SECURITY BREACH LIABILITY TERMS

DeepShield Systems, Inc.

Effective Date: January 1, 2024

1. DEFINITIONS

1. "Security Breach" means any unauthorized access, disclosure, acquisition, or use of Protected Data or Critical Infrastructure Systems maintained, processed, or transmitted by or on behalf of DeepShield Systems, Inc. ("Company").

2. "Protected Data" means any (i) customer data, (ii) operational technology (OT) system data, (iii) industrial control system (ICS) configurations, (iv) SCADA network information, or (v) critical infrastructure specifications protected under Company's security protocols.

3. "Critical Infrastructure Systems" means any industrial automation systems, maritime facility controls, offshore platform operations, or manufacturing process controls protected by Company's security solutions.

2. BREACH NOTIFICATION AND RESPONSE

1. **Notification Timeline**

Company shall notify affected customers of any Security Breach within:

(a) 24 hours of discovery for Critical Infrastructure Systems breaches

(b) 48 hours of discovery for Protected Data breaches

(c) Such shorter time period as required by applicable law or customer contracts

2. **Response Protocol**

Upon discovery of a Security Breach, Company shall:

(a) Activate its Incident Response Team

(b) Implement containment measures

(c) Conduct root cause analysis

(d) Deploy necessary patches or security updates

(e) Document all response actions taken

(f) Provide affected customers with detailed incident reports

3. LIABILITY LIMITATIONS

1. **Monetary Caps**

Company's aggregate liability for any single Security Breach shall not exceed:

(a) $5,000,000 for Critical Infrastructure Systems breaches

(b) $2,500,000 for Protected Data breaches

(c) The total fees paid by the affected customer in the preceding 12 months

2. **Exclusions**

Liability caps shall not apply to:

(a) Gross negligence or willful misconduct

(b) Violation of applicable cybersecurity laws

(c) Breach of confidentiality obligations

(d) Third-party claims for intellectual property infringement

4. INDEMNIFICATION

1. Company shall indemnify customers against third-party claims arising from Security Breaches caused by:

(a) Defects in Company's security platform

(b) Failure to implement promised security measures

(c) Negligent acts or omissions by Company personnel

2. Customer shall indemnify Company against claims arising from:

(a) Customer's misuse of Company's security solutions

(b) Customer's failure to implement recommended security measures

(c) Unauthorized modifications to Company's systems

5. INSURANCE REQUIREMENTS

1. Company shall maintain:

(a) Cyber liability insurance: minimum $10,000,000 coverage

(b) Technology E&O insurance: minimum $5,000,000 coverage

(c) Professional liability insurance: minimum $5,000,000 coverage

2. All policies shall:

(a) Name key customers as additional insureds

(b) Provide primary coverage without contribution

(c) Include breach response costs coverage

(d) Cover regulatory defense and penalties

6. MITIGATION AND REMEDIATION

1. **Required Actions**

Following a Security Breach, Company shall:

(a) Implement necessary security improvements

(b) Provide affected customers with compensatory services

(c) Conduct third-party security audits

(d) Update security protocols and documentation

2. **Cost Allocation**

Company shall bear all costs associated with:

(a) Breach investigation and response

(b) Customer notifications and communications

(c) Credit monitoring services (if applicable)

(d) System remediation and security upgrades

7. DISPUTE RESOLUTION

1. All disputes regarding Security Breaches shall be resolved through:

(a) Mandatory executive-level negotiation

(b) Mediation under ICC Rules

(c) Binding arbitration if mediation fails

2. Venue for all proceedings shall be Delaware, governed by Delaware law.

8. TERM AND SURVIVAL

1. These Security Breach Liability Terms shall remain in effect for the duration of any customer relationship plus three (3) years.

2. Sections 3, 4, and 7 shall survive termination indefinitely.

ACKNOWLEDGMENT

The undersigned acknowledges and agrees to these Security Breach Liability Terms.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Marcus Chen

Title: Chief Executive Officer

Date: