ManTech®
Securing the Future

2025 Standards of Ethics and Business Conduct

ManTech
Securing the Future

Message From ManTech's Chief Executive Officer and President

Colleagues,
ManTech's success over the last five decades is a direct result of the high ethical standards, dedication and values that our employees have consistently demonstrated while providing innovative technology and mission-focused solutions to our clients. The outstanding reputation ManTech enjoys today with clients, teammates and competitors rests on our steadfast 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. The Standards are the framework of our business culture, which is based on uncompromising integrity and ethical behavior — key differentiators in today's intensely competitive marketplace.

As a ManTech employee, you play a central role in distinguishing our company as a highly ethical, trustworthy and reliable business partner and an innovative industry leader. No matter how the world around us may change, ManTech's values remain grounded in truth, integrity and caring for each other and the mission. You play an important role in maintaining a professional work environment by treating one another with fairness and respect, so each of us can thrive.

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

We are proud of the contributions you make every day and how your work serves our clients, stakeholders and our great nation. Thank you for your commitment to doing what's right by exemplifying the highest level of conduct with uncompromising integrity and ethics.

Matthew Tait
CEO and President

The Foundation of our Standards

OUR MISSION

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

OUR VISION

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

OUR VALUES

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

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

Table of Contents

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

ManTech
Securing the Future

PolicyTech

Policies & Procedures

Select Policies & Procedures (P&P) are referenced and linked in the Table of Contents here and throughout ManTech's Standards of Ethics and Business Conduct. All ManTech P&Ps can be found on our PolicyTech site, which can be accessed through one.mantech.com by selecting the PolicyTech tile. The full set of P&P is organized on this site by Functional Area, which makes it a great place to start when you are looking for answers. You can also browse by popular topics or specific job roles.

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

Lead from the Front

Managers hold an important role and have a wide variety of responsibilities at ManTech. We count on our leaders to promote a strong culture of ethics and maintain a positive workplace environment. Be sure to:

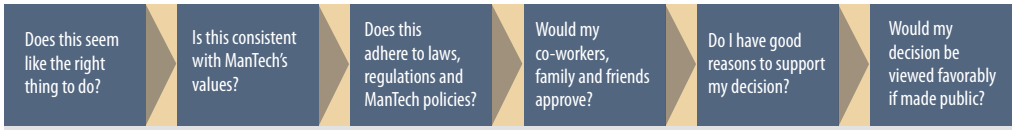
- **Engage with your team – know what,they are working on and provide clear direction.**
- **Develop trust – follow through on promises you make and demonstrate ethical decision making.**
- **Set a good example – model the behavior you want to see and motivate those around you.**
- **Be visible – turn on your camera or show up in person for higher quality interactions and expect the same, when feasible.**
- **Communicate clearly – make sure your team knows what to expect from you and what you expect from them.**
- **Demonstrate accountability – own your responsibilities at work and admit mistakes, and expect the same from your team.**
- **Keep an open door policy so that your team is comfortable raising concerns.**
- **Appreciate those that have the courage to come forward with concerns and know that ManTech has zero tolerance for retaliation.**

OUR STANDARDS

Built on the foundation of our strong corporate values and commitment to integrity in our business practices. Our Standards of Ethics and Business Conduct (Standards) serve as an important resource for decision making guidance. Our Standards emphasize ManTech's principles and describe how employees are expected to conduct business honestly, ethically, and respectfully by:

- Disclosing of personal and professional relationships that could result in a conflict of interest.
- Diligently and accurately recording time worked.
- Promptly reporting potential non-compliances, violations of these Standards, and related concerns.
- Valuing our differences and treating one another with respect.
- Making complete, accurate, and timely disclosures of non-compliances or related concerns.
- Complying with applicable policies, laws, regulations, and requirements.

When making a tough decision, consider:



A good decision will allow you to answer "yes" to all of these questions. If you need help, reach out to Enterprise Compliance or ask a question through ManTech's Helpline.

Managers have additional responsibilities and must shape company culture by modeling professional behavior and building an environment of trust and ethics within their organization and across the enterprise. Our success depends on the success of our managers' dedication to promoting team environments where compliance is expected, and ethical behavior is the norm. Managers are responsible for maintaining a workplace where employees feel comfortable raising concerns.

COMMITMENT TO NATIONAL SECURITY

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

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

As a ManTech employee, you are required to protect classified Government information and other forms of sensitive Government information. Uncompromising security is crucial to the success and safety of our clients and our nation. In support of this obligation, do not download any classified Government information or other forms of sensitive Government information to any storage media or to a non-ManTech printer. Be observant and 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 Enterprise Security Department. And promptly raise questions about security procedures and concerns to a facility security officer or the Enterprise Security Department.

Personnel and Physical Security (SC 100, & SC 300)

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

Cyber Security and Insider Threat (IT 200 & SC 100)

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

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

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

International Trade Compliance (CO 801)

Exports and imports of technical data, technology, defense services, defense and dual-use articles, are controlled by US Government laws and regulations. This means that: (i) ManTech may not export or import goods to or from any country that is subject to a U.S. trade embargo; (ii) ManTech may not export or import goods to or from individuals or organizations identified on lists of prohibited trade parties published by the U.S. Government; (iii) ManTech may not export goods for an end-use prohibited by US laws and regulation; (iv) ManTech may not export or import goods that are controlled by U.S. laws and regulations without first obtaining the required export/import authorization; (v) ManTech may not share controlled technical data or technology with foreign nationals

ManTech
Securing the Future

Technology Use and Data Protection

Constant vigilance is required to take advantage of AI technologies while protecting sensitive, proprietary, controlled unclassified (CUI) and classified information that belongs to ManTech, our clients, and our competitors.

Remember that you must:

- **Seek pre-approval to use AI tools and follow policy IT 116 - Generative Artificial Intelligence policy.**
- **Carefully validate the output and results generated by AI tools for accuracy.**
- **Maintain human accountability and control.**
- **Adhere to copyright laws.**
- **Understand and comply with ManTech and client policies for the handling of sensitive, controlled unclassified information (CUI) or classified documents.**
- **Do not bring to ManTech or otherwise disclose or make use of proprietary information from previous employers or other third party sources.**

Help protect ManTech's information and that of our clients by staying alert and reporting concerns to Security at 887-996-4248 or CSIRT@mantech.com.

Workplace Responsibilities

Regardless of where you work from, please ensure you always:

- **Record the time you work on each ManTech project and work the time you record.**
- **Disclose outside employment and ensure you are only recording productive time spent on ManTech work.**
- **Be truthful, ethical and transparent.**
- **Perform sensitive work in a separate space.**
- **Follow ManTech's Operational Security (OPSEC) Guidelines when accessing ManTech's computer systems.**
- **Seek participant approval before recording meetings.**
- **Comply with ManTech's Remote Work Policy and agreements, as applicable.**
- **Protect data belonging to ManTech, our teammates and our clients.**
- **Show respect in your interactions and communications with others.**

If you have questions, please get answers from the appropriate ManTech representative listed on the Addendum located on page 13.

(to include foreign national employees) without first obtaining the appropriate export authorization; (vi) ManTech may not perform services that are controlled by U.S. laws and 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 the appropriate export authorization; and (vii) ManTech may not respond to a boycott request, including furnishing information in response to such request or taking steps to comply with such a request, unless determined by International Trade Compliance that such a request does not violate antiboycott regulations. Export and import regulations are complex, so always start by seeking guidance from ManTech's Executive Director of International Trade Compliance at exports@mantech.com.

Information Technology Resource Use During International Travel (IT 112)

If you hold a security clearance, contact the Security Office both before and after any you travel outside the US. Regardless of whether you hold a security clearance., Iif you are planning to travel outside the US for any reason with ManTech IT resources or IT resources that contain ManTech or client information, contact the IT Department to arrange for the use of a loaner device before you travel. Please get answers to your questions about export control before you travel by asking ManTech's Executive Director of Export Compliance at exports@mantech.com.

COMMITMENT TO OUR CLIENT

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

Accurate Reporting and Records (FA 701 & FA 703)

As a professional services contractor, timesheet accounting and expense reporting are fundamental obligations of our business. It is critically important that time worked and expenses incurred are diligently and accurately recorded. Inaccurate records can have serious business and legal consequences for the Company, and ManTech takes its obligations seriously. For these reasons, failure to accurately record time and expenses can lead to disciplinary action, up to and including termination of employment.

You are responsible for understanding and complying with ManTech's timekeeping policy and procedures. Record all of your productive worked hours accurately and do so on a daily basis. Promptly submit your timecard for approval each reporting period. Accurately complete and promptly submit expense reports to your supervisor or a Time/Travel and Expenses Administrator. If you have the additional responsibility for reviewing and approving timecards and/or expense reports, closely monitor the time worked and/or the expenses claimed by your team. Always require timely corrections of any inaccurate submissions.

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

Organizational Conflict of Interest (CO 701)

The Government can prevent a contractor from competing for, receiving, or performing a contract when a contractor's 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 our ability to properly assess and mitigate a potential conflict, and to protect ManTech's eligibility to compete for Government contracts. Watch for and promptly report potential organizational conflicts of interest to management.

Truthful Cost or Pricing Data (CO 201 & CO 502)

The Truthful Cost or Pricing Data Statute (formerly known as the Truth in Negotiations Act) requires ManTech to submit certified cost or pricing data for procurements that exceed the Truthful Cost and Pricing threshold and do not qualify for any exceptions. If you are involved with supporting the development of new business and proposals, you are responsible for understanding and ensuring ManTech's compliance with this Statute.

Personal Information (PI) and Protected Health Information (PHI) (CG 308, CO 703, HR 401 & IT 102)

ManTech is obliged to protect the Personal Information (PI) and the Protected Health Information (PHI) entrusted to us by our employees, consultants and clients, so you must always: (i) limit access, use, transmission and storage of PI/PHI to authorized business activities and equipment; (ii) manage and protect PI/PHI in accordance with ManTech's Policies & Procedures and client agreements; and (iii) immediately report any potential or actual data breach to management and ManTech's Chief Information Security Officer.

Procurement Integrity and Antitrust (CG 311, CO 100 & CO 502)

ManTech must compete fairly and ethically for all business opportunities. Possession or use of a competitor's rates, a competitor's sensitive/proprietary information or the Government's source selection information can compromise the integrity of the procurement process and may violate the law. Challenge the source of any competitive intelligence that appears to be (i) the proprietary or confidential information of a competitor, (ii) suspicious, or (iii) inappropriately obtained or possessed. Never enter into an agreement with another business that would improperly limit competition. Never engage in bid rigging, price fixing, market division or allocation schemes, group boycotts, or any other anti-competitive conduct. Carefully consider topics for discussion at industry and trade events, and limit teaming to areas of cooperation that are required to perform a single bid together.

Offering and Accepting Gifts and Entertainment (CG 309 & CO 502)

Employees with decision-making authority are subject to stringent restrictions and are generally prohibited from accepting gifts. Keep in mind that offering and accepting gifts can create the appearance of impropriety or conflict of interest (e.g., an attempt to influence a business decision). To avoid the potential for such problems, every offer or acceptance of a gift, meal, entertainment (e.g., sporting event or outing, concert, etc.) or other accommodation made to or offered by a non-ManTech employee in connection with ManTech business must be professional in nature, infrequent, and not excessive in cost.

Do:

- ✓ Consult ManTech's Gifts and Entertainment policy.
- ✓ Stay within gift threshold limitations.
- ✓ Keep in mind that more stringent rules exist for Procurement professionals and decision-makers.
- ✓ Ensure gifts are received and given in an appropriate business setting.
- ✓ Reach out to Enterprise Compliance for guidance if you are unsure of what can be given or accepted.

Don't:

- x Give or accept cash or other cash equivalents.
- x Solicit business courtesies with monetary value.
- x Accept or offer a gift that could impair your impartiality or appear to create a conflict.
- x Accept or offer gifts frequently to/from the same company or individual.
- x Violate applicable laws or ManTech policies.

Organizational Conflict of Interest

An Organizational Conflict of Interest (OCI) can exist whether ManTech is the prime or just a subcontractor. Even the potential of an OCI can prevent ManTech from working on other contracts. The common bases for OCIs are:

- **Unequal Access to Information;**
- **Impaired Objectivity; or**
- **Biased Ground Rules.**

Consider these examples of potential OCIs:

- **ManTech has client-authorized access to nonpublic information as part of its performance on a Government contract (e.g., information on the client's cost estimate for an award), which could provide a competitive advantage in a future procurement (Unequal Access to Information).**
- **In accordance with a Statement of Work, ManTech evaluates services or solutions provided by ManTech (or an affiliate) on a different Government contract (Impaired Objectivity).**
- **ManTech develops evaluation criteria, specifications, or requirements, and plans to submit a proposal to perform the requirements (Biased Ground Rules).**

Remember that initial reviews of new opportunities are usually the best time to identify actual or potential OCIs. Contractors cannot simply "mitigate" all OCIs—performing some types of work can prevent the Company from pursuing other opportunities, including larger, more lucrative future contracts. It is also important to watch out for OCI issues associated with on-contract growth. Just like new business opportunities, on-contract growth can introduce new responsibilities that can present OCI issues.

Hiring Discussions

Working closely with current or former Government employees requires awareness of the restrictions that apply to hiring discussions. Hiring managers, recruiters and others engaged with potential candidates for ManTech employment must consult with Human Resources before engaging in any employment-related conversations with current Government employees.

Be mindful that:

- **Even preliminary, high level, or casual conversations with current Government employees about employment opportunities with ManTech can create legal risk to the individual and the Company.**
- **An Ethics Advisory Opinion letter for each current and former Government employee should be obtained, reviewed and cleared before having employment conversations with current and former Government employees.**
- **Hiring restrictions may also apply to family members of Government employees.**
- **Penalties for violating these restrictions may include suspension, debarment, civil fines, and criminal penalties, (including imprisonment).**

Be sure to contact HR when the situation arises and familiarize yourself with ManTech's HR 102 - Hiring and Contracting with Current and Former Government Employees policy.

It must not include any cash or cash equivalents (e.g., no gift certificates, no securities, no below-market loans, etc.) and must be compliant with applicable laws as well as the policies of ManTech and the other party. Always consult ManTech's Gifts and Entertainment policy and seek advice from Enterprise Compliance before offering or accepting a gift that does not clearly satisfy each of these requirements.

Be aware that gifts can come in many forms (e.g. golf outings, football/basketball games, airfare or hotel accommodations, dinner cruises, happy hour, conference registration fees, gift cards, etc.). When accepting or giving a gift of any kind, think about how others might view the offer or receipt of the gift.

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

Any form of bribery is strictly prohibited. It is unlawful to offer anything of value to a U.S. Government client or employee in return for favorable treatment on a contract or subcontract. Similarly, the U.S. Foreign Corrupt Practices Act (FCPA) prohibits ManTech and its employees and agents from giving anything of value, directly or indirectly, to a foreign official, a foreign political candidate, or a foreign government to influence business. Most foreign countries also prohibit gifting to government officials or government entities; even though the customary business practice in such countries is to exchange gifts. When gifting is both necessary and permissible, only ManTech (the company, not you) 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. All plans for gifting to foreign persons or entities are subject to pre-approval by the Chief Compliance Officer. Only plans for gifting to foreign persons or entities deemed necessary and permissible by the Chief Compliance Officer will be approved for action.

Hiring Current and Former Government Employees (HR 102)

Federal regulations strictly limit ManTech's ability to hire or use the services of current or former U.S. Government employees and their family members. Even casual or preliminary conversations about potential employment with ManTech can violate these regulations. Always obtain permission from Human Resources before engaging in any employment discussions (even casual or preliminary) with current or former employees of the U.S. Government. Require prospective candidates 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 are essential to ManTech's understanding of the post-Government employment restrictions that apply to candidates who are now or have been in Government service.

Combatting Trafficking in Persons (HR 105)

Trafficking in persons is a crime that involves compelling or coercing a person to provide labor or services, or to engage in commercial sex acts. The coercion can be subtle or overt, physical or psychological. Report suspicions of any such activity through the ManTech Helpline and ManTech will ensure that the Inspector General for the appropriate agency is promptly notified of all credible information. Reports may also be made directly to the National Human Trafficking Hotline at 1-888-373-7888.

COMMITMENT TO OUR EMPLOYEES

We are all responsible for contributing to the development and maintenance of a workplace environment that is free from unlawful discrimination and harassment and that does not infringe upon protected rights. Supervisors and managers have a heightened

responsibility for setting good examples and fostering workplaces that are diverse, inclusive, and respectful.

Workplace Conduct (HR 403)

At ManTech, we understand and appreciate the contributions that each employee makes to ManTech's culture. You are expected to help promote respectful and productive work environments. Always demonstrate positive and courteous behavior, make decisions with honesty and integrity, be responsible and reliable, understand the duties and expectations of your role, and be professional and productive. Be mindful that your actions can influence others and can impact the quality of work environments. Remember that employees like you make ManTech a great place to work.

Equal Employment Opportunity, Non-Discrimination and Harassment-Zero Tolerance (HR 303, HR 304, HR 306 & HR 404)

ManTech values and promotes diversity and inclusion and is an equal employment opportunity employer. We do not tolerate discrimination on the basis of race, color, sex, religion, creed, 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 protected status.

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

ManTech will take prompt action to prevent and correct conduct that violates ManTech's Policies & Procedures. Report all suspected discrimination or harassment by anyone (whether employee, consultant, vendor, or client) to management, the Human Resources Department and/or the ManTech Helpline, regardless of who is involved. ManTech will protect reporters who raise concerns of suspected discrimination and/or harassment from retaliation.

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

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

ManTech is also committed to maintaining a workplace free from violence, threats of violence, harassment, intimidation, or other abusive conduct, such as bullying. The unauthorized possession of weapons in the workplace is strictly prohibited. If you witness or hear about any threats or any violence in the workplace, promptly report this information to Security.

Maintaining a safe work environment also means adhering to Environmental, Health, and Safety (EH&S) laws, regulations, and company guidance. Employees can find Safety Guidelines and additional information on ManTech's Inside site. Be vigilant and deliberate in your efforts to comply with these guidelines and bring safety concerns to the attention of management immediately.

Respectful Communications

ManTech works hard to promote a diverse and welcoming workplace where we value one another's opinions, perspectives and contributions. Help maintain a respectful work environment by doing the following:

- **Think about how your words and actions may by perceived by others before you speak or act.**
- **Listen to what others have to say and aim to understand them.**
- **Be mindful of how your communications can come across to others and be especially mindful when using online communications.**
- **Act in ways that foster inclusive work environments and show appreciation for the value of differing opinions.**
- **Take responsibility for our actions and guard against making impulsive, negative assumptions—assume good intent.**
- **Be kind, truthful and transparent.**

Gift Giving and Receiving

Appearances Matter!

The rules governing gift exchanges with Government employees are very strict. When giving and accepting gifts, the circumstances and appearances matter. Gifts should never be given to influence or win business, must be professional in nature, infrequent and not excessive in cost, and not in the form of cash or cash equivalents. ManTech's policy on gifts explains permissible gifts, value thresholds, and additional restrictions. All gifts must be compliant with applicable laws as well as ManTech's Policies & Procedures and the rules of the receiving/giving party.

Decision makers must be particularly vigilant, and all employees must remember that tickets to events and coverage of other entertainment expenses likely exceed the gifts threshold and may not be accepted or given by ManTech employees. Procurement professionals and employees conducting business with the government or foreign entities are subject to additional restrictions and must consult with Enterprise Compliance for guidance.

Employee Data Privacy and Protection (HR 401)

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

Information Technology Use (IT 100, & IT 116)

ManTech may provide its employees and trusted parties with IT resources, including access to ManTech computing systems for use with the performance of legitimate ManTech business activities. With these IT resources, there is no expectation of privacy for personal information and personal property that employees and trusted parties may choose to store on ManTech's IT resources. ManTech reserves the right, for legitimate business reasons, to retrieve and inspect personal information and property, which employees and trusted parties store on ManTech IT resources.

Always use ManTech IT resources, services and data in a professional manner and in accordance with ManTech policy. Always act deliberately to help ensure the protection of ManTech's business resources and information. Do not use file sharing sites without first obtaining the express approval of Enterprise IT. Only use Generative Artificial Intelligence (AI) tools that have been pre-approved for your use by ManTech's Chief Information Officer. Remember to carefully review and validate any results generated by AI for accuracy and protect sensitive, classified, privileged, and proprietary information.

Never share log-in credentials with others. Cautiously consider the propriety of unsolicited emails and do not click on suspicious links or attachments. Be cautious with emails and texts from unknown sources as well as sources that seem familiar but appear to be imitations or variations of regular contacts. Watch for message content with unexpected language usage, grammatical errors, or formatting problems. Vigilance and caution are key, so always report doubts about the source or authenticity of a message, a link, or an attachment to ManTech's Security Operations Center at spam@mantech.com *before* you click.

Social Media and External Communications (IT 101)

Remember that social media sites are public forums and postings on these sites create permanent records that can be broadly accessed and disseminated. So, do not share any classified, sensitive, confidential, or proprietary information regarding ManTech or its clients. Do not post anything discriminatory, harassing, bullying, threatening, defamatory, or unlawful. And don't post content, images, or photos without proper authorization from the rightful owners. Always abide by ManTech policy and Government regulations, which prohibit the use of specific social media sites (e.g., TikTok) on devices used to conduct business for the Government. Always be respectful in your communications.

Only designated ManTech spokespersons are authorized to speak on behalf of ManTech in social media and public communications. Promptly refer all media contacts to ManTech's Enterprise Marketing & Communications Department. Do not represent ManTech in any public communication, unless you have specific, prior authorization from ManTech's Enterprise 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 Enterprise Marketing & Communications Department at EnterpriseCommunications@mantech.com.

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

ManTech prohibits retaliation against employees who ask questions, raise concerns, make complaints, participate in investigations, refuse to participate in suspected wrongful actions, report potential non-compliances, or otherwise exercise workplace rights protected by law (i.e. engage in Protected Activity). Retaliation includes any adverse action taken against an employee because the employee engaged in protected activity. ManTech prohibits retaliation in all cases, even if an investigation does not confirm the concerns raised, as long as the employee did not knowingly make a false allegation, provide false or misleading information in the course of the investigation, or otherwise act in bad faith. Any ManTech employee who retaliates against an employee who engaged in Protected Activity found to have engaged in retaliation will be subject to disciplinary action, up to and including termination.

ManTech counts on its employees to report potential non-compliances and is committed to protecting employees who do so. Employees who have concerns about retaliation should promptly report any such concerns to Human Resources, Enterprise Compliance, the ManTech Helpline, or the Inspector General. The ManTech Helpline is hosted by a third-party, which accepts reports of potential violations online or by telephone, and anonymously, if desired (see page 13 for more information about the 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, client, and supplier assets. We extend the protections and obligations of our Standards to our suppliers, as required.

Procurement (CO 502)

ManTech will procure materials, supplies, equipment and services from qualified suppliers that can meet delivery schedules and other procurement requirements. We ensure competition among potential suppliers, and we do so by following applicable Government regulations and contractual requirements, including those pertaining to small and small disadvantaged businesses. Suppliers are required to follow ManTech's Supplier Code of Conduct (or a sufficiently comparable code of conduct of their own). Refer to ManTech's Procurement Manual for guidance on meeting ManTech's procurement obligations.

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

No Unauthorized Use of Copyrighted Material (IT 100)

Copyright law prohibits unauthorized copying. The owner of copyrighted materials controls the right to make copies. Employees may not make unauthorized copies of software or copyrighted documents and may not 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 restrictions pertaining to software and other forms of copyrighted material licensed to, purchased by, or received by ManTech.

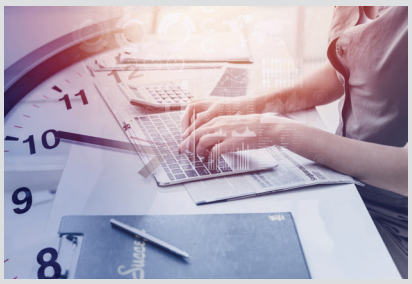
International Business and Travel

If you travel or conduct international business for ManTech, you must be aware of relevant laws/regulations and policies that can impact your work. And you must comply with certain restrictions on traveling overseas with ManTech's Information Technology equipment. Export Compliance (International Traffic in Arms Regulations (ITAR) and Export Compliance (International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR).

- **Through the ITAR, the EAR and other regulations that govern exports, the U.S. Government controls the exportation of sensitive equipment, software, and technology to protect our national security interests and foreign policy objectives. Always check with ManTech's Export Group before you export.**
- **Employees who travel internationally are responsible for understanding applicable travel requirements and export control responsibilities before traveling internationally.**
- **If you have questions, please contact the Export Group at exports@mantech.com.**

Foreign Corrupt Practices Act (FCPA)

- **Enhanced diligence of non-U.S. agents, consultants, and third-party representatives associated with foreign vendors with favorable results is required before ManTech may engage with such foreign persons and businesses.**
- **Before any gift, entertainment, or travel accommodation may be provided to a foreign official, an accurate description of plans must be submitted to Enterprise Compliance for review and, if compliant, pre-approval.**



Personal Conflict of Interest

A conflict of interest can exist when you participate in outside activities that could influence your professional objectivity in the performance of your job duties. Your outside activities can also conflict with programs supported by other ManTech employees in other parts of ManTech's operations.

Here are a few examples of outside activities that could impact your objectivity in making business decisions for ManTech or ManTech's clients:

- **Working a second job.**
- **Owning, operating, consulting, or performing services for another business.**
- **Serving on the advisory board of a vendor, teammate, competitor, or client.**
- **Maintaining close relations with a person who has ties to a vendor, teammate, competitor, or client.**
- **Holding a financial interest in a vendor, teammate, competitor, or client.**
- **Offering or accepting gifts/ entertainment that could influence a business decision.**
- **Consult ManTech's CG 306 – Personal Conflict of Interest Policy and Procedure for additional information. Remember that you are required to disclose *any* other employment (i.e. a second job) as well as other potential sources of Conflicts of Interest to Enterprise Compliance *before* you pursue such opportunities. Disclosures should be made to Enterprise Compliance.**

COMMITMENT TO OUR STAKEHOLDERS

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

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. While subpoenas, legal proceedings, audits or investigations are pending, preserve relevant records unless and until the Legal Department determines that such records may be destroyed as a result of a closure of the matter.

Financial Records and Compliance with Internal Controls (FA 101)

Financial transactions must be recorded in accordance with US Generally Accepted Accounting Principles (GAAP), 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.

ManTech follows internal control procedures to help ensure the full, fair, accurate, timely and understandable disclosure of financial and non-financial developments that could have a material effect on ManTech's operations or financial condition. Promptly report information that could have a material effect on the operations or financial condition of ManTech to the Chief Executive Officer, the Chief Financial Officer, the Chief Performance Officer, the Chief Accounting Officer, or any of the Sector General Managers.

No Insider Trading

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 any 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 a business, always be careful to 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 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 a candidate, campaign, political party, political committee, or legislative initiative without the prior approval of the Legal Department. Individual participation in the political process and individual campaign contributions must be made on an individual basis and never as a representative of ManTech. Don't make political contributions to obtain or retain business or other improper advantage for ManTech.

Conflict of Interest (CG 306)

A conflict of interest exists when financial interests, personal activities or relationships interfere with the objective performance of job duties for a client or ManTech. Personal relationships with vendors, teammates, or competing businesses can impact or appear to impact decisions made on behalf of clients or ManTech. Each employee owes a duty of

loyalty to ManTech and must refrain from assisting or establishing competing businesses through outside employment, provision of consulting services, or investment in such competing businesses. Remember that a conflict of interest can stem from a second job, a Board position, personal, employment, or financial relationships and interests, gifts (including travel, stocks, real estate, etc.), and other circumstances that can impact the employee's ability to remain impartial. Time charged must be productive hours worked on behalf of ManTech for a business purpose. Potential and actual conflicts of interest must be promptly disclosed to Enterprise Compliance for review.

IMPLEMENTATION OF OUR STANDARDS

Report Suspected Wrongdoing (CG 305, CG 403, & CO 304)

Compliance with our Standards and ManTech's Policies and Procedures is an essential requirement of your employment with ManTech. Every ManTech employee has an affirmative duty to report any actual or suspected potential non-compliance with or violations of law, regulations, contract requirements, our Standards, or ManTech's Policies & Procedures. You must promptly report any suspected potential non-compliances or violations to a supervisor or ManTech manager, Human Resources, Enterprise Compliance, or the ManTech Helpline.

Timecard fraud, false claims, other fraud matters, conflict of interest, bribes, gratuities or other questionable activity can lead to significant penalties or liability and severely impact ManTech's reputation and ability to work with the Government. Employees must promptly report the suspected violation. ManTech will not retaliate against any individual who makes such a report without fear of retaliation. These potential non-compliances include concerns about both internal non-compliances, such as violations of accounting practices, internal controls, or audits, as well as external non-compliances, such as potential violations of the Federal Acquisition Regulation (FAR) or other regulations directly to the federal agency's Inspector General pursuant to the whistleblower provisions or call the Department of Defense (DoD) Hotline at 800-424-9098.

Employees must report potential non-compliances or violations to the ManTech Helpline, a supervisor, members of management, Compliance, or the Audit Committee of the Board of Directors.

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

For additional questions, 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. Additionally, our Standards are publicly available and are also posted internally for your ease of reference.

ManTech's Response to Your Concerns

ManTech counts on and encourages employees and teammates to report concerns. All concerns reported will be thoroughly investigated, evaluated, and reviewed to determine whether a violation of our internal policies or external requirements has occurred. Reviews will be objective, fair, timely and are kept confidential to the greatest extent possible. If a violation has occurred, ManTech will take responsive corrective and disciplinary action. Do not conduct preliminary investigations on your own because such independent action can compromise the integrity of evidence and the validity of subsequent investigation by ManTech. Please report any concerns you have to a supervisor or manager, Human Resources, Enterprise , Compliance, or the Audit Committee of the Board of Directors.

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 questions and get answers. If you elect to file your report or raise your questions anonymously, be mindful that the level of detail you provide can impact ManTech's ability to understand and review or respond to your concerns. The ManTech Helpline is available to you by phone or internet:

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

Outside the U.S. or Canada:
See ManTech's helpline homepage for international dialing instructions.

Online:
Visit www.mantech.ethicspoint.com; or the Compliance & Ethics Inside page to access the ManTech Helpline.

Reporting Concerns Process

STEP 1
Speak Up

We value your willingness to report concerns and encourage you to reach out to:

- Human Resources
- Compliance
- Legal
- Management
- ManTech Helpline

STEP 2
Review

Your concerns will be taken seriously and treated confidentially. Reports will be directed to one of the teams listed for prompt review:

- Compliance/Internal Audit
- Human Resources
- Security

STEP 3
Investigation

You may be contacted by the investigator so they can obtain additional information. If you filed your report anonymously, please use your "report key" to check for follow up questions.

STEP 4
Corrective Action

If a violation has occurred, ManTech will take corrective and/or disciplinary action. This may include termination of employment or the potential loss of security clearance.

STEP 5
Determination

You will be notified as to whether the case was substantiated and the case will be closed out. Due to privacy concerns, it may not be possible to share details of the case with you.

Waivers of our Standards

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

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, customer, supplier, competitor, 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. The ManTech Policies & Procedures referred to in our Standards can be found on the ManTech intranet along with additional Policies & Procedures that govern many of the topics in our Standards. If you become aware of an issue that cannot be resolved through application of this guidance or you have questions about the application of this guidance, promptly seek answers from one of the sources referenced in the Addendum that follows.

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 potential non-compliances with or violations of law, regulations, contract requirements, policies, or ManTech's Standards.
- I have reported all potential non-compliances or violations of law, regulations, contract requirements, policies, or ManTech's Standards known to me today.
- (For Directors, Officers and Sector General Managers 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 Sector General Managers within the last five (5) years, in connection with a federal contract that resulted in a conviction or finding of fault.

_____
Your printed name

_____
Your employee ID number

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

_____
Your primary work site or location

_____
Your signature

_____
Today's date

* Paper forms are only accepted when online completion is not possible. Paper filers must execute and email this form to enterprise.compliance@mantech.com.

ADDENDUM

SOURCES OF HELP WITH RESOLVING YOUR QUESTIONS OR CONCERNS

Local and Sector Management Contacts

Your local management and Human Resources representatives are often an excellent starting point for resolving questions and concerns. In addition, your Sector General Managers or Operations Compliance Officers are available to assist you.

Contacts for Company-Wide Resources

The following resources are available to assist in your understanding of our Standards and reporting of issues and concerns. Individual contact information can be found on ManTech's Compliance & Ethics intranet site by clicking **HERE**.

Enterprise Compliance

Chief Compliance Officer
Senior Officer of Industry Compliance
Email: enterprise.compliance@mantech.com

International Trade Compliance

Executive Director of International Trade Compliance
Email: exports@mantech.com

Finance Matters

Chief Financial Officer
Chief Accounting Officer

Human Resources

Chief Human Resources Officer
Senior Employee Relations Manager

Information Services and Business Process

Chief Information Officer
Chief Information Security Officer
Email: CSIRT@mantech.com

Legal Department

General Counsel

Operations Compliance Officers

Chief Performance Officer
Senior Officer of Contracts
Vice President of Contracts and Subcontracts

Security Department

Chief Security Officer 877-996-4248 (option 9)

ManTech Helpline

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

The ManTech Helpline is Available 24/7

Online:
www.mantech.ethicspoint.com

By Phone:
(866) 294-9442

ManTech®

Securing the Future

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