

REGULATORY TRAINING REQUIREMENTS MATRIX 2023

DeepShield Systems, Inc.

Effective Date: January 1, 2023

Document Control #: REG-TRN-2023-001

Version: 2.0

1. PURPOSE AND SCOPE

1. This Regulatory Training Requirements Matrix ("Matrix") establishes the mandatory training requirements for all employees, contractors, and authorized third parties of DeepShield Systems, Inc. ("Company") engaged in the development, deployment, or support of industrial control system (ICS) security solutions and critical infrastructure protection systems.
2. This Matrix is designed to ensure compliance with applicable federal, state, and international regulations governing cybersecurity services for critical infrastructure and industrial operations technology (OT) environments.

2. REGULATORY FRAMEWORK

1. Primary Regulatory Requirements:
- NIST Cybersecurity Framework (CSF)
 - IEC 62443 Industrial Automation and Control Systems Security
 - Maritime Transportation Security Act (MTSA) requirements
 - NERC CIP Standards (as applicable to energy sector clients)
 - EU NIS Directive 2.0 compliance requirements

3. REQUIRED TRAINING BY ROLE CATEGORY

3.1. Technical Operations Personnel

Training Requirement	Frequency	Applicable Roles	Regulatory Basis
----- ----- ----- -----			
ICS Security Fundamentals	Annual	All Technical Staff	IEC 62443-2-4
OT Network Security	Semi-annual	Security Engineers	NIST SP 800-82
Maritime Cybersecurity	Annual	Maritime Division	MTSA Sec. 70103

| Incident Response | Quarterly | Security Operations | NIST CSF PR.IP-10 |

3.2. Management and Administrative Personnel

| Training Requirement | Frequency | Applicable Roles | Regulatory Basis |

|-----|-----|-----|-----|

| Security Governance | Annual | Management | ISO 27001 |

| Data Privacy | Annual | All Staff | GDPR Art. 39 |

| Export Controls | Annual | Sales, Engineering | EAR 734 |

| Risk Management | Semi-annual | Directors, VP+ | NIST CSF ID.RM |

4. CERTIFICATION REQUIREMENTS

1. Mandatory Certifications:

- CISSP for Security Architects
- GICSP for ICS Security Engineers
- CompTIA Security+ for Technical Support
- ISO 27001 Lead Implementer for Compliance Officers

2. Certification Maintenance:

- All certifications must remain active
- Renewal documentation required 30 days prior to expiration
- Company will reimburse certification maintenance fees per Policy FIN-2023-008

5. TRAINING DELIVERY AND DOCUMENTATION

1. Training Methods:

- Instructor-led classroom sessions
- Virtual instructor-led training (VILT)
- Self-paced online modules
- Hands-on laboratory exercises

2. Documentation Requirements:

- Training completion records maintained for 5 years
- Quarterly compliance reports to Security Steering Committee

- Annual audit of training records by Compliance Department
- Integration with HR management system

6. COMPLIANCE MONITORING

1. The Compliance Department shall:

- Monitor training completion rates monthly
- Issue non-compliance notices within 5 business days
- Escalate persistent non-compliance to management
- Provide quarterly compliance metrics to Board

2. Enforcement:

- Access to systems contingent on training completion
- Performance evaluations include training compliance
- Contract renewal dependent on certification maintenance

7. EXCEPTIONS AND WAIVERS

1. Exception Process:

- Written request to Compliance Officer required
- Business justification must be documented
- Maximum 90-day temporary waiver
- CEO approval required for extended waivers

8. REVIEW AND UPDATES

1. This Matrix shall be reviewed:

- Annually at minimum
- Upon significant regulatory changes
- Following major incident lessons learned
- As directed by Board or Security Committee

9. DOCUMENT CONTROL

Version History:

- 2.0: Current version (January 1, 2023)
- 1.1: Updated certification requirements (June 15, 2022)
- 1.0: Initial release (January 1, 2022)

Approved by:

- Security Steering Committee: December 15, 2022
- Board of Directors: December 20, 2022

10. ATTESTATION

The undersigned hereby confirms this Matrix is current and approved:

Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

Date: _