Customer CMMC Checklist

DETERMINE YOUR CMMC LEVEL

- ☐ Review DoD contract clauses.
  - Key words: DFARS 252.204-7012, -7019, -7020, -7021.
- ☐ Identify your required CMMC level.
  - Levels 1, 2, or 3 based on your contract and the type of data you handle (e.g., FCI or CUI).

CONDUCT A SELF-ASSESSMENT

- ☐ Use the DoD's Assessment Methodology to score your compliance.
  - Key words: NIST SP 800-171 (required for CMMC Level 2+).
- ☐ Submit your NIST SP 800-171 self-assessment score to the Supplier Performance Risk System (SPRS).

IDENTIFY & ADDRESS GAPS

- ☐ Conduct a gap analysis against CMMC practices and processes for your required level.
- ☐ Develop a Plan of Action & Milestones.
  - (POA&M) to remediate any deficiencies.

IMPLEMENT SECURITY CONTROLS

- ☐ Secure Controlled Unclassified Information (CUI) according to NIST SP 800-171 if applicable.
- ☐ Apply multi-factor authentication (MFA), encryption, and access controls.
- ☐ Implement security awareness training for employees.

ESTABLISH DOCUMENTATION & POLICIES.

- ☐ Develop and maintain security policies, procedures, and incident response plans.
- ☐ Ensure system security plans are documented and updated.

PREPARE FOR A CMMC ASSESSMENT (IF REQUIRED)

- ☐ Identify an authorized C3PAO for formal assessment.
  - Conduct a pre-assessment to validate readiness.

MAINTAIN COMPLIANCE & CONTINUOUS MONITORING

- ☐ Perform regular security assessments and update security measures.
- ☐ Monitor for threats and respond to security incidents promptly.