Remote Work Policy & Guidelines

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Policy Number: HR-2024-RW-001

Version: 2.0

1. Purpose and Scope

1. This Remote Work Policy ("Policy") establishes guidelines and requirements for remote work arrangements at DeepShield Systems, Inc. ("Company"). This Policy applies to all employees, contractors, and consultants who work remotely, whether on a full-time, part-time, or temporary basis.

2. Given the sensitive nature of the Company's industrial cybersecurity operations and critical infrastructure protection services, this Policy aims to maintain operational security while enabling workforce flexibility.

2. Definitions

1. "Remote Work" refers to work performed outside of Company facilities, including home offices, satellite locations, or other approved workspaces.

2. "Secure Work Environment" means a workspace that meets the Company's security requirements for handling sensitive information and accessing Company systems.

3. "Critical Operations Personnel" refers to employees directly involved in real-time monitoring, incident response, or critical infrastructure protection activities.

3. Eligibility and Authorization

1. Remote work eligibility is determined based on:

a) Job role and responsibilities

b) Security clearance requirements

c) Operational requirements

d) Performance history

e) Technical capabilities

2. Critical Operations Personnel must maintain a hybrid schedule with minimum on-site presence of three (3) days per week, unless otherwise authorized by the Chief Security Architect.

3. All remote work arrangements must be approved by:

a) Immediate supervisor

b) Department head

c) Information Security team

d) Human Resources

4. Security Requirements

1. Remote workers must:

a) Use Company-issued devices exclusively for work purposes

b) Maintain current security software and updates

c) Use approved VPN connections

d) Implement multi-factor authentication

e) Secure physical workspace from unauthorized access

2. Prohibited activities include:

a) Accessing Company systems on personal devices

b) Working from public locations without prior approval

c) Storing sensitive data on local drives

d) Sharing workspace with unauthorized individuals

5. Equipment and Technology

1. The Company will provide:

a) Laptop or workstation

b) Security tokens

c) Encryption software

d) Necessary peripherals

e) Technical support

2. Employees must maintain:

a) Minimum internet bandwidth of 100 Mbps

b) Dedicated workspace

c) Secure storage for physical documents

d) Backup power solutions

6. Work Hours and Availability

1. Remote employees must:

a) Maintain core hours of 9:00 AM - 3:00 PM EST

b) Be available via approved communication channels

c) Respond to critical incidents within 15 minutes

d) Update calendar and status indicators

2. Time tracking and overtime policies apply as per standard Company policies.

7. Performance and Productivity

1. Remote employees are subject to:

a) Regular performance reviews

b) Project milestone tracking

c) Time and activity monitoring

d) Security compliance audits

2. Managers must establish clear deliverables and metrics for remote team members.

8. Compliance and Security Incidents

1. Remote workers must immediately report:

a) Security breaches or suspicious activities

b) Lost or stolen equipment

c) Unauthorized access attempts

d) Policy violations

2. Failure to comply may result in:

a) Revocation of remote work privileges

b) Disciplinary action

c) Legal consequences

9. Policy Review and Updates

1. This Policy shall be reviewed annually by:

a) Legal Department

b) Information Security team

c) Human Resources

d) Executive Leadership

2. Updates will be communicated to all affected personnel with minimum 30 days notice.

10. Acknowledgment

I acknowledge that I have read, understand, and agree to comply with all provisions of this Remote Work Policy.

Employee Name: _

Employee ID: _

Date: _

Signature: _

Approved by:

Robert Kessler

Chief Financial Officer

DeepShield Systems, Inc.

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: January 15, 2024