PALANTIR USE CASE RESTRICTIONS

By using the Palantir Foundry Platform or Palantir's AI Platform ("AIP") (including any other technology made available by Palantir to Customer "Palantir Technology", which term if otherwise defined in the Agreement shall for purposes of these Palantir Use Case Restrictions have the definition provided in the Agreement), Customer agrees to abide by the following use case restrictions. Any capitalized terms not defined in these Use Case Restrictions will have the meaning provided to them in the Palantir Terms of Service, or any applicable agreement governing Customer's use of the Palantir Technology (the "Agreement").

In accordance with the Agreement, you and the Customer you represent (including such Customer's users) will not use the Palantir Technology for any Prohibited Use Case. Customer must obtain Palantir's prior written approval to use or permit any of Customer's users to use the Palantir Technology for any Use Cases Requiring Pre-Approval.

Prohibited Use Cases:

- Political parties, committees, campaigns, or organizations workflows
- Offensive cyber workflows
- Predictive policing efforts
- Influencing union organizing efforts
- Facial recognition for surveillance workflows
- Predatory targeting workflows
- Clinical judgment or decision making, medical advice, diagnostic or therapeutic purposes, and/or as a medical device or accessory (as defined by the applicable law).

Use Cases Requiring Pre-Approval:

- Law enforcement workflows (including, but not limited to, investigative watchlists)
- Immigration enforcement, monitoring, or surveillance workflows
- Mobility collecting, monitoring, or tracking workflows
- Video analysis workflows (e.g., CCTV)
- Tobacco, controlled substances, or illicit drugs related workflows
- Gambling related workflows.
- Employee monitoring workflows

- Biometric identity verification workflows
- Social media data use