# OT/IT CONVERGENCE SECURITY CONTROLS

**DeepShield Systems, Inc.**

*Document Version: 2.4*

*Effective Date: January 15, 2024*

*Classification: Confidential*

## 1. PURPOSE AND SCOPE

1. This document establishes mandatory security controls and governance requirements for the convergence of Operational Technology (OT) and Information Technology (IT) systems within DeepShield Systems, Inc. ("Company") and its client implementations.

2. These controls apply to all Company personnel, contractors, and third-party vendors involved in the development, deployment, or maintenance of integrated OT/IT environments.

## 2. DEFINITIONS

1. "Operational Technology (OT)" refers to hardware and software systems that monitor and control physical devices, processes, and events within industrial environments.

2. "Information Technology (IT)" encompasses all traditional enterprise computing systems, networks, and applications used for business data processing and communications.

3. "Convergence Zone" defines any area where OT and IT systems interface, integrate, or share data.

4. "Security Control" means any technical, administrative, or physical safeguard implemented to protect system integrity and confidentiality.

## 3. ARCHITECTURAL REQUIREMENTS

1. Segmentation Controls

a) Mandatory implementation of DMZ architecture between IT and OT networks

b) Physical and logical separation of critical OT components

c) Dedicated firewalls with OT-specific rulesets

d) Network segmentation using VLANs and security zones

2. Access Control Requirements

a) Role-based access control (RBAC) for all convergence points

b) Multi-factor authentication for administrative access

c) Separate authentication domains for OT and IT systems

d) Privileged Access Management (PAM) implementation

## 4. MONITORING AND DETECTION

1. Security Information and Event Management (SIEM)

a) Centralized logging of all cross-domain traffic

b) Real-time monitoring of convergence points

c) Integration with DeepShield's AI-driven anomaly detection

d) Automated alert correlation across OT/IT boundaries

2. Industrial Protocol Analysis

a) Deep packet inspection of industrial protocols

b) Baseline profiling of normal operations

c) Protocol-specific threat detection

d) Behavioral analytics for OT processes

## 5. INCIDENT RESPONSE AND RECOVERY

1. Incident Management Requirements

a) Dedicated OT/IT incident response procedures

b) Cross-functional response team composition

c) Escalation protocols for convergence-related incidents

d) Communication procedures during security events

2. Business Continuity

a) Failover mechanisms for critical systems

b) Recovery time objectives (RTO) for converged systems

c) Data backup requirements for OT environments

d) Regular testing of recovery procedures

## 6. COMPLIANCE AND DOCUMENTATION

1. Regulatory Requirements

a) Compliance with IEC 62443 standards

b) NIST Cybersecurity Framework alignment

c) Industry-specific regulatory requirements

d) Documentation of compliance evidence

2. Change Management

a) Formal change control procedures

b) Impact assessment requirements

c) Testing and validation protocols

d) Rollback procedures

## 7. TRAINING AND AWARENESS

1. Personnel Requirements

a) Mandatory OT/IT security awareness training

b) Role-specific technical training

c) Incident response drills

d) Annual certification requirements

## 8. AUDIT AND ASSESSMENT

1. Internal Audit Requirements

a) Quarterly security assessments

b) Penetration testing of convergence points

c) Configuration compliance reviews

d) Control effectiveness evaluation

2. External Validation

a) Annual third-party security audits

b) Vulnerability assessments

c) Compliance certification maintenance

d) Independent security testing

## 9. ENFORCEMENT AND EXCEPTIONS

1. Any deviation from these controls requires formal exception approval from:

a) Chief Security Architect

b) Chief Technology Officer

c) VP of Engineering

d) Documentation in the exception management system

## 10. DOCUMENT CONTROL

1. This document shall be reviewed and updated annually or upon significant changes to the technology environment.

2. The Chief Security Architect maintains ultimate authority over this document.

## APPROVAL AND EXECUTION

IN WITNESS WHEREOF, the undersigned have executed this document as of the Effective Date:

```

–

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

–

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: January 15, 2024
```

## REVISION HISTORY

Version 2.4 - January 15, 2024 - Updated monitoring requirements and compliance standards

Version 2.3 - July 1, 2023 - Added AI-driven detection requirements

Version 2.2 - January 10, 2023 - Updated architectural controls

Version 2.1 - June 15, 2022 - Initial release