2018 Standards of Ethics and Business Conduct

Tomorrow’s Technology – Timeless Values

50 YEARS

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; Former Assistant Secretary of Defense; Former Presidential Special Envoy during the Gulf War
- **Mary K. Bush** – President, Bush International; Former Managing Director, Federal Housing Finance Board
- **Barry G. Campbell** – Former Chairman and Chief Executive Officer, Tracor Systems Technology, Inc.
- **Walter R. Fatzinger, Jr.** – Director, Chevy Chase Trust Company and Director, ASB Capital Management, Inc.
- **Richard J. Kerr** – Former Deputy Director and Officer, Central Intelligence Agency
- **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 CHAIRMAN AND CEO AND THE EXECUTIVE TEAM

Dear Colleague,

ManTech has provided innovative technology and mission-focused solutions to our customers for almost five decades. ManTech celebrates its 50th Anniversary in 2018, and this milestone provides a great opportunity for reflection, on the business and the people that have contributed to our success as a company. In 1964, Martin Luther King Jr. said, “The time is always right to do what’s right,” and adhering to this sage principle has been, and continues to be, one of the keys to ManTech’s longevity. The outstanding reputation ManTech enjoys with our customers, teammates and competitors depends on our commitment to doing business the right way every day. In an increasingly competitive marketplace, adherence to our Standards of Ethics and Business Conduct remains critical. Our Standards guide us and support a culture of uncompromising integrity and ethical behavior at ManTech.

Please read our Standards of Ethics and Business Conduct carefully to make sure that you understand them and their important connection to ManTech’s continued success. They provide a foundation for ethical decision-making that will help you uphold ManTech’s core values and principles. If you have questions, please speak to your supervisor or any of the company resources identified in our Standards, including the ManTech Helpline.

We recognize and value the important role that each employee has in defining ManTech as an innovative industry leader and trustworthy business partner. We are proud of the outstanding job you do every day and how your work benefits our customers, our shareholders and ourselves. Thank you for your commitment to doing what’s right by conducting yourself with uncompromising integrity and ethics.
The Foundation of our Standards

ManTech’s Mission
ManTech advances customer success by delivering unique best value solutions, consulting services, and technologies that meet our clients’ mission-critical needs anytime and anywhere - and we create added value through quality, innovation, and partnership.

Core Values
Three core values form the basis of our corporate culture and operating principles. These values are the catalysts for our professional ethics and commitments. With uncompromising integrity and ethics, we value:

- Our position of **TRUST** with our customers – its foundation in partnership, mutual respect, fairness and commitment to mission, is fundamental to our success in each business engagement. This trust is based on our unsurpassed dedication to program execution.

- Our **PEOPLE** – our passion for mission, intellectual capital, creativity and ability to lead, build our reputation and ensure the success of our company. Talent and teamwork make our performances successful.

- Our **QUALITY** - in all that we do, through our quest for excellence, value creation and innovation, we seek to deliver the best value for our customers and improve the elements of our business. We understand the mission and we focus on the ideas and solutions that drive progress and success.
# Table of Contents

**STANDARDS**

- **Commitment To National Security**
  - Protection of Classified Government Information (SC 100) .......................................................... 1
  - Cyber Security and Insider Threat (IT 200 and SC 107) ................................................................. 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**
  - Time and Expense Reporting (FA 701 & FA 703) ...................................................................... 2
  - Procurement Integrity and Antitrust (CO 100 & CO 502) ................................................................. 2
  - Truthful Cost or Pricing Data (CO 202) ......................................................................................... 2
  - Personally Identifiable Information (PII) and Protected Health Information (PHI) (CO 703, HR 401, & IT 102) .................................................................................................................. 3
  - Organizational Conflict of Interest (CO 701) ................................................................................. 3
  - Offering Gifts and Entertainment ................................................................................................. 3
  - Anti-bribery, Kickbacks and Gifts in Foreign Countries or to Foreign Nationals (CG 310) ......... 3
  - Hiring Current and Former Government Employees (HR 102) .................................................... 4
  - Combating Trafficking in Persons (HR 105) ................................................................................ 4

- **Commitment To Our Employees**
  - Equal Employment Opportunity, Non-Discrimination and Non-Harassment (HR 304 & HR 306) ................................................................................................................................. 4
  - Drug-Free Workplace and Workplace Violence (HR 307 & HR 404) ........................................... 5
  - Employee Data Privacy and IT Equipment Usage (HR 401, IT 100, & IT 101) ............................... 5
  - No Retaliation (HR 304, HR 306 & CG 403) ................................................................................ 5

- **Commitment To Our Teammates and Suppliers**
  - Procurement Policies (CO 502) ...................................................................................................... 6
  - Receipt of Gifts and Entertainment (CG 306) .................................................................................. 6
  - No Unauthorized Use of Copyrighted Material (IT 100) ............................................................... 6

- **Commitment To Our Shareholders**
  - No Insider Trading (CG 301) ......................................................................................................... 7
  - Conflict of Interest (CG 306) ......................................................................................................... 7
  - Financial Records and Compliance with Internal Controls (FA 101) ........................................... 7
  - Retention of Books and Records (CG 501 & CG 503) .................................................................. 8
  - Political Contributions and Lobbying ......................................................................................... 8

- **Implementation Of Our Standards**
  - Report Suspected Wrongdoing (CG 305, CG 403 & CO 310) ...................................................... 8
  - ManTech’s Response to Your Concerns ...................................................................................... 9
  - Waivers of our Standards .......................................................................................................... 9
  - No Rights Created ...................................................................................................................... 9

- **Financial Code Of Ethics** ........................................................................................................ 10

- **ACKNOWLEDGEMENT FORM** .............................................................................................. 12

- **ADDENDA** ............................................................................................................................. 14

- **Sources Of Help With Resolving Your Questions or Concerns**
  - Local and Group Management Contacts ............................................................................... 14
  - Contacts for Company-Wide Resources .................................................................................. 14
  - The ManTech Helpline is Available 24/7 ................................................................................ 14

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

COMMITMENT TO NATIONAL SECURITY

Our commitment to the security of our great nation is absolute. ManTech’s position of trust and leadership with customers supporting our national security brings an enhanced obligation to protect these interests and, by extension, our own interests.

Protection of Classified Government Information (SC 100)

ManTech and its employees are required by law to protect U.S. Government classified information and other forms of sensitive Government data. Uncompromising security is critical 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. Contact a facility security officer or the Corporate Security Department with any questions.

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

ManTech is a national leader in cyber security and insider threat management technology and is continually monitoring for intrusion or exposures that could impact the security of ManTech and customer information. Report your concerns to ManTech’s Chief Information Security Officer 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 potential national security implications or to have 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 our policies and report potential violations to ManTech’s Chief Information Security Officer.

Export Control and Compliance (CO 801)

Export of certain items, including technical data, defense services and goods, may be governed by export control laws and regulations. Do not: (i) export goods to or from countries with respect to which the U.S. has a trade embargo in effect; (ii) export goods to or from individuals or organizations identified on lists of prohibited trade parties published by the U.S. Government agencies; (iii) export goods for an end-use prohibited by U.S. Government agencies; (iv) export goods that are controlled by U.S. regulations without a license exemption or obtaining any required license; (v) share controlled technical data with foreign nationals (even if done within the U.S. and even if the foreign national is employed by ManTech), without obtaining appropriate Government approvals; or (vi) perform services that are controlled by U.S. regulations for the benefit of certain foreign nationals (even if within the U.S. and employed by ManTech), without obtaining appropriate Government approvals. Seek guidance on export control compliance from ManTech’s Director of Corporate Export Control.

Did You Know?

Controlled Unclassified Information (CUI) is information from our federal government customers that needs to be safeguarded, consistent with applicable law, regulations, and government-wide policies, but is not classified. Our federal customers are adopting a recently established program for managing CUI across the Executive branch and ManTech has established a similar, responsive plan to meet customer requirements and our own internal data protection needs. Like many of the federal agencies we support, ManTech has a policy for identifying, marking, safeguarding, disseminating, and disposing of sensitive information, with procedures for protecting the CUI of our customers as well as sensitive information belonging to ManTech and our teaming partners.

As requirements mature, ManTech’s program will evolve to comply with new controls. Please be alert to circulated briefing and training materials to ensure you are always up to date with requirements for protecting the CUI of our customers as well as sensitive information belonging to ManTech and our teaming partners.
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. We must meet or exceed (and our purely commercial operations must maintain awareness of) all applicable U.S. federal regulatory requirements, with special emphasis on the following requirements:

Time and Expense Reporting (FA 701 & FA 703)

As a professional services contractor, timesheet and expense reporting is a fundamental part of our business. We must understand and comply with ManTech’s timesheet accounting and expense reporting policies and procedures and must accurately prepare, certify, submit and approve these important business documents. All work hours must be accurately recorded on a daily basis and submitted and approved each reporting period. Please raise any questions about how to properly record work activities with your Supervisor or Time Administrator.

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.

Truthful Cost or Pricing Data (CO 202)

The Truthful Cost or Pricing Data Statute requires ManTech to certify accurate, complete, and current cost or pricing data to the Government in certain procurements. Employees supporting the development of new business and proposals must understand and ensure ManTech’s compliance with this Statute.

FAQ

Q: I have been working on two separate projects for the same customer and it has been a challenge to keep track of how much time I spent on each one. Does it really matter, since both projects are for the same customer? Can I just charge half of my hours to one project and half to the other?

A: This is an area where employees must be especially careful; the time you charge to a project must be hours that you actually worked on that specific project. If you can’t recall what you worked on at the end of the day, look through emails and other records to help you reconstruct your workday.

The timesheet you submit and/or approve will serve as the basis for invoicing our customers. Inaccurate timekeeping records that are used to produce invoices for the government can lead to termination, debarment, imprisonment, and large fines.

Never submit or approve time that does not accurately reflect time worked and never charge time worked on one project to another project, even when it is for the same customer.

Always ask questions if you are unsure about how to charge your time or if you feel you’re being asked to record hours in a way that is inconsistent with policy.
Personally Identifiable Information (PII) and Protected Health Information (PHI) (CO 703, HR 401, & IT 102)

ManTech is obliged to protect Personally Identifiable Information (PII) as well as Protected Health Information (PHI) entrusted to us by our employees, consultants and customers. Access, use, transmission and storage of PII/PHI should be limited to authorized business activities and disposal or return of this information should take place in accordance with statutory and contractual requirements. Protect PII/PHI in accordance with ManTech’s policies and procedures and customer agreements. Immediately report any potential data breach to management and ManTech’s Chief Information Security Officer.

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 protect its eligibility to compete for Government contracts. Promptly report potential organizational conflicts of interest to management.

Offering Gifts and Entertainment

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 (including gift certificates, securities, below-market loans, etc.). Avoid giving gifts that others may interpret as an attempt to influence a business decision, even if given after the decision. Always seek advice from the Corporate Compliance Department to clarify the propriety of questionable gifts.

When working with the Federal Government, always consider the customer’s gift policies and whether gifts may be given. The Federal Executive Branch, which covers most of ManTech’s customers, has gratuity regulations that prohibit contractors from giving anything of value to Government employees, other than:

- ManTech advertising or promotional items (generally valued at less than $20, but no more than $50 in aggregate value, annually per federal employee);
- Modest refreshments such as coffee, soft drinks and donuts on an occasional basis; or
- Business-related meals and local transportation having a value of $20 or less per occasion, but no more than $50 in aggregate value, annually per federal employee.

Employees are generally prohibited from extending business courtesies, even of nominal value, to Federal Legislative Branch employees, which includes members of Congress and their staff, or to state or local Government employees. Requests for exceptions must be pre-cleared by the Corporate Compliance Department.

Antibribery, Kickbacks and Gifts 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
Standards of Ethics and Business Conduct

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 Corporate Compliance Department. When gifting is 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 limit ManTech’s ability to hire or use the services of current or former U.S. Government employees. In certain circumstances, even casual or preliminary conversations about the potential for 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. Instruct employment candidates who are now or have been employed by the Government to obtain an Ethics Advisory Opinion letter from the designated ethics official of their current or former Government agency. Ethics Advisory Opinion letters can clarify applicable post-Government employment restrictions.

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 and unethical. Penalties for violations are severe and may 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 foster workplaces that support honesty, integrity, respect and trust.

Equal Employment Opportunity, Non-Discrimination and Non-Harassment (HR 304 & HR 306)
ManTech promotes diversity 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.

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.

FAQ
Q: My supervisor often yells at me and my coworkers, and this makes me very anxious when I am at work. Even though she has never threatened anyone physically, I find her behavior unsettling. Is there someone I should talk to?
A: While each employee has a different idea of what is acceptable, you should voice your concerns. You have the right to work in a professional atmosphere free from harassment and abusive conduct.

ManTech policy HR 304 defines abusive conduct as conduct that a reasonable person would find hostile, offensive, and unrelated to an employer’s legitimate business interests, which can include verbal or physical conduct that a reasonable person would find threatening, intimidating, or humiliating. It can also include the gratuitous sabotage or undermining of a person’s job performance. Keep in mind that the prohibition against abusive conduct is not limited to work hours or the workplace.

Please reach out to the Employee Relations Center or the ManTech Helpline (listed in the Addenda) if you are uncomfortable discussing the matter directly with your supervisor.
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 any form of harassment in the workplace.

ManTech will take prompt action to prevent and, where necessary, discipline employees for behavior that violates these policies. 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).

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 alcohol or controlled substances in the workplace is strictly prohibited.

ManTech is also committed to maintaining a workplace free from violence, threats of violence, harassment, intimidation or other abusive conduct, such as bullying. Employees must 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 IT Equipment Usage (HR 401, IT 100, & IT 101)
ManTech respects the privacy of its employees. Employees who are provided access to personal information about ManTech employees must protect such information in accordance with the law and ManTech policy.

Employees should not expect privacy for personal information they have placed on or in ManTech’s 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 such information and property.

Employees are responsible for ensuring that ManTech’s IT equipment, services and data are used in a professional manner and in accordance with ManTech policy. Protection of ManTech information is of particular importance. Never share log in credentials. Be cautious when opening unsolicited emails and do not click on suspicious links or attachments. When in doubt, contact ManTech’s Security Operations Center.

Remember that social media sites are public forums and postings create permanent records that can be broadly accessed and disseminated. Employee postings should not negatively impact work, the work environment, work resources, business operations, or the reputations of ManTech, its business partners or its customers. Employees must not represent ManTech in any public communication, unless specifically authorized to do so by ManTech’s Corporate Marketing & Communications Department.

No Retaliation (HR 304, HR 306 & CG 403)
ManTech’s policies, Standards and the law protect employees from retaliation for engaging in a protected activity or reporting what they reasonably believe is 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

---

**Did You Know?**
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 by introducing malware through electronic communications. Phishing occurs through a variety of communication methods and can include emails, text messages, phone calls, and social media messages.

Phishing attacks are on the rise; caution and vigilance are required to avoid becoming a victim. With respect to electronic communications:

- Be suspicious of any unsolicited communication, particularly when there are misspelling or anomalies in email or web addresses
- 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 if you are unsure about the legitimacy of the message
- Report suspected phishing scams to CSIRT@mantech.com

By design many phishing communications appear authentic and can be very convincing. Your cautious and vigilant consideration of all communications and requests helps keep our data and resources secure.

Don’t Get Hooked

Phishing attacks are on the rise; caution and vigilance are required to avoid becoming a victim. With respect to electronic communications:

- Be suspicious of any unsolicited communication, particularly when there are misspelling or anomalies in email or web addresses
- 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 if you are unsure about the legitimacy of the message
- Report suspected phishing scams to CSIRT@mantech.com

By design many phishing communications appear authentic and can be very convincing. Your cautious and vigilant consideration of all communications and requests helps keep our data and resources secure.
Standards of Ethics and Business Conduct

good faith. Anyone found to have participated in retaliatory actions against someone 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 can assist employees with 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 14 for more information about the ManTech Helpline).

COMMlITMENT TO OUR TEAMMATES AND SUPPLIERS
We are committed to fair and open dealings with our teammates and suppliers and to the protection of shared sensitive/confidential information, which concerns company, customer, and supplier assets. We extend the protections and obligations of these Standards to our suppliers, as required.

Procurement Policies (CO 502)
ManTech will procure materials, supplies, equipment and services at the lowest reasonable cost from qualified suppliers who are able to 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. Refer to ManTech’s Procurement Manual for guidance on meeting ManTech’s procurement obligations.

Receipt of Gifts and Entertainment (CG 306)
Your business decisions should be based on sound, unbiased judgment. Ensure that interactions with suppliers, customers, competitors, contractors and consultants are in accordance with ManTech’s best interests and policies. Do not ask for gifts and do not accept gifts or other benefits if doing so could affect or appear to affect the objectivity of your business judgment. Only accept an unsolicited gift or business courtesy, including a meal or entertainment, when the item or offering is: (i) customary and a commonly accepted business courtesy; (ii) not excessively valuable; (iii) given and accepted without an express or implied understanding of obligation; and (iv) not a reward for any particular business decision already made or forthcoming. Promptly refuse/return any gift of cash or cash equivalents (including gift certificates, securities, below-market loans, etc.) of any value. Questions about the propriety of a gift or business courtesy, offered or received, should be promptly raised with the Corporate Compliance Department.

No Unauthorized Use of Copyrighted Material (IT 100)
Copyright law prohibits unauthorized copying, so do not make or use any unauthorized copies of software or copyrighted material. Do not duplicate or forward newsletters or other materials (whether by electronic or hard-copy methods) in violation of license and copyright restrictions. Understand and comply with all license and copyright restrictions pertaining to all software and copyrighted material licensed to, purchased by or received by ManTech.

FAQ
Q: The program I support has many subcontractor personnel that work closely with us to meet our contractual mission. Do our subcontractors have to follow our Standards of Ethics and Business Conduct?
A: Our subcontractors are contractually obligated to follow the ManTech Supplier Code of Conduct, or follow their own comparable Code of Conduct. The ManTech Supplier Code of Conduct is based on ManTech’s Standards but is focused on ethical matters that may be encountered as a supplier to ManTech. For ease of access, suppliers can find the ManTech Supplier Code of Conduct on our supplier portal and our internet site. You should expect subcontract personnel to meet or exceed ethical standards that are comparable to what we expect from our employees. Ethical or compliance concerns with a subcontractor or supplier should be reported. Our reporting mechanisms, including the ManTech Helpline, can be used to report a concern with a supplier and are also available to our suppliers so they can report an ethics or compliance concern.
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 our 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. Do not trade the securities of ManTech or any other company based on material, non-public information. Likewise, do not disclose material, non-public information to another person who may use such information in a securities transaction.

Before discussing non-public information about ManTech or another business, please 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.

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. Avoid engaging in personal activities that could impact or appear to impact decisions made on behalf of customers or ManTech. Refrain from collaborating with competing businesses, accepting outside employment with competing businesses, working for companies that have business dealings with ManTech, and investing in competing businesses. Notify management and the Corporate Compliance Department of any potential conflicts of interest.

During ManTech employment, do not engage in any outside business activity that is competitive with ManTech’s business. While employed at ManTech and during the 12-month period following termination of employment with ManTech, do not solicit or induce any current employee of ManTech to engage in employment discussions with a competing business or a company that has business dealings with ManTech. During this same period, do not participate in any bid process for a program or prospective program that is competitive with a bid by ManTech.

Financial Records and Compliance with Internal Controls (FA 101)

It is essential that we record financial transactions using generally accepted accounting principles (GAAP) of the U.S., as well as Government regulations, cost accounting standards, tax laws and the established practices documented in ManTech’s policies 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. Employees with financial reporting responsibilities are also bound by the Financial Code of Ethics, located on page 10 of our Standards.

ManTech is subject to securities laws and regulations, including the statutory and regulatory requirements of the Sarbanes-Oxley Act. Ensure compliance with ManTech’s internal control policies and procedures and the full, fair, accurate, timely and
Standards of Ethics and Business Conduct

understandable disclosure of financial and non-financial developments that could have a material effect on the operations or financial condition of ManTech. Promptly report any information that could have a material effect on the operations or financial condition of ManTech to the controller, the CFO, the Group President, the COO or the CEO.

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 ManTech is permitted to destroy such documentation as a result of a settlement, resolution or other final closure of the matter, as directed by the Corporate Legal Department.

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 any 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 not as a representative of ManTech. Do not make personal political contributions to obtain or retain business or to obtain any other improper advantage for ManTech.

Implementation Of Our Standards

Report Suspected Wrongdoing (CG 305, CG 403 & CO 310)
Every ManTech employee has an affirmative duty to report any actual or suspected violation of our Standards or policies. Therefore, if you have a reasonable basis for suspecting that a ManTech employee has violated or is violating our policies or Standards, you should promptly report your concerns to your supervisor or any ManTech manager. You may also report your concerns 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 Directors. Alternatively, employees may ask members of management 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 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” addenda. ManTech encourages employees to bring forward concerns and prohibits
ManTech’s Response to Your Concerns

All concerns reported in good faith and with sufficient detail will be evaluated and, as appropriate, investigated to determine whether a violation of our policies or Standards has occurred. 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 and executive officers may only be made by the Board of Directors or the Audit Committee of the Board and will be promptly disclosed if required by law.

No Rights Created

Our Standards are a statement of the fundamental principles and key policies and 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 practices and procedures but are not designed to cover every issue that can arise. They are intended to provide an overview and guidance on how to resolve questions about the appropriateness of your own conduct or the conduct of your coworkers. Policies cited in our Standards can be found on the ManTech intranet along with additional policies and 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, you should seek advice from one of the sources referenced in the Addenda 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 Group Presidents, the Chief Financial and Chief Accounting Officer and other employees with financial reporting responsibilities.

ManTech’s filings with the Securities and Exchange Commission must be accurate and timely. The Chief Executive Officer, the Group Presidents, the Chief Financial Officer, the Chief Accounting Officer, senior business operations personnel and any other employees involved in the financial reporting process 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 reinforce and add to the concepts set forth in our Standards. Specifically, you must agree that you will at all times:

- Act ethically, avoiding actual or apparent conflicts of interest.
- Provide and/or prepare information in a manner and of a quality to ensure the full, fair, accurate, timely and understandable disclosure of information in ManTech’s public communications, including the reports and documents that ManTech files with, or submits to, the Securities and Exchange Commission.
- Comply with financial reporting rules and regulations of federal, state, provincial and local governments and other appropriate private and public regulatory agencies.
- Act in good faith, responsibly, with due care, competence and diligence in the preparation of all financial information, without misrepresenting material facts or allowing your independent judgment to be compromised.
- Honor and protect the sensitive, restricted and personal information acquired in the course of your work, except when authorized or otherwise legally obligated to disclose such information. Sensitive, restricted and personal information acquired in the course of your work must not be used for personal advantage.
- Ensure the responsible use of and control over all assets and resources that you control.

Violation of this Financial Code of Ethics, including failure to report potential violations by others, is a serious matter that may result in significant disciplinary action, up to and including termination of employment with ManTech. If you believe a violation of this Financial Code of Ethics has occurred, you should contact the Corporate Compliance Department, the Corporate Legal Department or the ManTech Helpline. Alternatively, you may contact the Chairman of the Audit Committee of the Board of Directors through the ManTech Helpline.

**Did You Know?**

Integrity is often defined as the quality of being honest, virtuous and trustworthy, but this definition now includes reliability. This is particularly true when we think of structural integrity or the integrity of a system or process.

In both customer-facing, mission critical support as well as in ManTech back office systems and processes, ManTech is engaged in numerous activities that demand strict adherence to established procedures and protocols to ensure the reliability of process and output. Procedures and process are designed to mitigate risk and ensure reliability. These processes and controls help achieve compliance. In doing so, they must also achieve efficiency.

So, if you have a suggestion to improve a process or better mitigate a risk, please speak up! We are counting on you to make a difference. And we are counting on you to faithfully execute your control and process responsibilities; with integrity.
ACKNOWLEDGEMENT FORM

I hereby represent to ManTech that:

• I read and understand ManTech’s Standards of Ethics and Business Conduct.

• I will comply with the policies set forth in ManTech’s Standards and will report all suspected violations of ManTech’s Standards.

• I reported all suspected violations of ManTech’s Standards now known to me.

• (for Directors, Officers and BUGMs only) I reported in writing to the 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 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.
ADDENDA

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)
  Joe Kraus – (703) 610-9372

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
  David Roll, Senior Vice President and Chief Compliance Officer (703) 218-6426
  Sejal Patel, Senior Executive Director of Compliance (703) 259-3655

- 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
  Michael Tillison, Senior Vice President of Corporate Security (703) 218-6494

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 reports of violations of our Standards or policies. The ManTech Helpline also provides you with the option of asking a question and getting an answer from the appropriate resource. At your election, your report or question may be kept anonymous. However, providing your name may improve or expedite ManTech’s investigation of your report. 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:
Visit www.mantech.ethicspoint.com; or click the Compliance & Ethics tile on MyHUB to access the ManTech Helpline.

2018 | 14
Tomorrow’s Technology
Timeless Values

ManTech
Securing the Future

2251 Corporate Park Drive, Herndon, Virginia 20151
www.mantech.com