Critical Infrastructure Protection Training Records

DeepShield Systems, Inc.

Last Updated: December 31, 2023

Document Reference: DSS-CIP-TR-2023-12

1. Training Program Overview

1. DeepShield Systems, Inc. ("Company") maintains comprehensive Critical Infrastructure Protection ("CIP") training records in accordance with NERC CIP Standards, NIST Framework requirements, and industry best practices for industrial control system security.

2. This document details the Company's CIP training protocols, completion records, and compliance verification procedures for the period January 1, 2023 through December 31, 2023.

2. Required Training Modules

1. Core CIP Training Components:

- Industrial Control System Security Fundamentals (ICS-100)
- SCADA Network Protection Protocols (SNP-200)
- Maritime Infrastructure Security Standards (MIS-300)
- Advanced Threat Detection & Response (ATD-400)
- Regulatory Compliance & Reporting (RCR-500)

2. Role-Specific Training Requirements:

- Security Operations Center Personnel: Modules ICS-100, SNP-200, ATD-400
- Field Engineers: Modules ICS-100, MIS-300
- Compliance Officers: Modules ICS-100, RCR-500
- Development Team: Modules ICS-100, SNP-200
- Executive Leadership: Modules ICS-100, RCR-500

3. Training Completion Records

1. Aggregate Completion Statistics:

- Total Employees Required: 187
- Completion Rate: 98.4%

- Average Score: 92.3%
- Remediation Required: 3 employees
- Outstanding Completions: 3 employees (new hires pending initial training)

2. Department-Level Completion:

- Engineering: 100% (72/72 employees)
- Security Operations: 97.8% (45/46 employees)
- Product Development: 100% (35/35 employees)
- Compliance & Legal: 100% (12/12 employees)
- Executive & Administration: 95.5% (21/22 employees)

4. Training Delivery Methods

1. Primary Training Platforms:

- DeepShield Learning Management System (LMS) v4.2
- Virtual Instructor-Led Training (VILT) Sessions
- Hands-on Laboratory Exercises
- Quarterly In-Person Workshops

2. Assessment Methodologies:

- Computer-Based Testing (minimum 80% passing score)
- Practical Skills Evaluation
- Scenario-Based Assessments
- Annual Competency Reviews

5. Compliance Verification

1. Internal Audit Procedures:

- Quarterly training record reviews
- Random spot checks of completion certificates
- Annual comprehensive audit
- Third-party verification of training materials

2. Documentation Requirements:

- Digital completion certificates
- Assessment scores and feedback
- Attendance records for live sessions
- Annual competency attestations

6. Training Update Protocol

1. Course Material Reviews:

- Quarterly content updates based on threat landscape
- Annual comprehensive curriculum review
- Regulatory requirement alignment checks
- Industry standard compatibility verification

2. Version Control:

- Training materials version: v2023.4
- Last update: December 15, 2023
- Next scheduled review: March 15, 2024

7. Certification

The undersigned hereby certifies that this document accurately reflects the Critical Infrastructure Protection training records of DeepShield Systems, Inc. for the specified period.

CERTIFIED THIS 31st DAY OF DECEMBER, 2023

```

_

Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

_

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.
```

–

Robert Kessler

Chief Financial Officer

DeepShield Systems, Inc.
```

## 8. Legal Disclaimer

This document contains confidential and proprietary information of DeepShield Systems, Inc. Unauthorized disclosure, reproduction, or distribution is strictly prohibited. The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

*End of Document*
```