Remote Employee Equipment Policy

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Policy Number: HR-2024-001

1. Purpose and Scope

1. This Remote Employee Equipment Policy ("Policy") establishes guidelines and procedures for the issuance, use, maintenance, and return of company-provided equipment to remote employees of DeepShield Systems, Inc. ("Company").

2. This Policy applies to all full-time and part-time remote employees, contractors, and consultants who receive Company equipment for remote work purposes.

2. Equipment Issuance

1. Standard Equipment Package

- Company-issued laptop with required security configurations
- Dual-factor authentication token
- Secure VPN hardware key
- Industrial control system security monitoring tools (as required)
- Peripherals (keyboard, mouse, headset)

2. Additional Equipment

Additional equipment may be provided based on job function and management approval, including:

- External monitors (maximum 2)
- Specialized testing equipment for security validation
- Mobile devices for on-call personnel
- Network testing hardware

3. Security Requirements

1. All Company equipment must maintain:

- Current version of DeepShield's proprietary endpoint protection
- Approved encryption protocols

- Regular security patches and updates
- Secure boot configurations
- Hardware-level security modules enabled

2. Prohibited Actions
- Installation of unauthorized software
- Disabling security features
- Using equipment on unsecured networks
- Sharing equipment with non-employees
- Storing personal data on Company devices

4. Employee Responsibilities

1. Equipment Care
- Maintain equipment in good working condition
- Store in secure location when not in use
- Report damage or malfunction immediately
- Follow proper ergonomic setup guidelines
- Perform required maintenance and updates

2. Security Compliance
- Complete monthly security audits
- Report security incidents within 2 hours
- Maintain secure home office environment
- Use only approved remote access methods
- Participate in quarterly security training

5. Support and Maintenance

1. Technical Support
- 24/7 IT help desk access
- Remote troubleshooting assistance
- Hardware replacement within 48 hours
- Security incident response support

- Regular virtual equipment checks

2. Maintenance Schedule

- Monthly security updates
- Quarterly hardware diagnostics
- Annual equipment assessment
- Bi-annual software audit
- Equipment replacement every 3 years

6. Equipment Return

1. Return Triggers

- Employment termination
- Extended leave exceeding 90 days
- Equipment upgrade cycle
- Role change requiring different equipment
- Company request

2. Return Procedures

- Schedule return within 5 business days
- Complete data backup protocol
- Execute secure data wiping
- Ship via approved courier only
- Submit return confirmation form

7. Liability and Costs

1. Company Responsibility

- Initial equipment procurement
- Normal wear and tear
- Scheduled maintenance
- Security software licenses
- Approved upgrades

2. Employee Responsibility

- Damage from negligence
- Lost or stolen equipment
- Unauthorized modifications
- Personal software licenses
- Home office setup costs

8. Policy Compliance

1. Monitoring and Enforcement

- Regular compliance audits
- Activity logging and review
- Performance impact assessment
- Security violation tracking
- Equipment usage analytics

2. Violations

Failure to comply may result in:

- Equipment retrieval
- Remote access restriction
- Disciplinary action
- Cost recovery
- Legal action if applicable

9. Policy Updates

1. This Policy may be updated at Company's discretion with 30 days notice to affected employees.

2. Emergency security updates may be implemented immediately.

10. Acknowledgment

I acknowledge receipt and understanding of this Remote Employee Equipment Policy:

Employee Name: _

Employee ID: _

Date: _

Signature: _

Authorized by:

/s/ Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: January 15, 2024