2 Security Monitoring

- 24x7 Security Operations Center (SOC)
- Continuous Threat Monitoring
- Automated Intrusion Detection Systems
- Quarterly Penetration Testing

6. RISK MITIGATION STRATEGIES

1 Periodic Testing Protocols

- Quarterly Full Disaster Recovery Simulations
- Monthly Partial System Failover Tests
- Bi-Annual Comprehensive Infrastructure Stress Testing

2 Mitigation Mechanisms

- Automated Failover Triggers
- Intelligent Load Balancing
- Predictive Capacity Management
- Real-time Anomaly Detection

7. LIMITATIONS AND DISCLAIMERS

1 This document represents the Company's infrastructure status as of January 22, 2024. All specifications are subject to change without prior notification.

2 While extensive precautions have been implemented, no technology infrastructure can guarantee absolute immunity from potential disruptions.

8. CERTIFICATION

Executed by:

_

Dr. Elena Rodriguez

Chief Executive Officer

Nexus Intelligent Systems, Inc.

Date: January 22, 2024

9. CONFIDENTIALITY NOTICE

This document contains proprietary and confidential information. Unauthorized reproduction or distribution is strictly prohibited.