Engineering Team Communication Protocol

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.0

Classification: Confidential - Internal Use Only

1. Purpose and Scope

1. This Engineering Team Communication Protocol ("Protocol") establishes mandatory guidelines and procedures for all internal and external communications within and by the Engineering Department of DeepShield Systems, Inc. ("Company").

2. This Protocol applies to all engineering team members, contractors, and consultants engaged in development, maintenance, or support of the Company's industrial control system (ICS) security solutions, operational technology (OT) protection systems, and related technologies.

2. Definitions

1. "Confidential Information" means any non-public technical information, source code, system architecture, security vulnerabilities, customer implementations, or proprietary methodologies.

2. "Critical Communications" refers to any communications regarding security incidents, system vulnerabilities, or changes affecting production environments.

3. "Engineering Teams" includes all software development, security architecture, QA, DevOps, and technical support personnel.

3. Internal Communication Channels

1. Primary Channels

a) Secure Development Environment (SDE) Chat System

b) Internal Engineering Portal

c) Encrypted Email System

d) Secure Video Conferencing Platform

2. Channel Usage Requirements

a) All technical discussions must occur within approved channels

b) No discussion of source code or security architecture on unauthorized platforms

c) Mandatory encryption for all critical communications

d) Regular archival and backup of all communication logs

4. Security Classifications

1. Communication Classification Levels

- Level 1: Public Information
- Level 2: Internal Use Only
- Level 3: Confidential
- Level 4: Highly Confidential

2. Classification Requirements

a) All communications must be clearly marked with appropriate classification

b) Default classification is Level 2 if not specified

c) Level 3 and 4 communications require end-to-end encryption

d) Automatic classification monitoring system must be utilized

5. Documentation Standards

1. Technical Documentation

a) Must follow Company's standardized documentation template

b) Required peer review for all technical specifications

c) Version control mandatory for all documentation

d) Regular auditing of documentation accuracy

2. Communication Records

a) Retention of all critical communications for 7 years

b) Quarterly archival of routine communications

c) Mandatory logging of all external technical communications

d) Regular audit trail verification

6. External Communication Protocols

1. Customer Communications

a) All technical communications must be logged in Customer Relationship Management system

b) Technical details limited to authorized disclosure levels

c) Mandatory review process for technical documentation shared externally

d) Encryption requirements for customer-specific technical details

2. Vendor Communications

a) Non-disclosure agreements required for all technical discussions

b) Restricted sharing of system architecture details

c) Documented approval process for technical information exchange

d) Regular review of vendor communication compliance

7. Incident Response Communication

1. Security Incident Communications

a) Immediate notification to Security Response Team

b) Documented escalation procedures

c) Mandatory use of incident response communication channel

d) Regular testing of emergency communication procedures

2. Critical System Changes

a) Advance notification requirements

b) Change management documentation

c) Post-implementation communication requirements

d) Stakeholder notification protocols

8. Compliance and Enforcement

1. Monitoring and Auditing

a) Regular compliance audits

b) Automated monitoring of communication channels

c) Quarterly review of communication patterns

d) Documentation of violations and remediation

2. Violations and Consequences

a) Graduated response system for violations

b) Mandatory retraining for minor violations

c) Disciplinary procedures for serious violations

d) Regular review of enforcement effectiveness

9. Protocol Updates and Training

1. All Engineering Team members must complete annual training on this Protocol.

2. This Protocol shall be reviewed and updated annually or as required by significant operational changes.

10. Authorization

This Protocol is authorized and approved by:

James Morrison

VP of Engineering

DeepShield Systems, Inc.

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: January 15, 2024

End of Document