CONTROLLED DATA ADDENDUM

This Addendum supplements the Vendor NDA between Company and Vendor.

1. Applicability

This Addendum applies only if Vendor receives or accesses Controlled Data, including:

1.1 Controlled Unclassified Information (CUI).
1.2 Export-controlled data.
1.3 Customer-restricted technical data.

2. Regulatory Compliance

Vendor agrees to comply with applicable requirements of DFARS 252.204-7012, including safeguarding Covered Defense Information and reporting cyber incidents.

2.1 ITAR.
2.2 CMMC Level 2.

3. Minimum Security Requirements

Vendor shall:

3.1 Implement security controls consistent with NIST SP 800-171.
3.2 Restrict access to authorized users only.
3.3 Use secure systems and environments for storage and processing.
3.4 Enforce access controls to ensure only authorized users can access Controlled Data.
3.5 Process Controlled Data only within defined and secured system boundaries.

4. Incident Reporting

Vendor must:

4.1 Report any actual or suspected incident within 72 hours.
4.2 Provide relevant details for investigation.
4.3 Cooperate fully with response actions.
4.4 Vendor shall notify Company immediately upon discovery of an incident and in no case later than 72 hours.

5. Data Location & Storage

Vendor shall:

5.1 Store Controlled Data only in approved environments.
5.2 Not transfer data outside the United States without written approval.

6. Flow-Down Requirement

Vendor must ensure subcontractors:

6.1 Are bound by equivalent obligations.
6.2 Meet the same security requirements.

7. Audit Rights

Company may, upon reasonable notice, verify Vendor's compliance with this Addendum.

8. Survival

All obligations related to Controlled Data survive indefinitely.

9. Data Disposition

Vendor shall return or destroy Controlled Data upon request or termination and certify such destruction.