CYBERSECURITY CERTIFICATION REQUIREMENTS

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.4

Policy Number: DSS-SEC-2024-001

1. PURPOSE AND SCOPE

1. This document establishes the mandatory cybersecurity certification requirements for all technical personnel employed by or contracted with DeepShield Systems, Inc. ("Company") who have access to or responsibility for the Company's industrial control system (ICS) security platforms, operational technology (OT) environments, or critical infrastructure protection systems.

2. These requirements apply to all full-time employees, contractors, consultants, temporary workers, and other personnel who:

a) Develop, maintain, or support the Company's security solutions

b) Access client OT environments or SCADA networks

c) Participate in incident response activities

d) Manage or monitor industrial automation systems

2. BASELINE CERTIFICATION REQUIREMENTS

1. All technical personnel must maintain at least one of the following baseline certifications:

- Certified Information Systems Security Professional (CISSP)
- Global Industrial Cyber Security Professional (GICSP)
- Certified Information Security Manager (CISM)
- CompTIA Security+

2. Personnel working directly with industrial control systems must additionally hold:

- ISA/IEC 62443 Cybersecurity Certification
- Industrial Control Systems Security Certification

3. ROLE-SPECIFIC REQUIREMENTS

1. Security Architecture Team

- SABSA Chartered Security Architect
- TOGAF 9.2 Certification
- Cloud Security Alliance CCSK

2. Incident Response Team

- GIAC Incident Handler (GCIH)
- GIAC Response and Industrial Defense (GRID)
- EC-Council Certified Incident Handler (ECIH)

3. Maritime Security Specialists

- Maritime Transportation Security Clearance Program (MTSCP) Certification
- International Ship and Port Facility Security (ISPS) Code Certification

4. Development Team

- Certified Secure Software Lifecycle Professional (CSSLP)
- GIAC Secure Software Programmer (GSSP)

4. CERTIFICATION MAINTENANCE

1. Personnel must maintain active certification status through:

- Timely completion of continuing education requirements
- Payment of certification renewal fees
- Documentation of required practical experience
- Successful completion of recertification exams when required

2. The Company will maintain a certification tracking system to:

- Monitor certification expiration dates
- Track continuing education credits
- Issue renewal reminders
- Verify certification status

5. COMPANY SUPPORT AND REIMBURSEMENT

1. The Company will provide:

- Reimbursement for initial certification costs

- Coverage of annual renewal fees
- Paid time off for examination preparation
- Access to training materials and courses
- Mentorship programs for certification preparation

2. Reimbursement is subject to:
- Prior approval from department manager
- Successful completion of certification
- Minimum one-year service commitment
- Submission of proper documentation

6. COMPLIANCE AND ENFORCEMENT

1. Failure to maintain required certifications may result in:
- Temporary restriction of system access
- Reassignment to non-technical roles
- Performance improvement plans
- Potential termination of employment

2. Grace periods for certification renewal:
- 30 days for baseline certifications
- 60 days for role-specific certifications
- Extensions require written approval from Chief Security Architect

7. AUDIT AND REVIEW

1. The Human Resources department, in conjunction with the Security Operations team, will:
- Conduct quarterly certification audits
- Review certification requirements annually
- Update requirements based on industry standards
- Report compliance metrics to executive leadership

8. MODIFICATIONS AND UPDATES

1. This document shall be reviewed and updated annually or as required by:

- Changes in industry standards
- New regulatory requirements
- Evolution of Company services
- Identification of new security threats

9. AUTHORITY AND APPROVAL

This policy is issued under the authority of:

/s/ Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

/s/ Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: January 15, 2024