REMOTE ACCESS ADDENDUM

Exhibit R to the End User License Agreement — On-Prem

Version 1.3

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

REMOTE ACCESS ADDENDUM

This Remote Access Addendum (this "RAA") is Exhibit R to the End User License Agreement — On-Prem and to the Master Subscription Agreement (each, as applicable, the "Agreement") between H&A Security Solutions, LLC d/b/a Tellaro ("Tellaro") and Customer. This RAA applies when Customer purchases a service that requires Tellaro personnel to access hosts in Customer's environment (the "Customer Environment"): Premium Maintenance and Support for a self-hosted or Hybrid deployment, and Managed Vulnerability Scanning (each, a "Covered Service"). It does not apply to monitoring through the Tellaro search proxy, which requires no remote access. Capitalized terms not defined here have the meanings given in the Agreement. In the event of conflict between this RAA and the Agreement with respect to remote access, this RAA controls.

1. ACCESS METHOD — ZERO-TRUST TUNNEL

1.1 Architecture.

Tellaro accesses the Customer Environment through a zero-trust access connector that Tellaro installs on designated hosts, such as the hosts running the Software and the Tellaro-managed vulnerability scanner. The connector initiates an encrypted, outbound connection to Tellaro's zero-trust access service. Authorized Tellaro Personnel authenticate to that service with multi-factor authentication and receive access, including secure remote shell, only to the designated hosts. Customer is not required to provide a VPN, a jump host, or inbound network ports. Direct access from the public internet to the Software is not used.

1.2 Customer Provisioning.

Customer will: (a) designate the hosts on which the connector is installed and permit the outbound connectivity it requires; (b) provide a network path from those hosts to the in-scope systems reasonably needed to deliver the Covered Services; (c) for Managed Vulnerability Scanning, permit Tellaro to install scanning agents on in-scope devices and provide a segmented network (VLAN) path between those devices and the scanner; and (d) provide DNS, time synchronization, and other supporting infrastructure necessary for reliable connectivity.

1.3 Tellaro Provisioning.

Tellaro will provide Customer with: (a) the network destinations to which the connector and Tellaro agents connect; (b) a list of named Tellaro personnel authorized for access

(the “Authorized Tellaro Personnel”); (c) a security controls overview; and (d) a single point of contact for access management questions.

1.4 Automatic Updates.

The Tellaro agent and Tellaro’s outbound support tools retrieve their own updates by connecting out to Tellaro’s environment. No interactive access is required for those updates. Customer consents to these automatic updates. Tellaro maintains secure software-development and code-signing practices for updates, and updates are otherwise subject to the warranty disclaimers and limitations of liability in the Agreement.

2. CREDENTIALS AND IDENTITY

2.1 Identities.

Authorized Tellaro Personnel access the Customer Environment using named, individual identities managed in Tellaro’s identity provider with multi-factor authentication. Shared accounts are not permitted. Where a Covered Service requires a local account on a Customer host, Customer may issue it as a named account, and Tellaro will use it only through the zero-trust tunnel.

2.2 Account Lifecycle.

Tellaro will remove access for any Authorized Tellaro Personnel who departs Tellaro or no longer requires access within one (1) business day and will notify Customer of any local account Customer should disable. Tellaro will provide an updated Authorized Tellaro Personnel list at least quarterly and on Customer’s request.

2.3 No Persistent Access for Software Hosts.

Except as reasonably required to perform Premium Maintenance and Support on Platform Servers, Tellaro personnel do not maintain persistent administrative credentials on Software hosts in the Customer Environment. Where elevated access is needed (e.g., for support troubleshooting), it is granted on a just-in-time basis, logged, and revoked when the activity is complete.

3. PERMITTED ACTIVITIES

3.1 Scope.

Authorized Tellaro Personnel may, solely as necessary to deliver the Covered Services:

- review alerts, dashboards, and case data in the Software;

- access logs and configuration of the Software for support and troubleshooting;
- operate, scan policy, and report on the Tellaro VMS scanner (where Tellaro VMS is purchased);
- apply Updates and patches to the Software, and maintain the operating systems of, and diagnose hardware issues on, the hosts on which it runs (where Premium Maintenance and Support is purchased);
- perform tuning and detection-content adjustments at Customer's direction; and
- export reports and data necessary for the activities listed above.

3.2 Prohibited Activities.

Authorized Tellaro Personnel will not:

- (a) lateral-move to systems outside the scope of the Covered Services;
- (b) access, copy, or exfiltrate Customer Data outside the Customer Environment except as expressly necessary to deliver the Covered Services (and then only to systems and processes covered by Tellaro's security program);
- (c) make changes to Customer-side systems outside of the Software (other than the operating systems of Platform Servers under Premium Maintenance and Support) unless requested by Customer in writing;
- (d) install software not authorized by Tellaro or Customer;
- (e) bypass Customer security controls; or
- (f) use access granted under this RAA for any purpose other than performing the Covered Services.

4. LOGGING AND MONITORING

4.1 Customer-Side Logging.

Customer may log access to in-scope systems by Authorized Tellaro Personnel and may, on reasonable request, obtain Tellaro's session logs for the zero-trust tunnel.

4.2 Tellaro-Side Logging.

Tellaro will log all zero-trust tunnel sessions and all actions taken by Authorized Tellaro Personnel within the Software at a level sufficient to reconstruct activity, retain those logs in accordance with Tellaro's retention policy (no less than one year), and provide Customer with a summary of activity on reasonable request.

4.3 Anomaly Response.

If either party detects anomalous or unauthorized use of the access path, the detecting party will notify the other promptly, and Customer may suspend or revoke specific credentials pending investigation. Tellaro will cooperate reasonably in any investigation.

5. TELLARO SECURITY OBLIGATIONS

- Maintain a written information-security program aligned with industry standards (e.g., SOC 2, ISO 27001-aligned controls, or equivalent).
- Require Authorized Tellaro Personnel to complete background checks and annual security training.
- Use managed endpoints with full-disk encryption, EDR, and patching for any device used to access the Customer Environment.
- Require multi-factor authentication for Tellaro accounts used in connection with this RAA.
- Maintain incident-response procedures and notify Customer of any incident affecting the Customer Environment as provided in the Agreement.
- Provide Tellaro's SOC 2 Type II (or equivalent) report under confidentiality on Customer's reasonable request.

6. CUSTOMER OBLIGATIONS

- Permit the connector, agents, and network paths described in Section 1.
- Lifecycle-manage any local accounts issued to Authorized Tellaro Personnel per Section 2.
- Ensure that Tellaro's scope of access is consistent with what is necessary to deliver the Covered Services.
- Notify Tellaro of any changes to network paths, authentication systems, or host configurations that would affect Tellaro's access.
- Promptly suspend or revoke access on request from Tellaro or upon detection of anomalous activity.

7. DATA HANDLING DURING REMOTE ACCESS

Where Tellaro processes Customer Data outside the Customer Environment in the course of delivering the Covered Services (e.g., support diagnostics), such processing is

governed by the DPA (Exhibit C). Tellaro will minimize the data processed outside the Customer Environment to what is necessary for delivery and will return or delete such data per the DPA at the end of the Covered Service term.

8. SUSPENSION AND TERMINATION

8.1 Customer Right to Revoke.

Customer may suspend or revoke Tellaro's access at any time without notice if Customer reasonably believes Tellaro has engaged in a Prohibited Activity (Section 3.2) or is the subject of a security incident affecting Customer. Customer will notify Tellaro promptly and the parties will cooperate to resolve.

8.2 Effect on Covered Services.

Sustained suspension or revocation of access will impair Tellaro's ability to deliver the Covered Services. The parties will cooperate in good faith to remediate. If Customer's suspension or revocation is unrelated to Tellaro misconduct, Tellaro is excused from its obligations and response-time commitments for the affected Covered Services during the period of suspension or revocation, and fees continue to accrue.

8.3 Termination of RAA.

This RAA terminates upon expiration or termination of the Agreement, or upon termination of all Covered Services. On termination, Tellaro will cease access and remove the zero-trust connector, and Customer will disable any local accounts issued to Authorized Tellaro Personnel. Surviving Sections include 4.2, 7, 9, and any obligation that by its nature should survive.

9. LIABILITY

The limitation of liability provisions of the Agreement govern this RAA. For the avoidance of doubt, breaches of this RAA are subject to the same exclusions and caps as set forth in the Agreement.