



# LEGAL COMPLIANCE AND CORPORATE POLICY

Issued April 28, 2022

## LETTER FROM THE EXECUTIVE TEAM TO EMPLOYEES

The reputation of IES is one of the Company's most valuable assets. We are judged not only by what we deliver to our shareholders and customers but also by how we conduct ourselves on the job and the standard that we expect from our suppliers, subcontractors, customers, partners, employees, and others with whom we come into contact.

Compliance with the law and company policies is a minimum acceptable standard governing all activities undertaken on behalf of IES Holdings, Inc. ("IES, Inc.") and its subsidiaries (together, the "Company" or "IES"). Employees are expected to exhibit this commitment in all that they do each day. IES is particularly focused on the safety of its employees and expects its employees also to be focused and committed to compliance with safety laws, rules, regulations and policies. To this end, it is the obligation of every director and employee conducting Company business to carefully follow the guidelines set forth in this manual. Failure to do so could, in certain situations, expose the director, employee and the Company to unnecessary civil litigation and even criminal prosecution.

Many of these laws are complex, and it is not intended that you become an expert in each of these areas. The guidelines in this manual are designed to alert you to the types of business dealings which are within the danger zones of prohibited activity. It is not possible in these guidelines to cover every conceivable activity which might lead to a violation or, in many cases, to precisely define what constitutes illegal activity. If you are uncertain about the legality of a proposed activity, you should not proceed until you have secured legal clearance from the Law Department through normal reporting channels.

We have asked the General Counsel & Corporate Secretary to monitor this program. The Law Department will periodically review compliance procedures and guidelines with directors, officers and employees of the Company to ensure that they are understood and being followed. Any waiver of the procedures and guidelines relating to a member of senior management or a director of IES, Inc. may be made only by its Board of Directors and must require prompt disclosure to our shareholders and the public, as and to the extent required by applicable law.

In addition to the conduct of business in conformity with law, it is essential that we conduct our daily business in compliance with the highest legal and ethical standards. A strong commitment to ethical behavior and fair dealing by every person associated with the Company is vital to the well-being of the Company, its reputation, and our stockholders, as well as the public at large. Accordingly, this manual also includes the Company's "Corporate Integrity Policy" and "Conflict of Interest Policy."

You should report all violations or possible violations of these policies promptly. Quick action on suspected problems will allow us to correct inadvertent mistakes resulting from poor judgment, will minimize liabilities to others, and, most importantly, will preserve our corporate integrity. To allow you to report any financial impropriety, fraud, theft, violation

of this policy or discrimination, you are encouraged to contact the Ethics and Compliance Hotline at 1-800-347-9550 or [iesholdingsinc.ethicspoint.com](http://iesholdingsinc.ethicspoint.com). Our Ethics and Compliance Hotline is available 7 days a week, 24 hours a day, and is a third party provider to protect your ability to make an anonymous report if you desire. Any complaints made via this line will be brought to the attention of the IES General Counsel & Corporate Secretary. Complaints made relating to financial matters, fraud or theft will also be brought to the attention of the Audit Committee of the Board of Directors of IES, Inc.

Periodically, you will be required to sign a legal compliance certificate in order to remind you of the provisions of the manual and allow you to reaffirm your commitment to the legal compliance program.

Review this manual carefully and keep it in your personal files for ready reference. Our expectation is that you will give the legal compliance program your complete support - it is important.

Thank you for your commitment,  
IES Executive Team

## TABLE OF CONTENTS

Antitrust Guidelines.....	page 3
Conflict of Interest Policy .....	page 4
Intellectual Property .....	page 5
Corporate Integrity Policy .....	page 6
Electronic, Telephone and Computer Network Systems Usage Policy.....	page 7
Information Security Policy .....	page 9
Equal Employment Opportunity Guidelines .....	page 10
Prohibition of Discrimination, Harassment or Retaliation .....	page 11
Safety and Environmental Compliance.....	page 12
Government Requests for Information or Investigations.....	page 13
Proprietary Information Policy.....	page 14
Securities Law Guidelines .....	page 15
Legal Compliance Certificate.....	page 18

## ANTITRUST GUIDELINES

The Company believes in total compliance with the antitrust laws by all employees at every level of our business. The antitrust laws bear on numerous aspects of our relations with competitors and customers. Ignorance of what constitutes a violation of these laws is no defense.

The most dangerous area of the antitrust laws for Company employees most likely involves pricing procedures and bidding.

It is clear that unless the Company's pricing decisions are unilateral in nature, substantial legal problems will arise under the antitrust laws. The Company must always make independent pricing decisions on each of its products or services. Therefore, no employee of the Company is permitted to discuss or exchange prices, or to discuss or exchange information as to cost, terms or conditions of sale, with any competitors without prior approval from the Law Department.

**Q. A competitor called to discuss questions about a bid we are also involved in. Can I take the call?**

**A. Not without clearing with Legal, as this could be viewed as illegal "bid rigging."**

**Q. A competitor wants to discuss jointly negotiating with our copper suppliers to lower prices, which would help our margins. Is that okay?**

**A. Generally, no. You should check in with Legal, as the joint negotiation could be viewed as improper collusion that reduces competition.**

The following are examples of agreements among competitors, whether reached by express contract or unwritten understandings, which would be in violation of the antitrust laws:

- ◆ To fix selling prices maximum, minimum or otherwise;
- ◆ To change prices simultaneously;
- ◆ To fix buying prices for raw materials;
- ◆ To limit production or output or to divide markets; or
- ◆ To not sell or buy in a particular market area.

It is the intent of the Company to strictly maintain the integrity and legality of the bidding process. In connection with the bidding process for work contracts or otherwise, the Company neither condones nor permits collusion involving any IES entity, either with another IES entity or with a company not affiliated with IES. It is not in the interest of IES for two companies to competitively bid on the same aspects of the same project. If two IES companies intend to bid on the same project, they first must receive written authority to do so from the Executive Team. The two are required to disclose, in writing, to the customer that they are entities under common ownership. At no time may any IES entity enter any agreement or otherwise act to "rig" bids or make a complementary bid. All bids must be made solely in good faith ability and desire to perform the work and made in an ethical and legal manner.

## CONFLICT OF INTEREST POLICY

The Company prohibits employees from engaging in any activity, practice, or act which presents a conflict of interest with, or appears to present a conflict of interest with, the Company, its customers, or its suppliers. It is essential for employees who are confronted with a possible conflict of interest to promptly and fully disclose details of the situation to their company's President or the General Counsel or Chief Financial Officer. Specific requirements are as follows:

1. Employees must disclose to their managers any employment or contractual relationship with persons, firms, or organizations that could lead to a conflict of interest.
2. Employees must disclose any financial interest they or their immediate family have in any firm that does business with the Company or competes with the Company.

Examples of actual or potential conflicts of interest include, but are not limited to, the following. Your company or division may also have a specific Travel and Entertainment Policy or Procedure.

- ◆ Ownership of, or any other interest in, a firm that has done or desires to do business with the Company.
- ◆ Giving or accepting personal payments, political contributions, gifts or services to or from clients, government officials or vendors.  
*Gifts of nominal value and social invitations, if they do not place or appear to place the recipient under any obligation, are accepted.*  
*Special care must be taken with any such payments to foreign government officials. No such payments may be made without prior legal approval.*
- ◆ Placement of business with a firm that results in a direct economic benefit to the employee or any member of his or her family.
- ◆ Acceptance of a loan by the Company to or guarantee by the Company of obligations of an officer or employee or a member of his or her family.
- ◆ Use of corporate assets (e.g., corporate credit cards, corporate equipment, etc.) for non-business purchases and/or obligations.
- ◆ Management of an employee who is a family member or in a close personal relationship with the employee without disclosing to HR.
- ◆ Taking advantage of outside work opportunities gained.

## INTELLECTUAL PROPERTY

It is the policy of the Company that no employee shall knowingly appropriate, infringe or otherwise make improper use of a valid trademark, patent, trade secret, proprietary technology and other intellectual property belonging to another person or entity.

Besides prohibiting unauthorized reproduction of written or video materials, the federal copyright laws provide felony criminal penalties for all forms of willful copyright infringement, including computer software. Accordingly, unless pursuant to a valid license agreement, it is strictly against Company policy for any employee to copy or otherwise reproduce computer software or other materials subject to the protection of the copyright laws. All software license agreements shall be retained by the employee using the software, the IT manager at each company, or the Vice President, IT of IES.

When we say "Company Intellectual Property" that includes such things as ideas, inventions, improvements, conceptualizations, representations, designs, models, other work product, and all related documentation that is created or developed, in whole or in part, by employees in the course of their work on Company time or through the use of Company resources. The Company owns Intellectual Property beginning at the moment of creation or development. Employees must assist the Company in protecting, securing, maintaining, and enforcing the Company's rights in Company Intellectual Property. Employees are obligated to do so even after they stop working for the Company.

### DID YOU KNOW

Our companies' logos are trademark-protected corporate assets. That means that they may only be used by other companies with our permission and according to our trademark registrations, just as we may only use our clients' or vendors' logos with their permission.

**Q. A vendor has agreed to work with our department on a one-time project. Can I send the vendor the necessary data so they can complete the job?**

***A. Not without first confirming that the vendor is subject to a standard engagement letter which should require the vendor to keep our data confidential and clarify that IES owns the data.***

## CORPORATE INTEGRITY POLICY

- ◆ No false or artificial entries should be made or misleading reports issued.
- ◆ Inventories, payables, receivables, revenue and all other assets and liabilities of the Company shall be recognized and stated in accordance with the Company's standard practices.
- ◆ All information relating to the Company's business must be reported and recorded honestly and accurately and in a timely manner.
- ◆ No personal items are to be recorded on the Company's books and records or paid through the Company's financial system.

**Q. Can I use marketing tools from a prior employer in my current job, especially if I created the tools?**

***A. No, that information may be the prior employer's property. You may not use it unless you have the employer's written permission.***

## FAIR DEALING

Each director, officer and employee should deal fairly with the Company's customers, suppliers, competitors and employees; we should not take unfair advantage of any other party through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair dealing practice. We seek competitive advantages through superior performance, never through unethical or illegal business practices. Stealing proprietary information, or possessing trade secret information that was obtained without the owner's consent, is prohibited.

## INTEGRITY LINE

IES has contracted an independent group to create an Ethics and Compliance Hotline to encourage disclosure and help detect and prevent corporate financial improprieties, violation of policy, fraud, and discrimination around the IES system. Employees can report by simply calling the toll free line at 1-800-347-9550 and working with a trained professional who will guide them through the process or going online to [iesholdingsinc.ethicspoint.com](http://iesholdingsinc.ethicspoint.com). The Ethics and Compliance Hotline is available 7-days a week and 24-hours day and allows anonymous reports.

# ELECTRONIC, TELEPHONE AND COMPUTER NETWORK SYSTEMS USAGE POLICY

It is the policy of the Company to respect the individual privacy of its employees and contingent workers (independent contractors, temporary workers, and consultants working on Company premises). However, an employee or contingent worker may not expect privacy rights to be extended to work-related conduct or the use of the Company owned equipment, supplies, systems or property or for any personal electronic equipment used for business purposes. Employees and contingent workers may not **expect privacy for any information, documents or other tangible property on Company premises**, including but not limited to, desks, computer files, briefcases, offices, cabinets, lockers, and computer databases or any container brought onto company premises.

## Applicability

All electronic and telephonic communications systems and all communication and information transmitted by, received from, or stored in these systems are the property of the Company and, as such, are to be used primarily for job-related purposes. Any personal use or use for non-Company business is subject to this policy, and must be incidental, occasional and kept to a minimum. Management has the right to control the Company's communications systems and their use. Nothing herein prohibits employees from communicating to other employees about the terms and conditions of their employment and pay or any other subject matter protected by the National Labor Relations Act or the Pay Transparency Executive Order 13665, as long as such activities do not interfere with job duties or the efficient functioning of the Company's systems and equipment.

All original messages and information generated on or handled by the Company's communications systems, including backup copies, are the property of the Company.

To ensure that the use of electronic and telephonic communications systems and business equipment is consistent with the Company's legitimate business interests, the following guidelines will be followed:

- ◆ The information systems are not to be used in ways that are in violation of Company policies, disruptive or offensive to others, or in ways that are inconsistent with the professional image and good reputation of the Company.
- ◆ Display or transmission of sexually explicit images, messages, cartoons or any communication that can be construed as unlawful harassment or disparagement of another based on their race, color, national origin, sex (including pregnancy, childbirth, breastfeeding, or related medical condition), gender (including gender identity and gender expression), sexual orientation, religion, marital status, age, national origin, ethnicity, citizenship status, religious creed or belief, physical or mental disability, marital or familial status, protected veteran status, protected activity or other protected status is prohibited.
- ◆ Do not post or make statements on or through media advertisement, Internet home page, electronic bulletin board posting, electronic mail message, voice mail message, or any other public representation about the Company in such a way as to mislead others in thinking you are speaking on behalf of the Company without prior **written** authorization by a Company officer.

**Q. Can my work e-mail be accessed by the Company?**

**A. Yes, your work e-mail is Company property and you have no right to privacy with regard to work e-mail.**

\* \* \*

All users are personally accountable for messages that they originate or forward using Company electronic or telephonic communications systems. Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communications system is prohibited. "Spoofing," constructing electronic communications so it appears to be from someone else, is prohibited. The user name, electronic mail address, organizational affiliation, time and date of transmission, and related information included with electronic messages or postings must always reflect the true originator, time, date, and place of origination of the message or postings, as well as the true content of the original message.

Any violation of this policy will result in appropriate disciplinary action, up to and including termination of employment and the exercise of other legal remedies that may be available to the Company.



## Information Security Policy

- The Company's proprietary business information stored on electronic and computing devices, whether owned or leased by the Company, the employee or a third party, remains the sole property of the Company. You must ensure through legal or technical means that proprietary information is protected in accordance with our standards.
- You have a responsibility to promptly report the theft, loss or unauthorized disclosure of the Company's proprietary business information.
- You may access, use or share the Company's proprietary business information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- You must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware, and to avoid accessing Company information through public electronic networks that could compromise our information security.
- All mobile and computing devices that connect to the internal network must be secured with reasonably strong passwords. You may not provide access to another individual, either deliberately or through failure to secure its access, or access data, a server or an account for any purpose other than conducting Company business, even if you have authorized access.
- The Company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

**Q. What is a "phishing" e-mail and how can I avoid it?**

*A. These are e-mails that are designed by criminals to appear authentic but that steal your credentials or place malware on your device by persuading you to open a message, click on a link or open an attachment. Only open messages, links or attachments from known senders, be suspicious of unexpected e-mails even if you know the sender and check carefully whether the sender's e-mail address appears authentic. It is your responsibility to take responsible measures to protect the Company's information security.*

**Q. Why should I avoid public wi-fi networks when conducting Company business?**

*A. Public wi-fi networks may not be as secure as our Company network and may provide third parties access to your Company information and credentials. The best protection is to avoid them when conducting Company business or use a secured VPN connection when accessing Company systems.*

## **EQUAL EMPLOYMENT OPPORTUNITY GUIDELINES**

It is the policy of the Company that recruitment, hiring, transfer, promotion, layoff, recall, and other relationships with applicants and employees be nondiscriminatory with respect to race, color, sex (including pregnancy, childbirth, breastfeeding, or related medical condition), gender (including gender identity and gender expression), sexual orientation, religion, age, national origin, ethnicity, citizenship status, religious creed or belief, physical or mental disability, marital or familial status, legally protected medical condition, genetic information, protected veteran status protected activity (such as opposition to or reporting of prohibited discrimination or harassment), and relatives of protected veterans, and any other status protected by local, state or federal law. The Company has adopted this policy not merely because it is the law, but because of the abiding moral conviction that it is right and the knowledge that it is beneficial to the Company and its shareholders. The Company expects all of its employees to further its policy of equal employment opportunity and will take such action as may be necessary to ensure the Company's total commitment to it. This commitment applies to all aspects of employment - including recruitment, hiring, training, compensation, job assignment, advancement, performance feedback and separation. The Company is committed to make reasonable accommodations that enable qualified disabled individuals to perform the essential functions of their jobs.

### **IMPLEMENTATION OF POLICY**

Company officials must exercise great care in personnel selection and base all employment decisions on objective, job-related criteria. The first duty of officials with employment related responsibilities is to employ and advance the best qualified persons. Proper evaluation of an applicant may include a check of work and school records, background checks, personal interviews, a review of application papers, and the like.

The Company shall continue to implement and further develop programs which will ensure the strengthening of the Company's policy of equal employment opportunity. When required either by law or by internal evaluation, the Company will develop affirmative action plans, including programs for women, minorities, protected veterans and individuals with a disability, designed to ensure that the Company's policy of equal employment opportunity is effective.

Periodic evaluation of supervisors shall include evaluation of performance in this sensitive area. Unsatisfactory performance shall be considered just cause for discharge.

## PROHIBITION OF DISCRIMINATION, HARASSMENT OR RETALIATION

The Company is committed to providing a work environment that is free of discrimination and unlawful harassment or retaliation. Actions, words, jokes or comments based on an individual's race, color, sex (including pregnancy, childbirth, breastfeeding, or related medical condition), gender (including gender identity and gender expression), sexual orientation, religion, marital status, age, national origin, ethnicity, citizenship status, religious creed or belief, physical or mental disability, protected veteran status, protected activity (such as opposition to or reporting of prohibited discrimination or harassment), or any other legally protected characteristic will not be tolerated. All such unlawful harassment, discrimination or retaliation is a serious violation of Company policy and may be unlawful.

## COMPLAINT PROCEDURE

All employees who believe they are the victim of discrimination or harassment or who observe any violation of the Company's policies prohibiting such conduct must report their concerns to their supervisor or, alternatively, the Human Resources Department or to the Ethics and Compliance Hotline at 1-800-347-9550 or [iesholdingsinc.ethicspoint.com](mailto:iesholdingsinc.ethicspoint.com), 7 days a week, 24 hours a day. Any supervisor or manager who becomes aware of possible sexual or other unlawful harassment or discrimination must promptly advise Human Resources. Employees can raise concerns about discrimination and harassment and make reports without fear of retaliation.

### RETALIATION PROHIBITED

- ◆ IES will not retaliate against any employee for making a complaint in good faith or for cooperating in an investigation of a complaint. Retaliation is illegal and strictly prohibited by IES.

## WHISTLEBLOWER PROTECTION AND PROHIBITION AGAINST RETALIATION

The Company's prohibition against retaliation extends beyond complaints about discrimination or harassment. This policy also protects any employee who reports an activity that he or she believes is illegal, dishonest or fraudulent to a manager, HR representative or the Ethics and Compliance Hotline (800-347-9550 or [iesholdingsinc.ethicspoint.com](mailto:iesholdingsinc.ethicspoint.com)). Examples of illegal or unlawful activities are violations of federal, state or local laws, unsafe practices, billing for services not performed, or fraudulent financial reporting. If an employee has knowledge of or a concern about illegal or dishonest fraudulent activity, he or she must contact their supervisor or HR representative or the Ethics and Compliance Hotline (800-347-9550 or [iesholdingsinc.ethicspoint.com](mailto:iesholdingsinc.ethicspoint.com)). **The Company will not retaliate against an employee for filing a good faith complaint.**

## **SAFETY AND ENVIRONMENTAL COMPLIANCE**

All employees are expected to comply with the Company's safety and environmental policies and procedures. The Company recognizes that project productivity is directly correlated to safety performance and that one accident or injury can cause schedule delays and cost increases. More importantly, injuries to precious human assets are not acceptable to the Company, their families or our customers. The Company is committed to providing a safe, healthy and professional work environment. We follow all federal, state and local laws regarding workplace safety, health and the environment. You should report any safety or environmental accidents or violations of the law or our policies.

**Q. We use a contractor to dispose of spent oil. I know the contractor's foreman and I get the feeling that they may not be disposing of the oil the right way. Should I care about this?**

*A. Yes, you should report it to your supervisor, safety coordinator or the Law Department. What the contractor is doing could make IES legally responsible for the contractor's illegal activities. We also should not look the other way, as an improper disposal could present a serious environmental risk.*

## **GOVERNMENT REQUESTS FOR INFORMATION OR INVESTIGATIONS**

It is Company policy to cooperate with federal, state, and municipal authorities and investigators seeking information concerning Company operations. At the same time, the Company and its directors and employees are entitled to all the safeguards provided by law for the benefit of persons under investigation. Any employee who receives subpoenas, documents, or outside inquiries regarding equal opportunity, civil or criminal actions and/or inquiries or investigations regarding the company or its employees is not authorized to act as an agent for the Company without written authorization. No documents are to be submitted to an attorney, government agency or court on behalf of the Company without review by the Law Department.

**It is the Company's policies to preserve all records that may be relevant to a legal investigation or claim.** You may never destroy such records without consulting the Law Department, and you must cooperate with any legal retention notice you receive from the Law Department. Charges from state human rights/labor agencies or the EEOC should be reported immediately to both Human Resources and the Law Department by telephone and in writing. Inquiries or documents from, and investigations or inspections of the Company facilities or records by any local, state or federal agency should be referred immediately to Human Resources and the Law Department.

All documents or inquiries by attorneys and all other civil and criminal actions must be reported and/or referred to the Law Department.

## **PROPRIETARY INFORMATION POLICY**

Company information and data shall be afforded protection commensurate with its nature. Measures shall be taken to safeguard information and data where disclosure or misuse could adversely affect the operations, employees, customers, creditors or stockholders of the Company or affiliated entities.

## **NONDISCLOSURE OR PERSONAL USE**

Any non-public, proprietary technical, trade secret or business related information, regarding the Company's operations is considered "Company Confidential Information." Employees must not use Company Confidential Information for their own personal use or disclose such information to an unauthorized third-party without prior review and written approval of the department head responsible for the information.

Company Confidential Information includes things like financial statistics, customer lists and their requirements, pricing arrangements and other proprietary information, budgets, certain construction methods, estimates, bid and price structures and processes, strategic plans, information about acquisition targets, plans, and/or development.

**Personnel matters, other employees' private information, identifiable medical information, medical reports, and other similar information involving an individual's right to privacy are also considered confidential and governed by law.**

The Company uses a computer data security system that is designed to prevent unauthorized access to and use of the computer and the Company software and data residing in the computer. Any theft or unauthorized or malicious modification or destruction of the Company computerized data will be treated as a violation of Company policy and may also subject the violator to civil or criminal liability.

Employees must safeguard the Company's confidential information essential to the conduct of our business, taking care to prevent disclosure until such information becomes publicly available or IES no longer considers it confidential. Nothing in this Proprietary Information Policy prohibits employees from sharing information about the terms and conditions of employment or other information protected by the National Labor Relations Act (NLRA) and/or the Pay Transparency Executive Order 13665.

Employees should respect the confidentiality of other businesses and persons. Confidential information received from a customer or former employer should be used only for the purpose for which it was provided and in compliance with any agreements related to the disclosure of that information. Employees who previously worked for another company must not use or disclose the confidential information of that company.

**As a public company, serious problems could be caused for the Company and you by unauthorized disclosure of internal information about the Company.** Company personnel should not discuss internal Company matters or developments with anyone outside of the Company, except as required in the performance of regular corporate duties. Consistent with the foregoing, employees should be discreet with internal information and not discuss it in places where it can be overheard such as elevators, restaurants, taxis and airplanes.

## **PUBLIC STATEMENTS**

There are specific requirements and methods of public dissemination of Company information and so no one should make any public statements about the Company or its activities without prior approval of such statements by the Law Department and specific approval to be a Company spokesperson.

## SECURITIES LAW GUIDELINES

Directors, officers, and employees of the company who possess material information about the Company or its affiliates which has not been disclosed publicly are subject to legal obligations with respect to their personal use or disclosure of such information. The purpose of these guidelines is to review and summarize the laws and regulations applicable to the use or disclosure of such material information.

### INSIDE INFORMATION

The personal use or disclosure of "material inside information" (as defined below) is prohibited by the securities laws and is a violation of the Company's Conflict of Interest Policy. **A basic tenet of the securities laws is that persons with corporate information should not take advantage of such information by trading in the securities of the Company or its affiliates as long as such information is not available to other members of the investing public.** Disclosing such information to any others including relatives or friends, called "tipping," is also prohibited. Until it is made public, material information about the Company must be used only for Company business purposes and not for anyone's personal benefit.

### PROHIBITED TRANSACTIONS

Any director, officer, or employee of the Company who possesses material inside information must abstain from acting on such information by trading in the securities of the Company or its affiliates and from tipping such information to others.

In addition, an individual, as a result of his or her position with the Company, may have access to material inside information concerning another corporation. In such case, the prohibitions on trading and tipping could also apply, with respect to the securities of such other corporation. Particular care should be exercised for example where such information is developed in the course of a possible acquisition.

Speculative trading, such as in-and-out trading, is discouraged as a matter of policy. Accordingly, it is the Company's policy that no director or employee will engage in short sales (sale of securities not owned) or sales against the box (sale of securities owned but not delivered against the sale) of any of the Company's stock. Similarly, it is the Company's policy that no director or employee will purchase or sell puts or calls or otherwise trade in or write options on the Company's stock.

**To promote compliance, it is the Company's policy that directors and employees who hold an officer's or controller's position or who are employed by the Company at its headquarters or at the headquarters of any of the Company's operating segments will limit transactions in the Company's securities to "window-periods" that generally commence after the second full trading day following the release of annual or quarterly financial results and continue until two weeks prior to the end of the quarter. In addition, if such individuals desire to trade in Company securities at any time they are required to give advance written notice to and receive written approval from the General Counsel of such intention.**

Upon receipt of the notice, the General Counsel will notify the appropriate members of senior management and, after receiving advice, will notify the individual as to whether management believes that there exists material non-public

## DID YOU KNOW

Sharing confidential corporate information with a family member or friend could be criminal "tipping" under insider trading laws.

You may also have material nonpublic customer information and may not trade or "tip" when in possession of it.

Company information that could be the basis for possible insider trading violations. No trade shall be made at any time, if the person desiring to effect the trade has knowledge of material, non-public information.

## DEFINITION OF MATERIAL INFORMATION

The question of what constitutes "material inside information" is complicated, and you should not attempt to make this judgment without legal advice. For example, one test of materiality is whether a reasonable investor would attach importance to the information in determining whether to purchase, hold, or sell a security. This encompasses any fact which in reasonable and objective contemplation might affect the market price of the Company's securities. Thus, material facts include not only information disclosing the earnings of the Company but also those facts which affect the probable future of the Company and those which may affect the desire of investors to buy, sell, or hold the Company's securities.

Whether facts are material when the facts relate to a particular event and are non-public will depend at any given time upon a balancing of both the indicated probability that event will occur and the anticipated magnitude of the event in the light of the totality of Company activity.

## KEEP IT SIMPLE

- ◆ You may never trade in Company securities during a blackout period if you are in the restricted group.
- ◆ Even during an open window, you must receive permission to trade if you are in the restricted group.
- ◆ You may NEVER trade in securities of a company, including a customer, if you have access to material nonpublic information about the company.



## EXAMPLES OF MATERIAL INFORMATION

Information concerning the following may possibly be material. This list is not meant to be exclusive and other categories of information not included may well be material:

- ◆ A proposed merger or acquisition.
- ◆ A proposed exchange or tender offer. A significant new contract, expansion of operations, or entering into a new line of business.
- ◆ Long range plans and projections.
- ◆ Earnings reports.
- ◆ Operating reports.
- ◆ Financings.
- ◆ Bankruptcy proceedings.
- ◆ Major changes in management.
- ◆ Stock splits and stock dividends.
- ◆ Significant cost savings initiatives.
- ◆ A significant new contract, expansion of operations, or entering into a new line of business.
- ◆ Long range plans and projections.
- ◆ Earnings reports.
- ◆ Operating reports.
- ◆ Financings.

## TRADING AFTER DISCLOSURE

A director, officer, or employee possessing non-public material information may resume trading, with permission if in the restricted group, after such information has been publicly circulated for a reasonable period of time (typically after two business days).

## LIABILITIES FOR PROHIBITED TRANSACTIONS

A director, officer, or employee who violates the prohibitions of the securities law faces the possibility of an injunction proceeding by the Securities and Exchange Commission and private actions for rescission, restitution, or damages.

**Willful violations are also subject to criminal penalties, including imprisonment.** The Company itself may even be held liable in certain instances and therefore be subject to substantial fines. Violators of the Company's Conflict of Interest Policy are subject to disciplinary action up to and including dismissal for cause.

## WHAT TO DO IN CASE OF DOUBT

If you are uncertain whether information is material or whether it has been disclosed publicly, a prudent course of action would be to refrain from trading in securities of the Company or from disclosing the information to an outsider, until you have resolved the uncertainty. You should direct any questions on these matters through normal channels to the Law Department.

## Legal Compliance Certificate

I have received a copy of the Legal Compliance and Corporate Policy of IES Holdings, Inc. and its subsidiaries and have reviewed and understand its provisions. I agree to comply with the Company's policies and guidelines and to follow all laws relating to the performance of my duties.

I understand that the guidelines contained in the Legal Compliance and Corporate Policy do not cover all of the situations which may arise in my work. In the event of doubt regarding the legality or appropriateness of any proposed action, I will seek the advice of the Law Department prior to taking the action. I also understand that in situations where my personal liability is involved, I am free to consult privately with my own attorney.

I also understand that from time to time, the Company may review and revise this Policy and that I can access the most current version online at [www.ies-co.com/corporate-responsibility](http://www.ies-co.com/corporate-responsibility).

I am not aware of any violations of the Legal Compliance and Corporate Policy by any officer or employee which have not been reported to management through proper channels. I understand that any violations of this policy also can be reported through the Ethics Line at 1-800-347-9550 or [iesholdingsinc.ethicspoint.com](http://iesholdingsinc.ethicspoint.com)

---

Signature

Date

---

Name

---

City

State

Zip