Innovation & Action

INOAC

Code of Conduct & Business Ethics Policy

Published: February 2012
Revised: June 2021

Table of Contents

A. Applicability 4
B. Business Conduct and Ethics 4
C. Compliance with Laws and Human Rights 4
D. Commercial Bribery 8
E. Computer, Email and Internet Usage Policy 8
F. Responding to Media Inquiries 13
G. Confidentiality of Company, Customer or Supplier Information 14
H. Competitive Information 14
I. Record Retention 14
J. Sales: Defamation or Misrepresentation 14
K. Fair Dealing 14
L. Political Contributions 15
M. Personal Relationships and Dating 15
N. Workplace Safety 15
O. Reporting Ethical Violations 16
P. Responsibility and Implementation 16
Q. Conclusion 17

CODE OF CONDUCT &
BUSINESS ETHICS POLICY

INOAC USA, Inc. and its subsidiaries (the "Company") are committed to adherence with the highest ethical standards and conducting business with the utmost level of integrity.

An uncompromising adherence to high ethical standards is integral to creating and sustaining the strong foundation on which success is built and on which our Company can grow and prosper.

Each team member is responsible for the consequences of his or her actions. We must each be honest and ethical in our personal conduct as well as be a guardian of the Company's ethical standards.

Leaders in our Company have an added responsibility of setting an example by their personal performance and an attitude that consistently conveys these values. This example requires us to treat everyone – team members, customers, prospects, suppliers and competitors with honesty and respect.

If you are unsure of the appropriate action to take, utilize our Open-Door Policy to raise your concerns with any member of our leadership team or, follow the processes outlined in this *Code of Conduct & Business Ethics Policy*.

Kim Rulo
Vice President,
Human Resources

Rob DePotter
President, Chief
Operating Officer

A. Applicability

The word "team member" and references to "you" and "yours" used in this Code includes all team members, Officers and, when they are acting on behalf of our Company, Directors.

B. Business Conduct and Ethics

Our Company and each of our team members, wherever they may be located, must conduct their affairs with uncompromising honesty and integrity. Business ethics are no different than personal ethics. The same high standard applies to both. As a team member you are required to adhere to the highest standard regardless of local custom.

Team members are expected to be honest and ethical in dealing with each other, customers, suppliers and all other third parties. Doing the right thing means doing it right every time. Misconduct cannot be excused because it was directed or requested by another. In this regard, you are expected to alert a member of our leadership team whenever an illegal, dishonest or unethical act is reasonably suspected. You will never be penalized for reporting your reasonable suspicions. The following statements concern frequently raised business conduct and ethical concerns. A violation of the standards contained in this *Code of Business Conduct & Workplace Ethics Policy* will result in corrective action, including possible dismissal.

C. Compliance with Laws and Human Rights

1. General

It is our Company's policy to comply with all laws, rules and regulations that are applicable to its business in all countries, localities and jurisdictions in which we operate or do business.

2. Employment Conditions

It is our Company's policy to comply with all applicable employment laws, including those governing working conditions, wages, hours, benefits, minimum age for employment and human trafficking.

a. **Forced Labor:** the Company will not allow the use of forced labor of any kind nor will the Company ever tolerate physically abusive disciplinary practices.
b. **Human Trafficking:** the Company strictly prohibits the use of, or benefiting from in any way, human trafficking and human trafficking related activities. Furthermore, the Company shall not withhold identity papers/documents (such as passports or identification cards), work authorizations, or the requiring of recruitment deposits.
c. **Team Member Engagement:** While the Company continually strives to enhance team member engagement and job enrichment, the Company also recognizes the team members' freedom to organize and engage in protected concerted activity, and the Company will not interfere with those legal rights.
d. **Child Labor:** the Company will not use child labor nor will it employ any person who is below the age of 18. The only specific exception would be in instances where employment would be pursuant to a government-authorized apprenticeship, or job training programs that would be beneficial to the participants.
e. **Anti-Harassment and Non-Discrimination:** while team members and applicants for employment must be qualified and meet job requirements established by the Company, each person must be accorded equal opportunity to the full extent provided by law and without regard to race, color, religion, national origin, gender, sexual orientation, marital status, age, disability, genetic information or other characteristics protected by law. Each team member must respect the rights of fellow team members and third parties. Your actions must be free from libel, slander, harassment or any form of unlawful discrimination.

3. Environmental and Sustainability Matters

It is our policy to comply with all applicable laws and regulations for the protection of the environment. Each team member must abide by these laws and established environmental policies and procedures. Whenever practicable, the Company will use its best efforts to reduce and minimize the impact of its operations on the environment, and it will continually strive to create environmentally-sustainable strategies for the long-term benefit of our surrounding communities and planet.

The Company shall maintain records to enable the Company to report to government authorities the presence of any conflict materials (as defined by applicable law).

4. Fair Competition

Our Company must comply with all applicable fair competition laws. These laws are directed at ensuring that businesses compete fairly and honestly and prohibit conduct seeking to reduce or restrain competition through price fixing, bid rigging, bid allocation or other forms of collusion with competitors.

5. Conflicts of Interest

You must avoid any personal activity, investment or association which could appear to interfere with good judgment concerning the best interests of the Company. You may not exploit your position or relationship with the Company for personal gain. You should avoid even the appearance of such a conflict. For example, there is a likely conflict of interest if you:

i. Cause the Company to engage in business transactions with relatives or friends;
ii. Use confidential or nonpublic Company, customer or supplier information for personal gain by you, relatives or friends;
iii. Have more than a modest financial interest in our suppliers, customers, or competitors;
iv. Receive a loan, or guarantee of obligations, from the Company or a third party as a result of your position with the Company;
v. Compete, or prepare to compete, with the Company while still employed by the Company; or perform work (with or without compensation) for a competitor, governmental or regulatory entity, customer or supplier of the Company or do any work for a third party that may adversely affect your performance or judgment on the job or diminish your ability to devote the necessary time and attention to your duties.

There are other situations in which a conflict of interest may arise. If you have concerns about any situation, follow the steps outlined in the Section on "Reporting Ethical Violations" below.

6. Business Opportunities

You are responsible for advancing the Company's business interests where the opportunity to do so arises. In addition to avoiding conflicts of interest, you must not take for yourself or divert to others any business opportunity or idea discovered in the course of your employment in which the Company might have an interest.

7. Gifts, Bribes and Kickbacks

i. Other than nominal gifts given or received in the normal course of business (including travel or entertainment) which could not be considered as business inducements, neither you nor your relatives may give gifts to, or receive gifts from our customers and suppliers. Gifts should not be accepted from a supplier or potential supplier during, or in connection with, contract negotiations.
ii. Accepting cash or cash equivalents, including checks, money orders, vouchers, loans, stock or stock options, is not acceptable under any circumstances. Other gifts may be

given or accepted only with prior approval of your senior leadership. In no event should you put the Company or yourself in a position that would be embarrassing if the gift were made public.

iii. Dealing with government associates and officials is often different than dealing with private persons. Many governmental bodies strictly prohibit the receipt of any gratuities by their associates, including meals and entertainment. You must be aware of and strictly follow these prohibitions.

iv. Any team member who pays or receives bribes or kickbacks will be immediately terminated and reported, as warranted, to the appropriate authorities. A kickback or bribe includes any item intended to improperly obtain favorable treatment.

8. International Operations

The Company conducts its affairs consistent with the applicable laws and regulations of the countries localities and jurisdictions in which we operate or do business with. Business practices, customs and laws differ from country to country. When conflicts arise between the Company's ethical practices and the practices, customs and laws of a country, the Company seeks to resolve them consistent with its ethical beliefs. If the conflict cannot be resolved consistent with its ethical beliefs, the Company will not proceed with the proposed action giving rise to the conflict.

9. Covering Up Mistakes; Falsifying Records

Mistakes should never be covered up, but should be immediately and fully disclosed and corrected. Falsification of any Company, customer or third party record is prohibited.

10. Financial Integrity

Investors, creditors and others have legitimate interests in the financial and accounting information of the Company. The integrity of our financial reporting and accounting records is based on the validity, accuracy and completeness of the basic information supporting the entries to books and records of the Company. All financial books, records and accounts must accurately reflect transactions and events and conform to generally accepted accounting principles and to our system of internal controls. It is the responsibility of each team member to uphold these standards.

Team members are expected to cooperate fully with the internal audit function of the Company, our external auditors and any audits by governmental or regulatory authorities. Information must not be falsified or concealed under any circumstances. Examples of unethical financial or accounting practices include:

i. Making false entries that intentionally hide or disguise the true nature of any transaction;

ii. Improperly accelerating or deferring the recording of expenses or revenues to achieve financial results or goals;

iii. Maintaining any undisclosed or unrecorded funds or "off the books" assets;

iv. Establishing or maintaining improper, misleading, incomplete or fraudulent account documentation or financial reporting;

v. Making any payment for purposes other than those described in documents supporting the payment; and

vi. Signing any documents believed to be inaccurate or untruthful.

11. Foreign Corrupt Practices Act (FCPA)

It is the unqualified policy of the Company to conduct its business operations in strict compliance with the U.S. Foreign Corrupt Practices Act (the "FCPA") and all other applicable foreign and domestic anti-bribery laws. The Company is committed to the highest integrity and ethical standards in its business. Its operations will comply with the laws of the United

States and countries where it does business. No team member has the authority to act contrary to the provisions of this policy or to authorize, direct or condone violations of it by any other team member or by any agent of the Company.

This policy extends to all of the Company's domestic and foreign operations, including operations conducted by any departments, subsidiaries, agents, consultants or other representatives, and operations of any joint venture, distributor, or other business enterprise outside the U.S. in which the Company is a participant.

The FCPA prohibits making payments or providing anything of value to foreign officials for purposes of obtaining or retaining business, directing business to any person, or securing any improper advantage. Accordingly, no team member shall offer, promise, make, or facilitate the making of, payments or anything of value to foreign officials, to attempt to retain, or to retain, any business, or secure any improper advantage, as is prohibited by the FCPA.

Under the FCPA, "foreign official" is defined broadly. "Foreign official" means any officer or employee of a foreign government or any department, agency, or instrumentality thereof, or of a public international organization, or any person acting in an official capacity for or on behalf of any such government or department, agency, or instrumentality, or for or on behalf of any such public international organization. A "foreign official" may also be a person working for or on behalf of a government-owned or government-controlled business or a public utility. The FCPA also prohibits payments to a foreign political party or a candidate for foreign political office for the purposes of retaining or obtaining business or directing business to anyone.

"Anything of value" is also broadly defined under the FCPA. "Anything of value" includes cash, as well as non-monetary gifts, including, but not limited to, gifts to foreign officials or their family members, travel, entertainment, and discounts on services.

No team member should make any direct payment to a foreign official. If you would like to make a payment for or on behalf of a foreign official, you must contact the Company's Legal Counsel or VP, North American Human Resources, before making the payment. If you receive a request from a distributor, reseller, vendor, or other business partner or third party, asking for a payment or discount that is not provided for in the Company's contract with that party, contact the Company's Legal Counsel or VP, North American Human Resources.

In any instance where a team member believes a potential payment for what are believed to be legitimate travel or entertainment expenses, the team member must receive prior written approval for the payment from the Company's Legal Counsel or VP, North American Human Resources or inquire to these same resources if there is any question or uncertainty.

The FCPA also requires that a company maintain accurate books, records, and accounts, and proper internal accounting controls. Accurate books and records and a system of internal accounting controls are necessary to assure that the Company's transactions are authorized, recorded accurately, and periodically reviewed.

Penalties for violating the FCPA are severe. The FCPA provides for corporate and individual liability. A company and individuals can face criminal fines. Individuals are also subject to imprisonment for as much as five years per FCPA violation. In addition, violations of the FCPA may alsoresult in loss of certain licenses, permits or business opportunities, as well as long-term damage to a company's reputation and brand.

D. Commercial Bribery

It is important to note that the Company's anti-bribery policies and guidelines apply to private sector employees as well. While the FCPA does not expressly prohibit illegal payments relating to private sector employees, the U.S. government has increased its use of other U.S. laws to prosecute domestic and international private commercial bribery.

It is the policy of the Company that team members shall not give or receive gifts that may be considered gifts to obtain or retain business from private sector companies or employees. If you would like to give a nominal gift that you believe could not be considered a business inducement, contact the Company's Legal Counsel or VP, North American Human Resources, before making the gift.

The Company's policy on the FCPA and commercial bribery prohibits not only actual or direct bribery, but it also prohibits "willful blindness" and "conscious disregard" of facts and circumstances that could indicate an illegal payment. Team members who are aware of such circumstances and fail to take action to determine whether it is true or not, could be violating this policy.

If you have any questions or issues concerning the Company's anti-bribery policies, third parties, foreign officials, or payment practices, you should contact the Company's Legal Counsel or VP, North American Human Resources for further guidance.

E. Computer, Email and Internet Usage Policy

1. Ownership of Computers, Networking Equipment, Company as Sole Software Licensee, and Provider of Internet Access, and Ownership of the Company's Data

i. Computers, computer systems, computer networks, computer software, and Company provided digital devices, data, data files and computer information, e-mail software and servers, and access to the Internet via Company's networks, or by any other means furnished by the Company, including any wireless systems, furnished to you are intended primarily for the Company's business use. Any use of the Company's computers, computer systems, computer networks, computer software, data, data files and computer information, e-mail software and servers, and access to the Internet via the Company's networks, or by any other means provided by the Company, for the benefit of third parties is expressly forbidden, unless approved in writing by your direct supervisor or superior.

ii. All computers, computer systems, computer networks, and company provided digital devices are the sole property of the Company, and you are granted use of such equipment solely during the term of your employment.

iii. The Company is deemed to be the sole licensee of all computer and e-mail software. No sublicenses are deemed to have been created, and you are granted use of such software solely during the term of your employment.

iv. All access to the Internet provided by the Company to you is granted solely during the term of your employment.

v. All data, data files, and information that the Company provides you access to is the express intellectual property of the Company, and nothing in the provision of such access shall be deemed a transfer of title of such data, data files or information. All data, data files and information are deemed to be the Company's trade secrets, and you are required, as an express term of your continued employment, to maintain proper measures in order to ensure the secrecy of such data, data files and information. You shall not, unless expressly approved by your superior or supervisor, copy or otherwise transfer any data, data files or information from the Company's

computers, computer systems or networks to any computer, computer system or network not under Company's direct control.

2. Computer and Hardware Usage

i. The Company makes certain computers, computer systems, computer networks, computer hardware, and company provided digital devices available for your use during the term of your employment. Your use of the computers, computer systems, computer hardware, and company provided digital devices shall be primarily for your work duties. However, the Company grants you limited, reasonable use of the computers, computer systems, computer networks, computer hardware, and company provided digital devices for your personal use, provided, however, that such use does not violate any other term of this Policy. You shall ensure that proper anti-virus software is, at all times, running on any and all computers that the Company makes available to you.

ii. Given the adverse impact and effect on the overall performance of our networks and servers, utilizing the company's network and servers for streaming video services and music for personal use is strictly prohibited.
The use of dating apps and websites, pornography, and storage of inappropriate content is not allowed on company equipment.

3. Software Usage

i. The Company makes certain software applications available for your use during the term of your employment. Your use of the software shall be primarily for your work duties. The Company grants you limited, reasonable use of the software applications for your personal use, provided, however, that such use does not violate any other term of this Policy.

ii. The Company prohibits the illegal duplication of any software, and its related documentation, that the Company has licensed from any third parties, and which is made available to you.

iii. You may only use software, including e-mail software, on the computer systems according to the license agreement that accompanies the software. You shall only install one (1) copy of any software package on only one (1) computer, should you be unsure as to the terms of the software license agreement under which the software is used.

iv. You shall abide by all terms of any and all software license agreements, and shall not copy or distribute the software to any other person or entity.

v. You shall consult the Company, should you have any questions regarding the use of any software and whether any intended use comports with the terms of the software's license agreement. The Company shall provide sufficient access to any software license agreements or manuals, should any question arise as to the application of such software license agreement to local area networks or installation and use of software on multiple computers, or should any other question arise regarding the terms of any software license agreements.

vi. You shall not install, or uninstall, any software applications, updates, or modules without the Company's express written consent. If such consent is granted, you shall take all reasonable steps to ensure that the installation of such software proceeds without affecting software already installed on the target computer and that such software is free from viruses or other malicious code.

4. E-mail Usage

i. E-mail may not be used for purposes of solicitation, including invitations to enter into commercial ventures, or to solicit persons for religious or political causes, third party organizations, or other non-business matters. Transmission of offensive, sexually explicit, defamatory, or discriminatory e-mail or attached electronic files, or the use of e-mail for purposes likely to be deemed as illegal or harassment, is strictly prohibited.

ii. Your use of the Company's computers, computer systems and networks, and Internet connections to transmit e-mail shall be limited primarily to business communications. The Company grants you limited use of the Company's computers, computer systems and networks, and Internet connections to transmit and receive e-mail that does not violate Paragraph 4(i) or any other term of this Policy. The Company shall retain the sole discretion to determine whether your use of e-mail is an abuse of the privilege enumerated under this Paragraph.

iii. You waive any right to privacy in e-mail messages and you consent to the Company's access to e-mail sent and received on the Company's computers, computer systems and networks, or through Company's Internet connections. The Company reserves the right to read any e-mail messages and to inspect any files attached to any incoming or outgoing e-mail messages sent or received on the Company's computers,computer systems and networks, or through the Company's Internet connections.

iv. All e-mail transmitted by you shall be sent under your legal name and shall not be sent under any false name, nickname or alias. All e-mail shall include an electronic signature listing your legal name, job title, return e-mail address and phone contact number. The electronic signature shall also include a notice that the transmitted e-mail message is a confidential and privileged communication, if you have reason to believe that the e-mail message would be considered a confidential and privileged communication by yourself, the Company, or by the recipient of the e-mail message.

v. You shall ensure that proper anti-virus software is, at all times, and that such anti-virus software is monitoring your use of e-mail.

vi. The Company cannot guarantee that older e-mail messages will be saved or archived on the Company's e-mail systems. You should print out or otherwise save on your local storage media any older e-mail messages that you wish to retain. The Company retains the discretion to store, back-up and save any and all transmitted and/or received e-mail messages on storage media. The Company's storage and/or back-up of such e-mail messages shall be governed under the terms of Paragraph 4(ii).

5. Internet and Network Access Usage

i. The Company's computer networks and connections to the Internet are made available to primarily for the Company's business purposes. You shall clearly indicate that your opinions are your own and not those of the Company, should you disclose your status as an Employee of the Company on any Internet message board, chat room or other interactive area.

ii. You may not use the computer networks or the connections to the Internet for accessing, posting or downloading: sexually explicit images, files or messages; images, files or messages considered offensive or discriminatory; or any other files or messages that may reasonably be considered disrespectful of others. You shall consider information regarding the Company's business operations as confidential information, and shall not transmit any such information over the Internet, in any form.

iii. You shall not engage in any activity that may reasonably be considered as computer "hacking" or "cracking," and shall refrain from using the Internet to engage in any

activity prohibited by law, including posting, copying or transmitting any information that You may have reason to believe is copyrighted by a Third Party, including any music or video files. You shall not establish any other Internet connections, including wireless connections, to or from the Company's computers, computer systems or computer networks without express written approval from your immediate superior or supervisor.

iv. You shall take reasonable measures to ensure that any files downloaded through the Internet are free from viruses, Trojan horses, worms, or other malicious code. You shall inspect any and all files downloaded from the Internet for possible malicious code. You shall refrain from downloading files in violation of software licensing, copyright and trademark, and intellectual property laws.

6. Passwords

i. You will be prompted to choose at least one (1) password for access to the Company's computers, computer systems, computer networks and e-mail systems. Passwords shall be chosen that include multiple letters and/or numbers, and shall not be common dictionary words or your name.

ii. You shall not share or reveal any such passwords created and/or used on the Company's computers, computer systems, computer networks and e-mail systems to any third party or other person. You may, however, be required to reveal your password(s) to your direct supervisor or superior for purposes of computer maintenance. Should such disclosure occur, you shall be granted the opportunity to create new passwords for those revealed.

iii. You shall not attempt to ascertain the passwords of other personnel of the Company, of any System Administrators, and the System Administration. You shall not use any inadvertently ascertained or revealed passwords of other personnel of the Company to access any other computer, computer system, computer network, or network or e-mail account. Should you inadvertently ascertain or determine the password of another person employed by the Company, You shall immediately notify your superior or supervisor, who shall then be responsible for ensuring that the ascertained password shall be changed.

7. Monitoring Usage and Privacy of Data and Information

i. The Company may, at its sole discretion, monitor use of the Company's computers, computer systems, computer networks, e-mail system, or use of the Internet without specific or advance notice to you.

ii. You have no personal right or expectation of privacy to or in any data, data file or information stored on or transmitted through the Company's computers, computer systems or computer networks. The Company retains the right to open or otherwise inspect any data, data file, information or software application stored on the Company's computers, computer systems and computer networks, including e-mails sent and received by you. The Company has no responsibility to inform you of the Company's inspection of such computers or systems, even if you have stored personal data, data files or information on Company's computers or computer systems.

iii. Aside from the monitoring rights of the Company, the use of any recording equipment, devices, software, or applications is expressly prohibited with in all of the Company's facilities and offices, unless express written consent is provide by the Company.

8. Reporting of Known and Suspected Violations

i. You shall notify your immediate superior or supervisor, or any other member of the Company's management, should your superior or supervisor be unavailable, upon

learning of any known violations of or deviations from the terms of Policy, including any known violations by Employees or agents of the Company.

ii. You agree to notify your immediate superior or supervisor, or any other member of the Company's management, should you become aware of any computer, e-mail or Internet access usage that would likely be deemed to be a deviation from the terms of this Policy, including any known violations by other Employees or agents of the Company.

iii. You agree to obtain prior approval from your immediate superior or supervisor, or any other member of the Company's management, should your superior or supervisor be unavailable, before engaging in computer, e-mail or Internet access usage that would likely be deemed to be a violation or deviation from the terms of this Policy.

iv. You agree to notify your immediate superior or supervisor, or any other member of the Company's management, should you inadvertently engage in computer, e-mail or Internet access usage that would likely be deemed to be a violation or deviation from the terms of this Policy.

v. You are responsible for any and all willful unlawful actions undertaken by yourself, or any unlawful actions undertaken by others upon your request or guidance.

9. Violations of this Policy

i. You are responsible for protecting the Company's computers, computer systems, computer hardware and any media storing the Company's software or data from damage or loss. You shall be in violation of this Policy, should You intentionally, carelessly, willfully or maliciously damage the Company's computers, computer systems, computer hardware or any media storing the Company's software or data, including any denial of access to the Company's computers, computer systems, or computer networks. You will be financially responsible for any damage or loss caused by your failure to abide by the terms of this Paragraph.

ii. You shall be in violation of this Policy, should you intentionally, carelessly, willfully or maliciously infect Company's computers, computer systems or hardware with a virus, Trojan horse, worm, or other malicious code regardless whether such code causes actual damage to the Company's computers or computer systems. You will be financially responsible for any damage or loss caused by your failure to abide by the terms of this Paragraph.

iii. You shall be in violation of this Policy, should you intentionally, carelessly, willfully or maliciously restrict or impede access to the Company's electronic files, data,websites, e-mail systems and computer networks, including any systems used to access the Internet. You will be financially responsible for any damage or loss causedby your failure to abide by the terms of this Paragraph.

iv. You shall be in violation of this Policy, should you copy or distribute any data, data files, or information that is the Company's express intellectual property. Such disclosure or distribution may constitute a misappropriation of the Company's trade secrets and may subject you to civil liability for damages to the Company.

v. In addition to the responsibility for financial losses for violations enumerated in this Policy, you shall be subject to disciplinary action for intentional, willful or negligent violations of this Policy, including possible termination of your employment. Certain violations of this Policy could also be interpreted as violations of federal and state law, including, but not limited to, the Computer Fraud and Abuse Act. Any violations which the Company deems to be violations of applicable federal or state law shall be reported to the proper authorities.

F. Responding to Media Inquiries

1. Media Response Team

The designation as a Company Spokesperson is limited to the following business leaders who will serve as the "Media Response Team" and collectively discuss the best method to address unplanned media inquiries:

i. President & Chief Operating Officer
ii. VP-Communications
iii. VP – Human Resources

2. Media Inquiries

Periodically a reporter, producer or other news media may seek to gain information about the Company. Several examples of these requests include:

i. General information about the Company
ii. Information about an unexpected event such as an accident, natural disasters, theft, arrest, customer or team member complaint or a government regulatory action
iii. Insight into an action or event that could impact our industry, new competitive entrants, product launches or internal Company policies, or
iv. Input for a story in a local community such as changes in local governmental official, specific issues or public policies.

In all instances, all requests from the media shall be referred to the Media Response Team. Please do not say you are not allowed to speak to a reporter or need to get permission – rather, explain that "Company policy is to refer all media inquiries to our Media Response Team". It is particularly helpful if you provide contact information for one or more of these resources.

Whenever taking a call from the media, the same courtesy and professionalism in which we approach customers should be displayed. In order to promote our customer service image, it is important to respond quickly, courteously and professionally to all media calls. This is important because the handling of the initial call may be the reporter's first impression of the Company and that impression may end up in the story.

A similar process as described above will be used when someone from the media is requesting permission to take photographs or to film inside our facilities. Formal approval cannot be provided without talking in advance with the General Manager of the facility which will allow a decision to be based upon a number of considerations including but not limited to:

v. What does the Company have to gain from the photo and filming?
vi. How much disruption will this cause to our operations?
vii. What is the age and condition of the facility?
viii. Does the facility look "picture perfect" good?

A reporter, camera crew or photographer may show up unannounced and most likely to occur in crisis situations. When dealing with reporters and photographers who may show up unannounced, the facility manager and staff should act with the same courtesy and professionalism as we approach customers. Contact the Media Response Team immediately and to let them know which news source is there.

We cannot prevent the filming or photographing of common areas outside of our facilities which we do not operate. Examples would include public parking lots, courtyards and walkways. The following guidelines should be used when television camera crews or print photographers show up unannounced at your facility:

ix. Although we cannot prevent the media from photographing or filming the exterior of our facilities, we will contact their news room and/or editors for clarification.
x. The media cannot enter our facility to photograph or film without permission.
xi. The media cannot block the entrance to our facility or prevent people from entering our facility or conducting business as usual.

Be courteous and friendly, but also remember that no matter how congenial or affirming the reporter, photographer or camera crew are, everything you say and do may be observed and reported by the media representative for his/her audience.

G. Confidentiality of Company, Customer or Supplier Information

You may not use or reveal to others customer or supplier confidential or proprietary information except as authorized by your senior leadership or as legally required. This includes business methods, pricing and marketing data, strategy, computer code, screens, forms, experimental research, and information about the Company's current, former and prospective customers and team members.

H. Competitive Information

You may not accept, use or disclose improperly obtained confidential information of our competitors. When obtaining competitive information, you must not violate our customers' rights. Particular care must be taken when dealing with competitors, customers, former customers and former team members. Never ask for or receive confidential or proprietary competitive information. Never ask a person to violate a non-compete or non-disclosure agreement. If you are uncertain, senior leadership can assist you.

I. Record Retention

The Company's business records must be maintained for the periods in accordance with the specific policies of your business units. Records may be destroyed only at the expiration of the pertinent period. In no case may documents involved in a pending or threatening litigation, government inquiry or under subpoena or other information request be discarded or destroyed, regardless of the period specified in the applicable policy. In addition, you may never destroy, alter, or conceal with an improper purpose any record or otherwise impede any official proceedings either personally, in conjunction with, or by attempting to influence, another person.

J. Sales: Defamation or Misrepresentation

Aggressive selling should not include misstatements, innuendo or rumors about our competition or their products or financial condition. Do not make unsupportable promises concerning Company products.

K. Fair Dealing

No team member of the Company shall take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair-dealing practice.

L. Political Contributions

Company assets may not be used to make political contributions except in compliance with all applicable laws. You may, however, engage in personal political activity with your own resources on you own time.

M. Personal Relationships and Dating

A "Personal Relationship" is defined by the Company as a relationship between individuals who have, or have had, an ongoing relationship of a romantic or intimate nature.

A Personal Relationship between team members whereby one of the team members is a supervisor, subordinate, or direct/indirect report of the other member is strictly prohibited. The Company views all Personal Relationships involving supervisors, subordinates, or direct/indirect reports as a severe conflict of interest. The Company reserves the right to take prompt action if an actual, or potential, conflict of interest arises concerning individuals who engage, or have previously engaged, in a Personal Relationship during their employment with the Company.

In instances where there is no line of authority, or reporting involved, and if a conflict, or the potential for conflict, arises because of the Personal Relationship; the team members involved may be separated by reassignment, or termination from employment. If such a Personal Relationship between team members develops, it is the responsibility and obligation of the team members involved to disclose the existence of the relationship to Human Resources. However, in instances where there is no line of authority, or reporting involved; the team members involved will be given the opportunity to decide who is to be transferred to another position, or terminated, if no position is available. If no decision is made by the team members within 30 calendar days of the beginning of the Personal Relationship, then the Company will determine who is to be transferred or, if necessary, terminated from employment.

All Executives, Directors, Managers, and Supervisors are specifically prohibited from engaging in Personal Relationships with subordinates, or direct/indirect reports, and all Parties involved will be subject to discipline for such actions, up to and including termination.

N. Workplace Safety

The Company is committed to providing safe and healthy work environments and to being an environmentally responsible corporate citizen. It is our policy to comply with all applicable environmental, safety and health laws and regulations. It is the responsibility of each team member to comply with all company policies concerning safety, violence, harassment, substance abuse and similar matters in the workplace.

We are dedicated to designing, constructing, maintaining and operating facilities that protect our people and physical resources. This includes providing and requiring the use of adequate personal protective equipment and measures that all work be done safely.

New and evolving health and safety practices required of all team members, contractors, visitors and guests are in effect in each of our facilities. These practices outline numerous "safe at work" protocols that include the necessary processes, procedures, training, documentation and communications – all designed with your well-being in mind. We have modeled these protocols after government guidelines, the World Health Organization (WHO), the Center for Disease Control (CDC) and with information shared by our customers, suppliers and partners.

Local training is provided to safeguard yourself and your teammates. This training includes: enhanced cleaning and sanitizing procedures, some staggering of shifts/days, breaks, social distancing strategies, a periodic Questionnaire and on-site temperature screening, as appropriate.

By providing this training and these resources, we are clearly identifying the necessary measures needed to maintain a safe workplace. It is important that every team member embrace and be a champion for what is our "new normal." In order to achieve full success, all team members will need to be actively involved every day, during every shift and in every job position. These practices and procedures are now day-to-day requirements in each of our businesses.

O. Reporting Ethical Violations

Your conduct can reinforce an ethical atmosphere and positively influence the conduct of fellow team members. If you have evidence of a material violation of this Code, you must report it.

To report any type of ethics violations or misconduct, you should report it in the first instance to your local HR representative or appropriate business leadership at your location. If you are still concerned after speaking with your HR representative and/or local leader, or feel uncomfortable speaking with them (for whatever reason), you should share your concerns or questions to the Company's Legal Counsel or VP, North American Human Resources.

As an alternative, the Company has also contracted with a third-party firm, Lighthouse Services, for purposes of providing team members with an external method to report any suspected ethical violations. The contact information is:

Phone: (844) 618-2244
Website: www.intouchwebsite.com/tellINOAC
Email: tellINOAC@getintouch.com

You have the Company's commitment that you will be protected from retaliation for reports made in good faith.

P. Responsibility and Implementation

The Company encourages businesses throughout our supply chain to adopt and enforce similar policies in their own operations that are similar to those included here. Further, the Company will seek to identify and do business with organizations that conduct their businesses to standards that are consistent with this Policy including working to extend these principles within their own supply chain.

The Company will, as appropriate, seek the assistance of independent third-parties to assess compliance with this Policy.

All Company personnel must report known or suspected violations of this Policy through the established reporting channels. The Company prohibits retaliation against anyone who, in good faith, reports a violation.

The Corporate Compliance Officer (Legal Counsel) is responsible for interpreting this Policy with the concurrence, as appropriate, of the President, Chief Operating Officer, Vice President Purchasing and Supply Chain and Vice President of Human Resources.

Q. Conclusion

In the final analysis, you are the guardian of the Company's high ethical standards. While there are no universal rules, when in doubt ask yourself:

- Will my actions be ethical in every respect and fully comply with the law and with the Company's policies?
- Will my actions have the appearance of impropriety?
- Will my actions be questioned by my supervisors, fellow team members, customers, family or the general public?
- Am I trying to fool anyone, including myself, as to the propriety of my actions?

If you are uncomfortable with your answers to any of the above, you should not take the contemplated actions without first discussing them with a member of our leadership team. If you are still uncomfortable, please follow the steps outlined above in the Section "Reporting Ethical Violations."

Any team member who ignores or violates the *Code of Business Conduct & Workplace Ethics Policy*, and any manager who penalizes a subordinate for trying to follow this Code, will be subject to corrective action, which may include immediate dismissal. However, it is not the threat of discipline that should govern your actions. We hope you share our belief that a dedicated commitment to ethical behavior is the right thing to do, is good business and is the surest way for the Company to remain a highly successful company.

Acknowledgement

I hereby certify that I have read and understand the *Code of Conduct & Business Ethics Policy* of INOAC USA, Inc. and its subsidiaries.