SCIENCE APPLICATIONS INTERNATIONAL CORPORATION

October 2006

Standards of Business Ethics & Conduct Handbook

SAIC®
From Science to Solutions

SAIC®
From Science to Solutions

Good Values...Good Business

ETHICS AND QUALITY

ENTERPRISE **EQUITY** **EXPERTISE**

Business Practices

Entrepreneurial Spirit, Decentralization, Freedom and Responsibility

Business Growth and Market Diversification

Customer Orientation and Service

Prudent Risk Taking and Initiative

Attracting, Retaining and Applying the Best People to Customer Needs

Responsive and Reliable Business Partners

Competitive Goods and Services

Stakeholder Relationships

Ethical Behavior and Professional Integrity

Employee Participation

Promise and Commitment Keeping

Fair Rewards Based on Contributions to SAIC

Mutual Respect, Teamwork, Loyalty and Cooperation

Opportunity for Personal and Professional Growth

Law Abiding and Corporate Good Citizenship

Standards of Excellence

Quality Technical and Scientific Products and Services

Professional and Technical Standards of Excellence

Technical Curiosity, Creativity, Growth, and Innovation

Superior Performance and Continuous Improvement

Problem Solving and Solutions Orientation

Measurement of Client Satisfaction

Peer Review

Statement of Purpose

SAIC's success to date has resulted from outstanding performance by our employees and strict adherence to our core values. Our customers admire the twin principles of quality and ethics that are the foundation of the SAIC way of doing business. We worked hard for more than 37 years to build this reputation, which has been a key discriminator aiding our unprecedented growth. At SAIC, we can neither forget our origins, nor put at risk the core values and standards which made our growth possible. We must sustain our core values of ethics, integrity, innovation, entrepreneurship, customer service, and technical excellence, all supported by our culture of ownership, participation and accountability. The purpose of this standards handbook is to make clear to our employees that how we get where we are going matters. Here at SAIC, ethical ways are the only acceptable means to achieve our business goals. As employees of SAIC, each of us must accept our individual accountability to lead by example and insist on only the highest standards of business conduct from all. Our conduct must not only be right, it must look right. We will not tolerate unethical behavior in pursuit of business objectives.

The purpose of this handbook is to provide an overview of the core ethical values and essential compliance standards of conduct we must follow in our business dealings, both inside and outside the company. It concentrates on the core values and essential standards absolutely critical to the well being of SAIC, our customers and all others with a stake in our future. These standards "showcase" the core values of our vision, mission, values and Credo and provide a "roadmap" to the more detailed policies and procedures published in the SAIC Administrative Handbook, which is available on ISSAIC or from your managers.

The standards set forth herein are applicable to all directors, officers, employees and agents in carrying out business of SAIC, Inc. and its subsidiaries. Our standards adhere to the spirit of the law and go well beyond mere compliance with the letter of law and regulations. As such, these values and standards are not goals; they are the essential benchmarks of the SAIC way of doing business and must be met. At SAIC, we must be unwilling to compromise on ethics, integrity and excellence – top to bottom. To me, our standards are simply the only way to operate and anything less is unacceptable and will not be tolerated.

Ethics Motto:
Ethics and Quality: Good Values…Good Business

Ken Dahlberg
Chairman and CEO

Principles and Practices of SAIC

Quality: "Taking a long term view of what is important to SAIC, the quality of our technical efforts must always come first."

Organization: "We believe that leaving as much autonomy at the operating level and providing as many discretionary resources as possible to those who generate them is the best approach in the long term."

Growth: "Growth is necessary for maintaining the right working environment in SAIC…It provides opportunities for individuals to expand their technical areas of interest and to advance in management responsibilities...Growth, of course, is also important in creating the financial rewards necessary to attract and hold the best people."

Risk: "SAIC will carefully handle the funds available to invest in our future… No single investment, or anything else will be allowed to place the future of SAIC as a whole at risk."

Freedom: "SAIC has always provided its employees with more freedom to pursue their interests and professional careers than do most other companies."

Careers: "SAIC is endeavoring to provide three parallel career paths, each of which is considered to be equivalent within the company: the technical path, the management/ administrative path and the marketing path…Career opportunities must be equally appreciated in all three areas."

Leadership: "SAIC recognizes the importance of training for people in leadership positions who, perhaps for the first time, are making decisions that have a direct impact on the people who work for them."

Cooperation: "Success through unfair competition and unfair tactics should not be rewarded at SAIC...Success through cooperation, through combining the best talents of our people will be encouraged and rewarded."

Marketing: "Successful marketing is built primarily upon the reputation of the company and our technical staff for performing superior and in some cases, unique technical work."

Table of Contents

1 Statement of Purpose

2 Principles and Practices of SAIC

3 Table of Contents

4 Important Notice

5 Vision, Mission and Values
- Vision
- Mission
- Values

6 Ethics & Conduct
- Credo
- Ethics Motto

7 Key Messages

8 Disclosure Reporting Channels

9 Responsibilities
- General Responsibilities for All Associated with SAIC
- Company Responsibilities
- Governing Authority Responsibilities
- Vice President for Ethics and Compliance Responsibilities
- Employee Ethics Committee Responsibilities
- Manager and Supervisor Responsibilities
- Employee Responsibilities
- Responsibilities of Consultants, Subcontractors and Suppliers

11 Standards of Business Ethics & Conduct
- Financial Integrity Accurate Disclosure, Record Keeping, and Record Retention (SG-1, SG-18)
- Proper Recording and Disbursement of Funds and Other Assets (SG-1)

12 Timecharging
- Time Recording, Labor Charging, and Customer Billing (SG-1, SH-1, SC-4, SC-2)
- Employee Business Expense Reimbursement (SG-1, SC-12)
- Government Investigations (SG-1)

14 Conflicts of Interest: Other Employment, Outside Interests, or Related Transactions (SG-1)

16 Other Important Standards of Conduct
- Use of SAIC and Customer Property, Equipment and Facilities (SG-1)
- Copyrighted or Licensed Materials (SG-1, SG-3)
- Inventions and Intellectual Property (SG-6)
- Accurate Representation of Data or Credentials
- Employee Resumes
- Reporting Adverse Personnel Information (SG-13)
- Drug and Substance Abuse Policy (SG-21)
- Equal Employment Opportunity (SH-6)
- Harassment (SH-8)
- Staffing Policy (SH-2)
- Wage Determinations/Prevailing Wage and Benefits Requirements (SC-5)
- Public-Facing Communications (SG-10)
- Truth in Negotiations Act (SG-28)
- Marketing and Contracting and Conducting International Business (SG-9, SG-14)
- Foreign Corrupt Practices Act (SG-9)
- Foreign Person Access to Controlled Technology (SG-4)
- Alcohol Use (SG-21)
- Nonsmoking Policy (SG-22)
- Prohibited Items (SG-19)
- Environmental Compliance and Health and Safety (SG-1)
- Wearing Appropriate Identification
- Use of Audio or Video Recording
- Expert Witness Consulting
- Misconduct in Science (SG-1)

26 Proprietary and Confidential Information
- Definition (SG-8)
- Designating and Changing the Status and Disposal of Proprietary Documents and Equipment (SG-8)
- Relationships with Customers and Suppliers, Gifts and Gratuities (SG-1, SG-12, SG-15)
- Recruitment and Employment of Current and Former U.S. Government Personnel (SG-12)
- Agreements with Marketing Agents, Including Sales Representatives (SG-1)
- Political Contributions (SG-1)

33 Information and Data Protection (SG-3)
- Computer System Usage (SG-3)
- Accessing Computers or Networks (SG-3)
- Account Name and Password Security (SG-3)
- Disruptive Software (SG-3)
- Granting Privileges (SG-3, SG-4)
- Internet & World Wide Web Access and Appropriate Use (SG-3)
- Voicemail and Email (SG-1, SG-3)
- Consequences of Violation and Duty to Report (SG-3)
- Unlicensed Software Use (SG-3)

36 Certification of Procurement Policy
- Business Development Activities (SG-1, SG-15)
- Competitive Information Gathering
- Combating Trafficking in Persons (SG-1)
- Risk Policy (SG-27)
- Procurement Policy Act and Procurement Integrity Certification (SG-1, SG-15, SG-12)

39 Summary

41 SAIC Standards of Business Ethics and Conduct Certification

Important Notice

This standards handbook does not constitute an employment contract or a promise or commitment regarding future positions, future assignments, future compensation, or continued employment. SAIC reserves the right to transfer, demote, reassign, reclassify, or otherwise change an employee's terms and conditions of employment at its discretion. Moreover, nothing in this standards handbook in any way modifies the “at will” employment relationship between SAIC and its employees; therefore, either SAIC or any of its employees can terminate the employment relationship at any time with or without cause or notice.

Vision, Mission and Values

Vision

Our vision is to grow this enterprise to better serve our customers, our communities and our employees throughout the world by being the leading systems, solutions, and technical services company, solving our customers' most important business and mission-critical problems through innovative applications of technology and domain knowledge.

> "SAIC has a proud history of accomplishment to draw upon, as is demonstrated by our successful performance in support of our customers over the past 37 plus years. …We must grow and transform the way we do business to meet the new needs of our customers today and tomorrow. This transformation must be transparent to our clients, who must continue to experience the same excellent level of performance that has become SAIC's trademark."

Mission

SAIC is a company of people dedicated to delivering best-value services and solutions based on innovative applications of science and technology.

- We commit to exceeding our customers' expectations for quality, responsiveness and professional excellence while delivering within the agreed price and schedule.
- We maintain the highest standards of ethical behavior and professional integrity.
- We commit to recruit, retain and advance a diverse, talented team of highly motivated professionals to solve critical challenges to the benefit of our customers, suppliers, employees and the communities in which we live and work.
- We employ people of exceptional creativity, expertise and determination who work closely with one another and with our customers.
- We pursue technical growth and market diversification to increase value for our customers and opportunity for our employees.
- We motivate and reward outstanding performance.
- We foster a working environment that encourages technical objectivity, professional and financial growth, and entrepreneurial freedom.

Values

How we achieve our mission is as important as the mission itself.

- Driven by quality and customer satisfaction
- Committed to the highest standards of ethical behavior and professional integrity
- Built by excellent people and team effort
- Focused on technical growth and market diversification
- Motivated by a culture of employee ownership, participation and accountability
- Energized with an entrepreneurial spirit

Standards of Business Ethics & Conduct

"Our initial public offering (IPO) can allow us to sustain our culture – but only if all of us preserve, honor and respect our heritage and hold constant the truly intrinsic values of our culture. These are core, fundamental and everlasting, no matter what capital structure we adopt; if we integrate our values of ethics and integrity, significant employee ownership, technical excellence, customer satisfaction, entrepreneurial spirit, empowerment, pride, and long-term perspective into our approach to our markets, customers, employees, strategy and reward system, then they will continue to be real, vibrant and everlasting."

"It is important to try to make clear to our employees, that how we get to where we are going matters to us, that any route to the objective is not acceptable."

"Some things will remain constant, and that includes our values. We will continue to foster a culture of ownership and performance. We will maintain a long-term view, and we will do all of it without compromise in our ethics, integrity or commitment to excellence."

Ethics & Conduct

The company is committed to conducting its business in accordance with all applicable federal, state and local laws, rules and regulations and in accordance with high standards of business ethics. SAIC directors, officers and employees are expected to comply, and assist the company to comply, with all applicable laws and regulations. They also have a responsibility to assist the company to conduct our business in an ethical manner. SAIC standards of business ethics and conduct and the associated policies governing business ethics and legal and regulatory compliance are described in this handbook which includes the SAIC Credo. The SAIC Credo is a declaration of the principles and values which are the foundation of the standards of conduct and business practices which govern our ethics and compliance programs and our relationships with all SAIC stakeholders. In this brief document, we, the SAIC employees, express our core commitment to equity in all our stakeholder relationships. We define the enterprise values which underscore our continuous commitment to business best practices. We spell out the expertise values, which set the standards of excellence and quality, that are the hallmarks of our professional and technical products and services. The SAIC Credo should be prominently displayed in appropriate common areas within all SAIC facilities.

Ethics and Quality:
Good Values…Good Business

Credo

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 high ethical standards are essential to the achievement of our individual and corporate goals. As such, we fully subscribe to the following commitments:

To Our Customers:

- 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 Shareholders:

- 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 shareholders a fair return on investment.

Ethics Motto

As noted in the SAIC Credo above, we believe there is a strong link between ethics and quality at SAIC. This is reflected in SAIC's ethics motto:

Ethics and Quality: Good Values…Good Business

High ethical standards are essential to the achievement of our business goals and our commitment to deliver quality scientific and technical products and services to our clients. In addition, high ethical values in the workplace can help create an environment of mutual trust, respect and integrity that make SAIC a good place to work.

Key Messages

We all have a stake in upholding the company's ethical standards. In subsequent pages, you will review the specific and detailed elements of SAIC's standards of business ethics and conduct. But before you do, take a common sense look at why we have such a policy – and what your role is in it. There are three key messages at the heart of our ethics program that all employees must understand – Accountability, Action and Assistance.

(1) **Accountability: Ethical behavior at SAIC is an individual – as well as a management – responsibility.**
High ethical standards are essential to the achievement of our individual and corporate goals. We should never underestimate the importance of our individual ethical behavior on the general well being of our fellow employees and on SAIC as a whole.

To emphasize the responsibilities of both individuals and managers in the SAIC Ethics Program, the company requires that each employee be assessed annually, as part of the employee's performance review, on the employee's adherence to SAIC's standards of business ethics and conduct. In addition, managers and supervisors are evaluated annually on their effectiveness in implementing the standards of conduct in their organizations. As a manager, supervisor or employee, our accountability for ethical conduct and legal compliance is integral to our personal conscience and professional integrity. As such, our accountability is individual and we cannot shift it to others.

(2) Action: SAIC wants its employees to act in an ethical manner
SAIC is serious about ethics and compliance. Our Credo and standards require you to take responsibility and focus on the long-term reputation and well being of SAIC. You should have no doubts regarding SAIC's senior leadership's expectations in terms of ethical behavior or legal and regulatory compliance. If someone's words or actions should set a contradictory or poor example, review with them the Statement of Purpose letter at the front of this handbook or the following paragraph from SAIC's Administrative Policy SG-1.

"Any short-term gain bought at the expense of ethical and legal compliance harms the long-term interests of the company, is completely unacceptable, and cannot be tolerated."

There should be no doubt ethical behavior and legal compliance are "first things first" at SAIC.

(3) Assistance: Do not tolerate violations of our common ethical standards
If you see something wrong, disclose it. SAIC depends on all employees to report – not condone – misconduct. Misconduct affects you, the employee. It can lead to, at minimum, an unpleasant working environment for you and your co-workers, and in some situations to serious legal and financial costs or penalties for SAIC. Such costs and penalties affect all stakeholders. SAIC employees must not tolerate violations of SAIC's ethical standards. If an employee knows of or suspects a violation of law or ethical misconduct, the employee must disclose it to an appropriate company resource. Disclosure of actual or suspected violations of SAIC's standards of conduct is critical to the well-being of the company. Employees are encouraged to consult with their immediate supervisor first with regard to ethics and compliance issues, but direct recourse to the vice president for ethics and compliance, the chairman of the employee ethics committee, the senior vice president of human resources, or the general counsel is also appropriate, as is reporting through the various hotlines and other resources provided. Several channels are available for voicing an ethics concern:

Standards of Business Ethics & Conduct

"Professional integrity is essential to fulfill contractual obligations, to maintain the quality of our products, and to uphold the reputation of SAIC. It grows within each individual conscience and is fostered by maintaining a professional environment that tolerates only the highest quality output from each employee and the company as a whole."

"Our culture is built on a level of participation...that is very different from more rigid hierarchies...Employee participation in the two-way communications process contributes to commitment and responsibility on the part of both the individual and the corporation."

"In essence, we expect employees to treat each other in the manner in which they would like to be treated"

Disclosure Reporting Channels

1. Talk to your supervisor or someone in your management chain.

2. Talk to any of the following people in the Human Resources Department:

a. Your Local, Business Unit, Group or Corporate Human Resources Director.

b. The Senior Vice President/Director of Human Resources.

Bernie Theule

Mail Stop D-7 | 4242 Campus Point Court | San Diego, CA 92121 | (858) 826-2405

3. Contact the Employee Ethics Committee.

a. Call an Employee Ethics Committee member.

b. Email the Employee Ethics Committee.

c. Submit an Ethics Survey.

d. Send a confidential fax to the EEC at (858) 826-4879.

e. Call the Ethics Line at (800) 760-4EEC.

f. Call or write to the Chairman of the Employee Ethics Committee.

Michael P. Campbell

1997 Annapolis Exchange Pkwy. | Annapolis, MD 21401 | (410) 571-0401

g. Send a confidential fax to the Chairman of the Employee Ethics Committee at (410) 266-5738.

4. Call the SAIC Hotline at (800) 435-4234

5. Call or write to the General Counsel or the Vice President for Ethics and Compliance.

a. Douglas E. Scott

Mail Stop F-3 | 10260 Campus Point Drive | San Diego, CA 92121 | (858) 826-7325

b. Laura K. Kennedy

Mail Stop 3-5-9 | 1710 SAIC Drive | McLean, VA 22102 | (703) 676-8215

6. Write a letter to the Chairman of the Audit Committee of the Board.

c/o Secretary of the Audit Committee of the Board of Directors

SAIC-Location 399

Mail Stop F-3 | 10260 Campus Point Drive | San Diego, CA 92121

7. Write a letter to the Chairman and CEO.

8. Communications with the Board and Lead Director.

c/o Corporate Secretary, SAIC

SAIC-Location 399

Mail Stop F-3 | 10260 Campus Point Drive | San Diego, CA 92121

Email to: corporategovernance@saic.com

SAIC's management is committed at all levels to take disclosure communications seriously, listen carefully, investigate when necessary, and take appropriate corrective action when warranted. SAIC employees are encouraged to seek guidance about potential or actual violations of our standards of business ethics and conduct. Employees should understand that raising ethical concerns or reporting misconduct is expected and required. SAIC managers and supervisors at all levels have a special responsibility to create and maintain an ethical work environment in which the free, open, timely and "good faith" reporting of concerns or suspected violation of these standards are the responsibility of every employee.

Employee referrals on ethics and standards of conduct matters will be treated confidentially whenever practical and legally possible. Anonymous referrals are also permissible but are generally less effective because of the difficulty of investigating and resolving issues on an anonymous basis. Anonymous referrals should be your last choice.

An important point to remember is retaliation against employees who use disclosure reporting channels to report misconduct is unethical and could be unlawful. The company takes complaints of retaliation very seriously. When necessary, we investigate these complaints fully as violations of our standards of business ethics and conduct. If you are concerned about retaliation, the company will monitor for this. Retaliation of any sort against employees reporting legal or ethical misconduct is strictly prohibited and will not be tolerated. Employee concerns about any such retaliation should be reported immediately to the vice president for ethics

and compliance, the chairman of the employee ethics committee, the general counsel, the senior vice president of human resources, or chief executive officer.

Responsibilities

General Responsibilities for All Associated with SAIC

SAIC directors, officers, employees, agents, consultants, subcontractors and suppliers are expected to observe a basic code of conduct in all activities related to SAIC. Each must:

- Conduct our business in accordance with SAIC's high ethical standards.
- Comply with the letter and spirit of the laws of the United States and other jurisdictions in which SAIC does business.
- Use SAIC and customer resources appropriately.
- Never participate in, condone or ignore illegal or unethical acts.
- Raise ethical concerns immediately, and escalate them as necessary to all appropriate resources within the company.

Company Responsibilities

SAIC's executive leadership and board of directors are committed to an ethics and compliance program consistent with the values of the SAIC Credo and our voluntary commitment since 1987 to the public accountability standards, principles and best practices of the Defense Industry Initiative on Business Ethics and Conduct (DII). The company establishes policies, standards and procedures including internal controls to prevent and detect misconduct and communicates these standards and procedures and other aspects of the compliance and ethics program to all employees in the annual Standards of Business Ethics & Conduct Handbook. The company also uses periodic training programs and other appropriate communications means to disseminate ethics and compliance information.

Governing Authority Responsibilities

SAIC corporate governance guidelines related to the Audit Committee and the Ethics and Corporate Responsibility Committee of the Board of Directors are available on ISSAIC at https://issaic.saic.com/eon/corpgov/bcomm.html.

The Audit Committee of the Board of Directors has established procedures for the receipt, retention and treatment of complaints regarding accounting, internal accounting controls, auditing, or other financial matters. These procedures allow for the confidential and anonymous submission of concerns regarding questionable accounting or auditing matters.

Employee concerns regarding accounting, internal accounting controls, or auditing matters may be submitted in writing with an external envelope addressed to: Chairman, Audit Committee c/o Secretary of the Audit Committee of the Board of Directors, SAIC Location 399/MS F-3, 10260 Campus Pt. Drive, San Diego CA 92121 or by telephone to the SAIC Hotline at (800) 435-4234. Any written concerns should be enclosed in a sealed internal envelope marked "Chairman, Audit Committee eyes only". The correspondence will be sent to the chair of the audit committee who will determine the appropriate manner for investigating and responding to the concern.

Vice President for Ethics and Compliance Responsibilities

The vice president for ethics and compliance reports to the general counsel and has the primary responsibility, in consultation with the general counsel as appropriate, for rendering advice regarding activities that may be proscribed or regulated by Administrative Policy SG-1. The vice president for ethics and compliance provides a quarterly evaluation of the company's efforts to the Ethics and Corporate Responsibility Committee of the Board of Directors. The vice president for ethics and compliance collaborates with other

corporate functional departments to conduct periodic risk assessments and program effectiveness evaluations.

The vice president for ethics and compliance is responsible for maintaining the Compliance Resource Center (CRC) Web site (https://issaic.saic.com/committees/crc). This site provides the tools and resources SAIC employees need to understand their obligations to comply with the regulatory requirements imposed on SAIC. As government contractors operating in the domestic and international marketplace, SAIC is required to comply with a vast array of government regulations. These regulations span a wide range of functions, including legal, finance, human resources, security, information technology, environmental, and others. The CRC Web site is designed to provide employees easy access to the policies, procedures, and training materials they need to understand their obligations in each of these areas.

Employee Ethics Committee Responsibilities

The Employee Ethics Committee is responsible for the company's communications program to institutionalize principles of ethical conduct among employees through the development and maintenance of the SAIC Credo and educational, training and information resources. The Employee Ethics Committee provides a forum for reviewing ethical issues. The committee collaborates with other corporate functional departments on the investigation of cases of alleged misconduct or the review of other ethical issues raised by employees. The Employee Ethics Committee recommends appropriate courses of action to line management to resolve the issues brought forward by employees and may also recommend reasonable steps to prevent and detect similar issues including making any necessary modifications to the SAIC compliance and ethics program. The Employee Ethics Committee monitors ethics case, contact and survey data.

Manager and Supervisor Responsibilities

SAIC managers and supervisors are responsible to ensure every employee under their supervision has read the Standards of Business Ethics & Conduct Handbook, understands that these standards represent company policy and has signed and dated an annual certification to that effect. SAIC managers and supervisors have a particular responsibility to set an example in their behavior, provide guidance and leadership to their employees and monitor and act on any behavior by their employees that violates these standards. As part of each employee's annual performance review process, SAIC managers and supervisors should ensure that all employees at all assigned work locations have access to either an electronic or hard copy of the latest edition of the Standards of Business Ethics & Conduct Handbook. SAIC managers and supervisors and their associated human resource and other functional compliance related staff are the critical first line disclosure channels for ethics and compliance concerns raised by employees and other SAIC stakeholders. Managers or supervisors of employees are required to determine whether a disclosure is at variance with this handbook or the referenced policies, and should, if appropriate, involve the appropriate functional or compliance related staff. Any disclosure with serious ethical or compliance risks should be brought to the attention of the vice president for ethics and compliance, the chairman of the employee ethics committee, the general counsel or the senior vice president of human resources. An Ethics Disclosure Documentation Form is available on ISSAIC at https://issaic.saic.com/committees/ethics/submit/claim.asp. This form allows managers and supervisors the opportunity to record and document ethics disclosures they receive as part of their important leadership roles and responsibilities. This form is designed to assist managers and supervisors in complying with their critical disclosure management responsibilities.

Employee Responsibilities

The company is committed to conducting its business in accordance with all applicable federal, state and local laws and regulations, and in accordance with high standards of business ethics. SAIC employees are expected to comply and to assist the company in complying with each of these obligations. Each employee is responsible for conducting his or her work

in a manner consistent with SAIC's Credo, and the ethics policies and standards of conduct discussed in this handbook. Any employee who suspects or has knowledge of infractions of these standards of conduct should immediately raise their concerns through the "disclosure reporting channels." Employees are expected to sign a annual certification statement affirming that they have read SAIC's Standards of Business Ethics & Conduct Handbook and understand that it represents company policy with which they are expected to comply. On a periodic basis employees shall be required to take training on ethics and compliance issues appropriate to their roles and responsibilities. Employees should visit the Compliance Resource Center (CRC) Web site at https://issaic.saic.com/committees/crc to determine the required compliance training associated with their job code and functional roles and responsibilities.

Responsibilities of Consultants, Subcontractors and Suppliers

SAIC policy is to instruct its consultants, subcontractors, and suppliers that they are expected and required to comply fully with SAIC's standards of business ethics and conduct and to inform appropriate SAIC company officials immediately of any illegal or unethical conduct in their dealings with SAIC directors, officers and employees.

Standards of Business Ethics & Conduct

It is essential that every director, officer and individual employee read and understand the following standards. Where applicable, further specifics may be found in the individual policies cited in parentheses next to each heading. These policies can be found in the Administrative Handbook, which is available from your managers and supervisors and through ISSAIC at **https://issaic.saic.com/policy/ah/**.

Financial Integrity, Accurate Disclosure, Record Keeping and Record Retention (SG-1, SG-18)

The company is committed to providing full, fair, accurate, timely and understandable financial statements and disclosures in all periodic reports and documents that the company files with or submits to the Securities and Exchange Commission (SEC) and other securities law administrators and in other public communications made by the company.

The company has zero tolerance for fraudulent financial activities. These types of activities include, but are not limited to, the following fraud risks:

- Financial statement manipulation (i.e., improper revenue recognition, over/understatement of assets, significant management estimates, and significant/unusual transactions)
- Asset misappropriation (i.e., check kiting, personal purchases, creation of a fictitious vendor by an employee or using shell companies, and falsifying sales/hours)
- Other schemes with potential material effect on financial statements (i.e., unauthorized receipts or expenditures and unauthorized acquisition, disposition or use of assets)
- Financial misconduct by management (i.e., business expense fraud, conflicts of interest, insider trading, and unauthorized compensation)
- Disclosure fraud (i.e., financial statement and footnote manipulations, and misrepresentation of SEC filings)
- Aiding and abetting any type of fraudulent financial activities

All SAIC employees must assist the company in maintaining sufficient financial internal controls and procedures to provide a reasonable assurance of accurate financial information disclosures in periodic reports and business records in accordance with our policies and procedures, U.S. generally accepted accounting principles, and the rules and regulations of the federal and states' security laws by:

- Always maintaining accurate books and records that fully, fairly and accurately reflect the company's financial information and reporting of direct or indirect transactions.

- Assisting as appropriate to their roles and responsibilities in preparing financial statements, financial information, and other disclosures included in periodic reports in a manner that fairly presents in all material respects the financial condition, results of operations, and cash flows of the company.
- Refusing to tolerate the creation or insertion of false or misleading information in any SAIC financial or other business record.
- Cooperating fully with the internal auditors and the independent auditors in their work and not impeding their efforts in any way or concealing information from them.
- Not authorizing or condoning the use of any "off book" accounting, unrecorded bank accounts, "slush funds," or any other device which may be utilized to distort records or true operating results and financial statements.

Reporting false information is strictly prohibited. Misrepresentation of any nature may lead to severe civil or criminal liability. Misrepresentation may take the form of omissions and inaccuracies, as well as organizing information in a way that is intended to mislead or misinform.

SAIC must ensure that business records are available to meet the business needs of the company, including the legal, tax and other regulatory requirements, wherever SAIC conducts its business. Failure to comply with the requirement to preserve documents and other information as required by Policy SG-18, Records Retention, can result in serious adverse consequences to SAIC and its employees. Specifically, 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. Doing so may subject SAIC and any offending persons to severe civil and criminal penalties including substantial damage awards, fines and imprisonment.

Proper Recording and Disbursement of Funds and Other Assets (SG-1)
Funds and other assets of the company are to be used only for legal and proper business purposes. No false, improper or misleading entries shall be made in the books and records of the company. Complete and accurate information is to be given in response to inquiries from the company's internal auditors and certified public accountants. All payments made by or on behalf of the company for any purpose must be fully and accurately described in the documents and records supporting the payment. Any concerns or complaints relating to accounting, internal accounting controls or auditing matters should be reported to one of the disclosure reporting channels, including writing a letter to the chairman of the audit committee. The concerns and complaints will be investigated and appropriate corrective action taken if warranted. Complaints involving questionable accounting or auditing matters, like all complaints, can be submitted confidentially and anonymously.

Timecharging

Time Recording, Labor Charging, and Customer Billing (SG-1, SH-1, SC-4, SC-2)
Labor is SAIC's principal product. Labor charges form the basis for invoices to customers. SAIC's Electronic Time-Recording System (SETS), SAIC's desktop computer-based time recording system (STRS), or a SAIC official paper timecard represent the employee's invoice of time worked and are the sole means for recording labor charges in the SAIC time recording system. The SAIC time-recording system is how we ensure that employee labor costs are properly recorded and the customer is billed correctly. Inaccuracies in timecharging records could subject the company or its personnel to criticism and, under certain circumstances, could be deemed a violation of federal law subjecting the company and its employees to civil and criminal penalties. The employee's timecard affirms that the record reflects an accurate distribution of time charges in accordance with company policy.

All employees must maintain a daily record of their activities using either SAIC's Electronic Time-Recording System (SETS), SAIC's desktop computer-based time recording system (STRS), or filling out an official SAIC paper timecard. SETS is the primary time-recording mechanism and should be used unless it is impractical to use SETS. In these circumstances STRS shall be used or, if not possible to use STRS, the official SAIC paper-based timecard shall be used. With paper timecards, including STRS, the employee's signature on the time record is the attestation that the record reflects an accurate distribution of time charges in accordance with company policy. With SETS, the employee submitting the time record electronically is the attestation that the record reflects an accurate distribution of time charges in accordance with company policy. Each employee is personally responsible for maintaining an accurate, daily record of time spent by task and for preparing a timecard for each payroll period. The record must be maintained in original form and be available for review by both the government and company auditors. Each timecard is required to be certified correct by the employee and the employee's immediate supervisor or a designated approver. The approver of the timecard certifies that to the best of the approver's knowledge the timecard information is accurate and in accordance with company policies. When an employee's immediate supervisor is not available, a designated approver may approve the timecard. However, no approver should approve a timecard without general knowledge about the employee's work efforts. It is the responsibility of employees to ensure that their time is accurately recorded to all cost objectives upon which they performed work during a given payroll period. Time actually spent on a given task may be charged only to that task. Similarly, all time spent on a particular task must be charged to that task and not, under any circumstances, to another task. Any employee who is concerned that this policy is not being followed within the company should immediately contact their business unit controller, business unit manager, the Employee Ethics Committee, or the SAIC Hotline.

Your SAIC timecard is the basis for billing direct and indirect costs to our clients. We must all pay close attention to the accuracy of our timecards because errors on timecards cause errors in billings. In the case of government contracts, errors in billings can be construed as a false claim, which is a federal crime. Each timecard is required to be certified correct by the employee and the employee's immediate supervisor or a designated approver. It is particularly important to be attentive to the following guidelines:

- Employees must receive a project number for each task they perform, along with an explanation of the associated statement of work. Supervisors and employees are jointly responsible for understanding, and if necessary, verifying, the appropriateness of any charge number provided.
- If a charge number has not been assigned, then the hours worked must be charged to a suspense account.
- Employee labor must be recorded at least daily.
- If an employee is unable to submit the timecard due to absence, the timecard is processed as a "dummy."
- Employees must submit their own timecards, but only after the timecard is complete. By so doing, the employee certifies that the hours and project numbers are accurately recorded in accordance with company policies.
- Timecards should not be submitted earlier than the day before the timecards are due unless the employee will be on travel or personal leave.
- The approver of the timecard certifies that to the best of the approver's knowledge the timecard information is accurate and in accordance with company policies.
- Timecard corrections and adjustments must be made as soon as possible.
- After processing the timecard, errors must be corrected immediately upon discovery.

It is the responsibility of management to ensure that comprehensive formal timecharging training is provided to new employees immediately upon commencement of work and that refresher training is provided to employees at the time of their annual performance reviews.

Records of employee training shall be maintained. As part of his or her annual performance review, an employee's completion of formal timecharging training shall be confirmed.

This policy applies to SAIC Companies 1, 6, 9, 21 and 39 (ANX). Other SAIC companies must develop their own timecharging policy approved by the corporate controller.

Employee Business Expense Reimbursement (SG-1, SC-12)

SAIC uses the expense report as support for preparing bills to the government and other customers. Invoices that contain inaccurate costs can be considered a false claim resulting in penalties for SAIC. By signing an expense report and submitting it for approval, the employee is verifying that the request for reimbursement is valid and in accordance with company policy. The employee's signature on the expense report is the attestation that the expenses are accurately stated and recorded against the proper account. SAIC Administrative Policy SC-12, Employee Business Expense Reimbursement, more fully describes the procedures and policies for claiming business expense.

SAIC will reimburse employees for valid business expenses authorized by the company and will account for those reimbursed expenses in accordance with contractual regulations or requirements. Business unit general managers of SAIC companies engaged solely in commercial business may develop expense reimbursement policies commensurate with their business area and good business judgment. Company controllers must approve alternate expense reimbursement policies applicable to commercial business.

Government Investigations (SG-1)

SAIC will cooperate fully with government investigations. SAIC will cooperate fully with authorized investigatory representatives of the government (such as investigators, agents or attorneys) when such representatives request information or documents in the possession of the company to which the government has a legitimate right. The general counsel is designated as the focal point for coordinating responses to such requests or inquiries and for advising employees and other appropriate parties regarding the nature of the inquiry and the rights and obligations of the company, employees and other parties in connection therewith. Experience has shown that proper coordination of such responses by the company and its employees results in a more timely and accurate exchange of information.

With respect to normal, recurring contacts by such government personnel, the general counsel will generally delegate coordination to other authorized company representatives. Typically, government officials will make such requests through properly designated corporate channels, but occasionally requests for information or documents will come directly to other company employees. All such inquiries or requests must be coordinated with the general counsel or designated corporate office before any response is provided.

Conflicts of Interest: Other Employment, Outside Interests, or Related Transactions (SG-1)

SAIC employees must refrain from any private business or professional activity and from having any direct or indirect financial interest that would create a conflict between their private interests and their legal or moral responsibilities to this corporation. In their transactions with others, all employees are expected to act in the best interest of the corporation and not to their own private advantage. They are not to engage in any private business or professional activity or to enter into any financial transaction that involves the direct or indirect use of inside information (information that has not become public information) gained through their position with the company to further a private interest or for private gain for themselves or another person or entity. They are not to use their position in the company

in any way, nor to induce or coerce any person or entity to provide any financial benefit to themselves or another person or entity.

No employee may serve as a director, officer or employee of; serve in any managerial capacity for; or be retained or compensated in any capacity by any private or public entity, including the federal or any state or local government, that is a customer, vendor or competitor of this company without the prior written approval of SAIC's president, CEO or an appropriate designee.

No employee, nor any member of the employee's household or immediate family (relative of the employee or the employee's spouse), may speculate in materials, equipment, supplies or property to be purchased by the company based upon information gained in the performance of the employee's duties and not available to the general public.

No employee, nor any member of the employee's immediate family, shall be involved in any business transaction with the company wherein a conflict of interest exists, could exist, or appears or is perceived to exist. No employee, nor any member of the employee's immediate family, may have a substantial financial interest in an organization with which the company does business. Substantial financial interest includes being a proprietor or partner or owning stocks or bonds in excess of 10 percent of the total stocks or bonds of a corporation. If any departure from this policy is contemplated, the conditions outlined in Administrative Policy SG-1 must be fulfilled before the business transaction commences.

Although the foregoing is addressed to employees of the company, it is in general also applicable to outside directors. In dealings with any concern that they have reason to believe may be a customer, a supplier of goods or services to, or a competitor of the company or any of its subsidiaries, outside directors of the company should promptly disclose to the chairman of the board any instance in which they or any immediate member of their families:

- Receive or accept money or things of more than nominal value as gifts, loans (except bank loans) or compensation from such a concern.
- Hold any position or employment in such a concern.
- Own or acquire (in their name or in the name of others) any financial interest in such a concern.
- In general, outside directors should disclose to the chairman of the board any situation in which their personal activities or interests might appear to be in conflict with those of the company.

Annually, each officer of the company will be required to submit a conflict-of-interest disclosure statement to the Office of the General Counsel.

- **Organizational Conflicts of Interest (SG-1)**
  No contract shall be negotiated or executed if the interests of the particular customer are of such a nature as to compromise or threaten the company's ability to maintain unbiased objectivity in serving its other customers. In instances in which potentially conflicting situations may be created, agreements may be entered into if the parties involved have full knowledge of the potential conflict and consent to the arrangements in advance. The contract file should contain appropriate documentation of such arrangements.

- **Securities Trading (SG-2)**
  If a director, officer or employee has "material, nonpublic information" (as these terms are defined in SAIC Administrative Policy SG-2, Securities Trading) relating to SAIC, or any other company, including the company's customers, partners or suppliers, neither that person nor any related person shall buy or sell securities of such company while in possession of such information. In addition, such person shall not engage in any other action to take advantage of, or pass on to others, such information.

All nonpublic information should be considered confidential information. To use nonpublic information for public financial benefit or to "tip" others who might make an investment decision on the basis of this information is both unethical and illegal.

All SAIC insiders and related persons must obtain written clearance from SAIC's general counsel or a designated compliance officer before engaging in any type of trade transaction in SAIC stock or its publicly traded subsidiaries.

Violations of this policy will not be tolerated. Significant disciplinary actions, up to and including termination, may be imposed on employees who intentionally or even negligently fail to comply with this policy. The federal securities laws may also impose significant civil and criminal penalties and sanctions on the company and individuals involved in the insider trading.

Other Important Standards of Conduct

Use of SAIC and Customer Property, Equipment and Facilities (SG-1)

Employees are not authorized to use or allow the use of corporate property, software, equipment or facilities for non-company business unless the use is approved in advance by the employee's manager. Examples of activities that might be approved include the incidental and insignificant use of: (1) email for communications of a social nature; (2) reproduction or facsimile equipment to perform personal tasks that would otherwise require that the employee leave the company's facilities during business hours; (3) personal computers to support further education and training, preparation of professional papers intended for publication, and (where the activity is to be accomplished outside of normal business hours) occasional word processing, scheduling, or financial planning of a personal nature; and (4) local telephone calls.

Although the company does not regularly monitor voicemail or email messages, employees are on notice that they have no expectation of privacy in the use of company computers, voicemail and email systems. Although employees have certain passwords or codes to restrict access to computers, voicemail and email to protect those systems against unauthorized access by external parties, employees should understand that these systems are intended for business use, and all computer information, voicemail and email messages are considered company records and are not private. Therefore, SAIC maintains the right to enter into any of those systems without notice to inspect and review all data recorded.

Since SAIC reserves the right to access these systems without notice, employees should not assume that any information is private, including messages or data that are "deleted." Employees should also have no expectation of privacy relating to any information contained in their computer, whether on a hard drive, computer disk or any other medium.

Computer, voicemail, or email messages must not contain any material that may reasonably be considered offensive, disruptive, defamatory or disparaging toward any employee or company. Offensive content includes, but is not limited to, sexual comments or images, racial slurs, gender-specific comments, or any comments that would be offensive based upon an individuals age, sex, sexual orientation, religion, race, color, political beliefs, national origin, disability, or veteran or marital status.

Notwithstanding any approval by the company, if the use of company property, software, equipment or facilities has a personal or outside business purpose and the costs are reasonably ascertainable (for example, long-distance calls or the use of overnight mail), the employee shall be required to account for such expenses and reimburse the company.

If the employee is located at a customer facility or is otherwise using equipment that has been furnished by the customer or purchased on the customer's account, such equipment

and facilities can be used only to perform tasks under the contract for which it was provided. Thus, even the incidental and insignificant use of such property, software, equipment, or facilities for non-contract business without the specific written consent of an authorized customer representative is prohibited by this policy.

The use of company premises for non-business related activities is prohibited without the advanced written consent of the senior site manager for that location or the senior vice president, human resources. Employees using customer property, equipment and facilities must have specific written consent from an authorized customer representative before any employee use unrelated to the customer's program.

All directors, officers and employees should protect the company's assets and ensure that they are used for legitimate business purposes. Every employee is responsible for protecting, properly using, and accounting for all forms of company property that is within his or her possession or control. Company property includes a broad range of assets. It refers both to property that SAIC owns, and property that SAIC or its employees possess, by lease, loan or otherwise. Removal of company property from the premises for valid business reasons is permitted if authorized by the employee's supervisor and is done in full compliance with the property removal procedures. Damaged property must be reported to your supervisor, and theft or misuse of company property must be reported immediately to your supervisor. Except with proper authorization, no company property is to be taken, sold, loaned, given away, damaged, destroyed or otherwise disposed of, regardless of condition or value.

If there is theft or damage to SAIC property that requires the response of local law enforcement officials, employees are required to immediately notify Corporate Security.

Copyrighted or Licensed Materials (SG-1, SG-3)

It is both illegal and unethical to engage in practices that violate copyright laws or licensing arrangements. It is the policy of SAIC that all employees respect the rights conferred by such laws and arrangements and refrain from making or purchasing unauthorized copies of protected materials such as printed matter and computer software. For example, SAIC is committed to honoring its legal and contractual obligations with respect to the proper use of copyrighted materials of third parties, including personal computer software licensed from outside vendors. Copyrighted materials, including both printed matter such as books and magazines and software, must not be reproduced or distributed without proper authorization from the copyright holder. The amount paid for a software product represents a license fee for the use of a single copy unless another arrangement, such as a site license, has been negotiated. Reproduction of copyrighted software without proper authorization violates U.S. copyright law and is a federal offense. All employees are obligated to be familiar with and adhere to the terms of any license agreement relating to the software products they use. Administrative Policy SG-3, Information and Data Protection, provides more details on this subject.

Inventions and Intellectual Property (SG-6)

The intellectual property of the company, and the company's right to use and exploit this intellectual property, are recognized as valuable assets of the company. The intellectual property of the company shall not be sold, transferred or licensed exclusively to third parties without the prior written approval of the chief executive officer or his designee. Intellectual property, or inventions may include licenses for patents, know how, source code and other software, solution sets, processes, methodologies, tools and the like.

All employees must promptly disclose and report inventions conceived or developed by them as an employee of the company. Consultants must make similar disclosures and reports on inventions conceived or developed by them during the actual performance of services for the company. The company, in turn, may be obligated to disclose and report to its customers inventions that are conceived or made operational in the course of, or under, customer

contracts, depending upon the terms and conditions of such a contract. Administrative Policy SG-6, Inventions and Commercialization, provides more details on this subject.

Accurate Representation of Data or Credentials

SAIC provides customers with reports and studies that are used as the basis for important future decisions, some of which are critical to the security, safety and well-being of our communities throughout the world. It is the responsibility of all employees to ensure our customers receive a product that accurately reflects the results of our research and study. Principal investigators and division managers must ensure contractual projects have been properly reviewed according to SAIC policy.

Our customers are frequently billed according to the skill level of the individuals involved in a project. In addition, the company relies upon representations of education and professional experience in making representations to our customers. Moreover, education and experience are important factors in the selection and advancement of employees. It is crucial, therefore, that all employees ensure their resumes are accurate and complete, and any other representations to customers on employee education, experience and capabilities are correct. Employees who knowingly falsify their personal credentials are subject to disciplinary action up to and including termination of employment.

Employee Resumes

The company requires that the resumes of its employees be used in connection with the solicitation of new business, and each employee authorizes the use of his/her resume for such purpose as a condition of his/her continued employment. Notwithstanding such authorization, and in order to ensure the resumes relied upon by the company accurately reflect education and professional experience, it is the general policy of the company that a resume for anyone proposed to work on a contract may only be used with the approval of the individuals involved. In the case of consultants the approval must be in writing. If the employee-approved resume is modified in any substantive way to accommodate the format of a particular proposal, it is the responsibility of the proposal manager to obtain, and maintain in the proposal file, a record of the employee's approval of the changes to his/her resume. Employees have a responsibility to ensure the information on their resume is true and accurate to the best of their ability.

Reporting Adverse Personnel Information (SG-13)

Adverse information is any personal behavior, conduct, activity or a consequence of such activity, that calls into question an individual's integrity, trustworthiness, reliability or willingness to comply with established security guidelines or other action which may impact negatively upon SAIC or the workplace. It is SAIC policy to report all adverse information that may bear on the security clearance of a "cleared" employee, or an employee in process for a security clearance, consultant or temporary help personnel to the Department of Defense and other appropriate government agencies, as applicable. Examples of reportable actions include: 1) A disregard for security policy, procedures or safeguards; 2) The inability to live within one's means, as evidenced by legal or creditor actions brought to the company's attention; 3) Involvement with the possession, use or sale of illegal substances, use or abuse of alcohol or other controlled substances that impairs the worker's reliability or performance of duties; 4) Arrest or indictment for unlawful activity. Upon accepting responsibility for a personnel security clearance each employee is briefed on their individual responsibility to safeguard and protect classified information; to comply with applicable security policies, practices, procedures and directives; and their responsibility to report any change or event in their personal life that may have a bearing on the established personnel security clearance criteria. All managers and supervisors have a responsibility to be attentive to behavior patterns of persons in their charge that may adversely affect proper safeguarding of classified information, to initiate intervention and to seek corrective action. The director of corporate security is available to all managers and supervisors to provide confidential guidance and

assistance for all adverse-information matters under consideration. It is a requirement that all adverse information reports be routed through Corporate Security for transmission to the appropriate government office of adjudication.

Drug and Substance Abuse Policy (SG-21)

SAIC's policy is to maintain a drug-free workplace. The unlawful manufacture, distribution, dispensation, sale, transfer, purchase, possession or use of a controlled substance is prohibited in the SAIC workplace. SAIC employees must refrain from illicit drug use and substance abuse. Such practices are contrary to good physical and mental health, performance of superior work, and the safety, security and well-being of our communities throughout the world. Employees engaged in prohibited activities will be subject to disciplinary action at the sole discretion of SAIC, up to and including removal from regulated contract work, and termination of employment with SAIC. In addition, SAIC reserves the right to report any such prohibited behavior to the appropriate authorities. Employees must agree to notify SAIC of any criminal drug statute conviction for a violation occurring in the workplace no later than 5 days after such conviction as a condition of employment on such contracts and continued employment with SAIC. Employees further agree to abide by any and all of the terms contained in the Drug and Substance Abuse Policy (SG-21). Employees engaged in illicit drug use or substance abuse are encouraged to obtain professional help or to seek employment elsewhere.

Equal Employment Opportunity (SH-6)

SAIC is committed to providing employees and employee candidates the right to equal employment opportunity and a discrimination-free work environment. It is essential, therefore, that all employment practices are 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. This policy of equal employment opportunity applies to all personnel policies and procedures including recruitment and hiring, promotions, transfers, and terminations, as well as compensation, benefits and other terms, and conditions and privileges of employment.

SAIC takes affirmative action to recruit, hire and promote qualified minorities, women, disabled persons, and covered veterans. While all SAIC employees share in the responsibility for fostering a discrimination-free work environment where employees are treated with dignity and respect, managers assume responsibility for making good faith efforts and demonstrating performance toward the implementation of company affirmative action plans and achievement of plan objectives.

All SAIC employees should encourage and support our affirmative action efforts, as they serve as the foundation for establishing and maintaining a more diverse, creative and innovative workforce that will enable the company to remain competitive in the increasingly diverse global marketplace.

Incidents of suspected discrimination should be reported through the "disclosure reporting channels" identified under the "Key Messages" section on page eight of this handbook. All reported incidents shall be investigated in a confidential, objective, thorough and timely manner.

Harassment (SH-8)

Harassment of employees by the company, its employees, its managers/supervisors, agents, customers, subcontractors or vendors is unacceptable and will not be tolerated. Actions that create an offensive working environment resulting from unwanted and unwelcome behavior are prohibited. Any incident of harassment or discrimination that you observe or experience should be reported through the appropriate "disclosure reporting channels" identified under the "Key Messages" section on page eight of this handbook. All reported incidents shall be investigated in a confidential, objective, thorough and timely manner.

No employee shall be harassed, threatened, degraded or treated adversely because of his or her race, sex, sexual orientation, marital status, color, religion, national origin, ancestry, age, medical condition, disability, military service status, or any other basis prohibited by law. Discrimination and harassment in the workplace by any employee shall result in appropriate disciplinary action, up to and including termination of employment, and could result in personal, legal and financial liability.

No employee shall engage in any conduct of a threatening, abusive or violent nature toward any employee, supervisor, contractor, customer or any other person with whom he or she comes into contact during or as a result of his or her employment with SAIC.

Staffing Policy (SH-2)

Mobility at SAIC can be an important facet of employee professional growth and career progression. As such, managers and employees have a mutual responsibility for taking appropriate action when considering internal transfer conditions. The responsibility to initiate and complete an employee transfer is shared among the employee's current and future management and the HR managers of the releasing and receiving organizations. Employees are eligible to be considered for lateral or promotional movement provided that their overall performance is not rated unsatisfactory in the previous year's annual performance review documentation, they are not on a Performance Improvement Plan (PIP) at the time, and they have been in their current position for a minimum of 6 months. In the interest of promoting good communication, employees are encouraged, but not required, to inform their manager that they plan to interview for another job prior to the interview taking place. After the interview, if it appears likely that the employee will receive and accept an offer, the employee must notify his or her manager promptly. If placement is unlikely, the employee need not notify his or her manager.

A supervisor or manager shall not have closely related individuals (e.g., a spouse, domestic partner, person involved in a dating relationship, children, stepchildren, parents, in-laws, or siblings) under his or her direct or indirect supervision in order to prevent a conflicts of interest and/or allegations of favoritism or sexual harassment. Direct supervision includes any of the following responsibilities: assigning work, conducting performance or salary reviews, approving timecards or expense reports, or making recommendations affecting the person's employment, compensation or retention. Indirect supervision includes having program management, profit and loss (P&L), or budgetary responsibility for the affected group, business unit or organization.

The employment or transfer of individuals into a situation in conflict with this policy is prohibited. If a conflict with this policy occurs through any circumstances, the individuals involved are required to immediately report their situation to their manager; their HR manager; the corporate director, HR operations; and other senior management as necessary to determine the best course of corrective action. When special conditions apply, situations involving the indirect supervision of closely related individuals in conflict with this policy may, with the approval of the senior vice president of human resources, be resolved by establishing procedures to monitor and manage the conflict of interest situation.

Wage Determinations/Prevailing Wage and Benefits Requirements (SC-5)

Administrative Policy SC-5 confirms SAIC's commitment to provide its eligible employees with appropriate wages and fringe benefits as defined by the McNamara-O'Hara Service Contract Act (SCA), Davis-Bacon Act (DBA), and state and local prevailing wage law requirements in accordance with any associated wage determinations. SAIC will comply with SCA, DBA and prevailing wage laws, including both pay and fringe benefits, in accordance with applicable wage determination requirements as defined in our contractual obligations with federal, state and local governments. For employees working on multiple contracts, the company will ensure that the pay rate and fringe benefits for those hours charged to each covered contract meet the requirements of the applicable wage determina-

tion. The Corporate Compensation and Benefits Department is responsible for verifying compliance with applicable fringe benefit requirements and for maintaining a system that will accommodate the payment of compliant wages and fringe benefits to eligible employees. The system will be made available to all affected units of SAIC, and reports will be made available to all affected program managers.

Public-Facing Communications (SG-10)

- **News Releases (SG-10)**
  The reputation of the company rests in part upon the content and tenor of communications with the news media or communications generally accessible by the public, customers or potential customers that appear to originate from the company or appear to have been authorized by the company. Such communications are generally called public-facing communications. Examples of public-facing communications include, among other things, any advertising or marketing materials, endorsements, the content of Web sites and domain names attributable to the company, press releases, and comments to any of the news media either by official company spokespersons or by employees whose stated affiliation with the company is identified.

  No employee of the company is authorized to make any statements, to give any information related to the company or any of its activities, or to comment on the plans and activities of the company's customers to the news media without prior clearance by External Communications, the chief executive officer, or the executive in charge of Communications.

  No employee of the company is authorized to write opinions, letters to the editor, commentary, or any other form of communication to the news media that identifies the writer as an employee of the company without prior clearance by External Communications, the chief executive officer, or the executive in charge of Communications.

  As used in this policy, the term "news media" includes, without limitation, newspaper, magazine and other publishers; radio and television stations; and any other entity, including Internet Web sites and chat rooms.

  All inquiries from any representative of the news media must, under all circumstances, be immediately referred without comment directly to External Communications. While news media representatives may plead impending deadlines in order to elicit comments from other company sources, the representatives of External Communications are the company's sole official spokespersons. They will ensure appropriate coordination and review by the company's executive officers of any statements to the news media attributable to the company.

  This policy is not intended to restrict communications by employees as private citizens, but to ensure the coordination in advance of any discussion involving the company and communications by company employees who, by virtue of their stated affiliation or position within the company, may appear to be speaking on behalf of the company.

- **Interaction with Members of the U.S. Congress (SG-10)**
  Interaction in any way with members of the U.S. Senate or House of Representatives, or their respective staffs, whether through meetings or letters or other methods, including Internet communications, regarding SAIC business or interests must first receive approval from and be coordinated with the Government Affairs Office in Washington, D.C. Normally, such requests should be made at least 10 working days before any such interaction is scheduled. The Government Affairs Office shall ensure that these interactions do not contain content that would negatively reflect upon the reputation of the company or in any way contradict or impede efforts approved or initiated by the Government Affairs Office. Group managers and/or business unit general managers shall retain responsibility for ensuring that all requests for interaction are timely submitted

to the Government Affairs Office and that these interactions protect the interests of the company. Administrative Policy SG-1 requires the prior approval of the Government Affairs Committee for any political contribution to federal, state, local or foreign candidates for office or political parties and for the retention or renewal of any firm or individual for federal, state, local or foreign lobbying or government relations assistance.

- **Accuracy in Marketing Materials (SG-10)**
  The company has both a legal and an ethical responsibility to portray accurately and honestly the capabilities of the company's products and services in all marketing and advertising related materials.

  Inaccurate, misleading or exaggerated claims in marketing materials (including Web sites) and advertisements can raise unreasonable expectations among the company's customers and prospective customers. Such claims can force the company to deliver products or services never originally intended or to deliver products or services at higher-than-bid/expected costs to the company. In addition, such claims can lead to allegations of false or misleading advertising by competitors of SAIC. In the extreme, such claims may also result in formal charges that the company has engaged in false or deceptive advertising or misrepresented its performance capabilities, products or services, thereby impugning the credibility of the company and its employees and potentially creating liability for the company under various federal and state advertising and securities laws.

  All marketing and advertising related materials shall be reviewed by External Communications prior to publication or any other form of distribution. The corporate proposal centers and creative services centers in McLean and San Diego, and the External Communications can assist in the creation of and submission for approval of suitable marketing- and advertising-related materials when creation of these materials has been approved by the appropriate line manager. Group and business unit general managers shall have responsibility for ensuring the truthfulness of all claims contained in such materials as well as for the timely submission of such materials to the External Communications. For materials originating with corporate officers or staff, the relevant senior vice president shall be responsible for ensuring timely submission of these materials to the External Communications.

Truth in Negotiations Act (SG-28)

SAIC must comply fully with the Truth in Negotiations Act (TINA) in the conduct of its U.S. government business. The purpose of TINA is to give the government effective means of negotiating a fair and reasonable price. It requires disclosure of cost or pricing data to the contracting officer (or designated representative) and certification that such data is accurate, complete and current for negotiated procurements requiring TINA certification as of a mutually agreed-to date. The requirement for TINA compliance applies to all organizations generating or receiving cost or pricing data, whether SAIC is a prime contractor to the U.S. government or is a subcontractor under a U.S. government contract subject to TINA; or when a SAIC business units supports a U.S. government prime contract or subcontract through an inter-company work authorization or similar arrangement.

Administrative Handbook Policy SG-28 addresses U.S. government requirements for full disclosure of certain cost or pricing information when TINA applies. Submission of cost or pricing data may be required under negotiated contracts, subcontracts and modifications that exceed the "TINA threshold" unless the contract pricing action is specifically exempt from TINA disclosure requirements.

SG-28 also addresses SAIC's current practice of disclosing certain quantitative risk analyses and/or assessments, regardless of whether they meet the definition of "cost or pricing data" and thus, the disclosure requirements of TINA.

SG-28 policy applies to SAIC, its subsidiaries and affiliates that conduct business with the U.S. government.

Questions or clarifications related to TINA compliance or any of the provisions in this policy should be addressed to Corporate Contracts, Procurement, Pricing, or Legal. Additional detailed information and guidance related to the development and disclosure of cost or pricing data can be found within SAIC's Cost Estimating System Manual and supplements thereto.

Marketing and Contracting and Conducting International Business (SG-9, SG-14)

SAIC will pursue international business opportunities with the same values and code of conduct applied to domestic business – specifically, demonstrating the highest regard for and adherence to quality, ethics and compliance with U.S. and foreign laws, stock ownership, and fair financial return. All employees of SAIC share in the responsibility of ensuring adherence to these values and this code of conduct.

SAIC selectively establishes and operates internationally through subsidiaries and branch offices when required to promote business interests, to employ local nationals, or to obtain work and residence permits for expatriates; and when long-term profitability can be sustained.

All international business shall be conducted in full compliance with SAIC's Policy SG-9, Complying with the Foreign Corrupt Practices Act, and with Policy SG-14, Marketing, Contracting and Conducting International Business.

International business involves practices and issues which can differ greatly from domestic business practices. In addition, international business is governed by numerous statutes and regulations imposed by the U.S. government and by foreign governments. These laws apply to the solicitation and performance of international business, and may apply even though the customer is another SAIC-owned company or is located in the United States.

Any given foreign transaction may involve sales representation, business organization, taxation, employment, and legal issues that must be addressed during the earliest stage of marketing. Similarly, the United States government has imposed restrictions on doing business with certain countries. Similarly, the United States government has imposed restrictions on doing business with certain countries. Laws such as the Foreign Corrupt Practices Act (FCPA), Export Control Statutes, Sanctions Regulations, Anti-Boycott Act, and International Traffic in Arms Regulations (ITAR) address marketing conduct, the reporting of requests for certain information, and the transfer of technology outside the United States. This includes standard processes and controls to meet the requirements associated with the Sarbanes Oxley Act of 2002. Penalties for non-compliance with these laws are significant and can include heavy fines on individuals and the company, prison sentences, loss of export privileges, and debarment from United States or foreign government contracts.

In order to use the most advantageous business practices and to assure compliance with laws governing foreign sales, SAIC has instituted policy SG-14 to document the process required for coordinating and approving marketing, sales, proposal, acquisition, divestiture and contract activities involving international activities, foreign governments, or other foreign entities.

Foreign Corrupt Practices Act (SG-9)

The Foreign Corrupt Practices Act (FCPA) directly affects the conduct of international business. It criminalizes bribery as a means of getting business overseas or obtaining an unfair advantage. It also imposes civil liability on companies that do not accurately record all expenditures and transactions in their accounts. The scope of the FCPA is very broad: it is a crime for a United States company, its officers, employees, agents, etc., to promise to pay, pay, promise to give, give or authorize the paying or giving of anything of value, directly or indirectly, to foreign government officials in order to influence the official's acts or decisions, or to induce the official to use his influence with others to affect the acts or decisions of a foreign government or international organization, if this is done in order to obtain or retain

business or an unfair advantage. The term 'foreign government official' includes anyone acting in an official capacity, employees of state-owned enterprises, officials of public international organizations (such as the UN, World Bank, etc.), and candidates for public office or officials of political parties. In addition to the anti-bribery provisions, the FCPA contains accounting provisions. These provisions require that books and records accurately reflect all financial transactions.

SAIC is committed to compliance with the FCPA. Any officer, director, employee, consultant, agent or affiliated person who is aware of an actual or potential FCPA violation must report the violation to Corporate Legal immediately. Failure of any employee to comply with this policy may result in disciplinary action, up to and including termination of employment.

Foreign Person Access to Controlled Technology (SG-4)

SAIC complies with the International Traffic in Arms Regulations (ITAR) governing the export of military hardware, software and technical data; the Export Administration Regulations (EAR), regulating the export of dual-use hardware, software and technical data; and all other applicable U.S. government export regulations. These regulations restrict the transfer of export-controlled items abroad and to foreign persons, including employees, without first obtaining a license or applicable license exemption. SAIC also complies with the NISPOM (DOD 5220.22-M National Industrial Security Program Operating Manual), which covers the protection requirements for safeguarding, controlling and releasing classified information. Further, the NISPOM requires control measures to be established which preclude the unauthorized access to controlled technology by foreign persons. SAIC will restrict access by foreign persons to SAIC sites, including buildings, sections of buildings, rooms, or information system assets, as necessary to ensure SAIC compliance with contractual obligations and applicable U.S. export control and security regulations. SAIC Corporate Security and IT Security have implemented physical, computer system and administrative controls and procedures as necessary to ensure that controlled technology is safeguarded as required by the ITAR and NISPOM. It is the responsibility of the SAIC hiring manager (sponsor) of foreign persons to read and comply with the export analysis requirements of SAIC Policy SG-4.

SAIC is an equal opportunity employer. The controls contained in this policy are consistent with U.S. antidiscrimination laws and regulations and are necessary to ensure compliance with U.S. export and security laws and regulations.

Alcohol Use (SG-21)

No one may be intoxicated on company premises, within automobiles being used for company-related business or travel, or while conducting work or company business. Because the consumption of even small amounts of alcohol impairs judgment and safety, the consumption (including possession of open containers) of alcohol in all such circumstances is also strictly forbidden, with these exceptions:

- Responsible use during authorized business entertaining.
- Responsible use at social/business functions that are authorized by the appropriate manager provided that non-alcoholic beverages are also available.

Nonsmoking Policy (SG-22)

To provide SAIC employees with a safe and healthy workplace, smoking is not permitted inside any SAIC facility or within company automobiles. Smoking is permitted at certain designated areas outside of company buildings.

Prohibited Items (SG-19)

The unauthorized introduction of prohibited items by employees, consultants, temporary-agency personnel, interns, vendors, contractors or visitors to any SAIC facility is strictly

prohibited. Violators may be subject to disciplinary or adverse action, including termination of employment or contractual relationship. Additionally, contractors, vendors and visitors violating this policy may have the items confiscated and be restricted from further access to SAIC. Local law enforcement may be contacted if appropriate. SAIC shall comply with all federal, state and local laws with regard to reporting the possession of illegal items. Weapons discovered on SAIC property must be reported to Corporate Security immediately to coordinate appropriate action.

Prohibited categories of items include firearms, explosive or incendiary devices, any item brought onto the site that may be used to inflict bodily harm or to threaten or intimidate others, any recording devices or cameras, surveillance equipment, controlled substances, including illegal drugs and associated paraphernalia, except for prescription medicine and other items prohibited by law. Cellular phones equipped with camera and recording capability are not precluded from SAIC premises; however their use is still restricted in accordance with SAIC Policy.

Under specific and controlled circumstances, restricted items or materials that are determined not to be dangerous may be introduced onto SAIC property with the approval of the facilities manager, security manager, senior human resources manager, or senior management of the facility. Such exceptions may be made only if the items are necessary for performance on a contract or in pursuit of a business activity or the items are to be used in connection with a SAIC supported or sanctioned activity.

Environmental Compliance and Health and Safety (SG-1)

SAIC is committed to conducting its business in a manner that protects the health and safety of our employees, customers, business partners, community neighbors, and the environment. To accomplish this, SAIC must ensure compliance with applicable federal, state and local environmental, health and safety laws and regulations. A failure to comply may trigger a disclosure obligation to regulatory agencies and/or customers, with potential negative effects including civil or criminal penalties, fines, or loss of future business opportunities. Therefore, all employees are responsible for performing their activities in accordance with the requirements identified in SAIC's Environmental Compliance & Health and Safety Program Manual, location or contract-specific program requirements, and in accordance with all training or job instructions received.

Wearing Appropriate Identification

SAIC identification (ID) badges must be worn and visible above the waist at all times while on company premises. Employees should challenge any person not wearing a SAIC ID badge. Employees must immediately report the loss or theft of their ID badge to their manager and facility security manager. SAIC badges are company property. Employees should remove and secure the badge after exiting SAIC spaces. The ID badge should not be used for clearance verification. The security clearance and need-to-know requirement must be verified through SAIC security prior to releasing classified information. Detailed information on the SAIC identification badge scheme is available on ISSAIC at https://issaic.saic.com/security/corporate/access/badges.html

Use of Audio or Video Recording

While audio or video recording can sometimes create a useful record, no employee, except with the authorization of SAIC Corporate Secretary and the general counsel, shall audio or video record any business conversation, telephone call, or meeting without first informing every other participant and obtaining his or her consent to such recording.

Expert Witness Consulting

SAIC may be asked to enter into contracts for the company to provide consulting services in support of matters in litigation or arbitration in which SAIC is not a party or in proceedings

before regulatory or legislative bodies. Such consulting services may include SAIC preparing reports, company employees testifying as expert witnesses, or providing other support as non-testifying experts. In these circumstances care must be taken to avoid situations where SAIC could find itself advocating a position on behalf of one SAIC client that is opposed to the interests of another. In order to avoid such potential conflicts of interest, the relevant business unit must notify Corporate Contracts or Corporate Legal prior to the negotiation or execution of contracts under which the company is to provide consulting services as either a testifying or non-testifying expert.

Misconduct in Science (SG-1)

Research is the key element of SAIC's business base and the integrity of that research is vital to the company's reputation. Accordingly, any misconduct in the performance of research is a paramount concern for our employees. Misconduct means fabrication, falsification, plagiarism or other practices that seriously deviate from those practices that are commonly accepted within the technical community for proposing, conducting or reporting research. It does not include honest differences in interpretations or judgment of data. It is the responsibility of any employee involved in research to conduct it according to the highest standards of integrity and to report suspected misconduct. The responsibility for conducting inquiries or investigations concerning allegations or suspicions of misconduct in science resides with the vice president for ethics and compliance.

Proprietary and Confidential Information

Definition (SG-8)

Proprietary and confidential information is that broad category of information that must be protected by company employees from unauthorized disclosure or unauthorized use. Such information includes all information or knowledge that an individual or a company has and, at the time, finds it advantageous not to make public. It includes information in electronic media and paper copies, as well as information in the minds of employees.

Some general examples include, but are not limited to, information relating to SAIC's products and technical efforts, financial information, personnel information, and marketing information. A more detailed listing of examples is contained in attachment (1) to Administrative Policy SG-8, SAIC Proprietary Information, Technical Data, and Personal Information.

The company and its employees must safeguard not only the proprietary information it owns but also the proprietary information belonging to others which has been entrusted to the company to be kept confidential from other customers.

Designating and Changing the Status and Disposal of Proprietary Documents and Equipment (SG-8)

Managers are responsible for identifying both public and proprietary information, technical data, and personal information developed, produced or possessed by their organizational units and for instructing employees reporting to them regarding the proper handling and safeguarding of such information. Each SAIC employee should exercise reasonable care to protect information from unauthorized or inadvertent disclosure.

Employees should, as a matter of routine, mark each document containing proprietary information with one of the markings described in Policy SG-8 at the time the document is produced. Computer tapes and other recorded material should be identified by proper labeling easily visible while the material is being stored. In addition, there should be a warning notice at the beginning of all such material to ensure that the user is forewarned about the proprietary nature of its contents when accessed. It is the responsibility of the

organization that originates a document to determine whether it includes proprietary information, and when, due to changed circumstances, its proprietary status should be changed. All proprietary documents to be discarded should be shredded or placed in labeled containers provided for such purposes. In compliance with Policy SG-3 and SG-8 all computers that have been designated for redeployment within the company, for donation, or for resale must have all proprietary and sensitive information removed through the SAIC Asset Disposal Program. Floppy diskettes should be reformatted for reuse by the user.

Not all proprietary information or technical data in the company's possession may be properly marked: for example, salary reviews or medical/insurance records. Nevertheless, all such documents must be protected from unauthorized disclosure. Caution and discretion are necessary to ensure that divulging such information will not compromise the competitive position of the company, infringe on personnel information about specific employees, or result in the unauthorized export of technical data or export-controlled information.

- **Proprietary Information – New Hires (SG-1)**
  No proprietary information shall be solicited or obtained from any prospective employee of the company. New employees of the company shall not bring to the company any proprietary information belonging to their former employers. No employee of the company will be assigned to any task that would require the employee to use, disclose, or rely upon any proprietary information of any third party. It is the responsibility of business unit management to ensure that these standards are rigorously observed, and that any actual or apparent violation is brought to the attention of the Employee Ethics Committee or the general counsel.

  New employees should not take away from their former place of employment any information that could be considered proprietary by that employer, such as books, equipment, data storage media, tapes, computer printouts, or notes generated while performing in the course of that employment, or any items which may have been purchased or produced by the former employer for the performance of the employee's work. Violation of this policy will result in appropriate disciplinary action that may include the termination of the employment of the employees involved.

  Prospective employees who are employed at the time they are seeking employment with SAIC should cooperate fully with the existing employer and continue to perform their work diligently until they terminate.

- **Proprietary Information – Current Employees (SG-1, SG-8)**
  SAIC does business honestly, fairly and in accordance with the law. Accordingly, all directors, officers and employees are required to respect the confidential, proprietary or trade secret information (collectively, "proprietary information") of others, and of the company. No employee shall use or disclose, directly or indirectly, any proprietary information of the company or another, except in the course of his/her employment, and always in strict accordance with applicable copyright laws and with the terms upon which the proprietary information was disclosed, including the terms of any confidentiality or teaming agreement executed by the company. Any representation of proprietary information in writing, graphics, computer code or other embodiment shall be safeguarded from disclosure to unauthorized persons and shall be removed from company premises only as needed for company business. Administrative Policy SG-8 describes more fully the procedures for handling proprietary information. Typically, proprietary information is appropriately marked as such. However, even absent such a written designation, if information is received under circumstances in which the employee knows or reasonably should know that the information disclosed is intended to be proprietary information, then it shall be treated as such. Any questions concerning whether particular information or data should be treated as proprietary information should be referred to the general counsel.

- **Proprietary Information – Terminating Employees (SG-1, SG-8)**
  The obligation to protect proprietary information survives the termination of employment. Absent a specific agreement to the contrary, the obligation to protect proprietary information extends indefinitely.

  No such information shall be removed from the premises of the company by a terminating employee without the prior written consent of an authorized company representative. Permission to retain such information after termination must be in writing and approved by the SAIC general counsel prior to removal.

- **Proprietary Information – Competitors (SG-1)**
  Directors, officers and employees must not solicit or obtain, from any source, any proprietary information concerning a competitor. Information concerning competitors shall be obtained only through publicly available sources, or through unrestricted disclosures made by the competitor. So-called industrial espionage is prohibited, and no director, officer or employee shall knowingly induce a competitor or third party to disclose a competitor's proprietary information. Should a director, officer or employee inadvertently come into possession of information known or suspected to be the proprietary information of another (including, in a U.S. government procurement, bid-and-proposal or source-selection information) the director, officer or employee must safeguard and segregate that information, prevent copying or further disclosure, and seek immediate advice from the general counsel.

- **Antitrust Law Compliance (SG-1)**
  SAIC believes in fair and open competition. Under no circumstances should arrangements affecting pricing, terms of sale, production volume, or marketing policies, such as allocation of customers or territories, be entered into with any competitor or potential competitor. Any SAIC director, officer or employee must immediately leave any meeting or conversation in which such a discussion arises and report it to his or her management or the general counsel.

  SAIC is subject to the U.S. antitrust laws. Their objective is to benefit consumers by promoting vigorous competition. The company believes strongly in fair and open competition, and is committed to complying with the laws that promote it. Because some activities of the company are sensitive under the antitrust laws, it is important that each employee comply fully with these laws. Among other things, directors, officers or employees may not engage in activities that:

  - Restrict competition among clients (e.g., price fixing or allocating customers in the market) or unfairly restrict the ability of others to compete with our clients in the marketplace.
  - Place other competitors at an unfair disadvantage in their offerings of similar services to our clients (e.g., by disparaging their services or improperly obtaining or using their proprietary information).
  - Improperly favor SAIC products over those of others in the development of technical requirements or performance of certification of clients.

  The application of the antitrust laws to particular situations is not always clear, and directors, officers or employees are encouraged to seek legal advice from the Office of General Counsel as appropriate.

- **Privacy & Confidentiality – Employee Personal Information (SG-8)**
  SAIC respects the privacy and confidentiality of employee personal information acquired in the course of SAIC business. SAIC policy for the protection of personal privacy data and sensitive data is compliant with federal law and regulation, the California Civil Code Section 1798.82, and the European Union Directive 95/46/EC.

  To protect employee privacy, no employee shall access SAIC records – including databases – to obtain information about any current or former employee without an

authorized business need to know, nor should they disseminate such information to any unauthorized person. SAIC employees are obligated to protect personal and sensitive information that they have access to in the course of SAIC business. Personal and sensitive information includes compensation data and personal data concerning employees of SAIC and/or its affiliates. Confidential personal and sensitive information acquired in the course of SAIC business shall not be used for personal advantage. Direct or indirect unauthorized disclosure, unauthorized removal, or negligent handling of personal and sensitive information may result in disciplinary action up to and including termination of employment.

Any suspected breach of personal information, personal data, or sensitive information shall be immediately reported to Corporate Legal, Human Resources and to the director of IT security. If a breach is confirmed to have occurred, the incident will immediately be escalated to the chief information officer and the chief administration officer. Corporate Legal will ensure that any required notice is given concerning any verified breach of personal information to the affected subject persons.

- **Security Requirements – Government Classified Contracts**
  SAIC organizations and employees are responsible for following the contract classification specifications, protection requirements and security processes established for performance on government classified contracts. A copy of the classified contract DD254 must be submitted to Corporate Security for inclusion in the SAIC classification data base. The SAIC Security Standard Practice & Procedures (SPP) Manual is intended to provide SAIC facilities and locations with security policies and procedures, as well as guidance, deemed appropriate for implementation of the requirements, restrictions and other safeguards issued in accordance with the National Industrial Security Program Operating Manual (NISPOM) and/or other government security regulations. Any questions or issues related to such requirements shall be addressed to SAIC Corporate Security.

Relationships with Customers and Suppliers, Gifts and Gratuities (SG-1, SG-12, SG-15)

SAIC's business relationships must be free from even the perception that favorable treatment was sought, received or given as the result of a gift or gratuity. Therefore, except as provided herein, employees shall not offer or give any gift or gratuity to any customer nor shall employees accept or solicit any gift or gratuity from any supplier. In no instance shall a gift or gratuity be offered, given or accepted if it would violate law, regulation or the policies of the company or the recipient, or cause embarrassment to or negatively reflect on the company's reputation. The policy applies to both SAIC employees and any member of an SAIC employee's household or immediate family (any relative of the employee or the employee's spouse).

- **Gifts and Gratuities to Federal, State, and Local Government Employees**
  Federal, state and local government departments and agencies are governed by laws and regulations concerning acceptance by their employees of entertainment, meals, gifts, gratuities and other things of value from firms and persons with whom those government departments and agencies do business or over whom they have regulatory authority. It is the policy of SAIC, at minimum, to comply strictly with those laws and regulations.

- **Federal Executive Branch Employees**
  Executive agencies of the United States are SAIC's predominant customers. The Department of Defense, the various military departments, the many civilian agencies (such as GSA, DOE and NASA), and numerous other federal departments and agencies reside within the executive branch. SAIC employees are prohibited from giving anything of value to federal executive branch employees, except modest refreshments such as soft drinks, coffee and donuts on occasional basis in connection with necessary and

legitimate business activities. In the instance of office parties, picnics, and other SAIC-sponsored gatherings attended by executive branch employees, to avoid providing an improper gift or gratuity, it is acceptable practice to estimate the fair value of food, drink or other incidental items provided, and to have the executive branch employee contribute the appropriate amount in cash. Any exceptions to this policy must be approved in writing by the company's Office of the General Counsel, since the provision of gifts, gratuities or other items of value to federal executive branch employees may expose the giver, the recipient and the company to potential civil, criminal and administrative liability. Further information in this regard may be found in Administrative Policy SG-15, Procurement Integrity. It is important to note that employment, including the possibility of employment, may be considered a thing of value under applicable regulations, hence any discussion of future employment with any U.S. government employee is prohibited unless conducted in accordance with Administrative Policy SG-12, Recruitment and Employment of Current and Former U.S. Government Personnel.

- **Federal Legislative and Judiciary Branches, and State and Local Government Employees**
  Employees of the federal legislative and judiciary branches and employees of state and local government departments or agencies are subject to a wide variety of different laws and regulations. The laws and regulations pertaining to them must be consulted prior to offering such employees anything of value. Managers who approve these types of gifts and gratuities of any value are responsible for the propriety and reasonableness of expenditures and for proper recording. Managers responsible for approval of such payments must contact the Office of the General Counsel for guid-ance prior to any action.

- **Gifts and Gratuities to Non-Government (Commercial) Persons**
  It is an acceptable practice for SAIC employees to provide meals, refreshments, entertainment and other gifts and gratuities of reasonable value to non-government persons in support of domestic commercial business activities, provided:

  - The practice does not violate any law or regulation or the standards of conduct of the recipient's organization. It is the responsibility of the providing SAIC employee to inquire about and understand any prohibitions or limitations of the recipient's organization before offering any business courtesy.
  - The gift or gratuity courtesy must be consistent with customary marketplace practices, infrequent in nature, and may not be lavish or extravagant.
  - The employee has received management approval prior to offering or giving tangible gifts (including tickets to sporting, recreational or other events) to a non-government person or entity with which the company does or seeks to do business.
  - The gift or gratuity is not a "quid pro quo" for the award of a specific and definable business engagement.
  - The gift or gratuity does not arise under or relate to a government contract on either the federal, state or local level. It is the responsibility of the SAIC employee to confirm the commercial, non-governmental nature of the relationship between the company and the intended recipient before offering any business courtesy.

  Managers who approve these gifts or gratuities, including meals, refreshments and entertainment of value to non-government persons with which the company does or seeks to do business, are responsible for the propriety and reasonableness of expenditures and for proper recording. If in doubt, managers responsible for approval of such payments should contact the Office of the General Counsel for guidance prior to any action.

  A non-government (or commercial) person is someone who is not employed by or affiliated with a federal, state or local government or with any state-owned enterprises. Officials of public international organizations (such as the UN, World Bank, etc.), and candidates for public office or officials of political parties are considered governmental persons.

- **Gifts and Gratuities to Foreign Government Personnel, Public Officials and Non-Government Persons**
  When conducting commercial and international business, good judgment and moderation must be exercised to avoid misinterpretation or even the appearance of impropriety, which could have an adverse effect on the reputation of the company or its employees. When considering offering gifts or gratuities (including entertainment and meals) to individuals of another company, country or culture, it is important to assess the impact not only by SAIC standards but also by those of the recipient, who may ascribe a different value to it than was intended. Customer entertainment or gifts and gratuities should be consistent with local, customary business practices and business needs, must not violate the Foreign Corrupt Practices Act (in the case of foreign government and public officials, including persons associated with government owned or controlled entities), and must be legal in the local jurisdiction. Keep in mind that gifts or gratuities which are lawful or commonplace in foreign countries may still violate the FCPA.

  Employees may not give or offer to give, directly or indirectly, to such foreign government employees any entertainment, charitable contributions, meal or gift regardless of value, without the express written approval of corporate legal who must determine if the action is permissible under local and U.S. laws. Any meals provided to such foreign government employees should conform to as closely as possible to U.S. government per diem rates and advance approval from Corporate Legal is required for meals costing in excess of local per diem rates. Any gifts must be limited to tokens of esteem such as company logo items. Employees also may not make loans, guarantee loans, or make payments to such federal, state and local government employees. No gifts, entertainment or marketing activities that involve meals, travel or other expenditures for the benefit of a government official, official of an international organization, or employee of a state-owned enterprise may be made without the approval of the relevant division manger and the Corporate Legal Department prior to any action. Corporate Legal will assist in ensuring that customer entertainment or gifts and gratuities are consistent with local laws and customary business practices, and do not violate the Foreign Corrupt Practices Act. After such gifts or entertainment expenses have been approved, the relevant manger is responsible for the proper recording of such expenses.

  Managers who approve these types of gifts gratuities or entertainment are responsible for the propriety and reasonableness of expenditures and for proper recording. If in doubt, managers responsible for approval of such payments should contact the Office of the General Counsel for guidance prior to any action.

- **Acceptance by SAIC Employees of Business Courtesies**
  Although an employee may not use his or her position at SAIC to solicit a personal benefit of any kind or amount, it is permissible to accept unsolicited meals, refreshments, entertainment and other business courtesies such as local transportation, on an occasional basis, provided all of the following conditions are met:

  - The acceptance will foster goodwill and successful business relations.
  - The offer is from a non-governmental source (except for modest refreshments in the course of a necessary and legitimate business meeting).
  - The courtesies are consistent with customary business practices and are not lavish or extravagant under the circumstances (generally $50.00 or less).
  - The courtesies are not frequent and do not reflect a pattern or the appearance of a pattern of frequent acceptance of courtesies from the same entities or persons.
  - The employee accepting the courtesies is not a member of the procurement staff or a manager in a position to approve a particular procurement (see Standard Procurement Policies and Practices, Section 2.4).
  - The employee accepting the courtesies would feel comfortable about discussing the courtesies with his or her manager or coworker, or having the courtesies known by the public.

It is the personal responsibility of each employee to ensure that his or her acceptance of such meals, refreshments or transportation is proper and could not reasonably be construed in any way as an attempt by the offering party to secure favorable treatment. If in doubt, consult with your manager prior to accepting any business courtesies. Any exceptions to this policy must have prior written approval by the Office of the General Counsel.

- **Gifts to SAIC Employees**
  Business courtesies, however, are treated differently than gifts. While neither gifts nor business courtesies may be solicited, under the narrow circumstances described in the above paragraph, unsolicited business courtesies may be accepted by SAIC employees. In contrast, virtually all gifts - even if unsolicited - must be rejected. Specifically, SAIC employees are not permitted to accept compensation, honoraria, funds in any form or amount, or any other form of gift or gratuity from any entity, representatives of any entity, or any person that does or seeks to do business with the company. Gifts from customers, suppliers or vendors must not be accepted, except for advertising, promotional or other items of nominal value (generally $25.00 or less). If in doubt, consult with your manager prior to accepting any such gift. Any exceptions to this policy must have written approval by the Office of the General Counsel.

Recruitment and Employment of Current and Former U.S. Government Personnel (SG-12)

Administrative Policy SG-12, Recruitment and Employment of Current and Former U.S. Government Personnel sets forth procedures to be followed in recruiting and hiring current and former U.S. government employees and officials, including military personnel, in order to adhere to the requirements of certain federal laws and regulations governing the recruitment and employment of such persons. It is SAIC's policy to fully comply with these restrictions.

Before entering into any employment discussions with any current or former U.S. government employee, the person doing the recruiting on behalf of SAIC shall have all such candidates complete, execute and return the current version of the Employment Questionnaire and Certification (G/C 489). For purposes of this policy, the term "employment discussions" means any recruitment activity, discussions or communications, however tentative, which occur during or after the initial contact with the government employee, if the employee does anything other than reject the possibility of employment with SAIC. While employment discussions should be construed broadly, those discussions which are not geared towards any potential employment or consulting relationship with SAIC, but rather which are strictly limited to general industry discussions or which concern publicly available information regarding SAIC, are permissible.

Administrative Policy SG-12 provides a detailed summary of restrictions related to recruitment, outside employment, terminal leave and post government employment. Any questions relating to the recruitment and employment of current and former government personnel should be referred to the Office of the General Counsel.

Agreements with Marketing Agents, Including Sales Representatives (SG-1)

The engagement of all marketing agents/sales representatives (domestic or international) to provide legitimate business development services to the company requires the bilateral execution of SAIC's standard Domestic or International Sales Representative Agreement. Any such agreements calling for remuneration on a contingent basis must be approved in accordance with Administrative Policy SG-7, Authorities for Corporate Commitments.

No contingent fees shall be offered to reward anyone for assistance in obtaining U.S. government contracts unless they are agents regularly engaged in the business of soliciting sales for the type of products or services involved. (A fee is considered to be contingent when it is

payable depending on the degree of success the agent has in securing the government contracts, regardless of the manner in which the fee is computed.)

Political Contributions (SG-1)

Federal statute prohibits a corporation from making a contribution or expenditure of money, products, services or any other resource in connection with any election for president, vice president, senator, or representative to Congress, or in connection with any primary election or political convention or caucus held to select candidates for any of the foregoing offices.

In general, most U.S. states and many foreign countries have similar laws which prohibit corporate political contributions in connection with any election relating to political office or impose strict disclosure requirements on anyone making contributions permitted under the law. Failure to disclose political contributions made directly or indirectly through a lobbyist or agent on behalf of the company can result in severe penalties for SAIC, including fines and termination of contracts.

As a result, no SAIC employee may contribute corporate funds, or contribute personal funds in circumstances where it might reasonably be inferred that corporate reimbursement of the funds would be involved, to a political campaign, party or organization without the prior written permission of the CEO or the SAIC Government Affairs Committee. This requirement applies to all federal, state and local political activities, foreign or domestic.

Many states frequently prohibit direct and indirect contributions or payments made in any form or through any means, such as through lobbyists, consultants or others and also require accurate reporting of any fees paid to such third parties for lobbying or government relations services. No SAIC employee or organization may hire, retain or renew federal, state, local or foreign lobbying or government relations services without the prior written approval of the Government Affairs Committee and must report all fees paid to such entities on a quarterly basis to the committee.

Solicitation for personal campaign contributions from subordinate employees either inside or outside the office is absolutely prohibited. General solicitations for charity such as disaster relief are permitted, but one-on-one solicitation of subordinates is not permitted. This avoids even the appearance that the solicitation was improperly coercive in some way.

A person doing part-time work for a campaign or candidate as a volunteer (i.e., not at a manager's direction) may make occasional, isolated or incidental use of company facilities or resources, subject to the prior written approval of the Government Affairs Committee. Such approval is necessary to ensure compliance with Federal Election Commission rules.

This policy applies to officers, directors, employees, consultants and agents of SAIC and its wholly-owned or majority-owned subsidiaries. Any violations of this policy may be grounds for disciplinary action, up to and including termination of employment or the agent's agreement.

Nothing contained herein shall be deemed to prohibit officers or employees from engaging in political activities in an individual capacity on their own time and at their own expense, or from making political contributions or expenditures of their personal funds, or from expressing views and taking action as private individuals. However, no expenses incurred or contributions made for such political purposes will be reimbursed by the company.

Information and Data Protection (SG-3)

Good judgment and security measures must be used in the protection of all information, including any and all data on computers at SAIC. Portable information sources including

desktops, laptops, PDAs and memory sticks require extra care and consideration. All SAIC computers, both laptops and desktops, must be encrypted. This encryption policy is based upon increasingly serious requirements for data protection, and the potential for loss of client, company and employee personal data, and the consequent potential damage to SAIC's reputation if sensitive data are compromised. Personal awareness, as well as appropriate physical and software security measures, are necessary to ensure the safekeeping of this property and the data contained therein. Managers should see that all employees under his/her management are aware of company policies regarding sensitive information, password protection, encryption and back ups as described in Administrative Policy SG-3. Any loss of property including a desktop computer, laptop, memory stick or PDA must be immediately reported to Corporate Security. Failure to adhere to these policies will result in disciplinary action, up to and including termination.

Computer System Usage (SG-3)

SAIC computers, software and/or e-mail systems should be used only for official SAIC business. Non-SAIC-owned computing equipment should be used only in ways specifically authorized by the equipment owner. SAIC e-mail systems are intended for company business, not for personal communication or other inappropriate activities. All SAIC systems, network traffic, and messaging systems may be monitored at any time without notice. All persons using or accessing SAIC resources, including computing systems, network or messaging systems, consent to having their activities monitored as a condition of such access. SAIC may audit computer or e-mail accounts without notice to ensure their proper use. Approval requirements for incidental and insignificant personal use of computers and e-mail are outlined in the earlier paragraph Use of SAIC and Customer Property, Equipment and Facilities which is based on Administrative Policy SG-1. SAIC employees working on an external host site outside of SAIC must abide by the security policies of that site.

Accessing Computers or Networks (SG-3)

Employees must have proper authorization and follow specified procedures to access computers and computing networks. This includes company-owned or -operated computers; computers owned by third parties (customers or vendors); SAIC net or other wide area networks; or SAIC, customer, or vendor-owned local area networks.

No employee shall engage in any activity that compromises or intends to compromise the security or access controls of any computer system within SAIC or any outside company or agency, whether or not an intention to do harm exists. Any access or attempt to access any systems or resources for which the user is not a legitimate or authorized user ("hacking") is expressly forbidden. If an SAIC employee engages in such activity as part of his or her duties (e.g., as a testing service for a contract), those activities must be carefully coordinated and approved in advance by Corporate Information Security. Any violation of this policy will subject the employee to disciplinary action up to and including termination of employment.

Account Name and Password Security (SG-3)

Each SAIC employee with authorized access to a computer system using a password for access must prevent disclosure of any account name and/or password to others. Every SAIC individual granted access to SAIC systems must protect personal identification numbers (PINs) or passwords as well as other means of authentication, such as tokens or public key infrastructure (PKI) certificates. Each SAIC employee with authorized access to a computer system must do his or her utmost to prevent disclosure of any password to unauthorized users.

Disruptive Software (SG-3)

SAIC policy prohibits introducing into a computer system any software or hardware intended to disrupt normal operations, including viruses, worms, logic bombs, Trojan horses, adware or spyware. In addition to violating SAIC ethics standards, such actions may be illegal. Freeware programs that do not fulfill a specific business need may not be down-

loaded or installed on SAIC systems. This includes, but is not limited to software such as screensavers, games or e-mail enhancements. SAIC computers should be loaded only with business-related software approved by the company and/or local system administrator.

Granting Privileges (SG-3, SG-4)

Computer system managers or process owners are responsible for ensuring that users have only those access privileges needed to do their jobs. High-level privileges (access to operating system tools and/or systemwide data) should be granted only to systems programming staff for system maintenance. These high-level privileges shall be used only to access those files and systems required to perform authorized work. Computer system managers shall ensure that non-U.S. persons are granted access privileges consistent with Administrative Policy SG-4.

Internet & World Wide Web Access and Appropriate Use (SG-3)

Internet access to the World Wide Web is provided as a tool to support SAIC business purposes. SAIC computers, software and/or email systems should be used only for official SAIC business. Non-SAIC-owned computing equipment should be used only in ways specifically authorized by the equipment owner(s). It is SAIC's intention to provide the appropriate level of access to the Internet without assisting, promoting, allowing or contributing to any violations of law or engaging in conduct that would be offensive to others or damage SAIC's reputation. Each employee's use of SAIC's connections to the Internet to send email, post to newsgroups, participate in chat rooms, transfer files, login remotely to external systems, and visit external Web sites is traceable to SAIC and, therefore, these activities must be conducted with SAIC's reputation in mind. Use of SAIC's connections to the Internet for the purpose of posting to newsgroups or mailing lists, participating in chat rooms, and the like, is expressly limited to work-related forums. While a wide variety of Internet Web sites exist, many of which support business purposes, other sites exist that are inappropriate to contact through SAIC's systems. Examples of such sites may include but are not limited to:

- Sexually explicit or graphically oriented sites.
- Sites that could be perceived as promoting racism or bigotry.
- Sites that may conflict with company policies and/or business interests.

SAIC employees are expected to limit their Internet usage to appropriate sites. Those who violate this policy may be subject to disciplinary action, up to and including termination of employment.

Voicemail and Email (SG-1, SG-3)

SAIC computers, software, email, instant messaging, and voicemail systems should be used only for official SAIC business. SAIC messaging systems are intended for company business, not for personal communication or other inappropriate activities. SAIC may audit these systems without notice. Personal use of messaging systems is permitted with prior management approval per the terms of the SAIC Administrative Policy SG-1 that addresses incidental and insignificant use of company resources. It is important for each employee to recognize that while incidental and insignificant personal use of these systems is permitted, such usage is traceable to SAIC and may impact adversely SAIC if the usage is not appropriate.

Employees are reminded that there is no implied privacy in the use of company computers, voicemail and email systems. SAIC reserves the right to access these systems without notice. Employees should not assume that any information, including messages or data that are "deleted," is private.

Consequences of Violation and Duty to Report (SG-3)

Computer, voicemail or email messages must not contain any material that may reasonably be considered offensive, disruptive, defamatory or disparaging towards any employee, the company or third parties. Offensive content includes, but is not limited to, sexual com-

ments or images, racial slurs, gender-specific comments, or any comments that might offend someone because of their age, sex, sexual orientation, religion, race, color, political beliefs, national origin, disability, or veteran or marital status.

Examples of communications that are not permitted include, but are not limited to:

- Disparagement of other employees, customers, competitors or suppliers.
- Threatening statements made against anyone inside or outside the company.
- All messages sent to non-business-related bulletin boards and chat groups using company email or even a personal account if the messages are sent over company-provided networks, as such statements might be misconstrued as representing the opinion or policy of the company.
- Chain mail of any type (even if the employee is only forwarding it, not originating it).
- Language that would violate the company's policies on harassment, such as sexual jokes, racial slurs, homophobic remarks, disparaging remarks about religion, politics, beliefs, national origin, disability, or veteran or marital status.

Any SAIC employee who has received undesirable content in their e-mail should set their mail client to block or delete mail from that source. Additionally, SAIC employees who have knowledge of or suspect a violation of the communications guidelines found within SAIC Administrative Policy SG-3 should report this information to any SAIC disclosure channel outlined in the "Key Messages" section on page eight of this handbook. Any representatives of such disclosure channels must then immediately report this information to the HR director, U.S. operations or corporate group HR director or, in their absence, the corporate director, internal audit or the general counsel. Any employee who violates the provisions of Policy SG-3, or who fails to report inappropriate communications as described in this section, may be subject to disciplinary action up to or including termination of employment. Similarly, any member of the contractor workforce who violates this policy is subject to removal from SAIC locations and termination of the contract covering the assignment. Any other individuals (for example, a sponsored guest) who violate this policy may have their SAIC computer system access privileges revoked. Additionally, any individual who violates the company's computer security policies or practices may also be subject to criminal prosecution and/or civil litigation under state and/or federal law. It is the duty of all SAIC employees to immediately report any security breach or known vulnerability to their management and IT Security. The decision to initiate legal action will be made upon review by the Corporate Legal Department and the management responsible for security.

Unlicensed Software Use (SG-3)

The use of unlicensed or illegally copied software at SAIC is strictly forbidden. The use of peer-to-peer programs used to share software may result in a violation of software licensing or copyright infringement. Such programs are not permitted on any computer used to connect to SAICnet. SAIC employees learning of any misuse of software or related documentation within the company shall notify their supervisor, the chief information officer, or other designated individual responsible (such as an HR representative, the Ethics Line, or the Employee Ethics Committee). Any SAIC employee who knowingly makes, acquires or uses unauthorized copies of computer software licensed to SAIC or who places or uses unauthorized software on SAIC premises or equipment will be subject to appropriate disciplinary action, up to and including termination of employment.

Certification of Procurement Policy

Business Development Activities (SG-1, SG-15)

The procurement of goods and services by the U.S. government is governed by U.S. public law, the Federal Acquisition Regulation (FAR), and the policy/regulation of specific agencies

conducting the procurement activities. With respect to SAIC business development activities involved in the pursuit of U.S. government business, it is incumbent upon all directors, officers, supervisors, proposal managers, and other employees, as well as consultants, subcontractors or vendors involved in this process, to be fully aware of relevant law, regulations and policies and to comply fully with all provisions thereof. SAIC supports fully the requirements to protect the integrity of the procurement and source selection processes and the concept of fair, open competition as described in more detail in Administrative Policy SG-15, Procurement Integrity.

Moreover, SAIC consultants may not engage in unlawful activities in the business development process. Accordingly, SAIC managers must ensure that the tasking of the consultant in the statement of work and Consultant Agreement leaves no room for misinterpretation of instructions and clearly prohibits seeking, soliciting or in any way acquiring restricted information.

All decisions regarding internal allocations of business and the commitment of SAIC staff to contract work should be made in the context of the high ethical standards embodied in the SAIC Credo. Similarly, prior coordination is required between management and employees on commitments such as relocation or excessive compensated or uncompensated overtime.

Competitive Information Gathering

It is permissible to obtain public information about a competitor, but it is unethical and illegal to wrongfully obtain a competitor's trade secrets or other confidential information or to use a competitor's trade secrets or other information without authorization. Doing so can result in civil and criminal penalties.

SAIC directors, officers, and employees may obtain information from public sources where there is no expectation of privacy, such as press releases, marketing brochures, public presentations, legal filings, public Web pages, and demonstrations and discussions at trade shows. However, it is not permissible to conduct any form of espionage, or to engage in deception to obtain information. And, even if information is revealed freely, if the recipient of the information knows (or should know) that it is confidential information wrongfully obtained from another, or that is has been revealed by mistake, use or further disclosure of the information is not permitted.

Combating Trafficking in Persons (SG-1)

The US government has adopted a zero tolerance policy regarding contractors and contractor employees that engage in or support severe forms of trafficking in persons, procurement of commercial sex acts, or use of forced labor, as described in 48 CFR Part 22. All employees, consultants, contractors, and subcontractors performing any work under a Federal contract shall not engage in or support severe forms of trafficking in persons, procure commercial sex acts, or use forced labor. Any employee who violates this policy shall be subject to disciplinary action including, but not limited to, removal from the contract, reduction in benefits, or termination of employment.

All employees, consultants, contractors, and subcontractors working at overseas locations are required to be aware of and comply with that Host Nation's laws on this subject.

Any questions regarding this policy should be directed to the Corporate Legal Department.

Risk Policy (SG-27)

As SAIC grows and our business areas expand, we encounter new and greater risks to our employees and to the corporation. We have been challenged to identify and manage those risks under our employee ownership model. Now, as we enter an era of public ownership, we must be equally mindful of how risk, if not properly managed, can impact our company and the public's perception of the company. The company has issued a corporate policy, SG-27, which defines the responsibilities and processes for identifying risk and for developing

strategies to avoid, mitigate or manage risks in a way that allows the company to fulfill its mission. The policy assists line managers by listing risk drivers and business areas that have historically created situations that pose financial or legal issues; the possibility of negative publicity; or injuries to the public, the environment or our employees. All employees are part of the process of identifying risk within their Business Unit. On occasion, the risks will be so severe or unusual that additional resources should be applied to assist with identification and mitigation programs. The Corporate Risk Committee is the appropriate forum in those cases.

Procurement Policy Act and Procurement Integrity Certification (SG-1, SG-15, SG-12)

Section 27 of the Office of Federal Procurement Policy Act, as amended, 41 U.S.C. 423 (the "Act"), and as implemented in the Federal Acquisition Regulation ("FAR") at part 3.104, sets forth certain prohibitions on disclosing and obtaining procurement information, as well as engaging in discussions with U.S. government employees or officials regarding non-federal employment.

Section 27(a) of the Act (FAR3.104-4(a)) generally prohibits present or former government officials, or persons acting on behalf of or in an advisory capacity to the government with respect to a federal agency procurement (including contractor personnel) who by virtue of their office, employment or relationship, have or had access to contractor bid or proposal information or source selection information, from knowingly disclosing such information before award of a federal agency procurement contract to which the information relates. Section 27(b) of the Act (FAR 3.104-4(b)) prohibits any person from knowingly obtaining contractor bid or proposal or source selection information before the award of a federal agency procurement contract to which the information relates (unless allowed by law). Finally, Section 27(c) of the Act (FAR 3.104-4(c)), and administrative and judicial interpretations thereof, outlines the steps SAIC personnel must undertake when discussing the possibility of non-federal employment with current government officials or employees. Therefore, before engaging in substantive employment discussions (i.e., anything beyond initial contacts) with such individuals, SAIC employees must verify the government employee's duties do not include participation in any procurement or other matter involving SAIC or, if their duties do include such participation, the government employee has recused or disqualified himself or herself from participation in any procurement or other matter involving SAIC in accordance with FAR Part 3.104, unless such disqualification is waived by appropriate government authority pursuant to applicable federal regulations. The policies and procedures relating to the recruitment and hiring of current government employees are set forth in Administrative Policy SG-12.

All employees of SAIC are required to read the section of this handbook entitled "Procurement Policy Act & Procurement Integrity Certification" upon initial employment and to sign the certification attesting to their understanding and agreement to comply with the requirements of this section. Similar certifications will be required of all employees in connection with their annual performance review. A complete copy of the Act is available in the SAIC Legal Department and any questions regarding the foregoing or any other aspects of the Act should be addressed to that department.

Summary

It is the objective of each of us, as well as the company, to operate according to the highest possible standards. As a result, we have a serious responsibility to ensure our personal conduct is above reproach and, difficult as it may be at times, we also have obligations regarding the conduct of those who work around us. If you know of or suspect a violation of law or ethical misconduct, you must promptly disclose this information to your supervisor or someone in your management chain; to a local, business unit, group, or corporate human resources manager; to the vice president for ethics and compliance, to the Employee Ethics Committee; through the SAIC Hotline; the chairman of the audit committee; the Office of General Counsel; the chief executive officer of the company; or the lead director of the board of directors.

SAIC is serious about being an ethical company. Violations of the standards set forth in this book will not be tolerated, and will result in disciplinary action appropriate to the violation.

The SAIC Standards of Business Ethics and Conduct Certification

It is the objective of each of us, as well as the company, to operate according to the highest possible standards of ethical behavior and professional integrity. Signing this form affirms your commitment to that objective. Included is an additional certification of your commitment to comply with federal procurement integrity law. This form is to be completed by you and turned in to your supervisor, human resources representative, or division manager and will be retained by the company among your personnel records.

I have read the SAIC Standards of Business Ethics & Conduct Handbook and understand that it represents company policy with which I am expected to comply. I have sought and received clarification for any policies that were unclear to me. I understand that by signing my name below I am certifying that I will comply with all of SAIC's standards of business ethics and conduct. With my signature below, I also acknowledge my responsibility to make known to my supervisor or someone in my management chain, to a local, business unit, group or corporate human resources manager; to the vice president for ethics and compliance, to the Employee Ethics Committee; through the SAIC Hotline; the Office of General Counsel; the chairman of the audit committee; the chief executive officer of the company or the lead director of the board of directors any situation where I am aware of violations or possible violations of the standards that are described in the Standards of Business Ethics & Conduct Handbook and its referenced corporate policies.

I also understand that by signing my name below I am certifying that I have read and will comply with the requirements under the heading Procurement Policy Act and Procurement Integrity Certification in the SAIC Standards of Business Ethics & Conduct Handbook. These requirements reference Section 27 of the Office of Federal Procurement Policy Act, as amended, 41 U.S.C. 423 (the "Act") and, as implemented in the Federal Acquisition Regulations (FAR), at part 3.104 – a complete copy of which may be obtained at Federal Acquisition Regulations (http://www.arnet.gov/far/) or by contacting the SAIC Legal Department.

I will report immediately to the business unit contracts director of the SAIC business unit to which I am assigned, and to the certifying company official of the relevant bid or proposal activity, any information concerning a violation or possible violation of the act. I am also certifying that I have disclosed and will continue to disclose promptly, either to my supervisor, or someone in my management chain; to a local, business unit, group or corporate human resources manager; to the vice president for ethics and compliance, to the Employee Ethics Committee; through the SAIC Hotline; the Office of General Counsel; the chairman of the audit committee; the chief executive officer of the company or the lead director of the board of directors any information in my possession concerning conduct involving the company, or those acting on its behalf, that I have reason to believe is unethical or illegal.

By_____ _____

Employee Signature **Date**

_____ _____

Typed or Printed Name **Employee No.**

This procurement integrity certification concerns a matter within the jurisdiction of an agency of the United States, and the making of a false, fictitious, or fraudulent certification may render the maker subject to prosecution under Title 18, United States Code, Section 1001.

October 2006

Sample Standards of Business Ethics and Conduct form. Please fill out the actual form on page 41.

The SAIC Standards of Business Ethics and Conduct Certification

It is the objective of each of us, as well as the company, to operate according to the highest possible standards of ethical behavior and professional integrity. Signing this form affirms your commitment to that objective. Included is an additional certification of your commitment to comply with federal procurement integrity law. This form is to be completed by you and turned in to your supervisor, human resources representative, or division manager and will be retained by the company among your personnel records.

I have read the SAIC Standards of Business Ethics & Conduct Handbook and understand that it represents company policy with which I am expected to comply. I have sought and received clarification for any policies that were unclear to me. I understand that by signing my name below I am certifying that I will comply with all of SAIC's standards of business ethics and conduct. With my signature below, I also acknowledge my responsibility to make known to my supervisor or someone in my management chain, to a local, business unit, group or corporate human resources manager; to the vice president for ethics and compliance, to the Employee Ethics Committee; through the SAIC Hotline; the Office of General Counsel; the chairman of the audit committee; the chief executive officer of the company or the lead director of the board of directors any situation where I am aware of violations or possible violations of the standards that are described in the Standards of Business Ethics & Conduct Handbook and its referenced corporate policies.

I also understand that by signing my name below I am certifying that I have read and will comply with the requirements under the heading Procurement Policy Act and Procurement Integrity Certification in the SAIC Standards of Business Ethics & Conduct Handbook. These requirements reference Section 27 of the Office of Federal Procurement Policy Act, as amended, 41 U.S.C. 423 (the "Act") and, as implemented in the Federal Acquisition Regulations (FAR), at part 3.104 – a complete copy of which may be obtained at Federal Acquisition Regulations (http://www.arnet.gov/far/) or by contacting the SAIC Legal Department.

I will report immediately to the business unit contracts director of the SAIC business unit to which I am assigned, and to the certifying company official of the relevant bid or proposal activity, any information concerning a violation or possible violation of the act. I am also certifying that I have disclosed and will continue to disclose promptly, either to my supervisor, or someone in my management chain; to a local, business unit, group or corporate human resources manager; to the vice president for ethics and compliance, to the Employee Ethics Committee; through the SAIC Hotline; the Office of General Counsel; the chairman of the audit committee; the chief executive officer of the company or the lead director of the board of directors any information in my possession concerning conduct involving the company, or those acting on its behalf, that I have reason to believe is unethical or illegal.

By_____ _____

Employee Signature **Date**

_____ _____

Typed or Printed Name **Employee No.**

This procurement integrity certification concerns a matter within the jurisdiction of an agency of the United States, and the making of a false, fictitious, or fraudulent certification may render the maker subject to prosecution under Title 18, United States Code, Section 1001.

October 2006

Strength in Ethics – Pride in SAIC

Communication

Listen carefully.

Encourage open communications.

Stress employee participation.

Highly value employee opinions and suggestions and provide timely, courteous and constructive feedback.

Spell out performance goals.

Document job responsibilities.

Provide employees a say in how their work gets done.

Seek opportunities to provide special recognition.

Celebrate special events and employee contributions to SAIC and the community.

Market another's customer only after proper coordination.

Share appropriate information internally.

Make available timely and accurate information on financial and organizational changes.

Protect and respect privacy, proprietary, classified, technical, sensitive, and intellectual data.

Do not spread rumors, malicious gossip or make unsubstantiated allegations.

Do not defame a person's good name, professional reputation or character.

Do not use abusive, intimidating, threatening or hostile language.

Leadership & Supervision

Set the example.

Act responsibly.

Accept your accountability.

Treat all SAIC stakeholders with respect, dignity, integrity, fairness and equity.

Make the effort to find out how others want to be treated and then treat them that way.

Welcome, provide orientation and mentor new employees.

Apply SAIC human resources policies and procedures fairly.

Solve with the employee job-related problems and concerns.

Explain the measures used to evaluate job performance.

Evaluate job performance fairly and consistently.

Conduct performance reviews on a regular and timely basis.

Make performance reviews useful in helping improve job performance.

Document and take timely action to correct poor performance.

Give regular and forthright performance feedback.

Recognize, reward and promote only those who have earned it.

Supply work groups with the resources needed.

Maintain the integrity of reports and work products. Give credit where due and acknowledge the contributions of others.

Career Development

Take care of your people.

Inform employees on a timely basis about budget or management actions and decisions affecting them.

Provide opportunities for career growth and development.

Train to deliver quality products and services. Cross-train your people to do other quality work.

Encourage continuous employee growth and development.

Work with the employee to find opportunities to use their skills.

Give employees the chance to learn new skills at SAIC.

Encourage employees to balance their work and personal life. Be flexible when possible with work schedules or personal time off.

Be a professional and notify others impacted by career transition efforts or decisions.

Review the SAIC Availability List before looking outside the company.

Coordinate internal recruitment efforts of employees not on the SAIC Availability List.

Be responsive to internal job posting inquiries.

Ensure resumes and credentials are accurate and current, that any changes are authorized and that appropriate permissions for use are obtained in advance.

Commit others to projects only with their concurrence.