Information Security Governance Policy

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document ID: POL-ISG-2024-001

Version: 3.0

1. Purpose and Scope

1. This Information Security Governance Policy ("Policy") establishes the framework for protecting DeepShield Systems, Inc.'s ("Company") information assets, operational technology environments, and customer data through comprehensive security controls and risk management practices.

2. This Policy applies to all employees, contractors, consultants, temporary workers, and other personnel ("Users") who access Company systems, networks, or data, including industrial control systems (ICS) and SCADA environments.

2. Governance Structure

1. Information Security Steering Committee

- Chaired by the Chief Security Architect
- Includes CEO, CTO, VP of Engineering, and CFO
- Meets quarterly to review security posture and approve major initiatives
- Reports directly to the Board of Directors' Risk Committee

2. Security Operations Team

- Led by the Director of Security Operations
- Responsible for day-to-day security monitoring and incident response
- Maintains 24/7 Security Operations Center (SOC)
- Coordinates with OT security specialists for industrial environment protection

3. Risk Management Framework

1. Risk Assessment

- Annual comprehensive risk assessments of all critical systems

- Quarterly vulnerability assessments of OT environments
- Continuous monitoring of threat intelligence feeds
- Regular penetration testing of security controls

2. Risk Treatment

- Risk mitigation strategies must be documented and approved
- Implementation of controls based on NIST Cybersecurity Framework
- Special consideration for maritime and subsea infrastructure requirements
- Regular review and updating of business continuity plans

4. Security Controls

1. Access Control

- Role-based access control (RBAC) for all systems
- Multi-factor authentication required for privileged access
- Regular access rights review and certification
- Automated access revocation upon termination

2. Network Security

- Segmentation between IT and OT networks
- Encrypted communications for remote access
- Regular network architecture reviews
- Advanced threat detection systems

3. Data Protection

- Classification of data based on sensitivity
- Encryption requirements for data at rest and in transit
- Regular backup and recovery testing
- Secure disposal procedures for end-of-life equipment

5. Incident Management

1. Incident Response

- Documented incident response procedures

- Designated incident response team
- Regular incident response drills
- Integration with customer notification procedures

2. Breach Notification

- Legal compliance with breach notification requirements
- Customer communication protocols
- Regulatory reporting procedures
- Post-incident analysis and reporting

6. Compliance and Audit

1. Regulatory Compliance

- Maintenance of required certifications (ISO 27001, IEC 62443)
- Regular compliance assessments
- Documentation of control effectiveness
- Third-party audit support

2. Internal Audit

- Annual security control audits
- Quarterly compliance reviews
- Regular testing of security controls
- Independent assessment of control effectiveness

7. Training and Awareness

1. Security awareness training required for all Users
2. Specialized training for security team members
3. Regular phishing simulations and testing
4. OT-specific security training for relevant personnel

8. Policy Enforcement

1. Violations of this Policy may result in disciplinary action
2. Regular compliance monitoring and reporting

3. Annual review and updates of this Policy

4. Exception management process for special circumstances

9. Document Control

1. Policy Owner: Chief Security Architect

2. Review Frequency: Annual

3. Last Review Date: January 15, 2024

4. Next Review Date: January 15, 2025

Approval

APPROVED by the Board of Directors on January 15, 2024

_

Dr. Marcus Chen

Chief Executive Officer

_

Dr. Elena Rodriguez

Chief Security Architect

_

Sarah Blackwood

Chief Technology Officer