DATA PRIVACY AND PROTECTION POLICY

DeepShield Systems, Inc.

Effective Date: January 1, 2024

Document Version: 3.2

Last Updated: December 15, 2023

1. PURPOSE AND SCOPE

1 This Data Privacy and Protection Policy ("Policy") establishes the framework for protecting sensitive data, including customer information, operational technology (OT) data, industrial control system (ICS) configurations, and proprietary information within DeepShield Systems, Inc. ("DeepShield" or the "Company").

2 This Policy applies to all employees, contractors, consultants, temporary workers, and other personnel who have access to DeepShield's systems, networks, and data assets.

2. DEFINITIONS

1 "Critical Infrastructure Data" means any data related to customer industrial control systems, SCADA networks, or operational technology environments.

2 "Customer Data" means any information provided by or collected from DeepShield's clients, including network configurations, security parameters, and operational metrics.

3 "Proprietary Information" includes DeepShield's intellectual property, source code, AI algorithms, and security architecture specifications.

3. DATA CLASSIFICATION AND HANDLING

1 All data shall be classified into one of the following categories:

a) Level 1 - Public Information

b) Level 2 - Internal Use Only

c) Level 3 - Confidential

d) Level 4 - Highly Restricted

2 Critical Infrastructure Data and customer OT configurations shall always be classified as Level 4 -

Highly Restricted.

3 Data handling requirements for each classification level are detailed in Appendix A of this Policy.

4. SECURITY CONTROLS AND SAFEGUARDS

1 Technical Controls

a) Encryption of data in transit using TLS 1.3 or higher

b) AES-256 encryption for data at rest

c) Multi-factor authentication for all system access

d) Segmented network architecture with dedicated OT security zones

2 Administrative Controls

a) Regular security awareness training

b) Background checks for all employees

c) Role-based access control (RBAC)

d) Quarterly access reviews

5. DATA RETENTION AND DISPOSAL

1 Customer Data Retention

a) Active client data: Duration of service agreement plus 2 years

b) Archived data: 7 years from service termination

c) Audit logs: Minimum 5 years

2 Secure Data Disposal

a) Electronic media sanitization using DOD 5220.22-M standards

b) Physical destruction of storage devices

c) Certified disposal documentation requirements

6. INCIDENT RESPONSE AND BREACH NOTIFICATION

1 All suspected data breaches must be reported to the Chief Security Officer within 1 hour of discovery.

2 The Incident Response Team shall:

a) Assess breach severity and scope

b) Implement containment measures

c) Notify affected parties per contractual and regulatory requirements

d) Document incident details and remediation actions

7. COMPLIANCE AND AUDIT

1 Regular Assessments

a) Quarterly internal security audits

b) Annual third-party compliance reviews

c) Continuous monitoring of security controls

2 Regulatory Compliance

a) NIST Cybersecurity Framework

b) ISO 27001 requirements

c) Industry-specific regulations

8. POLICY ENFORCEMENT

1 Violations of this Policy may result in disciplinary action, up to and including termination of employment or service agreement.

2 The Chief Security Officer shall review this Policy annually and update as necessary.

9. EXCEPTIONS AND MODIFICATIONS

1 Exceptions to this Policy must be approved in writing by both:

a) Chief Security Officer

b) Chief Technology Officer

2 All exceptions shall be documented and reviewed quarterly.

APPROVAL AND EXECUTION

This Policy is approved and adopted by:

Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: January 1, 2024

End of Document