CODEVERTEX PROCUREMENT BUNDLE
Version: 2026.03

This bundle consolidates the core buyer-review documents used by procurement, legal, security, and leadership stakeholders.

Primary contact: contact@codevertex.io
Legal contact: legal@codevertex.io
Website: https://codevertex.io

=== CAPABILITY STATEMENT ===

CODEVERTEX ENTERPRISE CYBERSECURITY CAPABILITY STATEMENT
Version: 2026.02

Company Overview
CodeVertex Software Solutions is a multinational cybersecurity partner delivering enterprise offensive security, cloud exposure validation, red teaming, and remediation assurance programs for regulated and high-growth organizations.

Core Services
1) Web and API Penetration Testing
2) Cloud and Identity Attack-Path Validation
3) Red Team and Assumed-Breach Simulation
4) Continuous Security Validation Programs
5) Executive Cyber Advisory and Governance Reporting

Delivery Model
- NDA-first engagements
- Written authorization before testing
- Named points of contact and escalation matrix
- Executive and technical reporting cadence
- Retest-backed closure verification

Framework Alignment
- SOC 2
- ISO 27001
- PCI DSS
- HIPAA
- NIST CSF
- MITRE ATT&CK

Typical Deliverables
- Executive risk brief and board narrative
- Technical findings with exploit evidence
- Prioritized remediation plan with ownership mapping

- Retest confirmation and closure memo

Regions Served
USA, Spain, India, Ecuador, and global remote delivery.

Primary Contact
contact@codevertex.io
https://codevertex.io

=== SECURITY ASSURANCE BRIEF ===

CODEVERTEX SECURITY ASSURANCE BRIEF
Version: 2026.02

Security Governance Principles
- Authorization-first testing with documented scope boundaries.
- Least-privilege access to engagement artifacts.
- Controlled evidence handling and retention practices.
- Escalation protocol for critical and high-impact findings.
- Executive visibility through structured status communication.

Operational Controls
- Secure collaboration channels
- Confidentiality under NDA
- Evidence-backed reporting model
- Remediation accountability tracking
- Retest and closure validation workflow

Legal and Procurement Readiness
- MSA, NDA, DPA templates available
- Rules of engagement template available
- Security questionnaire package available
- Procurement and legal workflow documented

Enterprise Confidence Signals
- Response SLA: leadership reply within 24 hours
- Program outputs mapped to governance and audit use cases
- Cross-functional reporting for leadership and engineering teams

Contact
legal@codevertex.io
contact@codevertex.io

=== MSA SUMMARY ===

CodeVertex Master Services Agreement (MSA) Summary

This document outlines the commercial and legal structure used for enterprise cybersecurity engagements.

Key sections:
1) Services and scope governance
2) Commercial terms and invoicing model
3) Confidentiality and data handling obligations
4) Liability and limitation framework
5) Termination and post-engagement obligations

For contracting support, contact legal@codevertex.io.

=== MUTUAL NDA SUMMARY ===

CodeVertex Mutual NDA Summary

This document defines confidentiality obligations between CodeVertex and client stakeholders during pre-engagement and active delivery phases.

Core coverage:
1) Definition of confidential information
2) Permitted use and disclosure restrictions
3) Duration of obligations
4) Return or destruction of materials
5) Legal exceptions and required disclosures

For legal coordination, contact legal@codevertex.io.

=== DPA SUMMARY ===

CodeVertex Data Processing Addendum (DPA) Summary

This document defines data processing obligations for cybersecurity service delivery.

Core controls:
1) Roles of controller and processor
2) Processing purpose and data categories
3) Security controls and access governance
4) Incident notification protocol
5) Deletion and retention commitments

For data protection terms, contact legal@codevertex.io.

=== SECURITY QUESTIONNAIRE SUMMARY ===

CodeVertex Security Questionnaire Summary

This package provides standard responses for vendor security due diligence.

Coverage areas:
1) Security governance and policy framework
2) Access management and least-privilege model
3) Data handling and evidence protection controls
4) Vulnerability management and remediation validation
5) Incident response and escalation communications

For the latest questionnaire packet, contact contact@codevertex.io.

=== RULES OF ENGAGEMENT SUMMARY ===

CodeVertex Rules of Engagement Summary

This document defines testing boundaries and authorization requirements for all assessments.

Included controls:
1) Written authorization requirement
2) Scope boundaries and in-scope assets
3) Testing windows and communication channels
4) Critical finding escalation process
5) Evidence handling and closure validation

For engagement-specific terms, contact contact@codevertex.io.

=== BUYER REVIEW CHECKLIST ===

1) Review capability fit and scope coverage.
2) Confirm NDA/MSA/DPA review requirements.
3) Validate rules of engagement and authorization boundaries.
4) Align pricing band and engagement timeline.
5) Route final approvals to security, legal, and procurement stakeholders.