

Code of Conduct | 2010



SAIC
From Science to Solutions



Ethics...

it's who we are

Message from the CEO



A handwritten signature in blue ink, which appears to read "W. P. Havenstein". The signature is fluid and cursive.

Walt Havenstein
CEO

A culture of ethical behavior has been a hallmark of SAIC since our founding. Our passion is for solving hard problems, and we have always emphasized doing so in a way that upholds the highest standards of personal integrity and business conduct.

These standards are based on upholding the law everywhere we do business, taking individual and collective accountability for our behavior, and treating our customers, partners and each other with courtesy, respect and dignity.

At SAIC, we are committed to continuous improvement in every aspect of our business. This year, we are replacing our lengthy Standards of Business Ethics and Conduct Handbook with a shorter Code of Conduct that provides plain language guidance to clarify and simplify the standards of conduct. The format has changed, but our commitment to ethics has not. The new version uses scenarios to illustrate how those standards work in practice.

The manner in which we conduct ourselves defines who we are and how others perceive us. Please join me in a recommitment to each other and to our customers in making ethical behavior a pillar of our daily lives at SAIC.

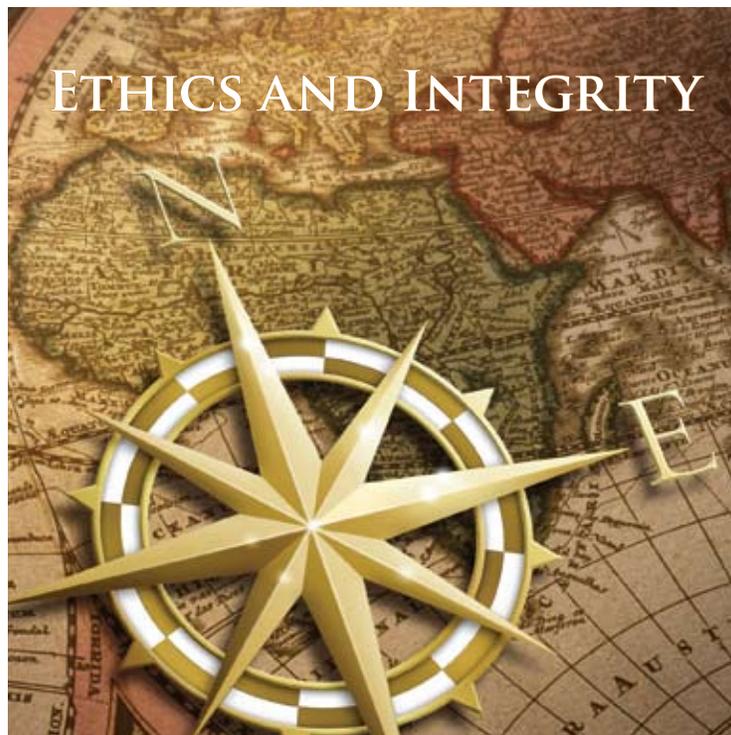
Table of Contents

	Page		Page
Our True North: Ethics and Integrity	1	Deal Fairly With Customers and Third Parties	
Our Credo: To Build Strong Partnerships	2	Personal Conflicts of Interest (SG-1)	14
Our Responsibility: To Hold Our Standards High	3	Organizational Conflicts of Interest (SG-32)	14
Our Code of Conduct	4	Recruiting and Hiring Government Employees (SG-12)	14
Protect SAIC and Customer Assets		Participation in the Political Process (SG-1)	15
Financial Integrity (SG-1)	6	Procurement Integrity (SG-15)	15
Use of SAIC and Customer Resources (SG-1)	6	Competitive Information Gathering (SG-1)	16
Expense Reimbursement (SC-12)	6	Market Competition (SG-1)	16
Timecharging (SC-2)	7	Gifts, Gratuities and Bribes (SG-1)	16
Privacy (SG-3, SG-8)	7	Nonsolicitation	16
Intellectual Property (SG-6)	7	Conduct International Business Properly	
Public-Facing Communications (SG-10)	8	Foreign Corrupt Practices Act (SG-9)	18
Confidentiality (SG-8)	8	Compliance with U.S. Export and Sanctions Regulations (SG-5)	18
Insider Trading (SG-2)	8	Report Misconduct	20
Foster a Safe and Healthy Work Environment		Zero Tolerance for Retaliation	21
Drug-Free Workplace (SG-31)	10	General Guidelines	
Harassment/Hostile Work Environment (SG-31)	10	Cooperation in Investigations (SG-1)	22
Prohibited Items in the Workplace (SG-31)	11	Record Retention (SG-18)	22
Environmental Health and Safety (SG-34)	11	Violations of the Code (SG-1)	22
Workplace Diversity and Equal Employment Opportunity (SH-6)	12	Mandatory Disclosures (SG-1)	22
Nepotism (SH-2)	12	SAIC General Policies	23
		Other ISSAIC Resources	23
		Acknowledgement and Certification	24

Throughout the Code, references are made to the corporate policies that cover specific topics of discussion. For example, a topic that has an “(SG-1)” notification indicates that the topic is covered in SAIC Standards General 1. “SC” refers to Standards Compensation and “SH” refers to Standards Human Resources. Page 23 of the Code includes a list of all SG policies by name.

OUR TRUE NORTH: Ethics and Integrity

Ethics and integrity have defined who we are since our founding in 1969. Our business is successful because we have a strong culture of ethics and integrity that enables us to attract outstanding individuals who work as a team to help our customers solve important problems.



Ethics and Integrity...

It's our job.

It's what we practice.

It's who we are.

OUR CREDO: To Build Strong Partnerships

We, as Science Applications International Corporation (SAIC) employees, are dedicated to the delivery of quality scientific and technical products and services, contributing to the security and well-being of our communities throughout the world. We believe high ethical standards are essential to the achievement of our individual and corporate goals. As such, we fully subscribe to the following commitment.

To Our Customer:

- We shall place the highest priority on the quality, timeliness, and competitiveness of our products and services.
- We shall pursue our objectives with a commitment to personal integrity and high professional standards.

To Our Fellow Employees, Present and Prospective:

- We shall promote an environment that encourages new ideas, high quality work, and professional achievement.
- We shall treat our fellow employees honestly and fairly, and we shall ensure equal opportunity for employment and advancement.
- We shall share the rewards of success with those whose honest efforts contribute to that success.

To Our Vendors, Suppliers and Subcontractors:

- We shall be fair and professional in all our business dealings and shall honor our commitments to our business partners.
- We shall endeavor to select vendors, suppliers and subcontractors who will adhere to our ethical standards and commitment to quality products and services.

To Our Neighbors:

- We shall be responsible citizens, respecting the laws and customs of each community in which we live or conduct business.

To Our Stockholders:

- We shall conduct ourselves so as to enhance and preserve the reputation of our Company.
- Consistent with the commitments expressed above, we shall strive to provide our stockholders a fair return on investment.

OUR RESPONSIBILITY: To Hold Our Standards High

All employees are responsible for behaving ethically and upholding our standards of business conduct.

Action

Act ethically and in accordance with our Code of Conduct and demand that others do the same. If you observe possible misconduct, you have a responsibility to report it through one of the eight available reporting channels. SAIC has zero tolerance for retaliation of any kind against individuals who, in good faith, raise questions, report concerns, or participate in investigations involving ethical issues.

Accountability

Everyone is accountable for his or her actions. Those who do not act ethically and conduct themselves in accordance with our Code may be subject to disciplinary action, up to and including termination.

Assistance

Questions of ethical behavior can be complex. When in doubt about your own course of action or that of others around you, seek assistance. Ask your manager, consult the Code, call the Ethics Line (800-760-4EEC), or contact your Employee Ethics Committee representative.



OUR CODE OF CONDUCT



This Code establishes the standards of business conduct that every employee is expected to meet. These standards, drawn from our corporate policies, describe our responsibility to:

- **Protect SAIC and customer assets**
- **Foster a safe and healthy work environment**
- **Deal fairly with customers and other third parties**
- **Conduct international business properly**
- **Report misconduct**
- **Protect employees from retaliation**

All employees are required to certify annually that they have read, understand and will comply with this Code of Conduct.

A man in a dark suit and tie is looking at a laptop in a blurred office setting. The background shows other people working, but they are out of focus. The man is in the foreground, looking down at the laptop screen. The laptop is silver and black. The text "Protect SAIC and customer assets" is overlaid on the image in white and yellow.

Protect SAIC and
customer assets

PROTECT SAIC AND CUSTOMER ASSETS

Employees have an obligation to protect SAIC and customer assets. SAIC policies relating to this obligation are summarized below.

Q&A

Q: I have a small side business that I operate out of my home. I've spoken to my manager, and we have determined that there is no potential conflict of interest with my SAIC work. Is it okay to give my SAIC contact information to my customers for their occasional use? May I install software related to my personal business on my SAIC computer, even though that software is not SAIC-authorized?

A: The answer to both of these questions is "no." Even if a side business does not present a conflict of interest, second jobs or self-employment must be kept completely separate from your SAIC-related activities. This includes use of company time, equipment, facilities and materials. Only software products approved for company use may be downloaded onto company computers. This type of outside activity is distinguished from occasional personal use, which is generally permitted with advance management approval.

Financial Integrity (SG-1)

Employees may use SAIC funds and other assets of the Company only for legal and proper business purposes. All assets, liabilities, revenues, expenses and business transactions must be completely and accurately recorded on SAIC's books and records in accordance with applicable law, accepted accounting principles, and SAIC financial policies and procedures.

All proposals, invoices and other submissions to the government must be accurate, current and complete. Employees who have concerns relating to accounting, internal accounting controls or auditing matters should submit them to the Chair of the Audit Committee of the Board of Directors.

Use of SAIC and Customer Resources (SG-1)

Employees may not use corporate property, software, equipment, or facilities, or upload/download software onto corporate equipment, for noncompany business. Employee computers, voice mail, and email messages must not contain offensive, disruptive, defamatory, or disparaging content. Incidental and insignificant personal use of company resources is generally permitted with advance management approval.

Employees do not have a right of privacy regarding any information that is stored on or transmitted over an SAIC information system, including email, voicemail or Internet. SAIC reserves the right to monitor, without notice or limitation, SAIC information systems and to disclose all content.

Employees located at customer facilities must make sure they use equipment that has been furnished by the customer only to perform tasks for which the equipment was provided. Even incidental and insignificant use of such property, software, equipment, or facilities for noncontract business requires specific written consent of an authorized customer representative.

Expense Reimbursement (SC-12)

Employees are responsible for honestly and accurately reporting their business-related expenses for reimbursement. An employee's signature on an expense report certifies that the information provided is complete and accurate and represents a valid business expense authorized by SAIC.

PROTECT SAIC AND CUSTOMER ASSETS

Q&A

Q: I recently attended a one-hour SAIC ethics training session, and at the end of the day, I charged that hour to the contract I am working on because that is the only charge number I have been given. I seem to recall from the training that this might be a problem. Is it?

A: Yes. You should never charge directly to a contract time spent on indirect labor; e.g., general training, staff meetings, bid and proposal efforts, or administrative support. Any timecharging errors must be corrected immediately upon discovery, with appropriate explanations included as necessary. Inaccuracies in timecharging records not only violate SAIC policy, but could violate federal law, subjecting the Company and its employees to civil and criminal penalties. Therefore, you are personally responsible for maintaining accurate daily records of time spent.

Timecharging (SC-2)

Employees are personally responsible for ensuring that their labor costs are properly recorded. This means maintaining an accurate, daily record of time spent by task and preparing a timesheet for each week. Inaccuracies in such records could constitute a violation of federal law and subject the Company and its employees to serious fines and penalties. Managers also have an obligation to review their employees' timecards for accuracy and to examine questionable entries.

Privacy (SG-3, SG-8)

Employees are expected to comply with all federal, state and international privacy laws and regulations and privacy-related contractual requirements applicable to personally identifiable information and protected health information (PII/PHI). Special protections are required for the access, storage and handling of PII and PHI. Employees must limit use, access, transmission and storage of PII/PHI to the minimum necessary to perform authorized business activities and dispose of PII/PHI as soon as legally and contractually permitted. If employees have any questions about these requirements, or have reason to believe that PII/PHI was or could have been subject to unauthorized access, they shall notify the SAIC Service Desk, Chief Privacy Officer, supervisor, Information Security Point of Contact, or the Ethics Office.

Intellectual Property (SG-6)

Intellectual property (IP), including patents, copyrights, trademarks and trade secrets, created by SAIC employees during the course of their employment at SAIC, is the property of SAIC. While employees may have personal or pre-existing IP created outside of their SAIC employment, no such outside or pre-existing IP may be brought into SAIC, disclosed to SAIC personnel or SAIC customers, or incorporated into SAIC work product, without prior written approval of the Legal Department. Employees who take such actions with their outside or pre-existing IP without prior written approval are deemed to have granted a broad license to SAIC and its customers in that IP.

PROTECT SAIC AND CUSTOMER ASSETS

Public-Facing Communications (SG-10)

No employee of the Company is authorized to engage in any form of externally facing communication that identifies SAIC, or the communicator as an employee of SAIC, without prior approval under the SG-10 process.

No employee of SAIC is authorized to make any statements, to give any information related to SAIC or any of its activities, or to comment on the plans and activities of SAIC's customers to the news media without prior approval by Media Relations, the executive in charge of communications, or the chief executive officer. All inquiries from any representative of the news media must, under all circumstances, be referred immediately without comment directly to Media Relations. It will ensure appropriate coordination and review by the Company's executive officers of any statements to the news media attributable to SAIC.

Confidentiality (SG-8)

Employees must observe obligations of confidentiality and nondisclosure of proprietary and confidential information, intellectual property, and trade secrets of SAIC and others, including customers, suppliers and former employers. Proprietary information includes financial, personnel, technical or business information owned or possessed by SAIC that has not been authorized for public release. Employees may not disclose sensitive information, including proprietary company information, without proper authorization. Employees must keep sensitive information, including any proprietary documents, protected and secure. If employees receive proprietary information belonging to a supplier, customer or competitor without proper authorization, they must immediately bring it to the attention of the Legal Department or Ethics Office.

Insider Trading (SG-2)

Employees and their immediate families are prohibited from trading in any SAIC securities at any time while they possess material nonpublic information involving the Company. Material nonpublic information includes information about SAIC that is not yet disclosed to the general public and would likely be considered important to an investor in SAIC securities. This prohibition also applies to material nonpublic information about SAIC customers, vendors, suppliers or other business partners. Failure to comply with this rule could result in violation of federal securities laws and subject the Company and individual employees to serious fines and penalties.



Q: I know that some of the information I work with is confidential. Does that mean I can't talk about it with anyone, including other employees?

A: Confidential means that the information should be kept secure, and should be discussed only with those who have a need to know for SAIC business purposes.

Q: Through my work at SAIC, I am aware that a customer plans to introduce a new product next month, but has not yet made a public announcement. May I buy stock in that customer's company now? I know this product will sell!

A: You may not purchase this stock until the information is known to the public. Information of this kind may have been provided to SAIC in confidence by the customer to assist SAIC in determining how to meet the customer's needs. Using this confidential information for personal purposes or disclosing it to others is a violation of SAIC policy and may be illegal.

Foster a safe and healthy **work environment**

FOSTER A SAFE AND HEALTHY WORK ENVIRONMENT

SAIC promotes a safe and healthy work environment for its employees, as expressed in the following policies.



Q: My manager picks on one of my co-workers constantly, often embarrassing him in front of the entire team for no apparent reason. Should I just keep my mouth shut to avoid becoming the next target?

A: No. When you witness inappropriate or unacceptable behavior, you should speak up. Address this situation directly with your manager or HR, or through one of the other eight internal reporting channels available to you.

Drug-Free Workplace (SG-31)

In furtherance of SAIC's commitment to maintaining a drug-free workplace, the following activities are prohibited:

- Smoking inside any SAIC facility, within any SAIC vehicle, or on SAIC property not designated a smoking area
- The abuse of alcohol in the workplace
- The unlawful manufacture, sale or possession of illegal drugs
- The illegal use of drugs
- The presence of illegal drugs in the workplace

Harassment/Hostile Work Environment (SG-31)

SAIC is committed to fostering a safe and healthy work environment that is free from harassment, whether sexual or otherwise. Harassment of employees by managers, supervisors, coworkers, or nonemployees is unacceptable and will not be tolerated. Similarly, SAIC will not tolerate harassment by its employees of nonemployees with whom SAIC has a business, service, or other relationship. Harassment includes unwelcome conduct that:

- Is sufficiently severe or pervasive as to interfere with an employee's work performance
- Creates an intimidating, hostile or offensive work environment
- Is made either an explicit or implicit condition of employment, or is the basis of an employment decision

FOSTER A SAFE AND HEALTHY WORK ENVIRONMENT



Prohibited Items in the Workplace (SG-31)

SAIC employees must never bring a prohibited item into any SAIC facility. Such items include the following:

- Firearms, explosive devices, incendiary devices, or any item brought onto Company premises for the purpose of inflicting bodily harm, or threatening or intimidating others
- Controlled substances, such as illegal drugs, unlawfully obtained prescription drugs, and associated paraphernalia
- Any recording or photographic devices, such as cameras, web cameras, surveillance equipment, and audio recorders
- Any other item or substance that is prohibited by law

Cell phones and personal digital assistants (PDAs) or other equipment outfitted with either a camera or recording capabilities are not prohibited, but the camera or recording capability may not be used.

Employees should contact Security if they observe any prohibited items in the workplace.

Environmental Health and Safety (SG-34)

SAIC is committed to conducting business in a manner that protects the health and safety of its employees, customers, business partners, community neighbors, and the environment. Therefore, SAIC employees are responsible for performing their activities in accordance with the requirements identified in SAIC's Environmental, Health, and Safety Program Manual, or as set forth by their respective locations and contract-specific programs.



FOSTER A SAFE AND HEALTHY WORK ENVIRONMENT

Q&A

Q: I see that a position was posted within a different SAIC business unit that sounds perfect for me, but it would mean that I would be the director of the department in which my boyfriend works. However, there would be a line of management between him and me, so I assume that would not be a problem, right?

A: Wrong. To prevent potential conflicts of interest and allegations of favoritism, you cannot be in the same reporting chain with any closely related individuals. The term “closely related individuals” is broadly defined to include persons involved in a dating relationship.

Workplace Diversity and Equal Employment Opportunity (SH-6)

Our company is committed to providing an inclusive environment where employees with unique differences, viewpoints and talents are sought and respected, creating an atmosphere in which our employees can thrive. SAIC values and respects a diverse employee population, and is committed to equal employment opportunity. All employment practices must be based upon an individual's capabilities and qualifications without regard to race, gender, age, color, religion, national origin, sexual orientation, disability, veteran or marital status, or any other protected characteristics as established by applicable law.

Nepotism (SH-2)

Employees should be reviewed, and their work performance evaluated, based on their performance and merits, not on family or close personal relationships. To prevent potential conflicts of interest and allegations of favoritism or sexual harassment, an employee is not permitted to have a reporting relationship with a closely related individual.



Deal fairly with customers and third parties



DEAL FAIRLY WITH CUSTOMERS AND THIRD PARTIES

SAIC is committed to pursuing its business objectives and interacting with customers and other third parties with personal integrity and in accordance with the high standards of business conduct they deserve. The following policies further this commitment.

Q&A

Q: I have been asked to serve on a federal advisory committee for a defense agency. The committee holds bimonthly meetings to discuss the future of network-centric warfare. Committee recommendations are submitted to the agency director. Several of my defense industry counterparts participate on the committee. Should I seek a conflict of interest review?

A: Yes. This outside activity requires prior review and approval from your managers, the Corporate Compliance Office and the Government Affairs Office. Your participation on this committee could create legal risks to the Company if, for example, you gain access to competitor proprietary or confidential information or participate in discussions that create an unfair competitive advantage for SAIC. Also, employee participation in high-profile public positions may raise appearance concerns that must be considered. Begin the conflict of interest review process by discussing the activity with your manager.

Personal Conflicts of Interest (SG-1)

Employees may not participate in any private business or professional activity or have any direct or indirect financial interest that would create a conflict between their private interests and their responsibilities to SAIC.

Employees who seek to participate in activities that involve outside organizations that are customers, competitors or suppliers; to serve on federal advisory committees; or to engage in other activities that could create legal or business risks must obtain prior approval from their managers and the Corporate Compliance Office.

Organizational Conflicts of Interest (SG-32)

SAIC employees must comply with Organizational Conflict of Interest (OCI) rules that prohibit them from serving in conflicting roles that might bias their judgment, create an unfair competitive advantage, or impair objectivity in their performance. Employees should be especially cautious of potential OCIs if a particular procurement opportunity will:

- Include work for which SAIC provided systems engineering and technical direction, prepared specifications or work statements, provided evaluation services, or obtained access to proprietary information
- Require setting or influencing the requirements or terms for a future opportunity in which SAIC might have an interest in bidding
- Result in SAIC's evaluating or recommending its own products and services, or those of its competitors
- Afford SAIC access to proprietary or other nonpublic information about its competitors

The Contracts Department must review and approve all situations that could raise OCI concerns.

Recruiting and Hiring Government Employees (SG-12)

Employees may not engage in discussions with current or former federal government employees, including military personnel, about employment at SAIC, unless that government employee either has disqualified him or herself from any involvement in SAIC contracts or has received a waiver from his or her agency. This policy applies not only to formal discussions involving resumes, but also to informal discussions that take place in hallways, cafeterias and conferences.

DEAL FAIRLY WITH CUSTOMERS AND THIRD PARTIES

Participation in the Political Process (SG-1)

All political activities by or on behalf of SAIC must be conducted in accordance with applicable law and the Government Affairs Handbook. Under federal law, SAIC is prohibited from making political contributions of any kind in connection with federal elections. However, these restrictions do not affect employee participation in the SAIC Voluntary Political Action Committee (VPAC). Employees are prohibited from making political contributions where it might reasonably be inferred that corporate reimbursement of the funds would be involved without prior written approval from the CEO or the SAIC Government Affairs Committee. All political contributions using corporate funds for state and local campaigns must be pre-approved by the Government Affairs Committee. All contributions, including personal contributions and contributions by family members, in jurisdictions with “pay-to-play” laws, must be approved and disclosed in accordance with SAIC policy.

All employees must comply with state and local laws while interacting with state and local officials. Prior to seeking election to, or accepting appointment to, any federal, state, or local government office, an employee must obtain approval from the Government Affairs Committee.

Procurement Integrity (SG-15)

Employees shall comply with all aspects of the Procurement Integrity Act, which generally prohibits employees from:

- Knowingly obtaining bid, proposal or source-selection information related to a current or future federal procurement
- Disclosing bid, proposal or source-selection information to which SAIC has received access in the course of providing support or advice to a federal agency
- Engaging in employment discussions with, employing or providing compensation to certain former government procurement or contract officials

Employees are responsible for seeking guidance if they are uncertain about their obligations under the Procurement Integrity Act. Certain employees who interact with the federal government are required to complete training in the Procurement Integrity Act and certify that they will comply with this law and the Company’s policies and procedures that implement this law.

Q&A

Q: What should I do if a government official begins to share what I believe to be confidential or proprietary competitor information during a meeting?

A: Stop the conversation immediately and ask if the information is confidential or proprietary competitor information or nonpublic source selection information. The rules prohibit you from improperly obtaining nonpublic procurement information, even if it is unintentional. Obtaining such information could result in criminal and civil penalties, as well as in administrative and contractual penalties and/or a bid protest.



DEAL FAIRLY WITH CUSTOMERS AND THIRD PARTIES

Competitive Information Gathering (SG-1)

Employees may obtain only publicly available information about a competitor, as found in public documents such as press releases, marketing brochures, public presentations, legal filings, public web pages, or demonstrations at trade shows. Wrongful acquisition of a competitor's trade secrets or other information is unethical and can result in civil and criminal penalties. Even if information is freely revealed by a third party, if an employee knows that the information is confidential and has been obtained wrongfully, such information must neither be used nor further disclosed, other than to the appropriate authorities.

Market Competition (SG-1)

Employees must not discuss with a competitor any of the following topics:

- SAIC costs or profits
- Pricing practices or policies
- Coordinating bids
- Customers, markets or territories
- Boycotts of suppliers or customers

Such discussions could violate the law and subject the employee to disciplinary action, up to and including termination.

Gifts, Gratuities and Bribes (SG-1)

SAIC business relationships must be free from even the perception that favorable treatment is being sought, received or given as the result of a gift or gratuity. SAIC is subject to a range of laws that prohibit the offering and acceptance of gifts to government customers and suppliers. As such, an employee may not offer or give a gift or gratuity to any customer, or accept or solicit a gift from any supplier, except as set forth in corporate policy SG-1.

Nonsolicitation

While employed by SAIC and for one year thereafter, SAIC employees shall not solicit or attempt to solicit any SAIC employee to leave his or her employment with SAIC.



Q: I work at a government facility with federal employees. Several SAIC employees have been invited to a lunchtime baby shower for one of the federal employees on the contract. Can we purchase a gift for her?

A: No. SAIC employees are prohibited from offering gifts to federal Executive Branch employees, except for modest refreshments such as soft drinks, coffee, and donuts. Our policy ensures that we are consistent with the federal gift rules, which prohibit an Executive Branch employee from accepting gifts from persons who do business with the employee's agency. Exceptions to this policy must be approved by the Corporate Compliance Office.



Conduct international business
properly

CONDUCT INTERNATIONAL BUSINESS PROPERLY

SAIC is committed to complying with the highest ethical standards and all applicable laws and regulations in its pursuit of business across the globe, including all applicable U.S. and foreign laws and regulations. SAIC policies relative to international business are summarized below.

Q&A

Q: A consultant from a company at an overseas location offered to assist me in setting up a meeting with a foreign government official. An advance payment was requested to help move things along. Since the payment will be made to the consultant, not to a government official, there's no reason to worry about it, right?

A: Wrong. We may be held responsible for the actions of third parties working on our behalf. All payments to consultants, agents, representatives and other third parties involving foreign business should be vetted through the Legal Department in advance.

Foreign Corrupt Practices Act (SG-9)

Employees are expected to conduct international business in accordance with the highest ethical standards and in compliance with the Foreign Corrupt Practices Act (FCPA). Employees are prohibited from giving anything of value either to win government business overseas or to obtain an unfair business advantage. In addition, they are required to record all expenditures and transactions accurately and thoroughly.

Compliance With U.S. Export and Sanctions Regulations (SG-5)

All employees are required to comply with U.S. regulations governing the export and re-export of controlled items and technology to certain persons, entities and locations outside of the United States and imports into the United States. In addition, U.S. persons are prohibited from investing or transacting business with designated countries and entities. Each SAIC Business Unit, Group or subsidiary has specified International Trade Compliance personnel responsible for their respective organizations' compliance with these regulations.

In accordance with U.S. export regulations, SAIC employees are responsible for protecting export-controlled information and technology from unauthorized disclosure to foreign persons or entities. All controlled information and technology must be protected properly through strict implementation of technology security measures, including established firewalls, information approval processes, physical protection, and technology control plans.



Report
misconduct



REPORT MISCONDUCT

Q&A

Q: I observed a situation that may violate company policy, or even the law, and I believe that my supervisor observed it as well. If my supervisor chooses to ignore the situation, should I do the same?

A: Disclosure of actual or suspected violations of law or SAIC policy is not only critical to the well-being of the Company, it is required of all employees. Your supervisor may not be as aware of the problem as you believe, and even if he or she is, the situation needs to be reported so that it may be addressed appropriately. If you are not comfortable discussing the matter with your supervisor, you should use another one of the eight internal reporting channels available to you.

As responsible employees, and in accordance with SG-1, we are committed to responding appropriately when we witness misconduct. That means reporting behavior that violates our policies and questioning behavior that appears inconsistent with our core values, regardless of the corporate position, level or business area of those participating in such behavior. Reporting observed misconduct is essentially black and white: if employees see something wrong, they should disclose it using one of the reporting channels listed below:

1. Talk to a **supervisor** or someone in the management chain, for example, the Business Unit General Manager, Group President, or other manager. This channel should be an employee's first course of action, unless it is inappropriate under the circumstances. If an employee is a manager, one of the most important roles he or she has is to listen to employees who have ethics questions or are facing ethical dilemmas, while assuring them that their concerns will be taken seriously. If possible, work to resolve the matter at the local level.
2. Talk to the local, Business Unit, Group, or Corporate **Human Resources Director**.
3. Contact the **Employee Ethics Committee (EEC)**.
 - Contact an EEC member: <https://issaic.saic.com/pocdb.nsf/webpages/EECHome>.
 - Submit a comment through the Ethics Survey.
 - Send a confidential, secure fax to the EEC: 858-826-4879.
 - Call the Ethics Line: 800-760-4EEC.
 - Call (703-676-8633) or fax (703-676-8510) the EEC Chair.
4. Call the **SAIC Hotline: 800-435-4234 (Corporate Legal)**.
5. Call or write to the **General Counsel** or the **Senior Vice President, Ethics and Compliance**.
6. Write to the **Chair, Ethics and Corporate Responsibility Committee of the Board**, or if the matter involves accounting, internal accounting control or auditing matters, to the **Chair of the Audit Committee of the Board** c/o Secretary of the Audit Committee of the Board of Directors, SAIC, 1710 SAIC Drive, M/S 1-4-2, McLean, VA 22102.
7. Write a letter to the **Chairman of the Board** or **CEO**.
8. Communicate with the **Board** or **Lead Director** c/o Corporate Secretary, SAIC, 10260 Campus Point Drive, M/S D7-5, San Diego, CA 92121
Email: corporategovernance@saic.com.

In a situation at work where no clear violation of policy appears to have occurred, but something just doesn't feel right, do not ignore that feeling. Ask questions, or seek the advice of an EEC member or a trusted leader.

ZERO TOLERANCE FOR RETALIATION

Q&A

Q: My supervisor told me to submit an expense report on his behalf for items that he bought for personal use only. I know I'm supposed to report misconduct, but I'm worried that reporting this could cost me my job. What should I do?

A: Disclosure of actual or suspected violations of SAIC's standards of conduct is expected of all employees. SAIC has a zero tolerance policy for retaliation against those who report misconduct in good faith. SAIC investigates all allegations of retaliation and takes appropriate corrective action whenever such investigations establish the existence of retaliation.



SAIC policy (SG-1) requires employees to report violations and encourages questions and reporting of possible violations of the Code of Conduct or any applicable laws and regulations. SAIC has zero tolerance for retaliation of any kind against individuals who, in good faith, raise questions, report concerns, or participate in investigations of an ethical nature. If an employee is concerned about retaliation or believes that he or she has been subject to retaliation for reporting a possible violation or for participating in an investigation, the employee should immediately contact the Chair of the Employee Ethics Committee; the Senior Vice President, Ethics & Compliance; the General Counsel; or the Executive Vice President, Human Resources, so that the concern can be addressed promptly. Retaliation against employees for good faith reporting of misconduct is considered a serious breach of SAIC's Code of Conduct and can result in serious disciplinary action, including termination.

GENERAL GUIDELINES

Cooperation in Investigations (SG-1)

SAIC is committed to full cooperation with government investigations involving requests for information and documents in its possession to which the government is legally entitled. While government officials typically address inquiries directly to SAIC's Legal Department, occasionally employees may be contacted directly with a request for documents or other information. In these instances, responses must be coordinated with SAIC's Legal Department, and the Legal Department will respond to the inquiring government party.

Record Retention (SG-18)

Employees must comply with SAIC's record retention policy. It is unlawful to destroy, conceal, alter or falsify any SAIC business or other record, document or object for the purpose of obstructing or influencing any lawsuit or other legal, regulatory or governmental proceeding or investigation.

Violations of the Code (SG-1)

Each SAIC employee shall comply with the letter and spirit of the Code of Conduct and shall promptly communicate any suspected violations to any one of the eight reporting channels. Violation of any provision of the Code of Conduct may result in disciplinary action, up to and including termination of employment with SAIC.

Disciplinary action may be taken against employees who authorized or participated in the violation, and also against:

- Anyone who deliberately failed to report a violation
- Anyone who deliberately withheld or misrepresented relevant materials or information concerning a violation
- The violator's supervisor or manager to the extent that he or she provided inadequate leadership, supervision or diligence

Mandatory Disclosures (SG-1)

SAIC's policy is to report to the government credible evidence of violations of federal law involving fraud, conflicts of interest, bribery, gratuities, civil false claims and significant overpayments. Employees are required to report any information involving possible violations to the SAIC Hotline (800-435-4234), the Legal Department, an EEC member, or the EEC Chair.



Q&A

Q: I received a call from the U.S. Department of Justice asking for specific information related to our internal investigations. I know that all our investigations are conducted thoroughly and fairly, so is it okay for me to just give DOJ what they want?

A: You should not respond, and you should refer the matter to SAIC's Legal Department for a response.

SAIC General Policies

SG-1 Standards of Business Ethics and Conduct
SG-2 Insider Trading and Disclosure Policy
SG-3 Information Systems Security Protection
SG-4 Foreign Person Access to Controlled Technology
SG-5 Compliance with U.S. Export and Sanctions Regulations
SG-6 Intellectual Property, Commercialization, and Publications
SG-7 Authorities for Corporate Commitments
SG-8 SAIC Proprietary Information, Technical Data, and Personal Information
SG-9 Complying with the Foreign Corrupt Practices Act (FCPA)
SG-10 Communications
SG-12 Recruitment and Employment of Current and Former U.S. Government Personnel
SG-13 Reporting Adverse Personnel Information
SG-15 Procurement Integrity
SG-16 Service of Process
SG-17 Use of Consultants
SG-18 Records Retention
SG-23 Telework Policy
SG-24 Executive Travel Policy
SG-25 Program Execution
SG-26 Corporate Business Continuance
SG-27 Risk Management
SG-28 Truth in Negotiations Act
SG-29 Trade Shows and Event Marketing
SG-30 Electronic Communications Policy
SG-31 Workplace Behavior and Environment
SG-32 Organizational Conflict of Interest
SG-33 Meeting/Event Planning and Conference Management
SG-34 Environmental Health & Safety

Other ISSAIC Resources

Compliance Resource Center
Corporate Communications
Corporate EH&S Program Manual
Corporate Environmental Health & Safety
Corporate Export Administration
Corporate Export/Import Compliance Manual
Corporate Finance
Corporate Legal
Corporate Security
Ethics and Compliance
Government Affairs
Government Affairs Handbook
International Business
IT Security
Organizational Conflicts of interest
Timecharging
Travel & Expense System

Acknowledgement and Certification

My signature below certifies the following:

- I have read SAIC's Code of Conduct, understand that it represents Company policy and our commitment to each other, and agree to comply with it.
- I have sought and received clarification from a responsible party (such as management, an EEC member, HR, or the appropriate corporate policy owner) of any portion of this Code of Conduct that is unclear to me.
- I have reported and agree to report to one of the Company's specified reporting channels all actual and potential violations of applicable law, this Code of Conduct, and the policies it represents.

Employee Signature

Printed Name

Employee Number

Date

Please submit this certification to your Human Resources Point of Contact (POC).



We, as Science Applications International Corporation employees, are dedicated to the delivery of quality scientific and technical products and services, contributing to the security and well-being of our communities throughout the world. We believe that high ethical standards are essential to the achievement of our individual and corporate goals.

