Statement of Work – DataWatcher

This Statement of Work (this "**SOW**") is made by and between Cyera US, Inc. ("**Cyera**") and the undersigned customer ("**Customer**") as of the last signature date (the "**SOW Effective Date**"). This SOW applies to Customer's use of Cyera's DataWatcher product ("**DataWatcher**"). DataWatcher shall be deemed part of the Platform. This SOW forms part of, and hereby incorporates by reference, the Master SaaS Agreement between the parties (the "**Agreement**"). All capitalized terms not defined in this SOW shall have the meanings given to them in the Agreement. In consideration of the mutual covenants and agreements contained herein and in the Agreement, and for other good and valuable consideration, including as stated in this SOW, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. DATAWATCHER PRODUCT AND SCOPE

1.1. DataWatcher offers end-to-end management of the Cyera Data Security Platform ("**DSPM / Omni DLP**"), including data security monitoring, risk analysis, and expert-led response support designed to resolve threats to Customer's critical data in hours, not days.

1.2. Core Activities:

- Program Strategy and Enablement (optional)
  - Annual program maturity mapping and quarterly roadmap updates
  - Quarterly CISO team briefings / workshops focused on:
    - Program build and management practices
    - Technology optimization
    - Other topics as agreed upon by Customer and Cyera
- Premium Support
  - 24 / 7 Support
  - Knowledge Base and Community Access
  - Standard and Customized Training
- Deployment and Platform Optimization
  - Platform activation and integration
  - Policy creation and tuning
  - Data owner identification and tagging
  - Platform hygiene and performance monitoring
  - Workflow creation and automation tuning
- Issues Management and Resolution
  - Ongoing review and escalation of high-risk issues and suggested remediation guidance
  - As mutually agreed upon, will assist with extended remediation support activities
    - Support ticket creation and submission
    - Data owner outreach and follow-up (resolution guidance and progress tracking)
- Breach Support
- 24/7 inbound support for Customer-initiated incident response efforts (4-hour response window)
- Detailed blast radius and materiality analysis
- Leading remediation practices and post-breach support

2. GENERAL ASSUMPTIONS

The following assumptions apply to the delivery of services described in this SOW ("**Services**"):

- Customer will provide timely access to relevant personnel, systems, infrastructure, documentation, and environments required for the performance of the Services.
- Customer will maintain responsible for internal communication, change management, and executive sponsorship as it relates to cybersecurity policy implementation and cultural alignment.
- Services are provided in accordance with the scope and specifications defined in this SOW or applicable service descriptions.
- Customer has valid licenses and maintenance agreements for all third-party systems, software, or tools to which Services are applied.
- Customer will promptly notify Cyera of any material changes to its IT environment that could impact the Services (e.g., system migrations, architecture changes, vendor changes).
- Cyera's obligations hereunder are expressly conditioned upon (a) the Customer's timely cooperation, and (b) Cyera being provided with the necessary access, information, and assistance reasonably required to perform the Services.

3. SERVICE LIMITATIONS AND EXCEPTIONS

- Cyera shall not be liable for Security Incidents or other breaches or losses resulting from:
    - Customer's negligence, misconfiguration, or failure to act on Cyera-provided recommendations.
    - Third-party software vulnerabilities or supply chain attacks not reasonably preventable by Cyera.
    - Unauthorized changes made to systems or environments without prior notice to Cyera.
    - Use of unsupported hardware or software environments unless explicitly agreed upon in writing.
- The Services do not include:
    - Legal or regulatory interpretation or representation.
    - Data recovery or forensics beyond agreed services.
    - Physical security services or physical incident management.
    - Business continuity or disaster recovery planning, unless explicitly included in this SOW.

4. SERVICE LEVEL DISCLAIMER

While Cyera will make commercially reasonable efforts to meet the service level commitments described in this SOW, 100% availability or prevention of all threats cannot be guaranteed. Occasional deviations due to factors beyond reasonable control (e.g., force majeure, upstream provider outages) do not constitute a breach of this SOW.

5. SHARED RESPONSIBILITY

The parties acknowledge that cybersecurity is a shared responsibility. Cyera's obligations are limited to the scope of Services explicitly described herein, and the Customer remains responsible for:

- Compliance with applicable laws and regulatory frameworks (e.g., GDPR, HIPAA, PCI-DSS).
- User access controls, endpoint protection (unless managed), physical device security and other cybersecurity and data controls.
- Provisioning appropriate access rights based on role (e.g., read-only, analyst, admin).
    - Cyera access will be time-bound and monitored per Customer's policy.
- Acting upon recommendations provided by Cyera.
    - Cyera may assist in drafting the change plan but may not implement changes unless mutually agreed to by the parties.
- Cyera will not perform the following without explicit written approval and adherence to a jointly defined change control process:
    - Delete or modify Customer data in production
    - Modify, remove, or disable any existing security policy or control
    - Execute destructive queries, platform resets, or bulk data actions
    - Make changes to Customer systems or environments not directly related to the Cyera platform
    - Act outside the agreed scope or permissions defined during onboarding
- All changes proposed by either party must follow a mutually agreed upon Change Management Procedure, which includes:
    - Defined approval workflow with named Customer stakeholders
    - Documentation of proposed changes, impact, and rollback plans
    - Minimum of one (1) business day's notice for any non-emergency platform changes
    - Written sign-off for changes that affect data classification policies, integrations, or visibility scope

Cyera will ensure all personnel assigned to perform Services hereunder have undergone background checks and have signed binding confidentiality and security agreements.

6. INDEMNIFICATION

In addition to the indemnification obligations in the Agreement, Customer agrees to indemnify and hold harmless Cyera from and against any claims, damages, or liabilities arising from (a) Client's misuse or misapplication of the Services or DataWatcher; (b) noncompliance with regulatory obligations outside the control of Cyera; and (c) data losses or breaches resulting from systems not under Cyera's management.

7. CHANGE MANAGEMENT

All changes to the scope of services must be documented and agreed upon in writing through a change order or

revised SOW. Unauthorized changes initiated by Customer may void the warranties set forth in this SOW.

8. **INCLUDED SERVICES**

The Services specifically include the following**:**

- Ongoing alerting of high-risk issues and suggested remediation guidance
- Ongoing 24x7 breach support
- Ongoing summaries of suggested and applied configuration changes
- Weekly issue reports focusing on key use cases and related remediation practices
- Monthly remediation progress tracking reports
- Monthly platform health/hygiene reports
- Quarterly program roadmap review
- Quarterly issue trending reports
- Quarterly dark web scanning
- Quarterly briefing/workshop
- Annual program maturity mapping

9. Pre-existing and Related Security Incidents. This SOW does not extend to Pre-existing Incidents or Related Security Incidents that include a Pre-existing Incident.

10. Notification. If Customer discovers during the Warranty Period a Security Incident that occurred during such Warranty Period, Customer shall notify Cyera of such Security Incident by sending an email to GRC@cyera.io no later than three (3) days after Customer discovers such Security Incident.

The undersigned parties have executed this SOW as of the SOW Effective Date.

Cyera US, Inc.	**Customer**
By:	By:
Name:	Name:
Title:	Title:
Date:	Date: