ACCEPTABLE USE POLICY

Exhibit B to the Master Subscription Agreement

Version 1.3

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

ACCEPTABLE USE POLICY

This Acceptable Use Policy (this "AUP") is Exhibit B to the Master Subscription Agreement and the End User License Agreement — On-Prem and applies to all use of the Tellaro Security Operations Platform and Add-Ons (the "Service"). By accessing or using the Service, Customer and its Authorized Users agree to comply with this AUP. Tellaro may update this AUP from time to time on thirty (30) days' notice; updates that materially diminish Customer's rights follow the same notice rules as in the SLA. Capitalized terms have the meanings given in the Agreement.

1. PROHIBITED USES

Customer and its Authorized Users will not use the Service to:

- (a) violate any applicable law, regulation, or third-party right;
- (b) transmit, store, or process content that is unlawful, defamatory, infringing, harassing, or obscene;
- (c) generate, distribute, or store malicious code, viruses, worms, ransomware, or similar harmful materials except for legitimate, authorized security research and testing;
- (d) launch or facilitate denial-of-service, intrusion, or other unauthorized attack against any network or system, including networks or systems not owned or authorized by Customer;
- (e) probe, scan, or test the vulnerability of any Tellaro system or network, or breach Tellaro security or authentication measures, without prior written consent;
- (f) access the Service for benchmarking, competitive analysis, or to develop a competing product or service;
- (g) reverse engineer, decompile, or attempt to derive the source code, models, or detection rules of the Service, except to the extent permitted by law;
- (h) circumvent or attempt to circumvent any access controls, licensed Seat or Device limits, or rate limits;
- (i) share, resell, or sublicense access credentials or use the Service to provide a service to any third party (other than as an Authorized User of Customer, or by a managed service provider for its clients as expressly permitted under a Tellaro Partner Agreement);

- (j) submit data to the Service that Customer does not have the right to submit, or that exceeds the lawful scope of Customer's authority to monitor;
- (k) intentionally interfere with the integrity or performance of the Service or other Tellaro customers' use of it; or
- (l) use the Service in a manner that violates U.S. export control laws or sanctions, including providing the Service to embargoed persons or jurisdictions.

(m) scan, test, monitor, or take response actions against any system, network, account, or asset that Customer does not own or is not authorized to permit Tellaro to scan, test, monitor, or act upon; or

(n) monitor any individual in violation of applicable privacy, wiretap, education, or employment laws.

2. CUSTOMER SECURITY OBLIGATIONS

Customer is responsible for the security of its own systems and credentials. Customer will:

- maintain strong authentication for all Authorized Users, including multi-factor authentication where supported by the Service;
- promptly disable credentials of personnel who no longer require access;
- notify Tellaro promptly of any suspected compromise of Customer credentials or unauthorized use of the Service;
- ensure that data submitted to the Service from Customer assets is collected lawfully and in accordance with Customer's privacy and security policies; and
- comply with the Documentation regarding sensor deployment, configuration, and supported environments.

3. SEAT AND DEVICE COUNTS AND INGEST

Customer will accurately represent its Seat, Staff User, and Device counts on the Order Form and will promptly notify Tellaro if an actual count exceeds the corresponding Order Form count by more than ten percent (10%). Tellaro may review Device counts and ingest volumes through the Service's telemetry and may request reasonable records of Staff User counts. Counts above the Order Form are subject to true-up as set forth in the Agreement, billed from the next billing period and not retroactively.

4. SUSPENSION

Tellaro may suspend Customer's access to the Service or any Add-On, without notice if reasonably necessary to address an imminent security or legal risk and with reasonable prior notice in other cases, if:

- Customer materially breaches this AUP and does not cure within ten (10) days of written notice (or immediately, for breaches of Sections 1(a)–(d) or 1(j)–(l));
- Customer's use poses a security, integrity, or legal risk to Tellaro, the Service, or other customers;
- Tellaro is required to do so by law or valid legal process; or
- Customer's account is more than thirty (30) days delinquent on undisputed amounts and Customer has not paid within ten (10) days after written notice.

Tellaro will lift suspension once the underlying issue is resolved. Suspension does not relieve Customer of its obligation to pay fees due under the Agreement.

5. REPORTING ABUSE

To report a suspected violation of this AUP, contact security@tellaro.io. Tellaro will investigate reports in good faith and respond as appropriate.