Employee Onboarding Checklist - Technical Roles

DeepShield Systems, Inc.

Last Updated: January 11, 2024

Document ID: HR-ONB-TECH-2024-01

1. Purpose and Scope

This document establishes the mandatory onboarding procedures for all technical roles at DeepShield Systems, Inc. ("Company"), including but not limited to software engineers, security architects, OT specialists, and infrastructure engineers. This checklist ensures compliance with Company security protocols, regulatory requirements, and operational standards.

2. Pre-Employment Requirements

1. Background Screening

- Criminal background check completion
- Education verification
- Professional certification validation
- Previous employment verification (7-year history)
- Export control compliance check (ITAR/EAR)

2. Documentation

- Signed offer letter
- Completed I-9 form with supporting documentation
- Signed Non-Disclosure Agreement (Form NDA-TECH-2024)
- Signed Intellectual Property Assignment Agreement (Form IP-2024)
- Completed Security Clearance Application (if applicable)

3. System Access and Security Protocols

1. Network Access

- Creation of corporate email account (@deepshield.com)
- VPN access configuration
- Multi-factor authentication setup

- Password management system enrollment
- Development environment access provisioning

2. Security Requirements

- Completion of Security Awareness Training (SAT-TECH-2024)
- Industrial Control Systems (ICS) Security Fundamentals certification
- SCADA security protocols training
- Maritime cybersecurity orientation (if applicable)
- Zero-trust architecture training

4. Technical Environment Setup

1. Hardware Provisioning

- Secure workstation configuration
- Development environment setup
- Testing environment access
- Hardware security module (HSM) access
- Secure code signing certificates

2. Software and Tools

- Source code repository access
- CI/CD pipeline permissions
- Bug tracking system credentials
- Technical documentation access
- Collaboration tools setup

5. Role-Specific Training Requirements

1. Core Technical Training

- DeepShield proprietary architecture overview
- AI/ML framework orientation
- OT network monitoring systems
- Threat detection algorithms
- Incident response procedures

2. Specialized Training

- Maritime infrastructure protection protocols
- Subsea systems security architecture
- Industrial automation security controls
- SCADA network defense mechanisms
- Critical infrastructure compliance requirements

6. Compliance and Policy Review

1. Required Policy Acknowledgments

- Information Security Policy
- Code of Conduct
- Remote Work Security Policy
- Data Classification Guidelines
- Incident Response Procedures

2. Regulatory Training

- NERC CIP compliance training
- NIST Cybersecurity Framework
- ISO 27001 requirements
- Maritime cybersecurity regulations
- Export control compliance

7. Department Integration

1. Team Integration

- Assignment of technical mentor
- Introduction to technical leadership
- Team collaboration protocols
- Project assignment briefing
- Performance expectations review

2. Knowledge Transfer

- Access to technical documentation

- System architecture reviews
- Current project status briefings
- Client environment orientations
- Emergency response procedures

8. Verification and Documentation

1. Completion Requirements

- All items must be completed within 30 days of start date
- Documentation stored in HR system (Workday)
- Security compliance verification
- Technical proficiency assessment
- Manager sign-off required

2. Ongoing Monitoring

- 30-day security review
- 60-day technical assessment
- 90-day performance review
- Continuous compliance monitoring
- Annual security recertification

9. Legal Notices

This document is confidential and proprietary to DeepShield Systems, Inc. All rights reserved. No part of this document may be reproduced or transmitted in any form without prior written permission. Failure to complete all required items may result in limited system access or delayed project assignments.

10. Document Control

Version: 3.2

Effective Date: January 11, 2024

Review Cycle: Annual

Document Owner: Technical Operations

Approved By: James Morrison, VP of Engineering

Security Classification: Internal Use Only

This checklist is maintained by the Technical Operations department in conjunction with Human Resources and Information Security. For questions or updates, contact techops@deepshield.com