Data Loss Prevention Policy

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document ID: POL-DLP-2024-01

Version: 2.0

1. Purpose and Scope

1. This Data Loss Prevention Policy ("Policy") establishes the requirements and procedures for protecting sensitive data assets of DeepShield Systems, Inc. ("Company") from unauthorized access, exfiltration, and disclosure.

2. This Policy applies to all employees, contractors, consultants, temporary workers, and other personnel ("Users") who have access to Company systems, networks, and data assets.

3. This Policy covers all Company data, with particular emphasis on:

- Industrial control system (ICS) configurations and security parameters
- Proprietary deep-layer security architecture specifications
- Customer operational technology (OT) network data
- SCADA system security protocols
- Artificial intelligence and machine learning models
- Source code and development documentation
- Client deployment configurations

2. Definitions

1. "Sensitive Data" means any information classified as Confidential or Restricted under the Company's Data Classification Policy, including but not limited to trade secrets, intellectual property, customer data, and security architecture specifications.

2. "DLP Solutions" refers to the technological tools and systems implemented to monitor, detect, and prevent unauthorized data transmission.

3. "Data Owner" means the individual or department responsible for the integrity and maintenance of specific data assets.

3. Data Loss Prevention Controls

1. Technical Controls

- Endpoint DLP monitoring and blocking
- Network DLP filtering and inspection
- Cloud access security broker (CASB) integration
- Email and messaging content filtering
- Removable media restrictions
- Encrypted data transfer protocols

2. Administrative Controls

- Regular DLP rule updates and refinement
- Incident response procedures
- User training and awareness programs
- Access control reviews
- Data classification enforcement
- Audit logging and monitoring

4. Prohibited Activities

1. Users shall not:

- Disable or circumvent DLP controls
- Transfer sensitive data to unauthorized external systems
- Use unauthorized cloud storage or file sharing services
- Remove sensitive data from Company premises without authorization
- Share access credentials or authentication tokens
- Process sensitive data on personal devices

5. Data Transfer Procedures

1. Internal Transfers

- Use approved secure file transfer protocols
- Verify recipient authorization
- Apply appropriate encryption

- Log all significant data movements

2. External Transfers

- Obtain written authorization from Data Owner
- Use Company-approved secure transfer methods
- Implement end-to-end encryption
- Document all external transfers
- Verify recipient security controls

6. Incident Response

1. Users must immediately report suspected data loss incidents to:

- Information Security Team (security@deepshield.com)
- Their immediate supervisor
- Legal Department (legal@deepshield.com)

2. The Information Security Team shall:

- Investigate all reported incidents
- Document findings and impact assessment
- Implement containment measures
- Coordinate with Legal for compliance requirements
- Develop remediation plans

7. Compliance and Enforcement

1. Compliance Monitoring

- Regular DLP system audits
- Periodic policy compliance reviews
- Random spot checks of data transfers
- System activity monitoring
- Access pattern analysis

2. Policy Violations

- May result in disciplinary action up to termination

- Could trigger legal action for serious breaches
- Will be documented in personnel files
- May require remedial training
- Could result in revocation of system access

8. Policy Review and Updates

1. This Policy shall be reviewed annually by the Information Security Committee.

2. Updates will be made based on:

- Changes in technology landscape
- New threat vectors
- Regulatory requirements
- Operational needs
- Incident lessons learned

9. Acknowledgment

I acknowledge that I have read and understand this Data Loss Prevention Policy and agree to comply with all its provisions.

```

**Name: _**

**Title: _**

**Date: _**

**Signature: _**

```

10. Document Control

Version: 2.0

Approved By: Information Security Committee

Approval Date: January 10, 2024

Next Review Date: January 10, 2025

End of Document