Secure Development Lifecycle Policy

Document ID: SDL-2024-001

Version: 3.2

Effective Date: January 15, 2024

Last Updated: January 15, 2024

Document Owner: Chief Security Architect

Classification: CONFIDENTIAL

1. Purpose and Scope

1. This Secure Development Lifecycle ("SDL") Policy establishes the mandatory security requirements and procedures for all software development activities at DeepShield Systems, Inc. ("Company") related to its industrial control system (ICS) security solutions and operational technology (OT) protection platforms.

2. This Policy applies to all employees, contractors, and third parties involved in the development, testing, deployment, and maintenance of Company software products, including but not limited to:

- DeepShield Core Platform
- Maritime Protection Module
- SCADA Defense Suite
- OT Network Monitor
- Subsea Infrastructure Protection System

2. Definitions

1. "Security Controls" means the safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

2. "Threat Modeling" means the structured process of identifying security threats and vulnerabilities in applications and systems.

3. "Security Testing" means the process of assessing and testing a system to discover security vulnerabilities that could be exploited.

3. SDL Phases and Requirements

1. Training Requirements

- All development personnel must complete annual security training
- Role-specific security training for security architects and penetration testers
- Quarterly security awareness updates for all development teams

2. Planning Phase

- Security requirements must be defined before development begins
- Threat modeling must be performed for all new features and components
- Security architecture review must be completed and documented
- Privacy impact assessment must be conducted for features handling customer data

3. Development Phase

- Use of approved secure coding standards
- Implementation of required security controls
- Regular code reviews with security focus
- Automated security testing integration
- Mandatory use of approved development tools and environments

4. Verification Phase

- Static application security testing (SAST)
- Dynamic application security testing (DAST)
- Interactive application security testing (IAST)
- Penetration testing for all major releases
- Security vulnerability assessment
- Third-party component security review

5. Release Phase

- Security documentation completion
- Final security review and sign-off
- Incident response plan update
- Security advisory preparation
- Deployment security verification

4. Security Controls and Standards

1. Mandatory Security Controls

- Multi-factor authentication for all administrative interfaces
- Encryption of data in transit and at rest
- Secure logging and monitoring
- Access control and authorization
- Input validation and output encoding
- Error handling and logging
- Session management
- Secure configuration management

2. Coding Standards

- Use of approved cryptographic libraries
- Secure communication protocols
- Protected memory management
- Secure file operations
- Database security controls
- API security requirements

5. Compliance and Audit

1. All development activities must comply with:

- ISO/IEC 27001:2013
- IEC 62443 Industrial Network and System Security
- NIST Cybersecurity Framework
- Company-specific security requirements

2. Regular audits will be conducted to ensure compliance with this Policy.

6. Roles and Responsibilities

1. Chief Security Architect

- Overall responsibility for SDL implementation
- Final security sign-off authority
- Policy maintenance and updates

2. Development Teams

- Implementation of security controls
- Adherence to secure coding standards
- Security testing execution

3. Security Team

- Security review and assessment
- Threat modeling support
- Security testing oversight

7. Exceptions and Violations

1. Exception Process

- All exceptions must be documented and approved by Chief Security Architect
- Temporary exceptions limited to 90 days
- Risk assessment required for all exceptions

2. Policy Violations

- Violations will result in disciplinary action
- Immediate remediation required for security issues
- Incident reporting and investigation procedures

8. Policy Review and Updates

1. This Policy shall be reviewed annually and updated as needed to reflect:

- Changes in technology and threat landscape
- New security requirements and standards
- Lessons learned from security incidents
- Industry best practices

9. Document Control

Approved by:

- Dr. Elena Rodriguez, Chief Security Architect
- James Morrison, VP of Engineering

- Sarah Blackwood, CTO

Date: January 15, 2024

This document contains confidential and proprietary information of DeepShield Systems, Inc. Unauthorized distribution or reproduction is strictly prohibited.