**Rules of Behavior -- CMMC Level 2 Environment**

These Rules of Behavior apply to all users accessing <COMPANY NAME> systems and data, including but not limited to those in Microsoft 365, Azure and Entra ID environments.

By signing or electronically accepting these rules, you acknowledge your responsibilities to protect Controlled Unclassified Information (CUI) and other sensitive data in accordance with CMMC Level 2 requirements.

**1. Privileged Users**

*(Administrators, Security Officers, or any user with elevated rights)*

When acting in this role, you must:

* Use elevated privileges **only** for authorized administrative tasks
* Always apply **Least Privilege and Separation of Duties** principles
* Only process authorized data required for official business
* Report all suspected or confirmed security incidents immediately via <COMPANY NAME>'s incident reporting process
* Follow approved change management and configuration management procedures
* Ensure only approved software, systems, and devices are used
* Keep privileged authentication credentials secure and never share them
* Maintain required security training and certifications
* Limit access to sensitive data strictly to job requirements
* Protect system resources from waste, loss, abuse, or unauthorized use
* Dispose of electronic and paper records in accordance with <COMPANY NAME> policy

**2. Non-Privileged Internal Users**

*(Standard organizational users)*

When acting in this role, you must:

* Use <COMPANY NAME> devices and systems only for approved business purposes
* Not install unapproved software or hardware
* Not bypass or alter system security settings
* Protect sensitive information from unauthorized disclosure
* Store and dispose of records according to <COMPANY NAME> policy
* Report suspected incidents, lost devices, or suspicious activity immediately
* Access only information required for your job duties

**3. Privileged External Users**

*(Vendors, contractors, or partners with administrative access)*

When acting in this role, you must:

* Access <COMPANY NAME> systems only for authorized purposes
* Limit actions to your assigned scope of work
* Keep authentication credentials secure and never share them
* Follow proper logon/logoff procedures; never leave sessions unattended
* Report incidents or suspected security issues immediately
* Not create unauthorized connections between systems or networks
* Safeguard all resources and always ensure CUI protection

**4. Non-Privileged External Users**

*(Vendors, contractors, or partners with standard access)*

When acting in this role, you must:

* Access <COMPANY NAME> systems only as instructed and for authorized purposes
* Not add or change software, hardware, or configurations
* Not circumvent security controls
* Follow <COMPANY NAME> data protection and wireless access policies
* Protect and properly dispose of all information and records according to <COMPANY NAME> policy

**5. Technology Usage Restrictions**

All users must additionally comply with the following technology restrictions:

**Artificial Intelligence and Machine Learning Tools**

* **Never upload, input, or process CUI or proprietary company information into public AI services** (including but not limited to ChatGPT, Claude, Bard, Copilot, or similar platforms)
* Use only company-approved AI tools that meet FedRAMP Moderate or equivalent security requirements
* Obtain prior written approval from the Information Security Officer before using new AI-powered applications or services
* Report any accidental disclosure of sensitive information to AI services immediately through the incident reporting process
* Understand that AI-generated content may require additional review and validation before use in official business

**File Sharing and Cloud Applications**

* Use only approved cloud services and file sharing platforms that meet <COMPANY NAME> security requirements
* Verify service security status and data handling agreements before uploading any business information
* **Never use personal cloud storage accounts** (personal Google Drive, Dropbox, OneDrive, etc.) for business data
* Only use government-approved secure file transfer services (such as SAFE.APPS.MIL) for CUI transmission to government clients
* Report unauthorized file sharing service usage or data spillage immediately

**Social Media and External Communications**

* Do not discuss company projects, capabilities, contract information, or sensitive business information on social media platforms
* Exercise extreme caution with professional networking platforms (LinkedIn, etc.) regarding work details and connections
* Do not post images of workspaces, documents, or screens that may contain sensitive information
* Report suspected social engineering, phishing attempts, or suspicious contact via social media immediately
* Understand that adversaries may use social media for intelligence gathering against defense contractors

**Software Installation and External Services**

* Install only approved software from authorized sources and software repositories
* Do not use unauthorized productivity tools, browser extensions, or software-as-a-service applications
* Obtain approval before subscribing to or using new online services for business purposes
* Do not use peer-to-peer file sharing applications or services
* Report malware, suspicious software behavior, or unapproved application usage immediately

**Portable Media and External Devices**

* Use only company-issued or approved portable storage devices
* Never use portable storage devices of unknown or unverified ownership
* Scan all external media for malware before use
* Follow proper media sanitization procedures when disposing of storage devices
* Report lost or potentially compromised portable media immediately

**Remote Work and Personal Devices**

* Use only approved remote access methods and company-managed VPN connections
* Do not process CUI on personal devices unless specifically authorized and configured
* Ensure home networks meet minimum security requirements when working remotely
* Use company-provided equipment for accessing sensitive systems whenever possible
* Report compromise of home network or personal devices used for business

**6. Insider Threat Awareness and Reporting**

All users must be aware of and report potential insider threat indicators, including:

**Behavioral Indicators Requiring Immediate Reporting**

* Attempts to access information beyond job requirements or authorized duties
* Unexplained interest in sensitive projects or information outside assigned responsibilities
* Unusual working hours or access patterns without business justification
* Attempts to bypass security controls or procedures
* Inappropriate questions about security measures, personnel, or system vulnerabilities
* Financial difficulties, unusual financial transactions, or lifestyle changes inconsistent with known income
* Expressions of strong dissatisfaction with company policies, management, or government contracts
* Unusual foreign contacts or travel, especially to countries of security concern
* Attempted or actual unauthorized disclosure of sensitive information

**Reporting Procedures**

* Report concerns immediately to your supervisor, Human Resources, or the Information Security Officer
* Use established incident reporting channels for security-related concerns
* Understand that reports will be handled confidentially and professionally
* Do not attempt to investigate suspected insider threats independently

**7. General Rules for All Users**

All users, regardless of role, must:

* Complete required security awareness training, CMMC-related training, and insider threat awareness training as assigned
* Attend annual refresher training and any additional training following significant security events
* Protect login credentials; never share passwords, tokens, or authentication devices
* Use strong, unique passwords and follow multi-factor authentication requirements
* Follow all applicable <COMPANY NAME> security, data handling, and acceptable use policies
* Immediately report lost devices, suspected phishing emails, malware infections, or unauthorized access attempts
* Never process classified national security information on <COMPANY NAME> systems
* Understand that <COMPANY NAME> systems may be monitored for security and compliance purposes
* Recognize that violations of these rules may result in disciplinary action, contract termination, and possible legal consequences
* Maintain situational awareness of current cybersecurity threats and attack methods
* Participate in security exercises and drills as required
* Report any conflicts between these rules and job requirements to management immediately

**8. Incident Response Requirements**

When security incidents occur, all users must:

* **Immediately** stop any activity that may be causing or contributing to the incident
* Preserve evidence by not altering, deleting, or moving files or data
* Report the incident through established channels within **1 hour** of discovery
* Provide full cooperation with incident response activities and investigations
* Follow instructions from incident response team members
* Maintain confidentiality regarding incident details except as authorized
* Document actions taken and observations made during the incident

**9. Data Classification and Handling**

All users must:

* Properly identify and mark CUI according to <COMPANY NAME> data classification procedures
* Handle different types of data (FCI, CUI, proprietary) according to their respective protection requirements
* Ensure CUI is only shared with authorized individuals who have appropriate clearances and need-to-know
* Use approved encryption methods for CUI in transit and at rest
* Follow proper data retention and destruction schedules
* Never mix personal and business data on the same systems or storage devices

**10. Compliance and Enforcement**

* These Rules of Behavior are mandatory for all users with system access
* Compliance will be monitored through technical controls, auditing, and periodic assessments
* Violations may result in immediate suspension of system access pending investigation
* Repeated or serious violations may result in termination of employment or contract
* <COMPANY NAME> reserves the right to update these rules as required by evolving threats, regulations, or business needs