
CabletequeGov Compliance Addendum

This CabletequeGov Compliance Addendum (this "**Addendum**") is entered into by **Cableteque Corp.** ("**Cableteque**" or "**Licensor**") and _____ ("**Licensee**"), and is effective as of _____ (the "**Addendum Effective Date**").

Recitals. Licensee has subscribed to the Licensed Software under order or quote reference _____ and has accepted the Cableteque End User License Agreement Rev 4.01 (the "**EULA**"). Licensee's use may involve Controlled Unclassified Information (CUI), Covered Defense Information (CDI), or export-controlled technical data (ITAR). The Parties enter into this Addendum to govern that use.

Capitalized terms not defined here have the meanings given in the EULA.

1. Incorporation and Order of Precedence

- 1.1. This Addendum is incorporated into and forms part of the EULA.
- 1.2. In the event of any conflict or inconsistency between this Addendum and the EULA, the AI Feature Addendum, the AI & Data Policy, the Privacy Notice, the Security & Compliance Overview, or any other Cableteque policy or informational document, **this Addendum controls with respect to the subject matter it addresses.**
- 1.3. Except for updates to Schedule A made in accordance with Section 3.2, this Addendum controls any version of those documents published, presented, or accepted within the CabletequeGov application after the Addendum Effective Date. **No subsequent in-application acceptance by Licensee or its users, and no unilateral update by Cableteque, will supersede, amend, or diminish this Addendum.**
- 1.4. Except as expressly modified here, the EULA remains in full force and effect.

2. CabletequeGov Environment and Access Controls

- 2.1. **Provisioning.** Licensee's subscription is provisioned in CabletequeGov.
- 2.2. **Environments.** Cableteque operates two separate environments. The Commercial environment supports ordinary commercial workloads. CabletequeGov is designed to support CUI, CDI, ITAR, and approved export-controlled workloads under applicable customer terms. CabletequeGov is

hosted on AWS GovCloud (U.S.), with defined processing functions performed in U.S.-only regions of Azure Government and Google Cloud Assured Workloads. All CabletequeGov processing occurs within U.S. regions.

- 2.3. **Access to export-controlled data.** Access to unencrypted Licensee Data, including export-controlled technical data, and to the means of decryption, is restricted to U.S. persons or other persons authorized under applicable U.S. export-control law. Personnel without such authorization may perform infrastructure or platform-support activities only where technical and organizational controls prevent access to such data or to the means of decryption.
- 2.4. **Cloud inheritance limitation.** Cloud-provider certifications and authorizations apply only to the provider services and authorization boundaries identified in documented CabletequeGov system boundary and applicable provider authorization boundaries.
- 2.5. **No export-control determination by Cableteque.** Cableteque does not determine, and does not represent, whether any Licensee Data is ITAR-controlled, EAR-controlled, CUI, or CDI. Cableteque makes no representation that Licensee's use of the Licensed Software satisfies Licensee's obligations under applicable export-control law.
- 2.6. **2.6. Current Compliance Status and Licensee Determination.** CabletequeGov is listed on the FedRAMP Marketplace as Legacy FedRAMP Ready at the Class C (Moderate) level. Legacy FedRAMP Ready status does not, by itself, constitute FedRAMP Certification (formerly authorization) or completed FedRAMP Moderate Equivalency. Cableteque is actively undergoing an independent FedRAMP Moderate Equivalency assessment and will make available compliance evidence regarding the CabletequeGov environment as described in its Security & Compliance Overview.

Licensee is responsible for determining, based on its applicable contracts, regulatory obligations, assessment requirements, intended data, and risk posture, whether CabletequeGov is appropriate for Licensee's use. Licensee may elect to use CabletequeGov prior to completion of Cableteque's FedRAMP Moderate Equivalency assessment where such use is not prohibited by applicable law or a binding contractual requirement. Such election reflects Licensee's own compliance determination within the parties' shared-responsibility model and does not constitute a representation by Cableteque that Legacy FedRAMP Ready status satisfies any particular Licensee requirement.

Where applicable law or a binding contractual requirement expressly requires a FedRAMP Moderate authorized or FedRAMP Moderate equivalent cloud service,

Licensee remains responsible for determining that the applicable requirement has been satisfied before submitting data subject to that requirement. Cableteque will reasonably cooperate with Licensee and its assessors in evaluating CabletequeGov's current compliance posture.

3. AI Processing Boundary and Provider Change Notice

- 3.1. **Named providers.** AI processing for CabletequeGov is performed by the providers identified in **Schedule A**, each operating within U.S.-region environments. Schedule A states each provider's function and processing region as of the Addendum Effective Date.
- 3.2. **Change Notice and Schedule A Updates.** Cableteque may update Schedule A to reflect a material change to an AI provider, processing region, or authorization status, provided that Cableteque gives Licensee at least thirty (30) days' prior written notice of such change. Any update to Schedule A made in accordance with this Section 3.2 is an expressly permitted modification to Schedule A and does not constitute a unilateral amendment prohibited by Section 1.3. Routine model-version updates and infrastructure changes that do not materially affect security, processing geography, authorization posture, or the handling of Licensee Data do not require notice or an update to Schedule A.
- 3.3. **Exception.** Where a change is required by a security incident, service disruption, provider discontinuation, or legal requirement, Cableteque will provide notice as soon as reasonably practicable.

4. DFARS 252.204-7012(c)–(g) Support

- 4.1. Cableteque supports Licensee's obligations under **DFARS 252.204-7012(c)–(g)** as follows.
- 4.2. **Notification.**
 - A.** Cableteque will notify Licensee's designated point of contact as soon as reasonably practicable, and in no event later than forty-eight (48) hours after discovery of a cyber incident affecting Licensee Data that Cableteque reasonably believes may be reportable under DFARS 252.204-7012, using information aligned to the DoD Incident Collection Format.
 - B.** Cableteque will notify Licensee's designated point of contact when the FedRAMP Moderate Equivalency Body of Evidence is available and will make it accessible to Licensee, subject to an executed NDA and reasonable access controls.

-
- 4.3. **Media preservation.** Upon discovery of a cyber incident affecting Licensee Data that Cableteque reasonably believes may be reportable under DFARS 252.204-7012, Cableteque will promptly preserve and protect relevant system images, logs, monitoring data, and other evidence reasonably necessary to support investigation and reporting of the incident. Cableteque will retain such materials for at least ninety (90) days following the date Licensee notifies Cableteque that its applicable cyber-incident report was submitted to DoD, or for any longer period required by applicable law or requested by DoD through Licensee.
 - 4.4. **Malicious software.** Cableteque will support submission of malicious software to the DoD Cyber Crime Center (DC3) at Licensee's direction, under documented chain of custody.
 - 4.5. **Forensic access.** Where DoD requests access in connection with an incident, Cableteque will cooperate through Licensee, subject to protection of other customers' data and third-party confidences.
 - 4.6. **Damage assessment.** Cableteque will provide evidence reasonably necessary to support Licensee's damage assessment.
 - 4.7. **Licensee obligations. Reporting to DoD, including DIBNet submission and maintenance of a DoD medium-assurance certificate, remains Licensee's obligation as the contractor.** Cableteque's role is support, not substitution.
 - 4.8. **Designated point of contacts.** Licensee will designate a primary notification contact upon execution of this Agreement. Licensee remains responsible for maintaining current contact information with Cableteque.

5. Data Classification, Retention and Deletion

- 5.1. **Classification.** All Licensee Data is treated as confidential and proprietary by default, regardless of labeling. Licensee remains responsible for determining whether its data is subject to CUI, CDI, ITAR, EAR or other regulatory restrictions, for identifying such data before submission, and for ensuring that its users are appropriately authorized.
- 5.2. **Encryption.** Licensee Data is encrypted in transit using TLS 1.2 or higher, or other approved cryptographic protocols appropriate to the applicable service, and at rest using cloud-native key-management services governed by Cableteque-controlled access policies. CabletequeGov uses cryptographic modules validated to FIPS 140-3 and listed in the NIST Cryptographic Module Validation Program.

- 5.3. **Privileged access.** Routine direct administrative access to production Licensee Data is disabled. Time-bound, least-privilege access may be granted to authorized personnel consistent with the personnel and access restrictions in Section 2.3 for approved support, security, legal, or incident-response purposes, and such access is logged and reviewed.
- 5.4. **Retention and Deletion.** Licensee Data processed in CabletequeGov is subject to the retention, retrieval, and deletion provisions set forth in Section 14 of the EULA and Cableteque's applicable Privacy Notice. Notwithstanding those provisions, for the period required or reasonably necessary, Cableteque may retain Licensee Data, system images, logs, monitoring data, or related records reasonably necessary to comply with applicable law, legal hold requirements, security and audit obligations, or the incident-preservation requirements of Section 4 of this Addendum. Any such retained data will remain subject to the security, confidentiality, access-control, and data-residency protections applicable to CabletequeGov and will be deleted in accordance with applicable retention schedules once the applicable preservation requirement has expired.

6. General

- 6.1. **Risk allocation.** Except as expressly modified by this Addendum, all warranty disclaimers, limitations of liability, exclusions of damages, remedies and other risk allocations in the EULA apply to this Addendum. **Nothing in this Addendum creates a separate or additional liability cap, indemnification obligation, or remedy.**
- 6.2. **Governing law.** This Addendum is governed by the same governing law and dispute-resolution provisions as the EULA.
- 6.3. **Counterparts and signature.** This Addendum may be executed in counterparts and by electronic signature.

Schedule A - Third-Party AI Infrastructure Providers

Provider	Function	Environment / Region
Google Vertex AI	Generative extraction and inference	Google Cloud Assured Workloads, U.S. regions
Microsoft Azure Document Intelligence	Optical character recognition	Azure Government, U.S. regions

Provider	Function	Environment / Region
AWS Bedrock	Generative extraction and inference	AWS GovCloud, U.S. regions

Signature

Cableteque Corp.	LICENSEE:
By: _____	By: _____
Name:	Name:
Title:	Title:
Date:	Date: