Standards of
Ethics and Business Conduct
2020

Tomorrow's Technology | Timeless Values

ManTech
Securing the Future

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

MANTECH'S BOARD OF DIRECTORS

- **George J. Pedersen**
  Executive Chairman and Chairman of the Board, 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**
  President and Chief Executive Officer, Quantum Spatial
- **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
- **Kevin M. Phillips**
  President and Chief Executive Officer, ManTech International Corporation

MESSAGE FROM THE PRESIDENT AND CEO AND THE EXECUTIVE TEAM

Dear Colleague,

ManTech has provided innovative technology and mission-focused solutions to our customers for more than five decades. Our success is a direct result of the dedication and values that we hold both individually and as a company, and we will remain steadfastly committed to these principles in the years to come. The outstanding reputation ManTech enjoys today with customers, teammates 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 a culture based on uncompromising integrity and ethical behavior—vital differentiators in today's intensely competitive marketplace.

Please read our Standards of Ethics and Business Conduct carefully to make sure that you understand the culture behind ManTech's continued success. Apply what you learn from the pages of our Standards to ensure ethical decision-making that upholds ManTech's core values and principles of business.

As a ManTech employee, you play a vital role in defining our company as a trustworthy business partner and an innovative industry leader. We are proud of the outstanding job you do 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.

If you have questions, please speak to your supervisor or any of the company resources identified in our Standards, including the ManTech Helpline.

George J. Pedersen *Kevin M. Phillips* *Judith L. Bjornaas* *Richard J. Wagner* *Matthew Tait*

Kevin M. Phillips
President and Chief Executive Officer

George J. Pedersen
Executive Chairman and Chairman of the Board

Judith L. Bjornaas
Executive Vice President and Chief Financial Officer

Richard J. Wagner
President
Mission, Cyber, and Intelligence Solutions

Matthew Tait
President
Mission Solutions and Services

The Foundation of our Standards

ManTech's Mission

ManTech advances customer success by delivering best-in-class solutions, consulting services, and technologies that meet our customers' mission-critical needs.

Our Vision

ManTech will be our customers' most trusted industry partner, integral to their success. Our mission-driven company will be a strategy-focused organization, operating as One ManTech.

Core Values

With uncompromising integrity and ethics we value:

- Our position of **TRUST**—with our customers. Its foundation in partnership, earned respect, fairness, credibility, and honoring our commitments is fundamental to success in all our engagements.
- Our **PEOPLE**—their passion for the mission, intellectual capital, creativity, and leadership ensure our reputation and the success of our company.
- **QUALITY** in all that we do—delivering best value to our customers through our quest for excellence, value creation, and innovation.

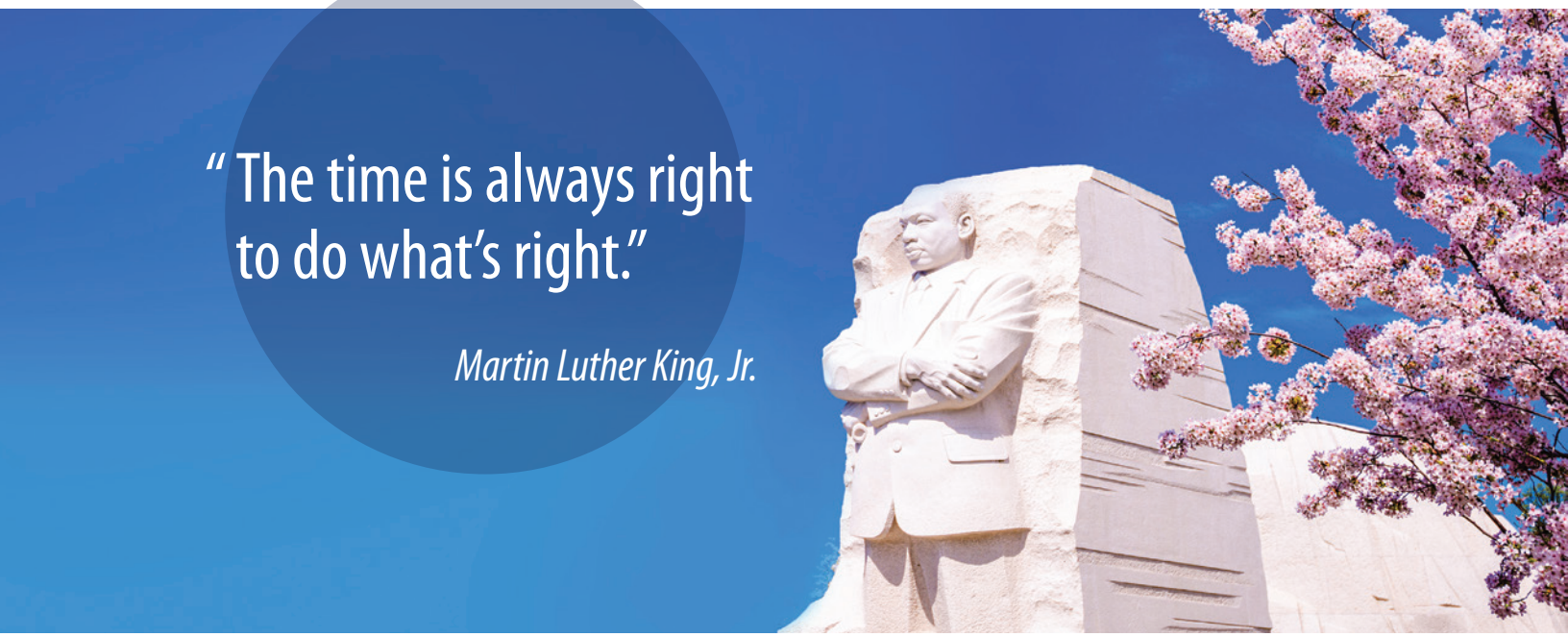


Table of Contents

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

Policies & Procedures

Specific Policies & Procedures are referenced and linked in the Table of Contents here and throughout our Standards of Ethics and Business Conduct. Our Policies & Procedures (P&P) intranet site can be found on Inside.ManTech.com, under Tools & Resources or accessed through the tile on MyHUB. All of ManTech's Policies & Procedures are listed on this site, which makes it a great place to start when you have questions. Each of the Policies & Procedures is organized by Functional Area, so you can reach out to the appropriate contact for any additional guidance you may need.

Sign up to receive Policies & Procedures announcement alerts by following the instructions in the Reference Documents section and see what was recently posted by clicking the link to Recently Added or Revised Policies.

OUR STANDARDS

Protecting Sensitive and Classified Information

Constant vigilance is required to prevent harm to ManTech's owned or operated security, resources or records. Help protect sensitive and classified information by staying alert, following policy, and reporting concerns to your management or security team.

Pay attention to potential warning signs of a 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**
- **Access or attempts to access secured locations or classified information without authorization**
- **Obtaining information not required for job duties**
- **Performing unnecessary work outside normal work hours**
- **Using company computer equipment and mobile devices in foreign countries without appropriate authorization and security measures**

Help protect ManTech and our national security by immediately reporting suspected security incidents.

Commitment to National Security

Our commitment to the security of our great nation is steadfast and absolute. The trust and reliance of our customers brings an enhanced obligation 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 doing business the right way—every day.

Protection of Classified Government Information (SC 100 & SC 201)

ManTech and its employees 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. 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. Raise questions promptly to a facility security officer or the Corporate Security Department.

Cyber Security and Insider Threat (IT 200 & SC 107)

ManTech is a national leader in cyber security and insider threat management technology and is continually monitoring 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 CSIRT@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 or 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. Follow the labeling and handling guidance provided 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 governed by export control laws and regulations. This means: (i) do not export goods to or from countries with respect to which the U.S. has a trade embargo in effect; (ii) do not export goods to or from individuals or organizations identified on lists of prohibited trade parties published by the U.S. Government agencies; (iii) do not export goods for an end-use prohibited by U.S. Government agencies; (iv) do not export goods that are controlled by U.S. regulations without a license exemption or obtaining any required license; (v) do 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 appropriate license; and (vi) do 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 Director of Corporate Export Control.

Information Technology Resource Use During International Travel (IT 112)

When preparing to travel outside of the United States, contact the Group Security Office *before* and *after* traveling. If traveling with computers, mobile phones or other electronic devices, contact the Group IT Department *before* and *after* traveling. Seek guidance on export control and compliance from ManTech's Director of Corporate Export Control.

Commitment to Our Customers

ManTech's professional services are focused primarily on the federal Government marketplace. This requires meeting or exceeding (and our purely commercial operations must maintain awareness of) all applicable U.S. federal regulatory requirements. Give special attention to compliance with the following requirements:

Accurate Reporting and Records (FA 701 & FA 703)

As a professional services contractor, timesheet accounting and expense reporting are fundamental parts 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 inappropriate claims. Promptly raise any questions about how to properly record work activities or submit justified expenses with Supervisors or Time/Travel and Expenses Administrators.

The need to accurately prepare, certify, submit and approve business documents extends beyond timesheets and expenses and includes all work performed, such as proposals, white papers and other submissions made to ManTech or our customers. All business documents must be accurate and truthful, so ensure the integrity of reports and records by verifying their accuracy and completeness.

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

workday.

Time

Timesheet Reporting

Q: As a supervisor I regularly approve timesheets for my staff. But several members of my team work at a different facility. How can I be sure their time entries are accurate?

A: Your timesheets and those you approve are essentially invoices to ManTech's customers. Keeping accurate time is a critical part of our business. To help ensure accuracy, supervisors should regularly monitor all of their staff members. When you are not co-located with members of your staff, you should consider:

- Checking on staff progress each day and setting measurable goals for them to achieve the next day
- Visiting jobsites periodically to check work product and meet with staff members
- Setting the right tone by expecting employees to keep you informed of absences or other work disruptions
- Asking resources at the worksite to help you monitor performance and attendance
- Requesting more information from employees about time entries whenever you spot potential issues

Do not approve timesheets if you believe they are incorrect! Take time to get the answers you need to ensure the accuracy of all time entries.

identification of potential and actual conflicts is critically important to ManTech's abilities 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) (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 violate the law. Challenge the source of any competitive intelligence that appears suspicious or inappropriately possessed and never enter into an agreement that would unfairly 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. Requests for exceptions must be pre-cleared by the Chief Compliance Officer. Additional guidance can be found in ManTech's Gifts and Entertainment policy (CG 309).

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

Did You Know?

ManTech must respect and protect the confidential information of our Federal customers and our competitors.

The Federal government is responsible for managing procurements fairly for all competitors. An offeror should not be privy to sensitive government procurement plans or evaluation criteria that the government has not officially distributed to all other competing contractors. Likewise, an offeror should not obtain or use the proposal or other proprietary information of another contractor without proper authorization from such contractor.

Sensitive procurement information is usually labeled as *Acquisition Sensitive* or as *Source Selection Information* by the government, and contractors should mark their proposals or other proprietary information with restrictive legends. However, labels or markings are not present on all sensitive documents. The true test is to review the content and the source – so be watchful for non-public information belonging to the government or a competitor and question the source of sensitive documents to verify that ManTech is in rightful possession of such information. ManTech's ability to compete is dependent on our adherence to the rules of fair competition.

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. Plans for gifting to foreign persons or entities must be pre-cleared by the Chief Compliance Officer. 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.

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, as well as 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. Penalties for violations can include criminal prosecution and/or termination of employment for employees found to have been involved in trafficking, and may subject ManTech to suspension of payments, loss of contracts and/or debarment from contracting.

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. Reports may also be made directly to the Global Human Trafficking Hotline at 1-844-888-FREE (or by email at help@befree.org).

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 to set good examples and to foster workplaces that support honesty, integrity, respect, and trust.

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

ManTech promotes diversity and inclusiveness, and is an equal employment opportunity employer. The company's policy is 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℠

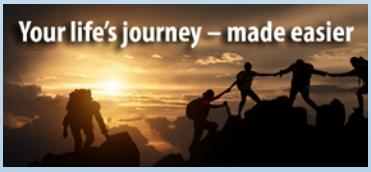
Employee Assistance Program

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

Toll Free: 800-424-4485
(TTY Users: 800-456-4006)

For online access go to:

- **MagellanAscend.com**
- **Select Log In**
- **Click on the Sign Up link**
- **Enter ManTech International Corporation as the Company Name**
- **Complete the registration process and see:**



Data Privacy

Phishing attacks include verbal and electronic communication techniques used by cybercriminals to trick unsuspecting people into revealing sensitive information like usernames and passwords or unwittingly providing access to electronic resources. Phishing occurs through a variety of communication methods, including emails, phone calls, and social media or text messages.

Phishing attacks are on the rise and becoming more sophisticated; caution and constant vigilance are now a necessity to avoid being victimized. With respect to the electronic communications you receive:

- **Be cautious with any unsolicited communication, particularly when there are misspellings or anomalies in emails or web addresses**
- **Recognize that cybercriminals do their research and will often try to use common ground to gain your trust**
- **Do not click on links or attachments in suspect emails, texts, or social media messages**
- **Be suspicious if your login credentials or personal information are being solicited, and directly contact the purported sender through a different communication method if you are unsure about the legitimacy**
- **Report suspected phishing scams to SPAM@mantech.com**

By design, many phishing communications appear authentic and can be very convincing. Your cautious and vigilant consideration of all communications and requests is critical to the security of our data and resources.

We are committed to a work environment in which all individuals are treated with dignity and respect. As such, ManTech prohibits abusive conduct and harassment of any applicant or employee based on any of the protected categories above. Harassment is verbal, physical or visual conduct that degrades or shows hostility towards another person based on that person's membership in a protected class. Conduct that a reasonable person would find hostile, offensive, and unrelated to an employer's legitimate business interests, is considered abusive conduct and will not be tolerated at ManTech. ManTech strictly prohibits all forms of harassment in the workplace.

ManTech will take prompt action to prevent and, where necessary, discipline employees for behavior 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 good faith reporters of suspected discrimination and harassment.

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

ManTech is committed to maintaining a workplace free of controlled substances and unauthorized alcohol. 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. Promptly report threats and observations of verbal or physical violence to security personnel. The unauthorized possession of weapons in the workplace is strictly prohibited.

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 our employees. Because ManTech respects the privacy of its employees, ManTech limits the collection of and access to personal data. Employees may review their own personal data with human resources representatives. ManTech will promptly update or correct any personal data that is inaccurate.

Information Technology Use (IT 100)

ManTech may provide its employees and agents with computer equipment and access to ManTech computing systems to facilitate their work for ManTech. This equipment and access are provided for use with legitimate ManTech business activities. There is no expectation of privacy for personal information and property that employees and agents 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 that is stored by employees and agents in such ManTech resources.

Use ManTech's IT equipment, services and data in a professional manner and in accordance with ManTech policy. 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. Phishing attacks are increasing clever because malicious actors are having to develop new and more enticing ways to fool and exploit

even trained IT users. 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 as well of message content with unexpected language usage, grammatical errors, or formatting problems. When in doubt about a message, a link, or an attachment, before you click—check *first* with ManTech's Security Operations Center at SPAM@mantech.com.

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 broadly 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.

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.

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

Our Standards, ManTech's Policies & Procedures, and the law protect employees from retaliation for engaging in a protected activity or reporting what is reasonably believed to be evidence of gross mismanagement or waste, abuse of authority, substantial and specific danger to public health and safety, or violation of law related to a federal contract. ManTech protects employees from retaliation when they have engaged in protected activity in good faith. Anyone found to have participated in retaliatory actions against an employee who made a good faith report or otherwise engaged in protected activity will be subject to disciplinary action, up to and including termination. Promptly report any concerns about retaliation resulting from reporting compliance or other concerns to a ManTech Compliance Officer, the ManTech Helpline, or the Inspector General. The ManTech Helpline is available to assist with meeting this requirement. 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 12 for more information about the ManTech Helpline).

Commitment to Our Teammates and Suppliers

ManTech is committed to fair and ethical dealings with our teammates 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 follow applicable Government 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.

Did You know?

According to Pew Research Center, 74% of Facebook users visit the site each day, and 51% visit Facebook several times a day. We recognize the importance of staying connected and the utility of social networking sites. However, employees should limit their use of these sites during work hours and ensure they protect ManTech while using social media. We recommend the following guidelines when accessing social networking sites:

- **Be responsible and professional in your use of ManTech property and systems; ManTech monitors internet usage and e-mail traffic on its IT systems**
- **Follow ManTech's policy governing the use of company-provided equipment (IT 100)**
- **Protect ManTech's reputation, trademarks, and proprietary information**
- **Don't engage in activities on the internet that can reflect negatively on ManTech, your colleagues or ManTech's customers**
- **Don't represent ManTech unless authorized to do so**

Please see ManTech's social media policy (IT 101) for additional guidance and be mindful of what you post online.

Did You Know?

In the course of your daily work, you may become aware of material, non-public information. You must be careful not to disclose material, non-public information to others even if you don't personally utilize the information. What an outside investor may consider important is often not limited to financial information about ManTech. Information about recent contract awards, hiring information, and possible acquisitions can also be material, non-public information, if it has not already been publicly disclosed.

People who inappropriately share material, non-public information can face severe consequences, which may include termination of employment, prosecution, fines, and imprisonment. Unless you are certain that information is public, do not discuss it outside of ManTech and do not use your insight regarding upcoming business decisions to make personal investments or give tips to others.

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 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. Promptly and always refuse/return any gift of cash or cash equivalents (this means no gift certificates, no securities, no below-market loans, etc.) of any value. Questions about the propriety of a gift or business courtesy, offered or received, must be promptly raised with 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 our business conduct adheres to the highest standards of professional ethics, 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.

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, Chief Financial Officer, Controller, or other persons employing similar functions 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 the operations or financial condition of ManTech. Promptly report information that could have a material effect on the operations or financial condition of ManTech to the Controller, the Chief Financial Officer, a Group President, or the Chief Executive Officer.

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/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 personal interests 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. Potential conflicts of interest should be promptly disclosed to the Corporate Compliance Department. 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.

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 our Standards or ManTech's Policies & Procedures to a supervisor, any ManTech manager, or the Human Resources Department. A report may also be made to the Corporate Compliance Department or the ManTech Helpline.

Timesheet fraud, false claims or 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. 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

Conflict of Interest

A conflict of interest can develop if you participate in outside activities that could influence your professional objectivity as a ManTech employee. While many outside activities do not create a conflict with ManTech's interests, you should always review your plans with Corporate Compliance to make sure there is not a conflict of interest *before* you take action.

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, teammate, competitor, or customer**
- **Failing to disclose a family or personal relationship involving a vendor, teammate, competitor, or customer**

Conflicts are not limited to the work you do for ManTech. You may have an outside conflict with work performed in another division of ManTech. For this reason, it is important to have a potential conflict independently evaluated by Corporate Compliance. For additional information, you should consult ManTech policy CG 306 – Personal Conflict of Interest and discuss any questions with Corporate Compliance.

Did You Know?

Your work environment plays an important role with reporting unethical behavior. Research indicates that when an employee's supervisor or coworkers are not highly ethical, employees are less likely to report their observations of unethical conduct or wrongdoing. Conversely, when supervisors and coworkers are highly ethical, employees are more likely to report their observations of unethical conduct or wrongdoing.

We all play an important role in maintaining an ethical environment at ManTech. The integrity you apply to your business decisions affects you, your coworkers and those who work for you. If you face an ethical dilemma and you are unsure how to handle it, ask your supervisor, Human Resources, Compliance or other members of management to assist you.

Additional resources are listed in the Addendum on page 9 and are available to you through the Compliance & Ethics intranet site.

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 Business Unit General Managers (BUGMs) 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 BUGM 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 a good faith reports of potential violations of our Standards or our Policies & Procedures.

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 our Standards if special circumstances warrant a waiver. Waivers of our Standards for Directors or Executive Officers may only be made by the Board of Directors or the Audit Committee of the Board.

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.

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, seek advice from one of the sources referenced in the Addendum that follows.

Your electronic acceptance or return of the acknowledgement form for our Standards represents your receipt, understanding and commitment to comply with them.

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 Controller, or other persons employing similar functions.

ManTech's filings with the Securities and Exchange Commission must be accurate and timely. The Chief Executive Officer, the Chief Financial Officer, and the Controller 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.
- The prompt internal reporting of violations of the Financial Code of Ethics to the Corporate Compliance Department, the Corporate Legal Department or the ManTech Helpline.
- Accountability for adherence to 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 now known to me.
- *(For Directors, Officers and BUGMs 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 BUGMs 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 group name

_____

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 Group Management Contacts

Your local management and Group Human Resources representatives are often an excellent starting point for resolving questions and concerns. In addition, your Group Presidents are available to assist you and to provide you with additional resources that address your concerns. At the Group level, you may also contact your respective Group Compliance Officers:

Mission Solutions and Services (MSS)
Bonnie Cook – (703) 814-4236

Mission, Cyber and Intelligence Solutions (MCIS)
Steve Deitz – (703) 326-1085

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

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

Export Compliance
Maria Assusa, Director of Corporate Export Control (703) 218-6393

Human Resources Department (703) 218-6365
Jeffrey Brody, Chief Human Resources Officer (703) 674-2648
Kimberly Highsmith, 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
James Webster, Chief Information Security Officer (703) 218-8208, email: CSIRT@mantech.com

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

Security Department
Daniel Payne, Senior Vice President and Chief Security Officer (703) 218-4694

The ManTech Helpline is Available 24/7

Online:
www.mantech.ethicspoint.com

By Phone:
(866) 294-9442

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:

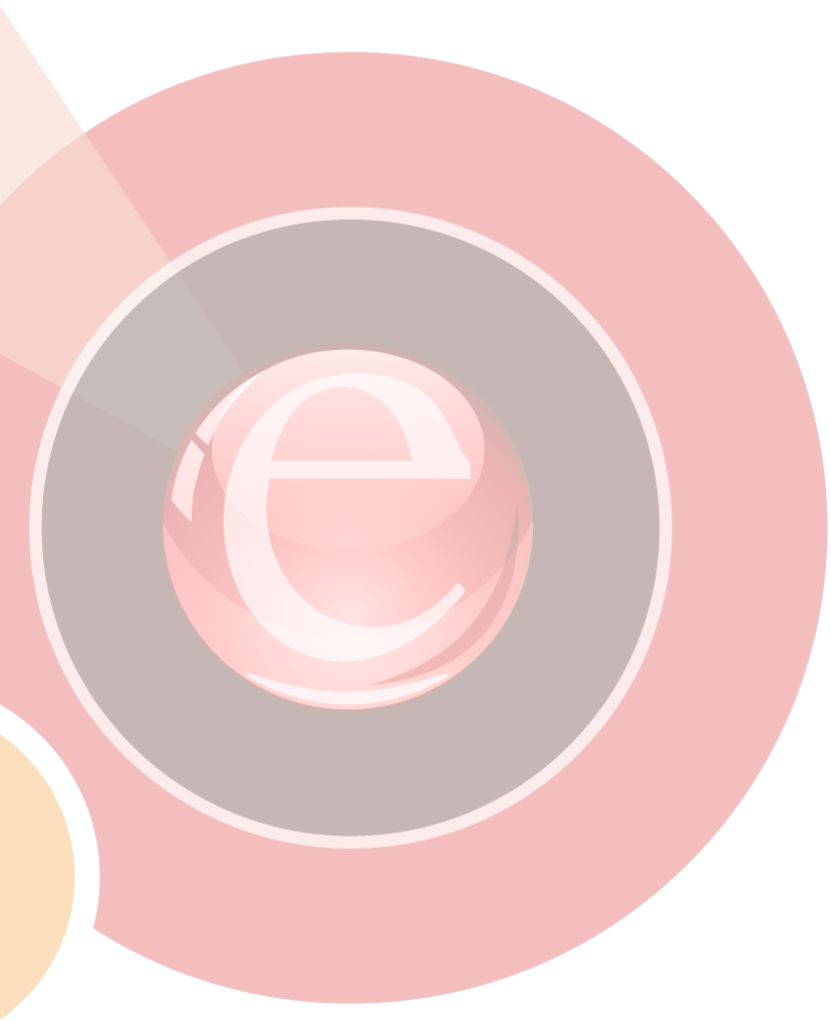
In the U.S. or Canada: Dial toll free - (866) 294-9442.

Outside the U.S. or Canada:

Dial an international operator and request a collect call (reverse charges) be placed to (503) 352-7174. All calls will be accepted.

Online:

www.mantech.ethicspoint.com; or click the Compliance & Ethics tile on MyHUB to access the ManTech Helpline.



ManTech

Securing the Future

2251 Corporate Park Drive
Herndon, Virginia 20171
mantech.com

9_194402