DATA PRIVACY COMPLIANCE FRAMEWORK

DeepShield Systems, Inc.

Effective Date: January 1, 2024

Document Version: 2.0

1. PURPOSE AND SCOPE

1 This Data Privacy Compliance Framework ("Framework") establishes the governing principles, requirements, and procedures for protecting personal data and ensuring compliance with applicable privacy laws and regulations at DeepShield Systems, Inc. ("Company").

2 This Framework applies to all Company employees, contractors, vendors, and third-party service providers who process personal data in connection with the Company's industrial cybersecurity and critical infrastructure protection services.

2. DEFINITIONS

1 "Personal Data" means any information relating to an identified or identifiable natural person, including but not limited to:

a) Employee data

b) Customer contact information

c) System access credentials

d) Operational technology (OT) user logs

e) Industrial control system (ICS) operator data

2 "Processing" means any operation performed on Personal Data, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, or erasure.

3. LEGAL BASIS AND REGULATORY COMPLIANCE

1 The Company shall process Personal Data in compliance with:

a) General Data Protection Regulation (GDPR)

b) California Consumer Privacy Act (CCPA)

c) Industrial control systems security standards (IEC 62443)

d) Maritime cybersecurity regulations

e) Critical infrastructure protection requirements

2 The Company shall maintain documentation of legal bases for all data processing activities, including:

a) Contractual necessity

b) Legal obligations

c) Legitimate business interests

d) Explicit consent where required

4. DATA PROTECTION MEASURES

1 Technical Controls

- Encryption of data at rest and in transit
- Multi-factor authentication for system access
- Network segmentation between IT and OT environments
- Regular security assessments and penetration testing
- Automated threat detection and response capabilities

2 Organizational Controls

- Role-based access control (RBAC)
- Regular employee privacy training
- Data protection impact assessments (DPIAs)
- Incident response procedures
- Third-party vendor assessment program

5. DATA SUBJECT RIGHTS

1 The Company shall honor the following data subject rights:

- Right to access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object to processing

2 Data subject requests shall be processed within 30 days of receipt, with possible 60-day extension for complex requests.

6. INTERNATIONAL DATA TRANSFERS

1 Cross-border data transfers shall be conducted only with:

- Standard contractual clauses
- Binding corporate rules
- Adequacy decisions
- Specific derogations as permitted by law

2 The Company shall maintain a register of international data transfers and corresponding safeguards.

7. INCIDENT RESPONSE AND BREACH NOTIFICATION

1 Data breaches shall be reported to:

- Chief Security Officer within 2 hours
- Affected data subjects within 72 hours
- Supervisory authorities as required by law
- Law enforcement agencies where appropriate

2 The incident response team shall document:

- Nature and scope of the breach
- Categories of data affected
- Number of individuals impacted
- Mitigation measures implemented
- Preventive actions taken

8. VENDOR MANAGEMENT

1 Third-party vendors shall be required to:

- Sign data processing agreements
- Maintain appropriate security controls
- Submit to regular audits
- Provide breach notification guarantees

- Demonstrate regulatory compliance

9. COMPLIANCE MONITORING AND AUDIT

1 The Company shall conduct:

- Quarterly internal privacy audits
- Annual external compliance assessments
- Regular policy reviews and updates
- Continuous monitoring of processing activities

10. GOVERNANCE AND ACCOUNTABILITY

1 Privacy governance shall be overseen by:

- Chief Privacy Officer
- Data Protection Committee
- Legal Department
- Information Security Team

2 Documentation requirements include:

- Records of processing activities
- Privacy impact assessments
- Consent records
- Training completion records
- Audit reports

11. AMENDMENTS AND UPDATES

1 This Framework shall be reviewed annually and updated as necessary to reflect:

- Changes in applicable laws
- New business requirements
- Technological developments
- Identified risks and compliance gaps

APPROVAL AND EXECUTION

IN WITNESS WHEREOF, this Framework has been approved and adopted by the Board of Directors of DeepShield Systems, Inc.

By:

Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

Date: January 1, 2024