SERVICE LEVEL AGREEMENT

Exhibit A to the Master Subscription Agreement

Version 1.3

H&A Security Solutions, LLC d/b/a Tellaro — 12178 N 1450th Street, Effingham, Illinois 62401

SERVICE LEVEL AGREEMENT

This Service Level Agreement (this "SLA") is Exhibit A to the Master Subscription Agreement between H&A Security Solutions, LLC d/b/a Tellaro ("Tellaro") and Customer (the "Agreement"). This SLA defines the service-level commitments applicable to the Tellaro Security Operations Platform (the "Platform SLA") and to the MSOC services included in the Managed Plans (the "MSOC Response SLA"). The MSOC Response SLA applies only when a Managed Plan is identified on an applicable Order Form.

1. DEFINITIONS

"Availability" means for a given calendar month, the percentage of total minutes during which the Platform is materially available for use by Authorized Users, measured by Tellaro monitoring.

"Excluded Time" means any period during which the Platform is unavailable due to (i) Scheduled Maintenance, (ii) Emergency Maintenance, (iii) a Force Majeure event, (iv) Customer-caused issues (including misuse, network or system failures on Customer's side, or breach of the Agreement), (v) issues with third-party services or networks not under Tellaro's control, (vi) suspension of the Service in accordance with the Agreement, or (vii) for Hybrid deployments, unavailability of the Customer-Hosted Components or Search Proxy.

"Incident" means (a) a security alert generated by the Service, or a suspected security event reported by Customer, that Tellaro classifies under Section 3.1, or (b) an event reported by Customer that causes, or is likely to cause, an interruption or material reduction in the quality of the Service.

"Scheduled Maintenance" means planned maintenance, upgrade, or change windows announced by Tellaro at least forty-eight (48) hours in advance.

"Emergency Maintenance" means unscheduled maintenance Tellaro reasonably determines is necessary to address an imminent risk to security, integrity, or availability of the Platform.

"Service Credit" means a non-cash credit applied to a future Tellaro invoice as Customer's exclusive remedy for failure to meet the Platform SLA, calculated as a percentage of the affected month's base subscription fee, meaning the monthly fee (or one-twelfth of the annual fee) for the Plan, excluding Add-Ons, standalone services, SentinelOne licensing, Premium Maintenance and Support, and one-time fees. Service Credits are not redeemable for cash and are not refundable.

2. PLATFORM SLA (TELLARO-HOSTED SERVICE ONLY)

2.1 Availability Target.

Tellaro will use commercially reasonable efforts to provide Platform Availability of 99.9% per calendar month, measured excluding Excluded Time.

2.2 Service Credits.

If Tellaro fails to meet the Availability target in a calendar month, Customer may request a Service Credit calculated as follows:

Monthly Availability	Service Credit (% of monthly base subscription fee)
≥ 99.9%	0%
< 99.9% and ≥ 99.0%	5%
< 99.0% and ≥ 95.0%	10%
< 95.0%	25%

2.3 Credit Request Process.

To receive a Service Credit, Customer must submit a written request to support@tellaro.io within thirty (30) days following the end of the affected month, identifying the dates and duration of unavailability. Tellaro will validate the request against its monitoring records and, if approved, apply the Service Credit to Customer's next Tellaro invoice as a reduction of future fees due. Customer is not eligible for Service Credits for any month in which Customer has undisputed amounts more than thirty (30) days past due.

2.4 Maximum Credits and Form of Remedy.

Service Credits in any single calendar month will not exceed twenty-five percent (25%) of that month's base subscription fee. Service Credits are Customer's sole and exclusive remedy for any failure of Availability and are payable solely as a non-cash credit against future Tellaro invoices. Service Credits are not redeemable for cash, will not be refunded if Customer departs the Service before applying them, and will not be paid out on termination or non-renewal of the Subscription Term.

2.5 Exclusions.

The Platform SLA does not apply to: (a) on-prem deployments where Customer hosts the software (see Section 4); (b) Excluded Time; or (c) any portion of the Service delivered through third-party Add-Ons (e.g., SentinelOne licensing), which are governed by their own service levels.

3. MANAGED PLAN RESPONSE SLA

This Section 3 applies to the Managed Plans (Identity, Protect, Defend, and Command).

3.1 Severity Definitions.

Tellaro classifies Incidents, in its reasonable judgment at triage, according to the following severity levels:

Severity	Description
Critical	Active, confirmed compromise; widespread outage of detection capability; or imminent risk to Customer environment requiring immediate response.
High	Suspected compromise or significant detection issue affecting multiple assets or critical assets; partial loss of detection coverage.
Medium	Single-asset issue, suspicious but unconfirmed activity, or non-urgent platform issue.
Low	Question, request for tuning, or informational item with no impact to detection.

3.2 Response Targets — Standard Hours.

Standard Hours are 8:00 AM to 5:00 PM Central Time, Monday through Friday, excluding Tellaro-observed U.S. holidays.

Severity	Active Triage (start of work)	Triage Complete (initial assertion delivered)
Critical	30 minutes	4 hours
High	1 hour	8 hours
Medium	2 hours	24 hours
Low	4 hours	72 hours

3.3 Response Targets — After Hours.

After Hours means any time outside Standard Hours. Critical and High Incidents are covered 24/7. Medium and Low Incidents reported After Hours are reviewed the next business day.

Severity	Active Triage (After Hours)	Triage Complete (After Hours)
Critical	30 minutes	4 hours
High	1 hour	8 hours
Medium	Reviewed next business day	Per Standard Hours table once reviewed
Low	Reviewed next business day	Per Standard Hours table once reviewed

3.4 Reporting an Incident.

Customer may report an Incident through any of the following:

- Email: support@tellaro.io
- Support portal: https://tellaro.zendesk.com

3.5 Customer Cooperation.

For alerts generated by the Service, response targets are measured from the time the alert is generated. For Incidents reported by Customer, they are measured from the time Tellaro receives the report with sufficient information to begin triage. Targets are paused while Tellaro is reasonably waiting on Customer for information, access, or

decisions, and do not apply during (a) a widespread event, such as a mass-exploitation campaign, affecting multiple Tellaro customers simultaneously, or (b) any period in which alert volume for Customer exceeds three times (3x) Customer's trailing thirty-day daily average, provided that Tellaro prioritizes Critical and High Incidents during such periods.

3.6 No Service Credits for MSOC.

The MSOC Response SLA establishes target response times. Response targets are not subject to monetary Service Credits; failure to meet a target is escalated through Tellaro's standard incident-management process, If Tellaro fails to meet the Active Triage target for more than thirty percent (30%) of Critical Incidents in each of three (3) consecutive calendar months (with at least three (3) Critical Incidents in each such month), Customer may, as its sole and exclusive remedy for failure to meet response targets, terminate the affected Order Form by written notice within thirty (30) days after the end of the third month and receive a refund of prepaid fees for the remainder of the Subscription Term.

3.7 Pre-Authorized Containment.

Where Customer has pre-authorized containment actions in the escalation and containment procedure agreed during onboarding (such as disabling an account, revoking sessions, or network-containing a host) and has granted Tellaro the access those actions require, Tellaro will use commercially reasonable efforts to take those actions within fifteen (15) minutes after Tellaro confirms the threat (as recorded in Tellaro's case management system) and will notify Customer alongside them. MSA Section 3.5 (Authorization for Scanning and Response Actions) applies to all such actions. Section 3.6 applies to this target.

4. ON-PREM DEPLOYMENTS

Where Customer hosts the software in its own environment (on-prem) under the End User License Agreement — On-Prem (rather than the SaaS Master Subscription Agreement), the Platform SLA in Section 2 does not apply, because Tellaro does not control the hosting infrastructure. Managed Plans are not available for self-hosted deployments, and the MSOC Response SLA in Section 3 does not apply to them. For Hybrid deployments, the Hybrid Deployment Exhibit (Exhibit H) governs the scope of this SLA.

5. REVIEW AND AMENDMENT

The parties will review this SLA annually and may amend it by mutual written agreement. Tellaro may also update this SLA from time to time on at least thirty (30) days' prior written notice; if any update materially diminishes Customer's rights, Customer may, as its sole remedy, terminate the affected Order Form for cause without penalty by giving notice within thirty (30) days after the update takes effect.