Secure Endpoint Management (SEM)
Solution Description

The following is included as part of the Secure Endpoint Management (SEM) Cyvatar Cybersecurity Solution, which shall be delivered in accordance with and subject to the terms of this Solution Description and the terms and conditions of the Agreement:

- Ransomware Protection
- Endpoint Detection & Response (EDR)
- Managed Detection & Response (MDR)
- 24/7 Security Operations Center (SOC) Monitoring

1. Member Delivery.

1.1. Security Engineer. As part of the Secure Endpoint Management (SEM) Solution, the Client will get access to a Cyvatar "Security Engineer" who will oversee the delivery of the solution.

1.2. Security Engineer Schedule & Tasks. The Security Engineer shall create a mutually agreed upon schedule to facilitate the delivery of the events/tasks set forth below. Notwithstanding the foregoing, all timelines, deliverables, and implementation efforts outlined in any mutually agreed schedule are estimates only.

1.2.1. Installation and Configuration of Third Party Product(s). Cyvatar shall oversee the installation and configuration of the relevant Third Party Product(s) which are approved by Client for installation into Client's environment. The potential list of Third Party Product(s) which may be relevant to the delivery of the Solution is listed in Section 4 below. The actual Third Party Product(s) installed/configured shall be approved by Client.

1.2.2. Assessment. Cyvatar shall continuously assess the risks associated with the relevant Third Party Product(s) available and shall also assess gaps based on security best practices. Gaps identified shall be documented with recommendations for remediation.

1.2.3. Remediation. Cyvatar shall continuously review gaps identified

through the assessment and shall work with Client to develop a remediation plan and schedule. Cyvatar shall lead the remediation until identified gaps are remediated, to the extent reasonably possible and approved by Client. Remediation work shall only be conducted after Client has agreed to recommended actions.

1.2.4. **Maintenance of Remediated Status.** Once all identified gaps are remediated through the remediation plan, to the extent reasonably possible and approved by Client, Cyvatar shall assist in maintaining that remediated status throughout the Subscription Term. Any remediation work shall only be conducted after Client has agreed to recommended actions.

1.2.5. **Monthly Executive Reporting.** Cyvatar shall deliver monthly reporting; the specific parameters reported shall be as mutually agreed.

2. **Client Obligations.** Client understands and agrees that in order for Cyvatar to provide the Secure Endpoint Management (SEM) Cyvatar Cybersecurity Solution, including relevant Professional Services, Cyvatar will need access to certain Client resources, personnel, and systems. As such, Client agrees to the following:

2.1. Client shall identify an internal point of contact for this engagement.

2.2. Client shall provide relevant information on proposed applications and computing systems, users and data.

2.3. Client is responsible for the initial installation of the Third Party Product(s) with the remote targeted assistance of Cyvatar.

2.4. Client is responsible for network, host, or cloud availability at all times; lack of network, host, or cloud readiness may result in lack of productivity and ability to provide Secure Endpoint Management (SEM) Cyvatar Cybersecurity Solution.

2.5. Client shall provide Cyvatar with necessary documentation, as needed.

2.6. Client will schedule any interviews with the appropriate individuals, as requested by Cyvatar.

3. **Included Third Party Product Licenses.** The Secure Endpoint Management (SEM) Cyvatar Cybersecurity Solution shall include reselling of licenses to certain of the following Third Party Products listed below. The specific Third Party Product(s) to be licensed, resold and installed shall be determined by the number and type of assets monitored and/or managed as part of the solution, technical requirements, and recommendations of Cyvatar after discussions with Client. The final list of Third Party Product(s) shall be approved by the Client after Cyvatar recommendation. The Third Party Terms that are relevant to the Third Party Products are listed below. Client agrees that as part of approving the Third Party Product for installation, it agrees that it has reviewed and is approving the Third Party Terms relevant to the use of the Third Party Product.

Third Party Product (Resale)	Third-Party Terms
SentinelOne's Singularity Complete	https://www.sentinelone.com/legal/terms-of-service/
Critical Start's Security Operations Center (CYBERSOC) ZTAP Services	https://www.criticalstart.com/drupal/sites/default/files/2025-06/Critical-Start-Terms-of-Service_11-21-2024_v1.12_clickthru.pdf
Rapid7 Managed Detection and Response (MDR)	https://www.rapid7.com/legal/eula/ https://rapid7.com/legal/terms
CyFlare Managed Detection and Response (MDR)	https://cyflare.com/wp-content/uploads/CyFlare-Solution-Terms-REV09_0125.pdf

4. **Exclusions**.
   - **4.1.** None of the above shall be performed onsite by Cyvatar.
   - **4.2.** None of the above shall include Cyvatar acting as an incident response team.
   - **4.3.** Notwithstanding anything to the contrary in this Agreement, Cyvatar shall not be required to provide end user access to the Third Party Product or

any component of the Solutions to the Client.

Attachment 1:
SentinelOne Managed Services - Flow Down Terms

Member (**"Client")** and Cyvatar ("**MSSP**") have entered an agreement ("**Solution Terms**") where MSSP is providing managed security services for the Client ("**Services**"). This Managed Services – Flow Down Terms, ("**Attachment**") shall be made part of the Solution Terms between MSSP and Client, and where this Attachment and Solution Terms conflict, this Attachment shall control. MSSP has licensed SentinelOne's platform including its malware protection, detection and remediation solutions, endpoint detection and response solutions, device discovery and control solutions, and other solutions and enhancements thereto offered by SentinelOne over time, ("**Solutions**") from SentinelOne, Inc. and is using the Solutions in its provision of Services.

1. **All Claims between MSSP and Client.** Client agrees that it will bring all claims under this Agreement as well as any claims arising out of its related use of Solution against MSSP and will not make any claim directly against SentinelOne. Client agrees that SentinelOne has no obligation or liability to Client under this agreement.
2. **Solution Use.** Client may only use Solutions for its internal business security and operations, in accordance with the Documentation in conjunction with the Services.
3. **Restrictions on Use.** Client may not do any of the following: (i) modify, disclose, alter, translate or create derivative works of the Solutions (or any components thereof) or any accompanying Documentation; (ii) license, sublicense, resell, distribute, lease, rent, lend, transfer, assign or otherwise dispose of the Solutions (or any components thereof) or any Documentation; (iii) use the Solutions for commercial or business uses not contemplated in Services such as offering Solutions to the benefit of other third-parties, Solution may only be used as directly related to Client's internal business operations and in conformity with the Documentation; (iv) use the Solutions in violation of any laws or regulations, including, without limitation, to store or transmit infringing, libelous or otherwise unlawful or tortious material, or

material in violation of third-party privacy rights; (v) use the Solutions to store, transmit or test for any viruses, software routines or other code designed to permit unauthorized access, disable, erase or otherwise harm software, hardware or data, or to perform any other harmful actions; (vi) probe, scan or test the efficacy or vulnerability of the Solutions, or take any action in an effort to circumvent or undermine the Solutions, except for the legitimate testing of the Solutions in coordination with MSSP and SentinelOne, in connection with considering a subscription to the Solutions as licensed herein; (vii) attempt or actually disassemble, decompile or reverse engineer, copy, frame or mirror any part or content of the Solutions, or otherwise derive any of the Solutions' source code; (viii) access, test, and/or use the Solutions in any way to build a competitive product or service, or copy any features or functions of the Solutions; (ix) interfere with or disrupt the integrity or performance of the Solutions; (x) attempt to gain unauthorized access to the Solutions or their related systems or networks; (xi) disclose to any third party or publish in any media any performance information or analysis relating to the Solutions; (xii) fail to maintain all copyright, trademark and proprietary notices on the Solutions and any permitted copy thereof; or (xiii) cause or permit any Solutions user or third party to do any of the foregoing.