ManTech.
Securing the Future

2022

Standards of **Ethics and Business Conduct**

Our Standards of Ethics and Business Conduct (Standards) are issued under the authority and approval of:

MANTECH'S BOARD OF DIRECTORS

- **George J. Pedersen**
  Chairman Emeritus, ManTech International Corporation
- **Kevin M. Phillips**
  Chairman of the Board, CEO and President, ManTech International Corporation
- **Richard L. Armitage**
  President, Armitage International; Former Deputy Secretary of State; Ambassador; and Former Assistant Secretary of Defense
- **Mary K. Bush**
  President, Bush International; Former Managing Director, Federal Housing Finance Board
- **Barry G. Campbell**
  Former Chairman and Chief Executive Officer, Allied Aerospace Industries, Inc.
- **Richard J. Kerr**
  Former Deputy Director and Officer, Central Intelligence Agency
- **Peter B. LaMontagne**
  Chief Executive Officer, Smartronix
- **Lieutenant General Kenneth A. Minihan**
  USAF (Ret.) – Managing Director of the Homeland Security Fund for Paladin Capital Group; Former Director, National Security Agency; Former Director, Defense Intelligence Agency

MESSAGE FROM MANTECH'S EXECUTIVE LEADERSHIP TEAM

Colleagues,

ManTech's success over the last five decades is a direct result of the high ethical standards, dedication and values you have consistently demonstrated while providing innovative technology and mission-focused solutions to our customers. The outstanding reputation ManTech enjoys today with customers, partners and competitors rests on a strong foundation: our determined commitment to doing business the right way — every day. The principles we live and work by at ManTech are set forth in our Standards of Ethics and Business Conduct. They provide the framework of our culture, which is based on uncompromising integrity and ethical behavior — key differentiators in today's intensely competitive marketplace.

As a ManTech employee, you play a central role in distinguishing our company as an ethical and trustworthy business partner and an innovative industry leader. No matter how the world around us may seem to change, ManTech's values for more than half a century remain grounded in truth, integrity and caring for each other and the mission. You play an important role in creating a work environment where each of us can thrive, and we ask you to help us do that by remembering to treat one another with fairness and respect.

Please read our Standards of Ethics and Business Conduct carefully and apply what you learn to ensure you are making ethical decisions that uphold ManTech's core values and business principles. All employees, officers and directors are expected to comply with the guidance and policies set forth in our Standards of Ethics and Business Conduct. If you have questions, please speak to your supervisor or any of the company resources identified in our Standards, including the ManTech Helpline.

We are proud of the contributions you make every day and how your work serves our customers, shareholders and this great nation. Thank you for your commitment to doing what's right by conducting yourself with uncompromising integrity and ethics.

Kevin M. Phillips *Judith L. Bjornaas* *Matthew Tait*

Kevin M. Phillips
Chairman, CEO and President

Judith L. Bjornaas
Executive Vice President and CFO

Matthew Tait
Chief Operating Officer

The Foundation of our Standards

Our Mission

Our mission is empowering our nation through a diverse and skilled workforce securely delivering innovative technology, consulting services and digital solutions for our customers' mission success, every day.

Our Vision

Our vision is *Securing the Future*® as the most trusted partner for U.S. Defense, Intelligence and Federal Civilian customers through the power of One ManTech. When these agencies think of an essential partner for their national and homeland security needs, they think ManTech.

Our Values

Our values are grounded in a bedrock of truth, integrity and caring for each other and the mission. We hold steadfast to:

- **TRUST** – We earn and protect the trust of our customers, employees and investors through an enduring foundation of respect, fairness, credibility and honoring our commitments, always.
- **INCLUSION** – We are an inclusive, diverse and talented workforce with a passion for mission success, intellectual capital, creativity and integrity. Our high ethical standards and investment in our people build confidence with our customers.
- **QUALITY** – We deliver exceptional quality to customers through differentiated technology solutions and an uncompromising focus on excellence, value and innovation.

ManTech
Securing the Future

Table of Contents

OUR STANDARDS 1

COMMITMENT TO NATIONAL SECURITY 1
- Protection of Classified Government Information (SC 100, SC 200 & SC 300) 1
- Personnel and Physical Security (SC 200 & SC 300) 1
- Cyber Security and Insider Threat (IT 200 & SC 401) 1
- Protection of ManTech Sensitive and Customer Controlled Unclassified Information (CG 308) 1
- Export Control and Compliance (CO 801) 1
- Information Technology Resource Use During International Travel (IT 112) 2

COMMITMENT TO OUR CUSTOMERS 2
- Accurate Reporting and Records (FA 701 & FA 703) 2
- Organizational Conflict of Interest (CO 701) 3
- Truthful Cost or Pricing Data (CO 202) 3
- Personally Identifiable Information (PII) and Protected Health Information (PHI) (CG 308, CO 703, HR 401 & IT 102) 3
- Procurement Integrity and Antitrust (CO 100 & CO 502) 3
- Offering Gifts and Entertainment (CG 309) 3
- Antibribery, Kickbacks and Gifting in Foreign Countries or to Foreign Nationals (CG 310) 4
- Hiring Current and Former Government Employees (HR 102) 4
- Combatting Trafficking in Persons (HR 105) 4

COMMITMENT TO OUR EMPLOYEES 4
- EEO, Non-Discrimination and Harassment-Zero Tolerance (HR 304 & HR 306) 4
- Drug-Free Workplace and Workplace Safety (HR 307 & HR 404) 5
- Employee Data Privacy and Protection (HR 401) 5
- Information Technology Use (IT 100) 5
- Social Media and External Communications (IT 101) 6
- Prohibition Against Retaliation (HR 304, HR 306 & CG 403) 6

COMMITMENT TO OUR PARTNERS AND SUPPLIERS 6
- Procurement (CO 502) 6
- Receipt of Gifts and Entertainment (CG 309 & CO 502) 7
- No Unauthorized Use of Copyrighted Material (IT 100) 7

COMMITMENT TO OUR SHAREHOLDERS 7
- No Insider Trading (CG 301) 7
- Financial Records and Compliance with Internal Controls (FA 101) 8
- Retention of Books and Records (CG 501 & CG 503) 8
- Political Contributions and Lobbying 8
- Conflict of Interest (CG 306) 8

IMPLEMENTATION OF OUR STANDARDS 9
- Report Suspected Wrongdoing (CG 305, CG 403, CO 310 & HR 302) 9
- ManTech's Response to Your Concerns 9
- Waivers of our Standards 9
- No Rights Created 10

FINANCIAL CODE OF ETHICS 10

ACKNOWLEDGEMENT FORM 11

ADDENDUM 12

Policies & Procedures

Select Policies & Procedures (P&P) are referenced and linked in the Table of Contents here and throughout ManTech's Standards of Ethics and Business Conduct. Our intranet site for Policies & Procedures (P&P) can be accessed through Inside.ManTech.com, under Tools & Resources. The full set of Policies & Procedures is organized on this site by Functional Area, which makes it a great place to start when you have questions. The site lists contacts for each Functional Area who may be contacted for additional guidance.

ManTech's Compliance & Ethics Program site is also available as a resource and you can email Corporate Compliance with questions.

**** Please note that policies referenced throughout our Standards can be located on the ManTech intranet by clicking on the policy link in parentheses ( ). ****

Data Protection

In today's world, data is a critical business asset that requires expert safeguarding. Constant vigilance is required to protect sensitive, controlled unclassified (CUI) and classified information belonging to ManTech and our customers.

Remember that you must:

- **Be aware of your surroundings and how other people may be able to overhear you. Conduct your confidential calls in private;**
- **Don't allow others (e.g., coworkers, family members, friends) to use your work computer at any time;**
- **Understand and comply with ManTech and customer policies for the handling of sensitive, controlled unclassified (CUI) or classified documents.**

Pay attention to the warning signs of a data loss security incident, which may include the following situations:

- **Possessing classified materials in an unauthorized location;**
- **Using an unclassified method to transmit classified information;**
- **Discussing classified materials on a non-secure telephone or in an unauthorized location;**
- **Attempting to access sensitive information without authorization;**
- **Obtaining information not required for the performance of job duties**

Help protect sensitive and classified information by staying alert and reporting concerns to Security at 877-996-4248.

OUR STANDARDS

COMMITMENT TO NATIONAL SECURITY

Our commitment to the security of our great nation is steadfast and absolute. The trust and reliance of our customers obliges us to protect their security and, by extension, our own. Our ongoing security campaign, *ManTech Secured*, renews and strengthens the high level of security around our people, operations and technology. *ManTech Secured* also demonstrates our strong focus on building a culture of doing business the right way — every day.

Protection of Classified Government Information (SC 100, SC 200 & SC 300)

As a ManTech employee, you are required to protect classified Government information and other forms of sensitive Government information. Uncompromising security is crucial to the success and safety of our customers and our nation. Do not download information to any storage media or to a non-ManTech printer. Promptly report any potential or actual violations of the security regulations and/or laws relating to the handling of classified Government information to a facility security officer or the Corporate Security Department. Be vigilant, observant and raise questions promptly to a facility security officer or the Corporate Security Department.

Personnel and Physical Security (SC 200 & SC 300)

Be mindful that Government contractors are often targeted by adversaries. Attempts to gain information can come in a variety of forms, so be aware of and comply with badge access requirements. Remember that each employee needs to badge in separately and visitors must be escorted during their visit to any ManTech business space. Stay alert, ask questions, and always promptly report any concerns to Security.

Cyber Security and Insider Threat (IT 200 & SC 401)

ManTech is a national leader in cyber security and insider threat management technology and is continually monitoring systems for intrusions or exposures that could impact the security of ManTech information or customer information. Be aware of suspicious behavior or activity and report such concerns to ManTech's Security Operations Center at spam@mantech.com or the Corporate Security Department.

Protection of ManTech Sensitive and Customer Controlled Unclassified Information (CG 308)

Information does not need to be classified to have national security implications. In fact, sensitive business information has significant value to ManTech and its business partners in the competitive marketplace. ManTech shares a responsibility with its customers and business partners to protect sensitive information in its possession and contained within its information technology systems, including customer Controlled Unclassified Information. Please follow the guidance on proper labeling and information handling set forth in ManTech's Policies & Procedures and report potential violations to ManTech's Chief Information Security Officer.

Export Control and Compliance (CO 801)

Certain exports, including technical data, defense services, and defense goods, are restricted by export control laws and regulations. This means that: (i) ManTech may not export goods to or from countries with respect to which the U.S. has a trade embargo in effect; (ii) ManTech may not export goods to or from individuals or organizations identified on lists of prohibited

trade parties published by the U.S. Government agencies; (iii) ManTech may not export goods for an end-use prohibited by U.S. Government agencies; (iv) ManTech may not export goods that are controlled by U.S. regulations without obtaining the required export license; (v) ManTech may not share controlled technical data with foreign nationals (even if planned for communication within the U.S. and even if the foreign national is employed by ManTech), without first obtaining the appropriate export license; and (vi) ManTech may not perform services that are controlled by U.S. regulations for the benefit of foreign nationals (even if directed by the government and even if the foreign national is employed by ManTech), without first obtaining appropriate approvals. Always seek guidance on export control compliance from ManTech's Executive Director of Corporate Export Control at exports@mantech.com.

Information Technology Resource Use During International Travel (IT 112)

When preparing to travel outside of the United States, contact the Security Office both *before* and *after* traveling, if you hold a security clearance. If traveling with ManTech IT resources or IT resources that contain ManTech or customer information, contact the IT Department to coordinate the use of a loaner device *before* and *after* international business or personal travel, whether or not you hold a clearance. Please get answers to questions about export control from ManTech's Executive Director of Corporate Export Control.

COMMITMENT TO OUR CUSTOMERS

ManTech's professional services are focused primarily on the federal Government marketplace. Our service to the federal Government requires ManTech to meet or exceed applicable U.S. federal regulatory requirements (and our purely commercial operations must maintain awareness of such requirements). A summary of key compliance requirements is set forth below:

Accurate Reporting and Records (FA 701 & FA 703)

As a professional services contractor, timesheet accounting and expense reporting are fundamental obligations of our business. Understand and comply with ManTech's timesheet accounting and expense reporting Policies & Procedures and accurately prepare, certify, submit and approve these important business documents. Record all work hours accurately and on a daily basis. Submit timecards for approval each reporting period. Supervisors and Project Leaders must closely monitor time and expense activity and require corrections for inaccurate submissions. Promptly raise any questions about how to properly record work activities or submit expense reports to your supervisor or a Time/Travel and Expenses Administrator.

Remote Work

When feasible and with appropriate approval from management, ManTech offers a flexible workplace environment to employees. If you have the ability to work remotely, please ensure you:

- **Charge the time you work and work the time you charge**
- **Conduct confidential work from a separate space in your home**
- **Follow Company Operational Security (OPSEC) Guidelines when accessing employer computer systems**
- **Seek participant approval prior to recording any virtual meetings**
- **Comply with ManTech's Remote Work Policy and applicable agreements**

Supervisors of employees who work remotely have the additional responsibility to ensure that remote workers are productive, record time accurately and correctly, and comply with ManTech Policies and Procedures (P&P).

If you have questions, please ask the appropriate ManTech representative listed on the addendum on page 12.

Antitrust

ManTech is committed to free and open competition and prohibits collusion with competitors. This means you should not engage in:

- **Bid rigging**
- **Price fixing**
- **Market division or allocation schemes**
- **Group boycotts**
- **Or any other anti-competitive conduct**

Follow these compliance tips:

- **Carefully consider topics for discussion when attending industry association and trade events. Communicate carefully and with a conscious effort to avoid even the appearance of impropriety.**
- **Strictly limit your teaming communications, plans and Teaming Agreements to areas of cooperation that are required to perform a single bid together. Don't engage in broad discussions or plans for teaming across multiple procurements.**

The obligation to accurately prepare, certify, approve and submit business documents extends beyond timesheets and expenses to include all work performed, such as proposals, white papers and other submissions made to ManTech or our customers. Ensure the accuracy and completeness of all business reports, records and other documentation for which you are responsible.

Organizational Conflict of Interest (CO 701)

The Government can prevent a contractor from competing for, receiving, or performing a contract award or task order when interest or involvement in other contracts could impair the contractor's objectivity or give the contractor an unfair competitive advantage. Early identification of potential and actual conflicts is critically important to ManTech's ability to properly assess and mitigate a potential conflict, and to protect its eligibility to compete for Government contracts. Promptly report potential organizational conflicts of interest to management.

Truthful Cost or Pricing Data (CO 202)

The Truthful Cost or Pricing Data Statute (formerly known as the Truth in Negotiations Act) requires ManTech to certify accurate, complete, and current cost or pricing data to the Government in certain procurements. Understand and ensure ManTech's compliance with this statute when supporting the development of new business and proposals.

Personally Identifiable Information (PII) and Protected Health Information (PHI) (CG 308, CO 703, HR 401 & IT 102)

ManTech is obliged to protect the Personally Identifiable Information (PII) and the Protected Health Information (PHI) entrusted to us by our employees, consultants and customers. Limit access, use, transmission and storage of PII/PHI to authorized business activities and equipment. Manage and protect PII/PHI in accordance with ManTech's Policies & Procedures and customer agreements. Immediately report any potential data breach to management and ManTech's Chief Information Security Officer.

Procurement Integrity and Antitrust (CO 100 & CO 502)

ManTech must compete fairly and ethically for all business opportunities. Possession or use of a competitor's rates, a competitor's sensitive/proprietary information or the Government's source selection information can compromise the integrity of the procurement process and may violate the law. Challenge the source of any competitive intelligence that appears suspicious or inappropriately possessed and never enter into an agreement that would improperly limit competition.

Offering Gifts and Entertainment (CG 309)

Every offer of a gift, meal, entertainment or other accommodation made to a non-ManTech employee in connection with ManTech business must be professional in nature, not excessive in cost, and not in the form of cash or cash equivalents (no gift certificates, no securities, no below-market loans, etc.). Do not give gifts that others may interpret as an attempt to influence a business decision, even if given after the decision. Always consult ManTech's Gifts and Entertainment policy and seek advice from the Corporate Compliance Department before offering or giving a gift.

When working with the Federal Government, always verify and comply with the customer's gift policies. The Federal Executive Branch has gratuity regulations that generally prohibit contractors from giving anything of greater than nominal value to Government employees. The Federal Legislative Branch, which includes members of Congress and their staff, generally prohibits gifts and courtesies. Any exception must be pre-approved

by the Chief Compliance Officer. Additional guidance can be found in ManTech's Gifts and Entertainment policy and all questions should be directed to the Chief Compliance Officer.

Antibribery, Kickbacks and Gifting in Foreign Countries or to Foreign Nationals (CG 310)

It is unlawful to offer or accept anything of value to/from a U.S. Government customer/employee in return for favorable treatment on a contract or subcontract. Similarly, the U.S. Foreign Corrupt Practices Act (FCPA) prohibits giving anything of value, directly or indirectly, to foreign officials, political candidates or foreign governments to influence business. Most foreign countries also prohibit gifting to government officials or government entities; even when the customary business practice in such countries is to exchange gifts. When gifting is both necessary and permissible, only ManTech (the company) may provide the gift and any gifts received by ManTech employees must be accepted on behalf of ManTech and shall become ManTech property. Gifts must be accurately accounted for in ManTech's books and records. Any plans for gifting to foreign persons or entities must be pre-approved by the Chief Compliance Officer.

Hiring Current and Former Government Employees (HR 102)

Federal regulations can limit ManTech's ability to hire or use the services of current or former U.S. Government employees and their family members. Even casual or preliminary conversations about potential employment with ManTech can violate these regulations. Consult with and obtain permission from the Human Resources Department before engaging in any (even preliminary) employment discussions with current or former employees of the U.S. Government. Require individuals who are now or have been employed by the Government to first obtain an Ethics Advisory Opinion letter from the designated ethics official of their current or former Government agency. Ethics Advisory Opinions help to clarify post-Government employment restrictions for prospective candidates and for ManTech.

Combatting Trafficking in Persons (HR 105)

Requiring employees to work or live under inhumane conditions or controlling the ability of employees to change jobs or work circumstances is illegal. Report suspicions of any such activity through the ManTech Helpline and ManTech will ensure that the Inspector General for the appropriate agency is promptly notified of all credible information. Reports may also be made directly to the National Human Trafficking Hotline at 1-888-373-7888.

COMMITMENT TO OUR EMPLOYEES

We are all responsible for contributing to the creation and maintenance of a workplace environment that is free from unlawful discrimination and harassment and that does not infringe upon protected rights. Supervisors and managers have a heightened responsibility for setting good examples and fostering workplaces that are diverse, inclusive, and respectful.

EEO, Non-Discrimination and Harassment-Zero Tolerance (HR 304 & HR 306)

ManTech promotes diversity and inclusiveness and is an equal employment opportunity employer. We do not to discriminate against any applicant or employee on the basis of race, color, sex, religion, age, sexual orientation, gender identity and expression, marital/parental status, pregnancy/childbirth or related conditions, national origin, ancestry, physical or mental disability, genetic information, status as a covered veteran or any other characteristic protected by law.

Help When You Need It

Magellan HEALTH℠

Employee Assistance Program

ManTech sponsors a confidential and free Employee Assistance Program (EAP), which provides resources to help you through many of life's challenges. The EAP provides employees and their families with helpful information on elder care, substance abuse, depression, financial or legal challenges, and much more. The EAP is available to employees and their families through Magellan Health:

Toll Free: 800-424-1836
(TTY Users: 711)

For online access go to:

- **www.magellanascend.com**
- **Select Find My Company/Log In**
- **Enter ManTech as the Company Name**
- **Explore the resources available to see:**

Social Media

Social media is an important method for staying connected. However, your use of social media must be consistent with ManTech's Standards of Ethics and ManTech policy. To support your efforts, we recommend following these guidelines when accessing social networking sites:

- **Be responsible and professional in your use of ManTech property and systems**
- **Follow ManTech's policy governing the use of company-provided equipment (IT 100)**
- **Protect ManTech's reputation and brand in the marketplace**
- **Protect ManTech's proprietary information**
- **Don't engage in activities on the internet that have the potential to reflect negatively on ManTech, your colleagues, or ManTech's customers**
- **Don't represent ManTech unless you are specifically authorized to do so by MARCOM**
- **Be mindful of posting personally identifiable information about yourself**

Please see ManTech's social media policy (IT 101) for additional guidance and always be cautious when you post on social media.

At ManTech, we are committed to providing a professional and respectful work environment in which all individuals are treated with dignity and respect. ManTech strictly prohibits harassment, bullying, or any other kind of abusive conduct, including but not limited to any unwelcome, hostile, or offensive conduct that is based on a person's protected class. At ManTech, we do not tolerate any conduct that constitutes harassment, bullying, or abuse of others.

ManTech will take prompt action to prevent and, where necessary, discipline employees for conduct that violates ManTech's Policies & Procedures. Report all suspected discrimination or harassment to management, the Human Resources Department and/or the ManTech Helpline, regardless of who is involved (whether employee, consultant, vendor, or customer). ManTech will protect from retaliation each good faith reporter of suspected discrimination and harassment.

Drug-Free Workplace and Workplace Safety (HR 307 & HR 404)

ManTech is committed to maintaining a workplace free of unauthorized alcohol and substances. The unlawful manufacture, distribution, possession or use of controlled substances in the workplace is strictly prohibited as is the unauthorized consumption of alcohol in the workplace. ManTech offers substance abuse resources through the Employee Assistance Program.

ManTech is also committed to maintaining a workplace free from violence, threats of violence, harassment, intimidation or other abusive conduct, such as bullying. The unauthorized possession of weapons in the workplace is strictly prohibited. Promptly report threats and observations of verbal or physical violence to security personnel.

Maintaining a safe work environment also means adhering to Environmental, Health, and Safety (EH&S) laws, regulations and company guidance. Employees can find Safety Guidelines and additional information on ManTech's Inside site. Each of us must be vigilant in adhering to these guidelines and bring safety concerns to management immediately.

Employee Data Privacy and Protection (HR 401)

In order to process payroll, communicate with taxing authorities on behalf of our employees, and conduct other necessary business activities, ManTech collects certain personal information from employees. ManTech limits access to collected personal data in order to protect employee privacy. Employees may review their own personal data with Human Resources representatives and ManTech will promptly update or correct any personal data found to be inaccurate.

Information Technology Use (IT 100)

ManTech may provide its employees and trusted parties with IT resources and access to ManTech computing systems for use with the performance of legitimate ManTech business activities. There is no expectation of privacy for personal information and personal property, which employees and trusted parties may choose to store in ManTech resources such as telephone systems, computer or electronic mail systems, office systems, offices, workspaces, desks, credenzas and file cabinets. ManTech reserves the right, for legitimate business reasons, to retrieve and inspect personal information and property, which employees and trusted parties store in such ManTech resources.

Always use ManTech IT resources, services and data in a professional manner and in accordance with ManTech policy. The protection of ManTech information is of particular importance. Never share log-in credentials with others. Be cautious when opening

unsolicited emails and do not click on suspicious links or attachments. Be cautious with emails and texts from unknown sources as well as sources that seem familiar but look to be imitations or variations of regular contacts. Beware of message content with unexpected language usage, grammatical errors, or formatting problems. When in doubt about the source or authenticity of a message, a link, or an attachment, check with ManTech's Security Operations Center at spam@mantech.com *before you click*.

Social Media and External Communications (IT 101)

Remember that social media sites are public forums and postings create permanent records that can be broadly accessed and disseminated. Don't share any classified, sensitive, confidential, or proprietary information regarding ManTech or its customers. Don't post anything discriminatory, harassing, bullying, threatening, defamatory, or unlawful. Don't post content, images, or photos without authorization from the owners and always be respectful in communications.

Only designated ManTech spokespersons are authorized to speak on behalf of ManTech in social media and public communications. Promptly refer all media contacts to ManTech's Corporate Marketing & Communications Department. Do not represent ManTech in any public communication, unless specifically authorized to do so by ManTech's Corporate Marketing & Communications Department. Before publicly discussing or publishing descriptions of work for ManTech, obtain prior approval for both the appearance and the presentation from ManTech's Corporate Marketing & Communications Department at CorporateCommunications@mantech.com.

Prohibition Against Retaliation (HR 304, HR 306 & CG 403)

ManTech prohibits retaliation against any employee who acts in good faith to ask questions, make complaints, participate in investigations, refuse to participate in suspected wrongful actions, or otherwise exercise workplace rights protected by law (i.e. engage in protected activity). Retaliation is adverse action taken against an employee in response to the employee's engagement in protected activity. ManTech personnel found to have participated in retaliatory actions against an employee who engaged in protected activity will be subject to disciplinary action, up to and including termination.

ManTech counts on its employees to report concerns about retaliation. Promptly report any such concerns to a ManTech Compliance Officer, the ManTech Helpline, or the Inspector General. The ManTech Helpline is hosted by a third-party, which enables employees to report potential violations online or by telephone, and anonymously, if desired (see page 9 for more information about the ManTech Helpline).

COMMITMENT TO OUR PARTNERS AND SUPPLIERS

ManTech is committed to fair and ethical dealings with our partners and suppliers and to the protection of shared sensitive and proprietary information, which concerns company, customer, and supplier assets. We extend the protections and obligations of our Standards to our suppliers, as required.

Procurement (CO 502)

ManTech will procure materials, supplies, equipment and services from qualified suppliers that can meet delivery schedules and other procurement requirements. We ensure competition among potential suppliers and we do so by following applicable Government

International Business

Do you travel or conduct business for ManTech internationally? Whether you are a buyer, program manager, business developer, or functioning in another capacity involved in overseas operations, you must be aware of relevant laws/regulations and policies that can impact your work.

Export Compliance (International Traffic in Arms Regulations (ITAR) and Export Administration Act (EAA)

- **Through the ITAR and other regulations that govern exports, the U.S. Government controls exports of sensitive equipment, software, and technology to protect our national security interests and foreign policy objectives. Always check with the Export Group before you export.**
- **Employees who travel internationally for ManTech are responsible for understanding applicable travel requirements and export control responsibilities before traveling.**
- **The EAA prohibits US persons and businesses from supporting or complying with the boycott policies of a foreign country when those polices do not align with US policy.**
- **If you have questions, please contact the Export Group at exports@mantech.com.**

Foreign Corrupt Practices Act (FCPA)

- **Enhanced diligence of non-U.S. agents, consultants, and third-party representatives is required before ManTech may engage with such foreign vendors.**
- **Gifts, entertainment, and travel provided to foreign officials must be vetted and pre-cleared by Corporate Compliance.**

Insider Trading

In the course of your daily work, you may come into possession, or become aware, of material non-public information about ManTech or another company (Inside Information). It is your responsibility to maintain the confidentiality of any such Inside Information.

Further, ManTech's Insider Trading Policy and U.S. law strictly prohibit our employees from trading (purchasing or selling) in our stock while in possession of Inside Information about ManTech. Depending on the facts and circumstances, information could be considered material even if it relates to a future or contingent event. ManTech's Insider Trading Policy provides examples of information that could be material. Information is considered to be non-public until it has been publicly disseminated and fully absorbed by the market.

regulations and contractual requirements, including those pertaining to small and small disadvantaged businesses. Suppliers are required to follow ManTech's Supplier Code of Conduct (or a sufficiently comparable code of conduct of their own). Refer to ManTech's Procurement Manual for guidance on meeting ManTech's procurement obligations.

Supply chain security is paramount. ManTech monitors new and emerging risks and updates our practices and procedures accordingly. As part of our due diligence, ManTech reviews each vendor's financial viability, eligibility to participate in the conduct of government business, provision of representations and certifications, acceptance of necessary Federal Acquisition Regulations clauses, and compliance in practice. ManTech regularly screens all vendors for restricted and denied party status.

Receipt of Gifts and Entertainment (CG 309 & CO 502)

Business decisions must be based on sound, unbiased judgment. Ensure that all interactions with suppliers, customers, competitors, contractors, and consultants comply with applicable laws and ManTech's Policies & Procedures. Don't ask for gifts and don't accept gifts or other benefits if doing so could affect or even appear to affect the objectivity of business judgment. Always promptly refuse/return any gift of cash or cash equivalents (this means no gift certificates, no securities, no below-market loans, etc.) of any value. Promptly seek answers to questions about the propriety of a gift or business courtesy, offered or received, from the Corporate Compliance Department. Refer to ManTech's Gifts and Entertainment policy for specific guidance. ManTech's procurement professionals must adhere to the additional restrictions set forth in ManTech's Procurement Manual.

No Unauthorized Use of Copyrighted Material (IT 100)

Copyright law prohibits unauthorized copying. Don't make unauthorized copies of software or copyrighted documents. Don't duplicate or forward newsletters or other materials (whether by electronic or hard-copy methods) in violation of license and copyright restrictions. Comply with all license and copyright restrictions pertaining to software and copyrighted material licensed to, purchased by, or received by ManTech.

COMMITMENT TO OUR SHAREHOLDERS

We commit to our shareholders that we conduct our business with the highest degree of integrity and honesty, and that we make timely, accurate, and transparent disclosure of financial and non-financial information about the company.

No Insider Trading (CG 301)

Personal use of non-public information about ManTech or another business, or the disclosure of such information to persons who do not have a legitimate business need for such information, is strictly prohibited. Don't trade the securities of ManTech or any other company based on material, non-public information. Don't disclose material, non-public information to another person who may use such information in a securities transaction.

Before discussing any non-public information about ManTech or another business, ensure that discussions cannot be overheard by others. Disclosure of material, non-public information to another party, whether intentional or accidental, can result in insider trading liability. Promptly report concerns about such disclosures to the Corporate Legal Department.

ManTech
Securing the Future

Financial Records and Compliance with Internal Controls (FA 101)

Financial transactions must be recorded using generally accepted accounting principles (GAAP) of the U.S., and in accordance with Government regulations, cost accounting standards, tax regulations, and ManTech's Policies & Procedures and manuals. Ensure that financial records accurately reflect the true nature and current condition of the transactions represented and that all costs, including labor, travel, and material costs, are charged in accordance with policy, contract terms and regulations. The Chief Executive Officer, the Chief Financial Officer, the Chief Operating Officer, the Controller, the Executive Vice President of Business Operations, and the Sector General Managers are also bound by the Financial Code of Ethics, located on page 10 of our Standards.

ManTech is subject to securities laws and the requirements of the Sarbanes-Oxley Act. ManTech follows internal control procedures to help ensure the full, fair, accurate, timely and understandable disclosure of financial and non-financial developments that could have a material effect on ManTech's operations or financial condition. Promptly report information that could have a material effect on the operations or financial condition of ManTech to the Chief Executive Officer, the Chief Financial Officer, the Chief Operations Officer, the Controller, the Executive Vice President of Business Operations, or the Sector General Managers.

Retention of Books and Records (CG 501 & CG 503)

ManTech is required to retain certain business records for specific periods of time. Only destroy records in compliance with ManTech's record retention policy. When subpoenas, legal proceedings, audits or investigations are pending, preserve relevant records unless and until the Corporate Legal Department determines that such records may be destroyed as a result of a closure of the matter.

Political Contributions and Lobbying

Due to the legal complexities of political contributions and lobbying, do not commit ManTech assets, funds, facilities, or personnel to benefit a candidate, campaign, political party, political committee, or legislative initiative without the prior approval of the Corporate Legal Department. Individual participation in the political process and individual campaign contributions must be made on an individual basis and never as a representative of ManTech. Don't make political contributions to obtain or retain business or other improper advantage for ManTech.

Conflict of Interest (CG 306)

A conflict of interest exists when financial interests, personal activities or relationships interfere with the objective execution of job duties for a customer or ManTech. Personal relationships with vendors, business partners, or competing businesses can impact or appear to impact decisions made on behalf of customers or ManTech. Each employee owes a duty of loyalty to ManTech and must refrain from assisting or establishing competing businesses through outside employment, provision of consulting services, or investment in such competing businesses. Remember that a conflict of interest may stem from a second job or Board position, employment or financial relationships and interests, gifts (including travel, stocks, real estate, etc.), and any other circumstance that could impact the employee's ability to remain impartial. Potential conflicts of interest must be promptly disclosed to the Corporate Compliance Department.

Personal Conflict of Interest

A conflict of interest can exist when you participate in outside activities that could influence your professional objectivity as a ManTech employee. Remember that conflicts are not limited to the work you perform for ManTech. You may have an outside conflict with work performed by other ManTech employees in a different part of ManTech.

Here are a few examples of outside activities that could impact your objectivity in making business decisions for ManTech (i.e. create a conflict of interest):

- **Owning, operating, or performing services for another business (i.e. performing a second job)**
- **Serving on the advisory board of a vendor, partner, competitor, or customer**
- **A close family or personal relationship with a person that has ties to a vendor, partner, competitor, or customer**
- **Offering or accepting gifts/ entertainment that may influence business decisions**

Consult ManTech policy CG 306 – Personal Conflict of Interest for additional information. Remember to always discuss any questions and review your plans with Corporate Compliance before you take action.

ManTech Helpline

The ManTech Helpline is open 24 hours-a-day/365-days-a-year to accept your reports of violations of our Standards or policies.

The ManTech Helpline also provides you with the opportunity to ask a question and get an answer from an appropriate resource. And while you may keep your report or question anonymous, providing your name may improve or expedite ManTech's review of your concern. The ManTech Helpline is available by phone or internet:

By phone:

In the U.S. or Canada: Dial toll free (866) 294-9442.

Outside the U.S. or Canada:

See ManTech's helpline homepage for international dialing instructions.

Online:

Visit www.mantech.ethicspoint.com; or click the Compliance & Ethics Program link on Inside.ManTech.com

IMPLEMENTATION OF OUR STANDARDS

Report Suspected Wrongdoing (CG 305, CG 403, CO 310 & HR 302)

Every ManTech employee has an affirmative duty to report any actual or suspected violation of our Standards or ManTech's Policies & Procedures. Promptly report suspected violations of our Standards or ManTech's Policies & Procedures to a supervisor, any ManTech manager, the Human Resources Department, the Corporate Compliance Department, or the ManTech Helpline.

Time card fraud, false claims, other fraud matters, conflict of interest, bribes, gratuities or other questionable activity can impact ManTech's ability to work with the Government and must be promptly reported to the Corporate Compliance Department or the ManTech Helpline, without fear of retaliation. You may choose to report violations of the Federal Acquisition Regulation (FAR) or other regulations directly to the federal agency's Inspector General pursuant to the whistleblower provisions or call the Department of Defense (DoD) Hotline at 800-424-9098. The ManTech Helpline may also be used to communicate concerns about accounting, internal controls, or auditing matters to the Audit Committee of the Board of Directors. Alternatively, a report may be made to the Chief Compliance Officer or members of management in order to communicate such concerns to the Audit Committee.

ManTech's Directors, Officers and Sector General Managers must report in writing to the Corporate Legal Department any knowledge of any legal or administrative proceeding brought against ManTech or a ManTech Director, Officer or Sector General Manager within the last five (5) years, in connection with the award or performance of a federal contract that resulted in a conviction or finding of fault.

A list of resources for reporting suspected wrongdoing or obtaining clarification of our Standards is available in the "Sources of Help with Resolving Your Questions or Concerns" addendum to our Standards. ManTech encourages employees to bring concerns forward and will protect from retaliation employees who make good faith reports of potential violations of our Standards or our Policies & Procedures. Our Standards are publicly available and posted internally for future reference.

ManTech's Response to Your Concerns

All concerns reported in good faith and with sufficient detail will be evaluated and reviewed to determine whether a violation of our Standards or ManTech's Policies & Procedures has occurred. Reviews are kept confidential to the greatest extent possible. If a violation has occurred, ManTech will take responsive corrective and disciplinary action, which may include termination of employment and the potential loss of security clearance. Do not conduct preliminary investigations, as independent action can compromise the integrity of evidence and the validity of subsequent investigation by ManTech.

Waivers of our Standards

ManTech may waive application of provisions of our Standards if special circumstances warrant a waiver. However, waivers of our Standards for Directors or Executive Officers may only be made by the Board of Directors and must be disclosed, as required by Nasdaq.

No Rights Created

Our Standards are a statement of the fundamental principles and key Policies & Procedures that govern our business conduct. They are not intended to and do not create a contract for employment or other contractual obligation to any employee, director, client, supplier, competitor, shareholder, other person or entity.

ManTech
Securing the Future

Our Standards cover a wide range of business policies, practices and procedures. They are not designed to cover every issue that may arise. Instead, they provide an overview and guidance on how to resolve questions about the appropriateness of your own conduct or the conduct of your coworkers. ManTech's Policies & Procedures cited in our Standards can be found on the ManTech intranet along with additional Policies & Procedures that govern many of the topics in our Standards. If you become aware of an issue that cannot be resolved through application of this guidance or you have questions about the application of this guidance, promptly seek answers from one of the sources referenced in the Addendum that follows.

FINANCIAL CODE OF ETHICS

This Financial Code of Ethics contains special commitments that are applicable to the Chief Executive Officer, the Chief Financial Officer, the Chief Operating Officer, the Controller, the Executive Vice President of Business Operations, and the Sector General Managers.

ManTech's filings with the Securities and Exchange Commission must be accurate and timely. The Chief Executive Officer, the Chief Financial Officer, the Chief Operating Officer, the Controller, the Executive Vice President of Business Operations, and the Sector General Managers bear a special responsibility for promoting integrity throughout ManTech and fostering a culture that ensures the fair and timely reporting of ManTech's financial results and operating condition to the public. Accordingly, if you hold one of the aforementioned positions, you are required to abide by the following Financial Code of Ethics, which have been reasonably designed to deter wrongdoing and to promote:

- Acting honestly and ethically, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships.
- Providing full, fair, accurate, timely and understandable disclosure of information in reports and documents that ManTech files with, or submits to, the Securities and Exchange Commission and in ManTech's other public communications.
- Complying with applicable governmental laws, rules and regulations.
- Promptly reporting violations of the Financial Code of Ethics to the Corporate Compliance Department, the Corporate Legal Department or the ManTech Helpline.
- Accountability for compliance with the Financial Code Ethics.

Violation of this Financial Code of Ethics is a serious matter that may result in significant disciplinary action, up to and including termination of employment with ManTech.

ACKNOWLEDGEMENT FORM

I HEREBY REPRESENT TO MANTECH THAT:

- I read and understand ManTech's Standards of Ethics and Business Conduct.
- I will comply with ManTech's Standards and will report all suspected violations of ManTech's Standards.
- I have reported all suspected violations of ManTech's Standards known to me today.
- *(For Directors, Officers and Sector General Managers only) I reported in writing to the Corporate Legal Department my knowledge of any criminal, civil or administrative proceeding brought against a ManTech entity or any of its Directors, Officers or Sector General Managers within the last five (5) years, in connection with a federal contract that resulted in a conviction or finding of fault.*

_____

Your printed name

_____

Your employee ID number

_____

Your sector name (Def/Fed Civ/Intel/CORP)

_____

Your primary work site or location

_____

Your signature

_____

Today's date

* Paper forms are only accepted when online completion is not possible. Paper filers must execute and email this form to corporate.compliance@mantech.com or fax to (703) 218-8221.

ADDENDUM

SOURCES OF HELP WITH RESOLVING YOUR QUESTIONS OR CONCERNS

Local and Sector Management Contacts

Your local management and Human Resources representatives are often an excellent starting point for resolving questions and concerns. In addition, your Sector General Managers are available to assist you and to provide you with additional resources that address your concerns. You may also contact the following Operations Compliance Officers:

Bonnie Cook, Executive Vice President of Business Services (703) 814-4236
JoAnne Dukeshire, Vice President of Contracts (703) 549-9261
Peter Ward, Vice President of Human Resources Sector Operations (301) 325-2054

Contacts for Company-Wide Resources

The following resources are available to assist in your understanding of our Standards and reporting of issues and concerns:

Compliance Department (703) 218-6489
Sejal Patel, Vice President and Chief Compliance Officer (703) 259-3655
Mark Quirk, Vice President of Industry Compliance (703) 218-8387

Export Compliance
Sharon Hinrichs, Executive Director of Export Compliance, email: exports@mantech.com

Finance Matters
Judith Bjornaas, Executive Vice President and Chief Financial Officer (703) 218-6421
Jay Romyn, Senior Vice President and Controller (703) 218-6463

Human Resources Department
Julie Anna Barker, Chief Human Resources Officer (703) 674-2918
Kimberly Highsmith, Executive Director of Employee Relations and Diversity (703) 218-8231

Information Services and Business Process (703) 218-6371
Michael Uster, Senior Vice President and Chief Information Officer (703) 218-8243
Paul Beckman, Vice President and Chief Information Security Officer, email: spam@mantech.com

Legal Department (703) 218-6099
Jeffrey Brown, Executive Vice President and General Counsel (703) 218-6098

Security Department
Daniel Payne, Senior Vice President and Chief Security Officer (703) 218-4694; 877-996-4248 (option 9)

ManTech Helpline

International dialing instructions can be found on ManTech's Helpline homepage.

The ManTech Helpline is Available 24/7

Online:
www.mantech.ethicspoint.com

By Phone:
(866) 294-9442

ManTech International Corporation
2251 Corporate Park Drive, Suite 600
Herndon, VA 20171

ManTech®
Securing the Future