General Code of Conduct

Institutional Shareholder Services

November 2019

ISSGOVERNANCE.COM

TABLE OF CONTENTS

I. INTRODUCTION

This General Code of Conduct (the "General Code") sets forth principles and requirements that apply to all employees of Institutional Shareholder Services Inc. and its direct and indirect wholly-owned subsidiaries worldwide (collectively referred to as the "Company"). It also covers certain obligations should you leave the Company for any reason. The General Code should be read together with other Company policies and procedures, which can be found on the Compliance section of the Company's website.

To the extent there is any conflict between this General Code and any other applicable Company policies or procedures, you are subject to the most restrictive policies and procedures.

The General Code cannot and does not specifically address every legal or ethical issue that you may face at the Company. You are responsible for being familiar with the General Code, adhering to the principles and rules stated herein and seeking guidance when you are uncertain as to the proper course of action. By following Company policies and procedures, adhering to the letter and the spirit of all applicable laws and regulations, and by applying sound judgment to your activities, you can demonstrate your commitment to the Company's business principles and ethics.

Ultimately, we are guided by the most basic principle: Doing the right thing!

II. DOING THE RIGHT THING

Doing the right thing means that employees must use good judgement, make appropriate and ethical decisions and take responsibility for their actions. Such judgements are not always clear cut so when in doubt try asking the following questions:

- Does my action comply with the letter and spirit of applicable laws, regulations and Company policies?
- Is my action consistent with the Company's core values?
- Could my action damage my reputation and/or the Company's, or embarrass me or the Company?
- Who might benefit from or be harmed by my action?
- How would my action be viewed by others if it were the subject of media reports?

If you are still unsure about the appropriateness of a course of action, please seek guidance from your supervisor, Human Resources representative, or Compliance.

III. PROTECTING THE COMPANY'S INTERESTS

Anti-Bribery Statutes

Most countries around the world, and all countries in which ISS operates, have anti-bribery and ethics laws and regulations that prohibit giving anything of value to government officials (and, in some countries, to private sector entities and persons) for securing an improper business advantage. These laws include the U.S. Foreign Corrupt Practices Act of 1977, which prohibits corrupt offers of anything of value, either directly or indirectly, to a government official to obtain or keep business. The U.K. Bribery Act similarly prohibits the giving and taking of bribes in both the private and public sectors.

In this context, the term "Government Official" is broadly defined and includes, any employee, officer or other individual acting in an official capacity for or on behalf of:

- Any government or government-owned or controlled entity or agency;
- Any political party, party official or political candidate; and
- Any public international or supra-national organization, such as the World Bank or similar organization with government members.

In addition, many government agencies have their own rules governing the acceptance by Government Officials of gifts, travel and entertainment.

You must check with Compliance to review any pre-approval guidelines prior to giving gifts, entertainment or anything else of value to a Government Official. You also must obtain pre-approval before inviting Government Officials to events sponsored by the Company.

Economic Trade Sanctions and Anti-Money Laundering Laws

The Company is committed to compliance with all applicable anti-money laundering laws and regulations. Money laundering is the process by which individuals or organizations attempt to conceal the true origin and ownership of the proceeds of illegal activities and integrate the funds back into the financial system. Participation in money laundering activities is a crime. Employees must be on alert for possible money laundering or suspicious conduct by clients, prospective clients and other third-parties. If an employee suspects suspicious activity, the employee must contact their supervisor and Compliance.

The Company and its employees are prohibited from opening an account, establishing or continuing a relationship or engaging in any direct or indirect transactions or dealings with a country, individual or entity that has been sanctioned by a recognized governmental body. Governmental bodies such as the United Nations Security Council, the U.S. Treasury Department's Office of Foreign Assets Control and the European Union have sanctioning powers. Sanction regulations are often applied very strictly and violations can potentially subject the Company and its employees to liability regardless of whether the Company or the employee were aware of the regulations.

Anti-Boycott Laws

It is a violation of U.S. law to participate in a foreign boycott not sanctioned by the U.S. government (a "foreign boycott"). Company employees must not refuse to do business or furnish information in furtherance of, or otherwise participate in, a foreign boycott. U.S. regulations also impose a reporting requirement on the receipt of foreign boycott requests. Violation of anti-boycott laws may result in criminal, civil and regulatory penalties. Any employee who receives a request to supply information or otherwise act in furtherance of an unsanctioned foreign boycott must immediately contact Legal and Compliance.

IV. SAFEGUARDING AND MAINTAINING INFORMATION

Confidential and Proprietary Information

The Company possesses, and will continue to possess, information that has been created, discovered and developed by the Company, has been disclosed to the Company by clients and other third parties under the obligation of confidentiality, has otherwise become known to the Company, or in which property rights have been assigned or conveyed to the Company. This information is confidential to the Company (or the entity which provided it to the Company) and has commercial value in the business of the Company (or the party providing it). All such information, except such information as is known or becomes known to the public without violation of the terms of this Section IV, is hereafter called "Confidential and Proprietary Information." Confidential and Proprietary Information includes, but is not limited to: client lists, client holdings, transaction and other client account details, client voting intentions, client proxy votes, client proxy voting policies, client investment, engagement and screening strategies, other information related to the Company's clients, details of Company contracts and pricing policies, Company financial statements, projections, marketing plans or strategies, new product developments or plans, business acquisition plans, new personnel acquisition plans, trade secrets, operation methods, software and computer programs, and any other information that is not generally known to the public.

Employees are prohibited from sending confidential and proprietary information to their own personal email.

The Company puts equal weight on the protection of both Company confidential information as well as the confidential information that is entrusted to the Company by its clients and other third parties. All employees are responsible for the safeguarding of Confidential and Proprietary Information. Both during and after the employee's employment with the Company, employees must keep all such Confidential and Proprietary Information strictly confidential.

Without limitation and by virtue of each Company employee's employment with the Company and/or by affirming agreement with this General Code, each Company employee agrees as follows:

(1) to hold Confidential and Proprietary Information in strict confidence, to protect the security, integrity and confidentiality of such information and to not permit unauthorized access to or unauthorized use, disclosure, publication or dissemination of such information;

(2) that all Confidential and Proprietary Information is and will remain the sole and exclusive property of the Company (or the party providing it to the Company, as the case may be), and will not be disclosed or

revealed by the employee except to other Company employees who have a need to know such information to fulfill their employment functions or as is otherwise required in the performance of his/her duties for the Company; and

(3) upon termination of employment or at the request of the Company, to ensure that all Confidential and Proprietary Information and all documents, notes and other writings or electronic records that include or reflect Confidential and Proprietary Information and which are in the employee's possession are returned to the Company.

In support of the foregoing obligations regarding confidentiality, employees must observe the following principles when dealing with Confidential and Proprietary Information:

a) Before sharing Confidential and Proprietary Information with others in the Company, be sure that you are permitted to do so;

b) Do not disclose confidential Company or client information to other employees unless they have a need to know such information to perform their work responsibilities; and

c) Do not disclose Confidential and Proprietary Information to anyone outside the Company unless you are specifically authorized to do so, including as is strictly necessary while performing your work responsibilities.

Material Non-Public Information

Each employee is required to maintain a standard of conduct in effecting securities transactions, for his or her own account or on behalf of others, which avoids both the reality and the appearance of gaining personal advantage based on material, non-public information or at the expense of any third party, including the Company's clients.

Antitrust and Trade Regulation Laws

Antitrust and trade regulation laws are designed to ensure fair competition. Some forms of joint activities are legally permissible, but others are not. Consult with Compliance if you have questions about the application of antitrust or trade regulation laws to the business.

Privacy Laws

Privacy and data protection laws are designed to help protect against misuse of personal information. All Company personnel must be aware of the responsibilities that come along with having access to and processing data that relates to an individual living person, such as names and contact information, government issued identification numbers (such as social security numbers, national insurance numbers, passport numbers, etc.) and similar personally identifiable information. A copy of the Company's external privacy statement can be found here.

In addition, the Company is deeply committed to protecting the privacy of its employees' personal information. The Company's internal privacy statement can be found here.

Internet and Electronic Communication Usage

All employees must be aware of the responsibilities that come along with having access to Company systems and sensitive information. When using systems owned by the Company employees must always exercise sound judgment. Employees must be aware that Company systems may not be used for any purpose prohibited by law or by Company policies.

"Company systems" include but are not limited to computer networks, laptops, email systems and other third-party messaging systems, e-signature cards, email attachments, approved instant messaging services, Internet access facilities, mobile devices (provided by the Company), podcasts, remote access capabilities, faxing capabilities, telephone and voicemail.

A copy of the Internet and Electronic Communication Usage Policy is listed as an appendix below.

To ensure compliance with company policies, communications and **usage will be monitored from time to time** to the extent not prohibited by applicable laws and regulations.

Intellectual Property

Intellectual property law generally covers four areas: copyrights, patents, trademarks, and trade secrets. The Company's intellectual property assets are valuable to the Company and are therefore critical to protect. To the maximum extent permissible by law and subject to any compulsory provisions of local law, the Company owns all rights, title and interest in and to all intellectual property created or developed by you during your employment with the Company and that ownership continues if you leave the Company. Without limitation and by virtue of each Company employee's employment with the Company and/or by affirming agreement with this General Code, each Company employee agrees that all such intellectual property is the sole and exclusive property of the Company and hereby assigns all right, title and interest in and to such intellectual property to the Company.

Record Retention

The Company maintains books and records in accordance with applicable laws and policies. No one shall destroy or alter records related to any forthcoming or ongoing investigation, lawsuit, audit, or examination.

V. TREAT OTHERS WITH DIGNITY AND RESPECT

The Company is committed to a work environment in which all individuals are treated with dignity and respect. It is the policy of the Company to ensure equal employment opportunity without discrimination or harassment on the basis of race, color, religion, age, gender, gender identity, sexual orientation, national origin, citizenship, disability, marital and civil partnership/union status, pregnancy (including unlawful discrimination on the basis of a legally protected pregnancy/maternity leave), veteran status or any other characteristic protected by law.

The Company has also adopted a "zero-tolerance" approach to slavery and human trafficking. The Company is committed to taking all reasonably practicable steps to ensure that slavery and human trafficking is not present either in our operations or supply chains. A copy of the Company's Slavery and Human Trafficking Statement can be found here.

VI. PROMOTE A SAFE AND HEALTHY WORKING ENVIRONMENT

The Company is committed to conducting its business in compliance with all applicable environmental and workplace health and safety laws and regulations. The Company strives to provide a safe and healthy work environment for employees. Achieving this goal is the responsibility of all employees.

VII. VIOLATIONS OF THE GENERAL CODE OF CONDUCT

The General Code, including any future amendments, forms part of the terms and conditions of your employment with the Company. If you violate the General Code, you will be subject to disciplinary action, including possible termination of your employment. Disciplinary action will depend on the circumstances and will be consistent with the Company's policies and procedures.

VIII. REPORTING CONCERNS

If you believe you or a fellow employee may have violated the law or Company policies, you have a duty to promptly notify your manager and/or Compliance. You may also contact your Human Resources representative as appropriate.

Nothing in the General Code prohibits you from reporting possible violations of the law or regulation to, or co-operating with the investigative activities of, an appropriate governmental agency or from participating in a government-sponsored whistleblower program.

Reporting Hotline

The Company encourages open communication with respect to ethical matters and business practices; however, in circumstances where you believe the concern you have reported to your manager or Compliance has not been appropriately resolved, or if you would prefer to report the concern through other channels, you may contact the Business Integrity Hotline. A link to the Business Integrity Hotline can also be found on the Company's SharePoint site.

The Business Integrity Hotline is available 24 hours per day, 7 days per week for you to raise concerns, including anonymously, if you have observed any conduct, whether by an employee, a manager, a client, a consultant, an agent, a supplier or a third party, that potentially violates the law, a regulation or Company policy, or that you otherwise believe is improper.

Non-Retaliation Commitment

The Company prohibits retaliation against an employee for reports or complaints regarding the misconduct of others that were made in good faith. Open communication of issues and concerns by all employees without fear of retribution is vital to the continued success of the Company.

IX. QUESTIONS

Please consult Legal and Compliance if you have any questions regarding the General Code or any other legal or compliance related issues.

X. APPENDIX

Internet and Electronic Communication Usage Policy

I. USE OF COMPANY SYSTEMS

Only approved Company messaging systems (and not personal email accounts) may be used to conduct or host Company business. Careful thought must be given when drafting and sending email, instant messages and other electronic communications. Users should avoid colorful, cavalier, colloquial or shorthand language that might be misconstrued.

All information stored in or transmitted using Company systems is the property of the Company. Employees should be aware that authorized persons (including managers) have access to their electronic files, including Internet usage records and email. The company will from time to time monitor compliance with applicable regulations and Company policies to the extent not prohibited by applicable law and regulations. Electronic communications may also be disclosed and in regulatory and litigation matters and internal investigations.

Users are prohibited from using Company systems in the following manner (these examples are illustrative)

- Sending, storing, viewing, posting, forwarding or circulating (including to personal email accounts) unlawful, offensive, harassing, threatening, fraudulent or other inappropriate materials, jokes or messages, including but not limited to, pornography or violent language or images and religious or political materials;
- Attempting to avoid or disable technologies or methods implemented by the Company to block access to certain websites (e.g., pornographic websites or sites providing access to personal email accounts);
- Using Company systems for personal gain or illegal purposes;
- Sending, viewing, posting, forwarding or circulating advertisements, or promotions not related to Company business in a manner that suggests the item has been endorsed by the Company;
- Sending, viewing, posting, forwarding or, internally or externally, electronic messages containing confidential or proprietary information of the Company for non-business or other inappropriate purposes.
- Removing or changing any email disclaimer installed by the Company;
- Automatic forwarding of email to external or personal email accounts;
- Creating Out of Office Autoreply messages that contain contact information that includes personal or external email accounts;
- Automatic forwarding of email from an account maintained by a previous employer to any Company email account;
- Hosting Company information on third-party services or using messaging services (e.g., calendar, email, online data and contact storage sites) that have not been approved by the Company;

- Sending, viewing, posting, forwarding or circulating externally any communication or material indicated for internal use (e.g., For Internal Use Only - Not for Redistribution), including those posted for use by Company management on the intranet;
- Using Company systems to misuse Company or third-party intellectual property rights; and
- Gaining unauthorized access to electronic systems, including third party systems.

In addition, when using Company systems users should recognize the following:

- Unintended recipients might see electronic messages transmitted or forwarded internally or externally (e.g., over the Internet);
- Records of electronic communications are retained by the Company even after deletion by the user;
- Messages might have false or misleading address components when sent by third parties (i.e., the appearance of the message's sender can easily be falsified);
- Messages transmitted might not be delivered or may be delayed; and
- Information sent via email or instant messaging services to external sites generally cannot be recalled once sent.

When browsing the Internet, users must follow the terms of use available on external websites, unless advised otherwise by Compliance. From time to time, the Company may deem it necessary to strip attachments from email to mitigate the risk of exposure from viruses. For example, executable files (.exe) will often be removed from email, as they are the most common means for transmitting viruses. The Company may use cookies and other similar technology for the purposes of improving web site content, performance and security, and monitoring use of the site or as required by law or regulation.

II. OFFENSIVE OR INAPPROPRIATE MATERIAL

If an employee receives electronic communication that contains offensive or inappropriate material and the employee believes that the Company should be aware of the communication and/or act in relation to it, the employees should contact Human Resources.

For further direction regarding the reporting of discriminatory or harassing conduct, including instances in which such reporting may be mandatory, please refer to the Company's policies prohibiting discrimination and harassment in the workplace, or contact Human Resources and/or Compliance.

III. SOFTWARE, VIRUSES AND ENCRYPTION

Unless specifically required as part of your job responsibilities, users are prohibited from:

- Downloading, transmitting, installing or using software that has not been approved by the Company;
- Using software in a manner inconsistent with applicable licenses governing the Company's use of that software;
- Using encryption technology regarding electronic communications without prior approval; and

- Creating or disseminating destructive programs such as viruses, Trojan horses or self-replicating code.

Please note that this list is not all-inclusive.

IV. UNSOLICITED COMMUNICATIONS AND SPAM

"Unsolicited Communications" mean any unwelcome telephone, Short Message Service ("SMS"), email (e.g., "SPAM") or other electronic communications, the primary purpose of which is advertising or solicitation of a product or service. Unsolicited Communications may only be transmitted by users in compliance with applicable rules and regulations. For additional details on the use of Unsolicited Communications, contact Compliance.

V. PERSONAL EMAIL ACCOUNTS

Users are prohibited from using Company systems to access personal email accounts, except as may be specifically authorized from time to time by the Company.

For their personal use, some users may have personal email accounts with various Internet service providers or Internet portal sites. Accessing personal email accounts using Company systems places the Company at risk by potentially introducing viruses and other high-risk attachments into Company systems. Therefore, such access is prohibited except as may be specifically authorized from time to time by the Company through secure methods.

As stated previously in this policy, only approved Company messaging systems (and not personal email accounts) may be used to conduct or host Company business.

VI. INSTANT MESSAGING

Users are not allowed to using Company systems to access instant messaging ("IM") services, except those services that have been approved by the Company for employees' use. It should be noted that the Company may retain records of all IM conversations on Company systems. The same discretion and thought used when writing emails sent using Company systems should be applied to the use of Company-approved instant messaging.

VII. EXTERNAL CHAT SITES, BLOGS, BULLETIN BOARDS AND NEWSGROUPS

Users are prohibited from using Company systems to post information to or otherwise communicate in external chat sites, blogs, electronic bulletin boards, newsgroups or other similar external services without the written approval of Compliance. Further, when accessing or using any of these services through non-Company systems, users are prohibited from disclosing any information learned or created in the course of their relationship with the Company, or otherwise posting information, including information about Company employees or clients, in a manner that is inconsistent with Company policies or the General Code.

VIII. PERSONAL USE OF COMPANY SYSTEMS

Company systems are intended for use in conducting Company business. Users are allowed to use these systems for reasonable and occasional personal use and in accordance with local office or business unit policy. Personal use of Company systems is subject to all provisions contained within this policy, including the Company's right to monitor such use.

When using Company systems for personal reasons, users should exercise sound judgment to protect the Company's reputation. In addition, users should avoid using Company systems to communicate sensitive and/or personal information that might cause distress or embarrassment if viewed by unintended recipients.

Personal use must be kept to a minimum and should not interfere with business responsibilities.